

**UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549**

FORM 10-K

(Mark One)

☒ ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934

For the fiscal year ended January 31, 2025

OR

☐ TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934

For the transition period from to

Commission File Number: 001-38933

CROWDSTRIKE HOLDINGS, INC.

(Exact Name of Registrant as Specified in Its Charter)

Delaware

(State or other jurisdiction of
incorporation or organization)

45-3788918

(I.R.S. Employer
Identification Number)

206 E. 9th Street, Suite 1400, Austin, Texas 78701

(Address of principal executive offices)

Registrant's telephone number, including area code: (888) 512-8906

Securities registered pursuant to Section 12(b) of the Act:

| <u>Title of each class of securities</u> | <u>Trading symbol(s)</u> | <u>Name of each exchange on which registered</u> |
|--|--------------------------|--|
| Class A common stock, par value \$0.0005 per share | CRWD | The Nasdaq Stock Market LLC (Nasdaq Global Select Market) |

Securities registered pursuant to Section 12(g) of the Act:

None.

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act of 1933, as amended. Yes ☒ No ☐

Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Act. Yes ☐ No ☒

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes ☒ No ☐

Indicate by check mark whether the registrant has submitted electronically every interactive Data File required to be submitted pursuant to Rule 405 of Regulation S-T (§232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit and post such files) Yes ☒ No ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, a smaller reporting company, or an emerging growth company. See the definitions of "large accelerated filer," "accelerated filer," "smaller reporting company" and "emerging growth company" in Rule 12b-2 of the Exchange Act.

Large Accelerated Filer

☒

Accelerated Filer

☐

Non-accelerated Filer

☐

Smaller reporting company

☐

Emerging growth company

☐

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

Indicate by check mark whether the registrant has filed a report on and attestation to its management's assessment of the effectiveness of its internal control over financial reporting under Section 404(b) of the Sarbanes-Oxley Act (15 U.S.C. 7262(b)) by the registered public accounting firm that prepared or issued its audit report. ☒

If securities are registered pursuant to Section 12(b) of the Act, indicate by check mark whether the financial statements of the registrant included in the filing reflect the correction of an error to previously issued financial statements. ☐

Indicate by check mark whether any of those error corrections are restatements that required a recovery analysis of incentive-based compensation received by any of the registrant's executive officers during the relevant recovery period pursuant to §240.10D-1(b). ☐

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes ☐ No ☒

The aggregate market value of the common stock held by non-affiliates of the registrant, based on the closing price of a share of the registrant's common stock on July 31, 2024 (the last business day of the registrant's most recently completed second fiscal quarter) as reported by the Nasdaq Global Select Market on such date was approximately \$53.5 billion.

As of February 28, 2025, the number of shares of the registrant's Class A common stock outstanding was 247,873,415, and the number of shares of the registrant's Class B common stock outstanding was 0.

DOCUMENTS INCORPORATED BY REFERENCE

Portions of the registrant's definitive Proxy Statement relating to its 2025 Annual Meeting of Stockholders are incorporated by reference into Part III of this Form 10-K where indicated. Such Proxy Statement will be filed with the United States Securities and Exchange Commission within 120 days after the end of the fiscal year to which this Annual Report on Form 10-K relates.

CROWDSTRIKE HOLDINGS, INC.

TABLE OF CONTENTS

| | Page No. |
|--|----------|
| Part I | |
| Item 1. Business | 4 |
| Item 1A. Risk Factors | 21 |
| Item 1B. Unresolved Staff Comments | 56 |
| Item 1C. Cybersecurity | 57 |
| Item 2. Properties | 58 |
| Item 3. Legal Proceedings | 58 |
| Item 4. Mine Safety Disclosures | 58 |
| Part II | |
| Item 5. Market for Registrant’s Common Equity, Related Stockholder Matters and Issuer Purchases of Equity Securities | 59 |
| Item 6. [Reserved] | 60 |
| Item 7. Management’s Discussion and Analysis of Financial Condition and Results of Operations | 61 |
| Item 7A. Quantitative and Qualitative Disclosures about Market Risk | 76 |
| Item 8. Financial Statements and Supplementary Data | 77 |
| Item 9. Changes in and Disagreements with Accountants on Accounting and Financial Disclosure | 118 |
| Item 9A. Controls and Procedures | 118 |
| Item 9B. Other Information | 119 |
| Item 9C. Disclosure Regarding Foreign Jurisdictions that Prevent Inspections | 119 |
| Part III | |
| Item 10. Directors, Executive Officers and Corporate Governance | 119 |
| Item 11. Executive Compensation | 120 |
| Item 12. Security Ownership of Certain Beneficial Owners and Management and Related Stockholder Matters | 120 |
| Item 13. Certain Relationships and Related Transactions and Director Independence | 120 |
| Item 14. Principal Accountant Fees and Services | 120 |
| Part IV | |
| Item 15. Exhibits and Financial Statement Schedules | 120 |
| Item 16. Form 10-K Summary | 120 |
| Signatures | 124 |
| Power of Attorney | 125 |

SPECIAL NOTE REGARDING FORWARD-LOOKING STATEMENTS

This Annual Report on Form 10-K contains forward-looking statements within the meaning of the Securities Act of 1933, as amended (the “Securities Act”), the Securities Exchange Act of 1934, as amended (the “Exchange Act”), and the Private Securities Litigation Reform Act of 1995. All statements contained in this Annual Report on Form 10-K other than statements of historical fact, including statements regarding our future operating results and financial position, our business strategy and plans and our objectives for future operations, are forward-looking statements. The words “believe,” “may,” “will,” “potentially,” “estimate,” “continue,” “anticipate,” “intend,” “could,” “would,” “project,” “plan,” “expect” and similar expressions that convey uncertainty of future events or outcomes are intended to identify forward-looking statements.

These forward-looking statements include, but are not limited to, statements concerning the following:

- our future financial performance, including our expectations regarding our revenue, cost of revenue, gross profit or gross margin, operating expenses (including changes in sales and marketing, research and development, and general and administrative expenses), and our ability to achieve, and maintain, future profitability;
- market acceptance of our cloud platform;
- the effects of increased competition in our markets and our ability to compete effectively;
- our ability to maintain the security and availability of our cloud platform;
- our ability to maintain and expand our customer base, including by attracting new customers;
- our ability to develop new solutions, or enhancements to our existing solutions, and bring them to market in a timely manner;
- anticipated trends, growth rates and challenges in our business and in the markets in which we operate;
- our business plan and our ability to effectively manage our growth and associated investments;
- beliefs and objectives for future operations;
- our relationships with third parties, including channel partners and technology alliance partners;
- our ability to maintain, protect and enhance our intellectual property rights;
- our ability to successfully defend litigation brought against us and respond to government investigations and inquiries;
- our ability to successfully expand in our existing markets and into new markets;
- sufficiency of cash and cash equivalents to meet cash needs for at least the next 12 months;
- anticipated developments relating to our valuation allowances for our deferred tax assets;
- our ability to expand internationally;
- our ability to comply with laws and regulations that currently apply or become applicable to our business both in the United States and internationally;
- our ability to develop, maintain, and improve our internal control over financial reporting;
- macroeconomic factors, including inflation and instability in the global credit and financial markets;
- our ability to successfully close and integrate acquisitions to contribute to our growth objectives;

- the attraction and retention of qualified employees and key personnel; and
- the July 19 Incident (as defined below), including potential or anticipated developments, our remediation and other efforts in connection with the incident, the outcome of lawsuits, claims and inquiries related to the incident, our customer commitment packages, and the effect on our customer and partner relationships and our business, results of operations and financial condition.

These statements are based on our current plans, estimates and projections in light of information currently available to us. These forward-looking statements may be affected by risks, uncertainties and other factors discussed elsewhere in this Annual Report on Form 10-K, including under “Risk Factors.” Furthermore, new risks and uncertainties emerge from time to time, and it is impossible for us to predict all risks and uncertainties or how they may affect us. If any of these risks or uncertainties materialize, our business, revenue and financial results could be harmed, and the trading price of our Class A common stock could decline. Forward-looking statements made in this Annual Report on Form 10-K speak only as of the date on which such statements are made, and we undertake no obligation to update them in light of new information or future events, except as required by law.

We intend to announce material information to the public through the CrowdStrike Investor Relations website ir.crowdstrike.com, SEC filings, press releases, public conference calls, and public webcasts. We use these channels, as well as social media and our blog, to communicate with our investors, customers, and the public about our company, our offerings, and other issues. It is possible that the information we post on social media and our blog could be deemed to be material information. As such, we encourage investors, the media, and others to follow the channels listed above, including the social media channels listed on our investor relations website, and to review the information disclosed through such channels. Any updates to the list of disclosure channels through which we will announce information will be posted on the investor relations page on our website.

PART I

ITEM 1. BUSINESS

Overview

Founded in 2011, CrowdStrike reinvented cybersecurity for the cloud and artificial intelligence (“AI”) era and transformed the way cybersecurity is delivered and experienced by customers. When we started CrowdStrike, cyberattackers had an asymmetric advantage over legacy cybersecurity products that could not keep pace with rapid changes in adversary tactics. We took a fundamentally different approach to solve this problem with the AI-native CrowdStrike Falcon cybersecurity platform – the first, true, cloud-native platform built with AI at the core, capable of harnessing vast amounts of security and enterprise data to deliver highly modular solutions through a single lightweight agent.

The CrowdStrike Falcon platform is designed to be the definitive platform for cybersecurity consolidation, purpose-built to stop breaches. The platform’s single, lightweight agent collects and integrates data from across the enterprise, including endpoints, cloud workloads, identities, and third-party sources. We use this to train our AI to detect and prevent threats and drive workflow automation to give security teams machine speed advantage to stop adversaries. By consolidating and replacing legacy point products and fragmented platforms across key areas of security and IT, the Falcon platform delivers a unified, modern approach that increases capabilities, reduces complexity, and lowers costs – all while stopping breaches.

We believe our approach has defined a new category called the Security Cloud, which has the power to transform the cybersecurity industry the same way the cloud has transformed the customer relationship management, human resources, and service management industries. Using cloud-scale AI, our Security Cloud enriches and correlates trillions of cybersecurity events per week with indicators of attack, threat intelligence, and enterprise data (including data from across endpoints, workloads, identities, DevOps, IT assets, and configurations) to create actionable data, identify shifts in adversary tactics, and automatically prevent threats in real-time across our customer base. The more data that is fed into our Falcon platform, the more intelligent our Security Cloud becomes, and the more our customers benefit, creating a powerful network effect that increases the overall value we provide.

CrowdStrike: The Architectural Purpose Behind the Platform

Our Falcon platform was purpose-built in the cloud to harness the power of data and AI to deliver the next generation of automated protection and provide threat hunters with the intelligence required to stop sophisticated attacks, including malware-free and fileless attacks. This approach has made CrowdStrike an industry leader in protection across endpoints, cloud workloads, identity and data (capable of protecting workloads across on-premise, virtualized, and cloud-based environments running on a variety of endpoints such as desktops, laptops, servers, virtual machines, cloud workloads, cloud containers, mobile, and IoT devices) and enables us to rapidly scale this best in class protection across new and emerging areas of enterprise risk.

Today, we offer 29 cloud modules on our Falcon platform via a SaaS subscription-based model that spans multiple large markets, including corporate endpoint and cloud workload security, managed security services, security and vulnerability management, IT operations management, identity protection, next-generation security information and event management (“SIEM”) and log management, threat intelligence services, data protection, SaaS security posture management, Security Orchestration, Automation and Response (“SOAR”) and AI powered workflow automation, and securing generative AI workloads.

Our Falcon platform is composed of tightly integrated, proprietary technologies that enable us to deliver superior protection and performance, while reducing complexity for our customers. Our Falcon platform consists of our easily deployed, intelligent lightweight agent, and our groundbreaking graph technology.

Our single, lightweight-agent approach has changed how organizations experience cybersecurity, delivering protection without impacting the user, resources or productivity. With the lightweight agent installed on each endpoint and cloud workload, our Falcon platform automates detection and prevention capabilities in real time across our entire global customer base. This also enables our Falcon platform to intelligently ingest data once and stream high fidelity data back into the Security Cloud to be re-used for multiple use cases, continuously improve our Falcon platform’s AI algorithms and make its real-time decision-making faster and smarter to keep customers ahead of changing adversary tactics.

Our graph technology correlates and contextualizes the vast data of our Security Cloud so we can collect data once and reuse it repeatedly to deliver solutions that solve our customers' biggest problems. The highly advanced graph technologies underpinning the Falcon platform include:

- Our Threat Graph, which uses a combination of AI and behavioral pattern-matching techniques to correlate and analyze trillions of cybersecurity events, enriched with threat intelligence, and third-party data to identify and link threat activity together to automatically prevent threats in real time across CrowdStrike's global customer base. This also provides customers with increased visibility of attacks for proactive threat hunting and timely detection and remediation of novel threats.
- Our Intel Graph, which analyzes and correlates data and threat intelligence to visualize the connections between adversaries and attacks to help customers prioritize investigations and gain a deep understanding of the threat landscape. The latest intel on adversaries, tactics, techniques, and procedures is delivered seamlessly within the CrowdStrike Falcon platform and is mapped to the MITRE ATT&CK® framework.
- Our Asset Graph, which dynamically monitors and tracks the complex interactions among assets, providing a single holistic view of the risks those assets pose. Asset Graph provides graph visualizations of the relationships among all assets such as devices, users, accounts, applications, cloud workloads and operations technology ("OT"), along with the rich context necessary for proper security hygiene and proactive security posture management to reduce risk in their organizations — without impacting IT.

The Falcon platform was purpose-built with the foresight that the future of cybersecurity would need to be cloud-native and AI-driven. While AI is revolutionizing many technology fields, including cybersecurity solutions, to be truly effective, algorithms that enable AI depend on the quality and volume of data that trains them and the selection of the right differentiating features from that data.

This is why we believe our Security Cloud and our cloud-native architecture creates a fundamental differentiator from our competitors. The expansive amount of high fidelity data crowdsourced and captured in our Security Cloud enables the continuous training of our algorithms. We call this cloud-scale AI. Our technology is uniquely effective because we not only have a massive amount of high fidelity data to continuously train our AI models but also because we couple that data with deep human cybersecurity expertise, which supports our industry-leading efficacy and low false positives.

By analyzing and correlating information across our massive, crowdsourced dataset, we are able to deploy our AI algorithms at cloud-scale and build a more intelligent, effective solution to detect threats and stop breaches that on-premise, cloud-hosted and hybrid products cannot match due to the inherent architectural limitations those products have with respect to data storage and analysis. The more data that is fed into our Falcon platform, the more intelligent the Security Cloud becomes, and the more our customers benefit, creating a powerful network effect that increases the overall value we provide.

Industry Background: The Trends Driving a Need for a New Approach to Security

We believe there are a number of important trends that drive the need for a new approach to security. These include:

- **The Increasing Sophistication and Disruption of Cybersecurity Threats:** Adversary sophistication continues to increase as militaries and intelligence services of well-funded nation-states, technically advanced criminal organizations and hackers advance their tactics. In addition, the commoditization of technologies like generative AI make it easier for low-skilled adversaries to move faster and launch more sophisticated attacks. This includes non-malware based attacks like social engineering that exploit user identities and credentials. These attacks are pervasive, targeting a broad range of industries including technology, transportation, healthcare, financial services, governments and political organizations, utility, retail, and public infrastructure. The number and scale of attacks continue to increase. The typical attack cycle starts with attackers attempting to penetrate endpoints to establish a beachhead. Once inside, adversaries steal and exploit legitimate credentials to escalate privileges, move laterally and progress and attack, often downloading malware or ransomware. At this stage in the threat lifecycle, the adversary is able to encrypt, destroy, or silently exfiltrate sensitive data.

- **An Expanded Attack Surface Driven By Hybrid and Remote Workforces:** Organizations everywhere are embracing digital transformation and are becoming more distributed as they adopt the cloud, increase workforce mobility, and grow their number of connected devices. They are adding more workloads to a myriad of different endpoints beyond the traditional cybersecurity perimeter, exposing an increasingly broad attack surface to adversaries. This trend accelerated significantly with the need to support an increasingly remote workforce in 2020 due to the COVID-19 pandemic and we believe this trend continues today.
- **A Growing Cyber Skills Gap:** Trained cybersecurity professionals are in high demand, and organizations continue to face a dire shortage of talent to fill much needed cybersecurity positions. As a result, existing cybersecurity teams are often overwhelmed by the velocity of cyberattacks. Adversaries exploit this vacuum by continuing to accelerate their sophisticated attacks.
- **The Need to Reduce Complexity and Simplify Security Operations:** Organizations are increasingly looking to reduce the complexity of their security and IT stack. Modern security requires fewer point products, fewer agents and technologies that consume fewer resources. Increasingly, organizations are looking to standardize on trusted platforms that deliver an immediate return on investment and lower total cost of ownership.

Competitive Market: Existing Security Solutions Are Limited and Exacerbate Ongoing Trends:

We believe the aforementioned trends are exacerbated by the architectural limitations of legacy cybersecurity products and fragmented platforms, which are characterized by:

- **On-Premise Security and Bolt-On Cloud Products That Lead to Constrained and Impacted Users:** On-premise products are siloed, lack integration, and have limited ability to collect, process, and analyze vast amounts of data—attributes that are required to be effective in today’s increasingly dynamic threat landscape. Meanwhile, these solutions often require more agents on the endpoint as new capabilities are patchworked together, which can have a dramatic negative impact on user performance.

Many on-premise vendors have tried to solve this problem by simply extending on-premise products to the cloud. Since their products were not purpose built to run in the cloud, traditional on-premise issues such as complex deployments, data silos, lack of integrations, limited scalability, and high maintenance costs continue to manifest. We believe that any product that was originally designed for on-premise deployments and migrated to the cloud cannot by definition be a cloud native solution.

Some other vendors attempt to solve this problem by acquiring disparate products and stitching them together into fragmented platforms. This can force customers to focus on implementing integrations, not security outcomes and stopping the breach. The resulting complexity can impede workflows and slow down response time.

- **Legacy Signature-Based Products That Are Not Effective Against Unknown Threats:** Signature-based products are designed to detect attacks that are already cataloged as previously identified threats. As a result, such products are fundamentally unable to prevent unknown threats resulting from shifts in attacker tradecraft. An attacker may be able to bypass a signature-based defense with just a slight modification to an existing attack. Many significant breaches seen in the last two decades have involved the failure of a legacy signature-based antivirus product to detect a previously unknown or modified version of a previously known attack.
- **Malware-Focused Products That Miss Sophisticated Attacks:** Traditionally, organizations have focused on protecting their networks and endpoints against malware-based attacks. These attacks involve malware built for the specific purpose of performing malicious activities, stealing data, or destroying systems. Our 2024 Global Threat Report observed that over 70% of attacks comprise non-malware, hands-on-keyboard activity. Additionally, we found that eight out of 10 attacks involve compromised or stolen credentials, with these identity-based attacks easily able to bypass legacy approaches to protection. Therefore, a malware-centric defensive approach will leave the organization vulnerable to attacks that do not leverage malware.

- **Application Whitelisting Products That Are Ineffective:** Application whitelisting products resort to an “always allow” or “always block” policy on an endpoint to allow or prevent processes from executing. Whitelisting relies in part on manually creating and maintaining a complex list of rules, burdening end users and IT organizations. This does not prevent fileless attacks from exploiting legitimate whitelisted applications, compromising the integrity of the whitelisting product.
- **The Limitations of Legacy SIEMs:** Originally designed years or even decades ago for a vastly different cybersecurity landscape, legacy SIEM solutions struggle to meet the demands of modern security operations. These systems lack the scalability to handle today’s data volumes and adversary speed, while escalating costs make centralized data collection and retention increasingly difficult. Poor scalability contributes to siloed, disjointed SOC architectures, forcing analysts to manually correlate data across multiple consoles, diverting time and resources from threat detection and response. Complex onboarding processes further delay time-to-value, requiring significant effort to integrate new data sources. As a result, legacy SIEMs hinder operational efficiency, limit visibility, and increase the risk of data breaches.

CrowdStrike: Built for This Moment and the Future

We believe that the cloud-native architecture of the Falcon platform and Security Cloud provides a sustainable advantage in addressing the needs of our customers as their businesses and the threat landscape continues to evolve.

We offer our customers compelling business value that includes ease of adoption, rapid time-to-value, superior efficacy rates in detecting threats and preventing breaches, and reduced total cost of ownership by consolidating legacy, siloed, and multi-agent security products in a single solution. We also allow thinly-stretched security organizations to automate previously manual tasks, freeing them to focus on their most important objectives. With the Falcon platform, organizations can transform how they combat threats, transforming from slow, manual, and reactionary to fast, automated, and predictive, while gaining visibility across the threat lifecycle.

Key benefits of our approach and the CrowdStrike Falcon platform include:

- **The Power of the Crowd:** Our crowdsourced data enables every customer to benefit from contributing to the Security Cloud. As more high fidelity data is fed into our Security Cloud, our AI models continue to train and improve, increasing the overall efficacy of the Falcon platform. This unique data layer is powered and turned into action by three complementary graph databases (Threat Graph, Intel Graph, and Asset Graph) to put threats, adversaries, and assets into the context needed to make the rapid, informed decisions that stop breaches.
- **Driving AI Innovation and Security:** We are a pioneer in leveraging AI to transform cybersecurity, combining AI for cybersecurity with cybersecurity for AI. The Falcon platform’s AI-native architecture uses advanced models and the power of the Security Cloud to detect and stop breaches, while innovations like Charlotte AI represent a significant advancement in agentic AI—delivering autonomous security decisions within customer-defined guardrails to triage detections, reduce noise, and accelerate response. Charlotte AI, powered by high-fidelity data and continual training, reduces routine investigation workloads, bridging critical skills gaps for stretched teams. As AI continues to evolve, CrowdStrike is driving the next generation of AI-powered agentic cybersecurity—enabling AI to act independently while ensuring human oversight and control. Beyond delivering AI-driven protection, we also secure the AI systems organizations depend on, helping customers safeguard generative AI applications, protect sensitive data, and mitigate the risks posed by AI misconfigurations and vulnerabilities. By advancing AI innovation and security, we empower organizations to stay ahead of adversaries, increase operational efficiency, and securely embrace the AI-driven future.
- **High Efficacy, Low False Positives:** The vast telemetry of the Security Cloud and the best practices employed in continually training our AI models results in exceptionally high efficacy rates and low false positives, delivering proven performance in real-world scenarios.

- **Consolidation of Siloed Products:** Integrating and maintaining numerous security products creates blind spots that attackers can exploit, increases costs, and negatively impacts both end-user system performance and the experience of the security analyst. Our cloud-native platform gives customers a unified approach to address their most critical areas of risk seamlessly. We empower customers to rapidly deploy and scale industry leading technologies across Endpoint Security, Identity Protection, Cloud Security, Next-Gen SIEM and Modern Log Management, Data Protection, Exposure Management, IT Automation, ITSecOps and Risk, Threat Intelligence, and SaaS Security Posture Management from a single platform.
- **Reducing Agent Bloat:** Our single intelligent lightweight agent enables frictionless deployment of our platform at scale, enabling customers to rapidly adopt our technology across any type of workload running on a variety of endpoints. The agent is non-intrusive to the end user, requires no reboots and continues to protect the endpoint and track activity even when offline. Through our single lightweight agent approach, customers can adopt multiple platform modules to address their critical areas of risk without burdening the endpoint with multiple agents. Legacy approaches often require multiple agents as they layer on new capabilities. This can severely impact user performance and create barriers to security.
- **Rapid Time to Value:** Our cloud-native platform was built to rapidly scale industry leading protection across the entire enterprise, eliminating lengthy implementation periods and professional services engagements that next-gen and legacy competitors may require. Our single agent, collect once and re-use many times approach enables us to activate new modules in real time.
- **Elite Security Teams as a Force Multiplier:** Adversaries are relentlessly innovating new forms of sophisticated attacks, bypassing traditional malware to exploit user credentials and identities. In this evolving landscape, automation and autonomous security are no longer sufficient on their own. Stopping today's sophisticated attacks requires a combination of powerful automation and elite threat hunting. Falcon Complete provides a comprehensive monitoring, management, response, and remediation solution to our customers and is designed to bring enterprise level security to companies that may lack the resources or expertise to do so on their own.

CrowdStrike Falcon OverWatch, part of CrowdStrike Counter Adversary Operations, combines world-class human intelligence from our elite security experts with the power of the Falcon platform. OverWatch is a force multiplier that extends the capabilities and improves the productivity of our customers' security teams. Because our world-class team can see attacks across our entire customer base, their expertise is enhanced by their constant visibility into the threat landscape. Additionally, the insights of our OverWatch team can then be leveraged by the Falcon platform to further enhance its autonomous capabilities, creating a positive feedback loop for our customers.

- **Alleviating the Skills Shortage through Automation:** CrowdStrike automates manual tasks to free security teams to focus on their most important job – stopping the breach. Our Falcon Fusion capability automates workflows to reduce the need to switch between different security tools and tasks, while our Falcon Insight XDR module provides a unified solution that enables security teams to rapidly and efficiently identify, hunt, and eliminate threats across multiple security domains using first and third party datasets.
- **Lower Total Cost of Ownership:** Our cloud-native platform eliminates our customers' need for initial or ongoing purchases of hardware and does not require their personnel to configure, implement or integrate disparate point products. Additionally, our comprehensive platform reduces overall personnel costs associated with ongoing maintenance, as well as the need for software patches and upgrades for separate products.

Securing Identities and Data Across the Pillars of Modern Enterprise Security

As modern attacks and adversaries grow more sophisticated, CrowdStrike believes that stopping breaches in the modern era requires security that delivers unified visibility and protection across three critical areas: Endpoint and Cloud workloads, Identity Threat Protection and Data Protection.

Approximately eighty percent of breaches today use stolen credentials and identities. Stopping these advanced attacks requires a holistic approach that delivers true end-to-end protection across workloads, identities, and data. CrowdStrike is able to natively enforce protection at the device layer, the identity layer, and the data layer, extending our bold vision for security by driving modern Defense in Depth to the enterprise.

By delivering these powerful capabilities through a unified platform with a single agent, CrowdStrike is able to connect the endpoint and workload to user identity, and the data that is being used and accessed. Customers can see the full health and state of endpoints and workloads, in context with the identity that is using and accessing them, aligned with where data is being created, who is using it, where it flows and how it is protected. CrowdStrike delivers this through a unified platform experience. This is how CrowdStrike believes security should and must be delivered today to combat advanced adversaries and stop breaches in the modern era. This means security solutions that are easy to deploy, easy to manage, and highly effective.

The CrowdStrike Falcon Platform: Built to Innovate and Scale

Our platform approach allows us to rapidly innovate, build, and deploy highly integrated modules that address critical customer problems and access additional market opportunities. Our Falcon platform is composed of two tightly integrated proprietary technologies: our lightweight agent and our Security Cloud. Our cloud-delivered modules integrate seamlessly within the Falcon platform to provide customers with a unified set of cloud-delivered technologies across Endpoint Security, Identity Protection, Cloud Security, Next-Gen SIEM and Modern Log Management, Data Protection, Exposure Management, IT Automation, ITSecOps and Risk, Threat Intelligence, and SaaS Security Posture Management.

The Falcon platform also encompasses recently acquired technologies where integration may be ongoing. We can rapidly and cost effectively develop and deliver additional cloud modules on our Falcon platform without the need for additional agents, and are expanding options for our new customers to test modules on a trial basis as well as offering in-application trials for existing customers. Our expanding set of open APIs and the Foundry app development platform allow customers and partners to build their own capabilities on top of the Falcon platform.

Unifying data from our modules and customers into a single cloud infrastructure gives us significant advantages in developing and delivering innovative AI capabilities to detect and prevent threats, as well as improving user productivity and efficiency through cutting-edge generative AI systems such as our Charlotte AI module.

CrowdStrike Falcon Platform: Unified Security Across Major Categories

Our cloud-native Falcon platform integrates seamlessly with our single lightweight agent to deliver robust functionality across key areas of cybersecurity and IT operations. The Falcon platform delivers 29 cloud modules, enabling customers to address their most critical areas of risk with speed, confidence, and visibility through one unified platform. Key areas of focus include:

Endpoint Security: The Falcon platform offers next-generation antivirus, endpoint detection and response (“EDR”) and extended detection and response (“XDR”) to defend against malware, fileless attacks, and advanced threats. With cross-domain telemetry and unified incident management, we enable organizations to detect, investigate, and respond to threats across the security stack efficiently and effectively.

Cloud Security: CrowdStrike provides robust cloud security solutions to protect workloads, containers, and applications in real time. Our offerings include runtime protection, cloud security posture management, application security posture management and more to secure multi-cloud environments and enhance the resilience of cloud-native applications. By integrating seamlessly into developer workflows, we empower teams to shift security left and mitigate vulnerabilities before deployment.

Exposure Management: CrowdStrike’s exposure management solutions unify data from multiple sources, including IT hygiene, vulnerability management, and external attack surface management. These capabilities allow organizations to predict attack paths, prioritize remediation efforts, and proactively reduce their risk exposure. Real-time insights and guided actions empower customers to address vulnerabilities before they can be exploited.

Managed Services Subscription: Falcon Complete Next-Gen Managed Detection and Response (“MDR”) delivers a comprehensive managed security service subscription that combines 24/7 expert monitoring, investigation, response, and remediation to stop breaches across the entire attack lifecycle. Delivered by CrowdStrike’s team of security experts and powered by the AI-native Falcon platform, it combines industry-leading endpoint protection and extends managed protection across cloud security, identity protection, asset visibility, and Next-Gen SIEM, with 24/7 managed threat hunting from Falcon Adversary OverWatch for a full-stack MDR service. Falcon Complete Next-Gen MDR is also backed by an underwritten limited warranty policy, underscoring our commitment to breach protection and customer confidence.

Counter Adversary Operations: CrowdStrike’s Counter Adversary Operations include proactive threat hunting and intelligence capabilities. These solutions leverage the insights of elite security experts and the power of Threat Graph to identify and mitigate advanced threats, providing customers with actionable intelligence to strengthen their defenses.

Identity Protection: Identity protection solutions from CrowdStrike safeguard against identity-based attacks with real-time detection, behavioral analytics, and policy enforcement. These capabilities provide visibility into anomalies and lateral movement, enabling organizations to defend their most critical assets.

Next-Generation SIEM and Log Management: CrowdStrike’s Next-Gen SIEM and log management solutions deliver AI-driven detection, investigation, and response capabilities, alongside high-performance log management for any data source. This comprehensive approach enhances security operations and enables organizations to respond to threats with speed and precision.

Generative AI: Innovations like Charlotte AI leverage generative AI and natural language processing to automate time-intensive tasks, enabling security analysts to work more efficiently. Charlotte AI transforms hours of routine investigation into minutes, addressing critical skills gaps and enhancing operational efficiency. Powered by the Falcon platform’s unique data advantage, Charlotte continues to evolve, delivering time savings and workflow automation to meet the demands of modern security operations.

IT Automation: Falcon for IT converges security and IT operations, providing visibility into enterprise assets and enabling rapid resolution of issues. With generative AI workflows and automation capabilities, Falcon for IT empowers organizations to streamline IT processes, resolve operational challenges quickly, and maintain a secure and efficient infrastructure.

SaaS Security: Adaptive Shield, a CrowdStrike company, delivers continuous monitoring and proactive risk mitigation for business-critical SaaS applications. With context and visibility, organizations can address risks from users, devices, and non-human identities.

Data Protection: Falcon Data Protection prevents data theft by combining content with context, providing real-time visibility into sensitive data movement across endpoints, web applications, cloud drives, and USB storage devices. This modern approach empowers organizations to secure enterprise data without disrupting productivity, addressing the unique risks of the GenAI era.

Application Development: The Falcon Foundry no-code application development platform allows customers to quickly create their own apps to solve custom security and IT use-cases with full access to CrowdStrike’s data, threat intelligence, automation, and cloud-scale infrastructure.

Bringing CrowdStrike to the Market

We primarily sell the Falcon platform through our direct sales team that leverages our network of channel partners to maximize effectiveness and scale. We have a low friction land-and-expand sales strategy. Key elements of our growth strategy include:

- **Growing Our Customer Base by Replacing Legacy and Other Endpoint Security Products.** Given the limitations of existing legacy and other endpoint security products, many organizations are replacing their existing legacy and other endpoint security products with our Falcon platform. We will continue to invest in customer acquisition programs, including our channel partnerships and new programs, like our free trial program of Falcon Prevent that is easily downloaded from our website and AWS Marketplace.

- **Further Penetrating Existing Customers.** Our growth will depend in part on our ability to continue to expand our relationships with our customers by deploying on additional endpoints in their environment and cross-selling more cloud modules. When customers deploy our lightweight agent, they can easily add additional cloud modules. We also offer in-application trial usage of additional modules to cross-sell to existing customers. While some new customers initially deploy our Falcon platform broadly across the organization, others elect to deploy only in selected business units and later deploy on additional endpoints and subscribe to additional modules. Over time, we seek to deploy our solution enterprise-wide for all customers. The power of our land-and-expand strategy is evidenced by our 112% dollar-based net retention rate as of January 31, 2025.
- **Leveraging Our Falcon Platform to Enter New Markets.** Because we leverage a single data model and open cloud architecture, we are uniquely positioned to continue innovating and rapidly deploying new cloud modules on our platform. For example, Falcon Discover includes use cases outside of security, such as application license management, AWS spend analysis, and asset inventory. Because our lightweight agent collects diverse endpoint data once for repeated use, we can expand our addressable market by rapidly adding new cloud modules that leverage this data. We intend to continue to develop new cloud modules for broader endpoint use cases.
- **Broadening Our Reach into New Customer Segments.** While we initially targeted large sophisticated enterprises, we have expanded our go-to-market efforts to include customers of all sizes with a dedicated inside sales team focused on smaller organizations. We also released Falcon Complete in 2018, our turnkey solution that combines the most popular cloud modules of our Falcon platform with our remediation and response capabilities, to create a solution for customers with limited or no internal security expertise. As a result, we can sell our Falcon platform to the largest enterprises or smallest businesses with any level of security sophistication and budget. We continue to look for new ways to broaden our reach into new customer segments.
- **Broadening Our Reach into U.S. Public Sector Verticals.** We continue to invest heavily in the acquisition of customers in the U.S. federal government as well as the state, local, and higher education verticals. Our platform is authorized by several federal agencies via the Federal Risk and Authorization Management Program (“FedRAMP”). Additionally, Department of Defense organizations can rely upon CrowdStrike’s Impact Level 5 provisional authorization to satisfy their cloud-based security requirements. To further meet the compliance demands of the government, customers can elect to deploy the Falcon platform in the AWS GovCloud. We have also successfully been embedded into several strategic government-wide cybersecurity programs and contracts, such as the Department of Homeland Security’s Continuous Diagnostics and Mitigation Approved Products List, which serves to provide federal agencies with innovative security tools. As a result, the Cybersecurity and Infrastructure Security Agency has leveraged a significant investment in our platform to support modernization efforts within the Federal Civilian Executive Branch. Further evidence of our progress into these critical markets is demonstrated by virtue of the fact that 25 of the 50 U.S. states have standardized on CrowdStrike’s platform at the enterprise level.
- **Expanding Our International Footprint.** We are expanding our international operations and intend to invest globally to broaden our international footprint. We grew our international revenue from \$967.5 million for fiscal 2024 to \$1,270.7 million for fiscal 2025, representing an increase of 31%. We intend to grow our international customer base by increasing our investments in our overseas operations, including adding headcount in Europe, the Middle East, Asia-Pacific, including Japan, and expanding data centers overseas.
- **Extending Our Falcon Platform and Ecosystem.** We designed our architecture to be open, interoperable, and highly extensible. We launched the CrowdStrike Marketplace, the first open cloud-based application PaaS for cybersecurity, which allows customers to purchase CrowdStrike products and provides an ecosystem of trusted partners and applications for our customers to choose from. We plan to continue investing in the CrowdStrike Store to empower our partners by making it easier to build applications and to enable our customers to more easily discover, try, and purchase additional cloud modules from both trusted partners and us.

Technology

We have designed an innovative architecture from the ground up to overcome the limitations of existing security products and deliver cloud-based solutions. The key design principles of our Falcon platform include:

Cloud Native Architecture. We built the Falcon platform entirely in and for the cloud, enabling collection and analysis of a massive, crowdsourced dataset from all of our customers to stop breaches. Our platform is designed to be redundant, resilient, and high-performing. Delivering security from the cloud enables agility, ease of use, and protection for workloads on a variety of endpoints wherever they are located. As customer adoption grows, the network effect of each additional endpoint added to the Falcon platform will amplify the breadth and depth of our dataset and intelligence.

Falcon Agent. We designed an intelligent lightweight agent that is installed on each endpoint or cloud workload. This agent incorporates identification and prevention of known and unknown malware and fileless attacks using machine learning, AI, exploit blocking, and advanced behavioral techniques, to protect workloads across all endpoints while capturing and recording high fidelity endpoint data. Our agent is capable of acting autonomously and continues to collect data and protect workloads running on endpoints even when offline. The agent recommences transmitting data to our Falcon platform when the connection to the cloud has been re-established. Our lightweight agent is built to support Windows, Mac, and Linux operating systems. The agent is hardened against attacks and uses a combination of kernel and user-mode modules to collect and transmit high fidelity endpoint events as they take place on a system. It correlates these events using a local situational model on the endpoint, analyzes via agent-based AI models and is capable of taking a variety of preventative and responsive actions on the endpoint, either automatically or via human control. Events are streamed by the agent to the cloud in real time in order to be further analyzed in the Threat Graph, where additional correlation and AI algorithms can be applied. The agent is also capable of being remotely reconfigured in real time based on analytics in our cloud platform to collect and analyze different events or take other actions as risk and threat postures change.

Threat Graph. Threat Graph is our proprietary, powerful, scalable, and dynamic graph database. Threat Graph continually looks for malicious activity by combining AI with behavioral pattern-matching techniques to look beyond file features and track the behaviors of every OS process and software program executed on an endpoint in a customer's network environment. By applying powerful graph analytics and AI algorithms to cybersecurity, we enrich the data collected with our proprietary and third-party threat intelligence, such as adversary capabilities, motivations, attributions, and threat indicators. The graph data model allows our AI algorithms to identify relationships between events that are not directly related but which could indicate an attack that would otherwise remain undetected. We believe that our AI algorithms are advantaged by the rich proprietary dataset that we use to train them. Threat Graph provides customers with complete real time and historical visibility and insight into events occurring on their endpoints for hunting and searching, even if the endpoint is unreachable or no longer exists.

Threat Graph also provides query and hunting capability over the full set of high-fidelity events collected in the graph. This correlated data, natively represented in a graph structure, enables new products and cloud modules to be created rapidly since the platform provides the visibility, collection, correlation, and actions over data as reusable building blocks. This collect-once, use repeatedly approach is the reason why we have been able to deliver new cloud modules covering IT hygiene and vulnerability management quickly and enables us to continue expanding the Falcon platform rapidly in the future.

Intel Graph. Intel Graph analyzes and correlates massive amounts of data on adversaries, their victims and their tools, providing extraordinary insights into shifting adversary tactics and techniques, powering our adversary-focused approach with world-class threat intelligence.

Asset Graph. Asset Graph dynamically monitors and tracks the complex interactions among enterprise entities, providing a single holistic view of the risks those assets pose. Asset Graph provides graph visualizations of the relationships among entities and assets such as devices, users, accounts, cloud workloads, along with the rich context necessary for proper security hygiene and proactive security posture management to reduce risk in their organizations.

High Fidelity Data and Smart Filtering. The presence of a local graph model in our agent enables it to track the state of the machine in real time, perform rapid machine learning and behavioral analysis, and provide efficient event streaming to the cloud. We call this "smart filtering." This allows us to keep performance overhead on the endpoint to a minimum, dramatically reduce the bandwidth required for agent-cloud communication, efficiently process large volumes of data, and separate signals from noise. The Falcon agent collects and analyzes unfiltered data with local machine learning and behavioral algorithms on the endpoint but only streams high fidelity endpoint events to the cloud to just send what is necessary for detection, prevention and investigation of attacks. This smart filtering architecture allows us to reduce network load for our customers. The Falcon platform collects an array of high fidelity endpoint events, such as code execution, network, file system and user activity. This information can be used for a variety of use cases beyond security, such as IT operations and vulnerability management.

Management Interface. The Falcon platform management interface gives customers an intuitive and informative view of their complete environment, with timely alerts and detailed search capabilities. We provide real-time endpoint and cloud workload visibility to allow customers to review details and respond to threats instantly and effectively, from anywhere, and maintain an index of these events for future use.

APIs and Integrations. Our Falcon platform and architecture is built around a rich set of APIs that efficiently and effectively complement and expand a customer's existing security infrastructure, such as security information event management, or SIEMs, intrusion prevention systems and intrusion detection systems. The platform includes streaming, query and batch APIs allowing customers and partners to integrate a variety of solutions seamlessly. It also includes rich management and control APIs. The platform allows third parties to develop additional cloud modules and features, furthering the power of the Falcon platform. By connecting existing security systems to the Falcon platform, we allow our customers to further leverage their security investments.

Data Center Operations

We have data center co-location facilities throughout the United States and in Europe, and we also utilize third-party data centers located in the United States and Europe. Our technology infrastructure, combined with select use of third-party resources, provides us with a distributed, resilient and scalable architecture on a global scale.

Professional Services

In addition to our Falcon platform and cloud modules, we also offer incident response, forensic investigatory, and breach recovery services; technical assessment and strategic advisory services; Next-Gen SEIM consulting; platform deployment and operational services; as well as training and certifications to assist organizations that have experienced a breach or who are assessing their security posture and ability to respond to breaches.

- **Incident Response, Forensics, and Recovery Services.** Our incident response services typically begin by deploying our lightweight agent to a customer's endpoints or cloud workloads to provide visibility in order to determine if an attacker is currently in the environment, what assets have been compromised, and how much damage has been done. In addition to enriching the response team's understanding of the attack, the full suite of Falcon platform's next-gen prevention capabilities, cloud security, exposure management, and identity protection offerings can also be leveraged to help to slow down and prevent an active attacker from moving at-will throughout a compromised customer's environment, increasing the risk and potential damage to the customer. We also provide customized surgical recovery services by providing the tools and staffing to eject attackers out of the network, lock down credentials from further use, remediate impacted systems and ensure adversaries stay out. In addition to providing valuable breach remediation to our customers, our incident response services also act as a strong lead generation engine for our Falcon platform and cloud modules. After experiencing the benefits of our platform firsthand, many of our incident response customers become subscription customers.
- **Technical Assessment and Strategic Advisory Services.** Our proactive security services include technical assessment services designed to help organizations understand their cyber maturity levels. These services include both endpoint and cloud workload compromise assessments, cybersecurity maturity assessments, security program in-depth assessments, service organization control assessments, IT hygiene assessments, and active directory security assessments. We also advise customers on readiness and preparation through the execution of table-top exercises, live fire exercises, red team/blue team assessments, and advanced adversary emulation exercises. We have also added AI red-teaming to help organizations understand where these models can have risk, where they can be exploited and where to take corrective security actions. All of these services are designed to evaluate our customers' security profile so they can identify areas of vulnerability, secure their network, and improve their response if their defenses are breached. Our services also align to executive and board level cybersecurity training and awareness, including by helping public companies more confidently comply with public disclosure requirements relating to assessing, identifying and managing material cybersecurity risks, and reporting material cyber incidents. Our programs are designed to help organizations effectively achieve cybersecurity risk reduction objectives and to maximize investments.

- **NextGen SIEM Professional Services.** Our NG-SIEM professional services offer a comprehensive suite of deployment packages and ongoing support options designed to help organizations seamlessly implement and optimize the Falcon NG-SIEM platform. Our Essentials, Advanced, and Premium Deployment Packages provide standardized implementations that prioritize data ingestion aligned with critical use cases from the MITRE ATT&CK framework, ensuring maximum impact in detecting and responding to threats. For customers requiring deeper, hands-on expertise, we offer Resident Engineer Services in flexible durations of 3, 6, or 12 months supporting both NG-SIEM as well as LogScale. These experts embed directly with customer teams to provide tailored guidance, ongoing optimization, and support for evolving security needs. Our services are designed to accelerate time-to-value, enhance security posture, and ensure the long-term success of SIEM deployments within any organization.
- **Platform Deployment and Operational Services.** Our deployment and operational services are designed to help customers maximize the value of their investment in the CrowdStrike Falcon platform. These services provide seamless deployment of Falcon modules across endpoint, cloud, identity, Next-Gen SIEM and many other modules ensuring rapid time-to-value and alignment to CrowdStrike's recommended security configurations to prevent breaches. Our integration services focus on enabling customers to align Falcon modules with their existing security ecosystems, leveraging our APIs and Falcon Fusion SOAR automation for improved operational efficiency. Additionally, our operational services provide tailored guidance and best practices to optimize platform performance, streamline workflows, and address specific cybersecurity challenges. The goal of these services are to empower organizations to fully operationalize CrowdStrike's solutions, enhance security posture, and achieve measurable outcomes in cyber risk reduction with the Falcon platform.
- **CrowdStrike University Training and Certification.** We offer training and certification services to customers and partners on CrowdStrike technologies and cybersecurity topics to facilitate the adoption of CrowdStrike and to broaden and deepen their skills. CrowdStrike University is an online learning management system that organizes all CrowdStrike e-learning, instructor-led training and certification preparation courses in one place, providing a personalized learning experience for individuals who have an active training subscription. CrowdStrike currently offers proctored exam certifications through industry leading training partner Pearson Vue for its CrowdStrike Certified Falcon Administrator, CrowdStrike Certified Falcon Responder, CrowdStrike Certified Falcon Hunter, CrowdStrike Certified Cloud Specialist, and CrowdStrike Certified Identity Specialist programs. We provide comprehensive training and certification programs to empower customers and partners with the knowledge and skills needed to maximize the value of CrowdStrike technologies and strengthen their cybersecurity expertise. CrowdStrike University provides a centralized, online platform for accessing a wide range of training options including on-demand e-learning, instructor-led training, and certification preparation. Our offerings are designed to accommodate varying levels of proficiency from foundational concepts to advanced skills in threat detection, incident response, cloud security, intelligence and other proactive security operations aligned to the Falcon platform. Our CrowdStrike Certified Falcon Administrator, Responder, Hunter, Cloud Specialist, and Identity Specialist certifications validate the skillsets of our customers and partners to ensure they are properly equipped to operate the Falcon platform. Our training offerings provide a structured learning path to accelerate CrowdStrike adoption, drive operational success, and equip professionals with validated expertise in modern cybersecurity practices.

Customers

Some of the world's largest enterprises, government organizations, and high-profile brands trust us to protect their business. As of January 31, 2025, we are trusted by more than 74,000 organizations, including our end customers and those of our Managed Security Service Providers ("MSSP"), worldwide. Historically, we and our channel partners have primarily sold to large organizations, but have increasingly focused on selling to small and medium-sized businesses, particularly through our trial-to-pay model. We engage our customers through our global customer and technical advisory boards in which we solicit feedback from our customers on a regular basis allowing us to understand their evolving needs. We have used this feedback to develop new cloud modules, such as Falcon FileVantage, and we intend to continue to develop new cloud modules based on our customer's feedback. Our business is not dependent on any particular end customer.

Sales and Marketing

Our sales and marketing organizations work together closely to drive market awareness, build a strong sales pipeline and cultivate customer relationships to drive revenue growth.

Sales

We primarily sell subscriptions to our Falcon platform and cloud modules through our world-class, global sales team, which is comprised of field sales and inside sales professionals who are segmented by a customer's organizational size. Our sales team also leverages a powerful go-to-market sales motion with our vast ecosystem of channel and alliances partners. We also use our sales team to identify current customers who may be interested in free trials of additional cloud modules, which serves as a powerful driver of our land and expand model. By segmenting our sales teams, we can deploy a low-touch sales model that efficiently identifies prospective customers.

Marketing

Our marketing organization is focused on building our brand reputation, increasing the awareness and reputation of our platform, and driving customer demand. As part of these efforts, we deliver targeted content to demonstrate thought leadership in the security industry, including speaking engagements with the security industry's foremost organizations to provide expert advice, issuing regular reports on the state of the industry, educating the public about cybersecurity threats, and identifying and naming adversary groups. We also engage in paid media, web marketing, industry and trade conferences (including our annual Fal.Con conference), analyst engagements, whitepaper development, demand generation via digital and web, and targeted displacement campaigns. We employ a wide range of digital programs, including search engine marketing, online and social media initiatives, and content syndication to increase traffic to our website and encourage prospective customers to sign up for a free trial of the Falcon platform. Additionally, we engage in joint marketing activities with our channel and technology alliance partners.

Partnership Ecosystem

We operate a partner-first go-to-market strategy to land new logos and expand in existing accounts. We partner with a diverse set of partners. We work with a wide array of go-to-market partners in our technology alliance partners to design go-to-market strategies that combine our platform with products or services provided by our technology alliance partners. These partner integrations deliver more secure solutions and an improved end user experience to their customers. Our technology alliance partnerships focus on security analytics, network and infrastructure security, threat platforms and orchestration, and automation. We launched the CrowdStrike Store, the first open cloud-based application PaaS for cybersecurity and the industry's first unified security cloud ecosystem of trusted third-party applications. In addition, Falcon for AWS, available in the AWS Marketplace, allows customers to easily purchase and take advantage of the metered billing (pay-as-you-go) pricing option to scale their consumption as their business needs change.

Research and Development

Our research and development organizations are responsible for the design, architecture, operation and quality of our cloud native Falcon platform. In addition, the research and development organizations work closely with our customer success teams to promote customer satisfaction.

Our success is a result of our continuous drive for innovation. Our internal team of security experts, researchers, intelligence analysts, and threat hunters continuously analyzes the evolving global threat landscape to develop products that defend against today's most sophisticated and stealthy attacks and report on emerging security issues. We invest substantial resources in research and development to enhance our Falcon platform, and develop new cloud modules, features and functionality. We believe timely development of new, and enhancement of our existing products, services, and features is essential to maintaining our competitive position. We work closely with our customers and channel partners to gain valuable insight into their security management practices to assist us in designing new cloud modules and features that extend the capability of our platform. Our technical staff monitors and tests our software on a regular basis, and we also make our Falcon platform available for third-party validation. We also maintain a regular release process to update and enhance our existing solutions. In addition, we engage security consulting firms to perform periodic vulnerability analysis of our solutions.

Our research and development leadership team is located in Seattle, Washington and Sunnyvale, California. We also maintain research and development centers in Irvine, California, Minneapolis, Minnesota, Bucharest, Romania, Israel and India. We employ subject matter experts in a number of jurisdictions around the world. We plan to continue to dedicate significant resources to research and development.

Competition

We primarily compete with established and emerging security product vendors. While the market for traditional endpoint and IT operations solutions has historically been intensely competitive, we believe that the architecture of our cloud-native, single agent platform fundamentally differentiates us compared to both next-gen and legacy competitors in the security industry. Additionally, as we look to enter into adjacent markets and expand our total addressable market, we may face new competitors. However, we do not believe any of our competitors currently have a true platform offering equivalent to the Falcon platform, which can be leveraged to win in legacy markets and define new categories.

Our competitors currently include the following by general category:

- legacy antivirus product providers who offer a broad range of approaches and solutions including traditional signature-based antivirus protection;
- alternative endpoint security providers who generally offer a mix of on-premises and cloud-hosted products that rely heavily on malware-only or application whitelisting techniques;
- network security vendors who are supplementing their core perimeter-based offerings with endpoint or cloud security solutions;
- cloud security vendors, including those who focus on public cloud infrastructure and services;
- identity security vendors that seek to identify and secure user accounts and related activities;
- professional service providers who offer cybersecurity response services; and
- legacy SIEM vendors who offer a range of log management and security capabilities.

We compete on the basis of a number of factors, including but not limited to our:

- ability to offer a unified and modular platform that enables rapid innovation, scaling, and deployment;
- ability to identify security threats and prevent security breaches;
- ability to integrate with other participants in the security ecosystem;
- time to value, price, and total cost of ownership;
- brand awareness, reputation, and trust in the provider's services;
- strength of sales, marketing, and channel partner relationships;
- customer support, incident response, and proactive services; and
- ability to rapidly ingest and search both first and third-party data.

Although certain of our competitors enjoy greater resources, recognition, deeper customer relationships, larger existing customer bases, or more mature intellectual property portfolios, we believe that we compete favorably with respect to these factors and that we are well positioned as a leading provider of endpoint and workload security solutions.

Intellectual Property

We believe that our intellectual property rights are valuable and important to our business. We rely on trademarks, patents, copyrights, trade secrets, license agreements, intellectual property assignment agreements, confidentiality procedures, non-disclosure agreements, and employee non-disclosure and invention assignment agreements to establish and protect our proprietary rights. Though we rely in part upon these legal and contractual protections, we believe that factors such as the skills and ingenuity of our employees and the functionality and frequent enhancements to our solutions are larger contributors to our success in the marketplace.

We continue to grow our global portfolio of intellectual property rights in connection with our products, services, research and development, and other activities to protect our proprietary technology relevant to our business. We file patent applications to protect our intellectual property and believe that the duration of our issued patents is sufficient when considering the expected lives of our products. We intend to continue pursuing additional intellectual property protection to the extent we believe it would be beneficial and cost-effective. Despite our efforts to protect our intellectual property rights, they may not be respected in the future or may be invalidated, circumvented, or challenged. Our industry is characterized by the existence of a large number of patents and frequent claims and related litigation based on allegations of patent infringement or other violations of intellectual property rights. We believe that competitors will try to develop products that are similar to ours and that may infringe our intellectual property rights. Our competitors or other third-parties may also claim that our security platform and other solutions infringe their intellectual property rights. In particular, some companies in our industry have extensive patent portfolios. From time to time, third parties have in the past and may in the future assert claims of infringement, misappropriation and other violations of intellectual property rights against us or our customers, with whom our agreements may obligate us to indemnify against these claims. Successful claims of infringement by a third party could prevent us from offering certain products or features, require us to develop alternate, non-infringing technology, which could require significant time and during which we could be unable to continue to offer our affected products or solutions, require us to obtain a license, which may not be available on reasonable terms or at all, or force us to pay substantial damages, royalties, or other fees. For additional information, see the section titled “Risk Factors—Risks Related to Intellectual Property, Legal, and Regulatory Matters—The success of our business depends in part on our ability to protect and enforce our intellectual property rights.”

Backlog

We enter into both single and multi-year subscription contracts for our solutions. We generally invoice our subscription customers at the beginning of the subscription term, or in some instances, such as in multi-year arrangements, in installments. Until we have the contractual right to invoice, these contract amounts are classified as backlog. They are not recorded in deferred revenue or elsewhere in our consolidated financial statements. As of January 31, 2025, we had backlog of approximately \$2.8 billion. We expect backlog will change from period to period for several reasons, including the timing and duration of customer agreements, varying billing cycles of subscription agreements, and the timing and duration of customer renewals. Because revenue for any period is a function of revenue recognized from deferred revenue under contracts in existence at the beginning of the period, as well as contract renewals and new customer contracts during the period, backlog at the beginning of any period is not necessarily indicative of future revenue performance. We do not utilize backlog as a key management metric internally.

Seasonality

Given the annual budget approval process of many of our customers, we see seasonal patterns in our business. Net new ARR generation is typically greater in the second half of the year, particularly in the fourth quarter, as compared to the first half of the year. In addition, we also experience seasonality in our operating margin, typically with a lower margin in the first half of our fiscal year due to a step up in costs for payroll taxes and annual sales and marketing events. This also impacts the timing of operating cash flow.

Human Capital Resources

As of January 31, 2025, we had 10,118 full-time employees. We also engage temporary employees and consultants as needed to support our operations. None of our employees in the United States are represented by a labor union or subject to a collective bargaining agreement. In certain countries in which we operate, we are subject to local labor law requirements which may automatically make our employees subject to industry-wide collective bargaining agreements. We have not experienced any work stoppages, and we consider our relations with our employees to be good.

Attraction, Retention, and Talent Development

Supporting our people is a foundational value for CrowdStrike. We believe the company's success depends on our ability to attract, retain and develop employees. The skills, experience and industry knowledge of key employees significantly benefit our customers, operations and our overall company performance.

Our talent sourcing is aligned to our organizational strategy to provide the expertise and skills needed to move our mission forward. We have created a high-performance talent model that pinpoints the top traits and qualities we look for in talent and that may already exist within the organization, then consistently use that model to develop interview questions, screen candidates, and make hiring decisions.

CrowdStrike has always been a mission-focused organization. We hire and develop people based on their merits and alignment to our mission of stopping breaches. Our work requires us to consider problems from all angles. We believe that an open, collaborative environment strengthens our ability to build strong teams, serve our customers and drive innovation.

To attract high performers, we have a team dedicated to building and promoting our employer brand focused on creating a strong employer value proposition, which includes:

- Competitive pay and benefits
- Flexible working arrangements
- Role and task diversity
- Professional development opportunities
- Organizational reputation and culture

We provide robust compensation and benefits programs to help meet the needs of our employees. In addition to base salary, these programs (which vary by country/region) include annual bonuses or commission plans, equity awards, an employee stock purchase plan, a 401(k) plan or pension schemes internationally, healthcare and insurance benefits, health savings and flexible spending accounts, paid time off, family leave, family care resources, flexible work schedules, adoption and infertility assistance, and employee assistance programs.

We invest resources to develop the talent needed to remain a leader in cybersecurity. We deliver numerous training opportunities, provide rotational assignment opportunities, have expanded our focus on continuous learning and development, and ensure we manage performance, provide feedback, and develop talent.

Distributed Workforce

For CrowdStrike, the ability to work remotely or in a hybrid arrangement is a deliberate strategy that we believe fuels rapid innovation and helps us attract, hire and retain the best and brightest around the world, regardless of their specific location. Our culture is purpose-built around this ability, creating a competitive advantage for both the company and its customers and minimizing disruption from localized issues such as natural disasters, political events, or health emergencies.

CrowdStrike has had a distributed workforce since its inception. While working remotely has its advantages, we also believe that building community and engagement happens at a faster pace when people can come together.

Since the beginning, we recognized that creating high-functioning, effective remote and hybrid teams would require careful planning and system design to not only establish the culture but help it grow and evolve organically. We have designed our processes, systems, and teams so that most employees can perform their jobs without needing to be physically present in the same room or even in the same time zone. Part of supporting our remote and hybrid culture also involves actively encouraging personal well-being through initiatives, including wellness programs, engagement programs (speaker series, employee resource groups, gift exchanges, mentorship opportunities, virtual events, etc.), community outreach activities, recognition programs, and groups to connect people, no matter where they are geographically, with similar interests, life circumstances or backgrounds. We continue to find ways to bring our employees together to build community and camaraderie.

Our People and Core Values

At CrowdStrike, we embrace the mantra of “One Team. One Fight.” Our global team is passionate about working together toward our mission to stop breaches, knowing they will be fully included, supported and valued along the way. We are Fanatical About the Customer, Relentlessly Focused on Innovation and believe that our Limitless Passion drives Unlimited Potential for every CrowdStriker. Our Core Values sum up our culture. We provide the support and resources needed to enable people to do their best work.

Information about our Executive Officers

The following table sets forth certain information with respect to our current executive officers as of March 10, 2025:

| Name | Age | Position |
|------------------|-----|---|
| George Kurtz | 54 | President, Chief Executive Officer and Director |
| Burt W. Podbere | 59 | Chief Financial Officer |
| Shawn Henry | 62 | Chief Security Officer |
| Michael Sentonas | 51 | President |

There is no family relationship between any of our directors or executive officers and any other director or executive officer.

George Kurtz - President, Chief Executive Officer, and Director

Mr. Kurtz is one of our co-founders and has served as our President, Chief Executive Officer, and a member of our board of directors since November 2011. From October 2004 to October 2011, Mr. Kurtz served in executive roles at McAfee, Inc., a security technology company, including as Executive Vice President and Worldwide Chief Technology Officer from October 2009 to October 2011. In October 1999, Mr. Kurtz founded Foundstone, Inc., a security technology company, where he served as its Chief Executive Officer until it was acquired by McAfee, Inc. in October 2004. Since November 2017, he has also served as Chairman of the Board, and as President for the CrowdStrike Foundation, a nonprofit established to support the next generation of talent and research in cybersecurity and artificial intelligence through scholarships, grants, and other activities. He also served on the board of directors of Hewlett Packard Enterprise, an enterprise information technology company, from June 2019 to April 2023. Mr. Kurtz holds a B.S. in accounting from Seton Hall University. Mr. Kurtz also holds a CPA license from the State of New Jersey with an inactive status.

Burt W. Podbere - Chief Financial Officer

Mr. Podbere has served as our Chief Financial Officer since September 2015. From May 2014 to August 2015, Mr. Podbere served as Chief Financial Officer for OpenDNS, Inc. (acquired by Cisco in 2015), a cloud-delivered network security company, where he oversaw the finance function. From October 2011 to April 2014, he served as Chief Financial Officer for Net Optics, Inc. (acquired by Ixia in 2013), a manufacturer of network monitoring and intelligent access solutions for physical and virtual networks. Since November 2017, he has also served as Treasurer and as a board member for the CrowdStrike Foundation, a nonprofit established to support the next generation of talent and research in cybersecurity and artificial intelligence through scholarships, grants, and other activities. Mr. Podbere is a Chartered Accountant and holds a B.A. from McGill University.

Shawn Henry - Chief Security Officer

Mr. Henry has served as our Chief Security Officer since March 2012. From March 2012 to October 2022, Mr. Henry also served as President of CrowdStrike Services. Mr. Henry previously worked for the FBI from 1987 through March 2012, including most recently as Executive Assistant Director of the FBI’s Criminal, Cyber, Response and Services Branch. Since June 2016, Mr. Henry has served as a faculty member specializing in cybersecurity for the National Association of Corporate Directors, an organization providing training and education for private and public company directors. Mr. Henry previously served as a cybersecurity and national security analyst for NBC News. Since November 2021, Mr. Henry has served as a director of ShoulderUp Technology Acquisition Corp., a blank check company that completed its initial public offering in November 2021. Mr. Henry also serves on the board of directors of CLEAR, a technology identity company, and served on the

board of Global Cyber Alliance, a nonprofit organization dedicated to reducing cyber risk, from 2015 to December 2024. Additionally, Mr. Henry serves on the advisory boards of several organizations. Mr. Henry holds a B.B.A. from Hofstra University and an M.S. in criminal justice from Virginia Commonwealth University.

Michael Sentonas - President

Mr. Sentonas has served as our President since March 2023. Prior to being appointed President, Mr. Sentonas served as our Chief Technology Officer since February 2020, and as our Vice President, Technology Strategy from May 2016 to February 2020. Immediately prior to joining us, Mr. Sentonas served at McAfee Corp. from March 2004 to April 2016 in various positions, and finally as Chief Technology Officer – Security Connected from November 2013 to April 2016. Mr. Sentonas is a board member of the CrowdStrike Foundation, a nonprofit established to support the next generation of talent and research in cybersecurity and artificial intelligence through scholarships, grants, and other activities, and a member of the Forbes Technology Counsel, an organization for senior technology executives. He is an active public speaker on security issues and advises government and business communities on global and local cyber security threats. Mr. Sentonas holds a B.S. in computer science from Edith Cowan University, Western Australia.

Corporate Information

Our principal executive offices are located at 206 E. 9th Street, Suite 1400, Austin, Texas 78701 and our telephone number is (888) 512-8906. We are a holding company and all of our business operations are conducted through our subsidiaries, including CrowdStrike, Inc. Our website address is www.crowdstrike.com. Information contained on, or that can be accessed through, our website does not constitute part of this Annual Report on Form 10-K.

Available Information

Our Annual Report on Form 10-K, Quarterly Reports on Form 10-Q, Current Reports on Form 8-K, and amendments to these reports are filed with the SEC pursuant to Sections 13(a) and 15(d) of the Exchange Act. Such reports and other information filed or furnished by us with the SEC are available free of charge on our website at <https://ir.crowdstrike.com/financial-information/sec-filings>, as soon as reasonably practicable after we file such material with, or furnish it to, the SEC. The SEC maintains a website that contains the materials we file with or furnish to the SEC at www.sec.gov.

ITEM 1A. RISK FACTORS

A description of the risks and uncertainties associated with our business is set forth below. You should carefully consider the risks and uncertainties described below, as well as the other information in this Annual Report on Form 10-K, including our consolidated financial statements and the related notes and “Management’s Discussion and Analysis of Financial Condition and Results of Operations.” The occurrence of any of the events or developments described below, or of additional risks and uncertainties not presently known to us or that we currently deem immaterial, could materially and adversely affect our business, results of operations, financial condition and growth prospects. In such an event, the market price of our Class A common stock, or “common stock,” could decline, and you could lose all or part of your investment.

Summary of Risk Factors

Our business is subject to numerous risks and uncertainties, any one of which could materially adversely affect our business, results of operations, financial condition, and growth prospects. Below is a summary of some of these risks. This summary is not complete, and should be read together with the entire section titled “Risk Factors” in this Annual Report on Form 10-K, as well as the other information in this Annual Report on Form 10-K and the other filings that we make with the SEC.

- The July 19 Incident has had, and is expected to continue to have, an adverse effect on our business, sales, customer and partner relations, reputation, results of operations and financial condition.
- We have experienced rapid growth in recent periods, and if we do not manage our future growth, our business and results of operations will be adversely affected.
- We have a history of losses, and while we have achieved profitability in certain periods, including fiscal 2024, we may not be able to achieve or sustain profitability in the future.
- If organizations do not adopt cloud-based SaaS-delivered endpoint security solutions, our ability to grow our business and results of operations may be adversely affected.
- If we are unable to successfully enhance our existing products and services and introduce new products and services in response to rapid technological changes and market developments as well as evolving security threats, our competitive position and prospects will be harmed.
- If we are unable to attract new customers, our future results of operations could be harmed.
- If our customers do not renew their subscriptions for our products and add additional cloud modules to their subscriptions, our future results of operations could be harmed.
- Our sales cycles can be long and unpredictable, and our sales efforts require considerable time and expense.
- We face intense competition and could lose market share to our competitors, which could adversely affect our business, financial condition, and results of operations.
- If our solutions fail or are perceived to fail to detect or prevent incidents or have or are perceived to have defects, errors, or vulnerabilities, our brand and reputation would be harmed, which would adversely affect our business and results of operations.
- As a cybersecurity provider, we have been, and expect to continue to be, a target of cyberattacks. If our or our service providers’ internal networks, systems, or data are or are perceived to have been compromised, our reputation may be damaged and our financial results may be negatively affected.
- We rely on third-party data centers, such as Amazon Web Services, and our own colocation data centers to host and operate our Falcon platform, and any disruption of or interference with our use of these facilities may negatively affect our ability to maintain the performance and reliability of our Falcon platform, which could cause our business to suffer.

- We rely on our key technical, sales and management personnel to grow our business, and the loss of one or more key employees could harm our business.
- If we are unable to attract and retain qualified personnel, our business could be harmed.
- Our results of operations may fluctuate significantly, which could make our future results difficult to predict and could cause our results of operations to fall below expectations.
- If we are not able to maintain and enhance our CrowdStrike and Falcon brands and our reputation as a provider of high-efficacy security solutions, our business and results of operations may be adversely affected.
- Claims by others that we infringe their proprietary technology or other intellectual property rights could result in significant costs and substantially harm our business, financial condition, results of operations, and prospects.
- We are required to comply with stringent, complex and evolving laws, rules, regulations and standards in many jurisdictions, as well as contractual obligations, relating to data privacy and security. Any actual or perceived failure to comply with these requirements could have a material adverse effect on our business.
- Failure to comply with laws and regulations applicable to our business could subject us to fines and penalties and could also cause us to lose customers or negatively impact our ability to contract with customers, including those in the public sector.
- We are currently, and may in the future become, involved in litigation that may adversely affect us.
- We have in the past experienced, and may in the future experience, warranty claims, product returns, and claims related to product liability and product defects from real or perceived defects in our solutions or their misuse by our customers or third parties and indemnity provisions in various agreements potentially expose us to substantial liability for intellectual property infringement and other losses.
- Future acquisitions, strategic investments, partnerships, or alliances could be difficult to identify and integrate, divert the attention of key management personnel, disrupt our business, dilute stockholder value and adversely affect our business, financial condition and results of operations.

Risks Related to Our Business and Industry

The July 19 Incident has had, and is expected to continue to have, an adverse effect on our business, sales, customer and partner relations, reputation, results of operations and financial condition.

On July 19, 2024, we released a content configuration update for our Falcon sensor that resulted in system crashes for certain Windows systems (the “July 19 Incident”). We have incurred, and expect to continue to incur, significant costs and expenses related to the incident, including in connection with remediation efforts, customer and partner relations, measures taken to address the damage to our reputation, and other measures taken in response to the incident. Our management and other personnel have devoted, and may continue to devote, significant time and resources to address the impacts of the July 19 Incident. We also have hired, and in the future may hire, additional personnel to assist with our ongoing efforts. Any real or perceived failure, by us or the third-party service providers we engage, to remediate and respond to the July 19 Incident could adversely impact our business. While we are investing in enhancements to software resiliency, testing and customer controls following the July 19 Incident, we cannot guarantee that such enhancements will be effective, or that our products do not have or will not have defects, errors, or vulnerabilities.

The July 19 Incident has harmed, and is expected to continue to harm, our business, sales, customer and partner relations, and our reputation. As a result of the incident, certain of our existing or prospective customers have elected to, and may in the future elect to, defer purchasing decisions relating to our products and services or not purchase our products and services at all. Customers have also decided, and may in the future decide, to terminate or not renew their agreements with us. The July 19 Incident has negatively impacted, and may in the future negatively impact, our existing or prospective partners’ ability or willingness to promote our products or services. Certain of our competitors have aggressively approached our current and prospective customers and partners to attempt to capitalize on the incident, and may continue to do so. Furthermore, we have agreed to, and expect to agree to in the future, provide incentives in connection with our commercial arrangements with our

customers, including subscription period extensions, discounts or promotional modules. The July 19 Incident has received negative media coverage and harmed our reputation and brand. If we are unable to regain the trust of our current and prospective customers and partners, or if negative media coverage and publicity continues, our reputation and brand may suffer further, exacerbating the effects discussed herein. These factors may result in harm to our business, results of operations and financial condition.

We are party to a number of legal proceedings relating to the July 19 Incident, such as lawsuits filed by or on behalf of third parties, including securities litigation brought on behalf of certain purchasers of our common stock, derivative litigation asserting claims against certain officers and directors, and putative class actions brought by individual consumers. We have also received inquiries from governmental authorities and other third parties, and governmental authorities may seek to impose undertakings, injunctive relief, consent decrees or other penalties, which could, among other things, materially increase our expenses or otherwise require us to alter how we operate our business. Third parties, including governmental authorities, may take certain actions in response to the July 19 Incident that may negatively impact our business and operations and may result in additional costs and expenses relating to compliance, product development or other matters. Some customers and other third parties claiming to have been impacted by the incident have asserted claims against us or otherwise communicated their intent to seek indemnification or compensation from us. Additional claims may also be asserted by or on behalf of customers, customers' insurers, partners, stockholders or others seeking monetary damages or other relief. These lawsuits, claims and inquiries are resulting, and are expected to result in the future, in the incurrence of significant costs and expenses, the diversion of management's attention from the operation of our business and other negative impacts on our business and operations.

While we maintain insurance policies that may cover certain costs, claims and liabilities in connection with the July 19 Incident, we expect that our insurance coverage will not cover all costs, claims and liabilities actually incurred, and we cannot be certain that our insurance will continue to be available to us on commercially reasonable terms, or at all, or that any insurer will not deny coverage as to any future claim. The successful assertion of one or more large claims against us that exceed available insurance coverage, or the occurrence of changes in our insurance policies, including premium increases or the imposition of large deductible or co-insurance requirements, could have a material adverse effect on our business, including our financial condition, results of operations and reputation.

We have experienced rapid growth in recent periods, and if we do not manage our future growth, our business and results of operations will be adversely affected.

We have experienced rapid revenue growth in recent periods and we expect to continue to invest broadly across our organization to support our growth. For example, our headcount grew from 7,273 employees as of January 31, 2023, to 10,118 employees as of January 31, 2025. Although we have experienced rapid growth historically, we may not sustain our current growth rates and our investments to support our growth may not be successful. The growth and expansion of our business will require us to invest significant financial and operational resources and the continuous dedication of our management team. Our future success will depend in part on our ability to manage our growth effectively, which will require us to, among other things:

- effectively attract, integrate, and retain a large number of new employees, particularly members of our sales and marketing and research and development teams;
- further improve our Falcon platform, including our cloud modules, and IT infrastructure, including expanding and optimizing our data centers, to support our business needs;
- enhance our information and communication systems to ensure that our employees and offices around the world are well coordinated and can effectively communicate with each other and our growing base of channel partners and customers; and
- improve our financial, management, and compliance systems and controls.

If we fail to achieve these objectives effectively, our ability to manage our expected growth, ensure uninterrupted operation of our Falcon platform and key business systems, and comply with the rules and regulations applicable to our business could be impaired. Additionally, the quality of our platform and services could suffer and we may not be able to adequately address competitive challenges. Any of the foregoing could adversely affect our business, results of operations, and financial condition.

We have a history of losses, and while we have achieved profitability in certain periods, we may not be able to achieve or sustain profitability in the future.

We have incurred net losses each year prior to fiscal 2024, and we may not achieve or maintain profitability in the future. We experienced net losses of \$19.3 million and \$183.2 million for fiscal 2025 and 2023, respectively, and net income of \$89.3 million for fiscal 2024. As of January 31, 2025, we had an accumulated deficit of \$1.1 billion. While we have experienced significant growth in revenue in recent periods, and have achieved profitability during certain periods, including fiscal 2024, we cannot assure you when or whether we will reach sustained profitability. We also expect our operating expenses to increase in the future as we continue to invest for our future growth, which will negatively affect our results of operations if our total revenue does not increase. We cannot assure you that these investments will result in substantial increases in our total revenue or improvements in our results of operations. We also have incurred and expect to continue to incur significant additional legal, accounting, and other expenses as a public company. Any failure to increase our revenue as we invest in our business or to manage our costs could prevent us from achieving or maintaining profitability or positive cash flow.

If organizations do not adopt cloud-based SaaS-delivered endpoint security solutions, our ability to grow our business and results of operations may be adversely affected.

We believe our future success will depend in large part on the growth, if any, in the market for cloud-based SaaS-delivered endpoint security solutions. The use of SaaS solutions to manage and automate security and IT operations is at an early stage and rapidly evolving. As such, it is difficult to predict its potential growth, if any, customer adoption and retention rates, customer demand for our solutions, customer consolidation on our platform, or the success of existing competitive products. Any expansion in our market depends on a number of factors, including the cost, performance, and perceived value associated with our solutions and those of our competitors. If our solutions do not achieve widespread adoption or there is a reduction in demand for our solutions due to a lack of customer acceptance, technological challenges, damage to our reputation including as a result of the July 19 Incident, competing products, privacy concerns, decreases in corporate spending, weakening economic conditions or otherwise, it could result in early terminations, reduced customer retention rates, or decreased revenue, any of which would adversely affect our business, results of operations, and financial results. We do not know whether the trend in adoption of cloud-based SaaS-delivered endpoint security solutions we have experienced in the past will continue in the future. Furthermore, to the extent we or other SaaS security providers experience security incidents, loss or disclosure of customer data, disruptions in delivery, or other problems, the market for SaaS solutions as a whole, including our security solutions, could be negatively affected. You should consider our business and prospects in light of the risks and difficulties we encounter in this new and evolving market.

If we are unable to successfully enhance our existing products and services and introduce new products and services in response to rapid technological changes and market developments as well as evolving security threats, our competitive position and prospects will be harmed.

Our ability to increase revenue from existing customers and attract new customers will depend in significant part on our ability to anticipate and respond effectively to rapid technological changes and market developments as well as evolving security threats. The success of our Falcon platform depends on our ability to take such changes into account and invest effectively in our research and development organization to increase the reliability, availability and scalability of our existing solutions and introduce new solutions. If we fail to effectively anticipate, identify or respond to such changes in a timely manner, or at all, our business could be harmed. Even if we adequately fund our research and development efforts there is no guarantee that we will realize a return on such efforts.

Success in delivering enhancements and new solutions depends on several factors, including the timely completion, introduction and market acceptance of the enhancement or new solution, the risk that such enhancement or new solution may have quality or other defects or deficiencies (such as those experienced in connection with the July 19 Incident), especially in the early stages of introduction, as well as our ability to seamlessly integrate all of our product and service offerings and develop adequate sales capabilities in new markets. Failure to effectively deliver, integrate, and manage perceptions with respect to enhancements and new solutions could erode our competitive position, significantly impair our revenue growth, and negatively impact our operating results.

If we are unable to attract new customers, our future results of operations could be harmed.

To expand our customer base, we need to convince potential customers to allocate a portion of their discretionary budgets to purchase our Falcon platform. Our sales efforts often involve educating our prospective customers about the uses and benefits of our Falcon platform. Enterprises and governments that use legacy security products, such as signature-based or malware-based products, firewalls, intrusion prevention systems, and antivirus, for their IT security may be hesitant to purchase our Falcon platform if they believe that these products are more cost effective, provide substantially the same functionality as our Falcon platform or provide a level of IT security that is sufficient to meet their needs. We may have difficulty convincing prospective customers of the value of adopting our solution. Even if we are successful in convincing prospective customers that a cloud native platform like ours is critical to protect against cyberattacks, they may not decide to purchase our Falcon platform for a variety of reasons, some of which are out of our control. For example, any deterioration in general economic conditions, including as a result of the geopolitical environment, the outbreak of diseases or other public health crises, volatility in the banking and financial services sector, or inflation (as well as government policies such as raising interest rates in response to inflation), have in the past and may in the future cause our current and prospective customers to delay or cut their overall security and IT operations spending, and such delays or cuts may fall disproportionately on cloud-based security solutions like ours. Economic weakness, customer financial difficulties, constrained spending on security and IT operations, and the impact of the July 19 Incident may result in decreased revenue, reduced sales, an increase in multi-phase subscription start dates, shorter terms for customer subscriptions, lengthened sales cycles, increased churn, lower demand for our products, and adversely affect our results of operations and financial conditions. Furthermore, we may need to exercise more flexibility in customer payment terms as customers navigate a more challenging economic environment. Additionally, if the incidence of cyberattacks were to decline, or be perceived to decline, or if organizations adopt endpoints that use operating systems we do not adequately support, our ability to attract new customers and expand sales of our solutions to existing customers could be adversely affected. If organizations do not continue to adopt our Falcon platform, our sales will not grow as quickly as anticipated, or at all, and our business, results of operations, and financial condition would be harmed.

If our customers do not renew their subscriptions for our products and add additional cloud modules to their subscriptions, our future results of operations could be harmed.

In order for us to maintain or improve our results of operations, it is important that our customers renew their subscriptions for our Falcon platform when existing contract terms expire, and that we expand our commercial relationships with our existing customers by selling additional cloud modules and by deploying to more endpoints in their environments. Our customers have no obligation to renew their subscription for our Falcon platform after the expiration of their contractual subscription period, which is generally one to three years, and in the normal course of business, some customers have elected not to renew. In addition, customers that previously signed multi-year subscription contracts may renew for shorter contract subscription lengths, and customers may cease using certain cloud modules altogether. Even if customers choose to renew their subscription of certain cloud modules, they may decline to purchase additional cloud modules or choose not to consolidate onto our Falcon platform. Our customer retention, renewals and expansion may decline or fluctuate as a result of a number of factors, including our customers' satisfaction with our products and services, our customers' ability to fully utilize their product subscriptions, our pricing, customer security and networking issues and requirements, our customers' spending levels, decreases in the number of endpoints to which our customers deploy our solutions, mergers and acquisitions involving our customers, industry developments, competition, the impact of the July 19 Incident, including the impact of our customer commitment packages, and general economic and geopolitical conditions. Any such impacts on customer renewals may be associated with a variety of different factors, including customers electing to renew with shorter subscription periods, fewer cloud modules, fewer endpoints or smaller contract values. If our efforts to maintain and expand our relationships with our existing customers are not successful, our business, results of operations, and financial condition may materially suffer.

Our sales cycles can be long and unpredictable, and our sales efforts require considerable time and expense.

Our revenue recognition is difficult to predict because of the length and unpredictability of the sales cycle for our Falcon platform. Customers often view the subscription to our Falcon platform as a significant strategic decision and, as a result, frequently require considerable time to evaluate, test and qualify our Falcon platform prior to entering into or expanding a relationship with us. Large enterprises and government entities in particular often undertake a significant evaluation process that further lengthens and adds uncertainty to our sales cycle. In addition, uncertain economic conditions may lead to additional scrutiny of budgets by current and prospective customers, which has resulted in, for example, longer sales cycles for products and services, and may result in shifting demand for IT products and services, and slower adoption of new technologies. We have also experienced, and expect to continue to experience, longer sales cycles in connection with the July 19 Incident. We

may also experience longer sales cycles as customers seek to consolidate on our Falcon platform and negotiate larger deals, including in connection with our flexible subscription offering.

Our direct sales team develops relationships with our customers, and works with our channel partners on account penetration, account coordination, sales and overall market development. We spend substantial time and resources on our sales efforts without any assurance that our efforts will produce a sale. Security solution purchases are frequently subject to budget constraints, multiple approvals and unanticipated administrative, processing and other delays. As a result, it is difficult to predict whether and when a sale will be completed. The failure of our efforts to secure sales after investing resources in a lengthy sales process could adversely affect our business and results of operations.

We face intense competition and could lose market share to our competitors, which could adversely affect our business, financial condition, and results of operations.

The market for security and IT operations solutions is intensely competitive, fragmented, and characterized by rapid changes in technology, customer requirements, industry standards, increasingly sophisticated attackers, and by frequent introductions of new or improved products or services to combat security threats. We expect to continue to face intense competition from current competitors, as well as from new entrants into the market. If we are unable to anticipate or react to these challenges, our competitive position could weaken, and we could experience a decline in revenue or reduced revenue growth, and loss of market share that would adversely affect our business, financial condition, and results of operations. Our ability to compete effectively depends upon numerous factors, many of which are beyond our control, including, but not limited to:

- product capabilities, including performance and reliability, of our Falcon platform, including our cloud modules, services, and features compared to those of our competitors;
- our ability, and the ability of our competitors, to improve existing products, services, and features, or to develop new ones to address evolving customer needs;
- our ability to attract, retain, and motivate talented employees;
- our ability to establish and maintain relationships with channel partners and direct customers;
- the strength of our sales and marketing efforts;
- the strength of our reputation and brand, including the impact to our reputation and brand as a result of the July 19 Incident; and
- acquisitions or consolidation within our industry, which may result in more formidable competitors.

Our competitors include the following by general category:

- legacy antivirus product providers who offer a broad range of approaches and solutions including traditional signature-based anti-virus protection;
- alternative endpoint security providers who generally offer a mix of on-premise and cloud-hosted products that rely heavily on malware-only or application whitelisting techniques;
- network security vendors who are supplementing their core perimeter-based offerings with endpoint or cloud security solutions;
- cloud security vendors, including those who focus on public cloud infrastructure and services;
- identity security vendors that seek to identify and secure user accounts and related activities;
- professional service providers who offer cybersecurity response services; and
- legacy SIEM vendors who offer a range of log management and security capabilities.

Many of our competitors have greater financial, technical, marketing, sales, and other resources, greater name recognition, longer operating histories, and a larger base of customers than we do. They may be able to devote greater resources to the development, promotion, and sale of services than we can, and they may offer lower pricing than we do. Further, they may have greater resources for research and development of new technologies, the provision of customer support, and the pursuit of acquisitions. Our larger competitors have substantially broader and more diverse product and services offerings as well as routes to market, which allows them to leverage their relationships based on other products or incorporate functionality into existing products to gain business in a manner that discourages users from purchasing our platform, including our cloud modules. Conditions in our market could change rapidly and significantly as a result of technological advancements, including with respect to AI. Our competitors may more successfully incorporate AI into their products, gain or leverage superior access to certain AI technologies, and achieve higher market acceptance of their AI solutions. Conditions in our market could also change rapidly and significantly due to partnering or acquisitions by our competitors or continuing market consolidation. Some of our competitors have recently made acquisitions of businesses or have established cooperative relationships that may allow them to offer more directly competitive and comprehensive solutions than were previously offered and adapt more quickly to new technologies and customer needs. These competitive pressures in our market or our failure to compete effectively may result in price reductions, fewer orders, reduced revenue and gross margins, increased net losses and loss of market share. Further, competitors that specialize in providing protection from a single type of security threat may be able to deliver these targeted security products to the market quicker than we can or convince organizations that these limited products meet their needs. Even if there is significant demand for cloud-based security solutions like ours, if our competitors include functionality that is, or is perceived to be, equivalent to or better than ours in legacy products that are already generally accepted as necessary components of an organization's IT security architecture, we may have difficulty increasing the market penetration of our solutions. Furthermore, even if the functionality offered by other security and IT operations providers is more limited than the functionality of our platform, organizations may elect to accept such limited functionality in lieu of adding products from additional vendors like us. If we are unable to compete successfully, or if competing successfully requires us to take aggressive pricing or other actions, our business, financial condition, and results of operations would be adversely affected.

Competitive pricing pressure may reduce our gross profits and adversely affect our financial results.

If we are unable to maintain our pricing due to competitive pressures or other factors, our margins will be reduced and our gross profits, business, results of operations, and financial condition would be adversely affected. The subscription prices for our Falcon platform, cloud modules, and professional services may decline for a variety of reasons, including competitive pricing pressures, discounts, anticipation of the introduction of new solutions by our competitors, or promotional programs offered by us or our competitors. The cybersecurity market remains very competitive, and competition may further increase in the future. Competitors may reduce the price of products or subscriptions that compete with ours or may bundle them with other products and subscriptions.

If our solutions fail or are perceived to fail to detect or prevent incidents or have or are perceived to have defects, errors, or vulnerabilities, our brand and reputation would be harmed, which would adversely affect our business and results of operations.

Real or perceived defects, errors or vulnerabilities in our Falcon platform and cloud modules, the failure of our platform to detect or prevent incidents, including advanced and newly developed attacks, misconfiguration of our solutions, or the failure of customers to take action on attacks identified by our platform could harm our reputation and adversely affect our business, financial position and results of operations. Because our cloud native security platform is complex, it has contained, and may in the future contain defects, errors or vulnerabilities that are not detected until after deployment. For example, the July 19 Incident harmed our brand and reputation, business and results of operations. In addition, we identified a transport layer security issue that impacted certain Falcon Linux sensors, which led us to release a security fix and publish a security advisory to remediate the matter in February 2025. If we fail to timely detect defects or errors before deployment in the future, our brand and reputation, business and results of operations will suffer further. We cannot assure you that our products will detect all cyberattacks, especially in light of the rapidly changing security threat landscape that our solution seeks to address. Due to a variety of both internal and external factors, including, without limitation, defects or misconfigurations of our or third-party solutions, our solutions could be or become vulnerable to security incidents (both from intentional attacks and accidental causes) that cause them to fail to secure endpoints and detect and block attacks. Furthermore, any defects, errors or vulnerabilities in third-party technology or solutions we rely on could result in disruptions to our operations and adversely impact our business, financial condition and results of operations. In addition, because the techniques used by computer hackers to access or sabotage networks and endpoints change frequently and generally are not recognized until launched against a target, there is a risk that an advanced attack could emerge that our cloud native security platform is unable to detect or prevent

until after some of our customers are affected. Additionally, our Falcon platform may falsely indicate a cyberattack or threat that does not actually exist, which may lessen customers' trust in our solutions.

Moreover, as our cloud native security platform is adopted by an increasing number of enterprises and governments, individuals and organizations behind advanced cyberattacks may intensify their efforts to defeat our security platform. If this happens, our systems and subscription customers could be specifically targeted by attackers and could result in vulnerabilities in our platform or undermine the market acceptance of our Falcon platform and could adversely affect our reputation as a provider of security solutions. Because we host customer data on our cloud platform, which in some cases may contain personally-identifiable information or potentially confidential information, a security compromise, or an accidental or intentional misconfiguration or malfunction of our platform or third-party platforms, could result in personally-identifiable information and other customer data being accessible such as to attackers or to other customers. Further, if a high profile security breach occurs with respect to another next-generation or cloud-based security system, our customers and potential customers may lose trust in cloud solutions generally, and cloud-based security solutions such as ours in particular.

Organizations are increasingly subject to a wide variety of attacks on their networks, systems, and endpoints. No security solution, including our Falcon platform, can address all possible security threats or block all methods of penetrating a network or otherwise perpetrating a security incident. If any of our customers experiences a successful cyberattack while using our solutions or services, such customer could be disappointed with our Falcon platform, regardless of whether our solutions or services blocked the theft of any of such customer's data, if the customer failed to protect its own credentials, or if the attack would have otherwise been mitigated or prevented if the customer had fully deployed aspects of our Falcon platform. Similarly, if our solutions detect attacks against a customer but the customer does not address the vulnerability, customers and the public may erroneously believe that our solutions were not effective. Security breaches against customers that use our solutions may result in customers and the public believing that our solutions failed. Our Falcon platform may fail to detect or prevent malware, viruses, worms or similar threats for any number of reasons, including our failure to enhance and expand our Falcon platform to reflect the increasing sophistication of malware, viruses and other threats. Real or perceived security breaches of our customers' networks could cause disruption or damage to their networks or other negative consequences and could result in negative publicity to us, damage to our reputation, and other customer relations issues, and may adversely affect our revenue and results of operations.

As a cybersecurity provider, we have been, and expect to continue to be, a target of cyberattacks. If our or our service providers' internal networks, systems, or data are or are perceived to have been compromised, our reputation may be damaged and our financial results may be negatively affected.

As a provider of security solutions, we have in the past been, and may in the future be, specifically targeted by bad actors for attacks intended to circumvent our security capabilities or to exploit our Falcon platform as an entry point into customers' endpoints, networks, or systems. In particular, because we have been involved in the identification of organized cybercriminals and nation-state actors, we have been the subject of intense efforts by sophisticated cyber adversaries who seek to compromise our systems. Such efforts may also intensify as geopolitical tensions increase. In addition, bad actors have attempted to leverage the July 19 Incident to facilitate malicious activity, including, for example, through sending phishing emails posing as CrowdStrike support. Such activity, whether or not successful, could result in additional harm to our business. We are also susceptible to inadvertent compromises of our systems and data, including those arising from process, coding, or human errors. Moreover, we utilize third-party service providers to, among other things, host, transmit, or otherwise process electronic data in connection with our business activities, including our supply chain, operations, and communications. Our third-party service providers and other vendors have faced and may continue to face cyberattacks, compromises, interruptions in service, or other security incidents from a variety of sources. A successful attack or other incident that results in an interruption of service or that compromises our or our service providers' internal networks, systems, or data could have a significant negative effect on our operations, reputation, financial resources, and the value of our intellectual property. We cannot assure you that any of our efforts to manage this risk, including adoption of a comprehensive incident response plan and process for detecting, mitigating, and investigating security incidents that we regularly test through table-top exercises, testing of our security protocols through additional techniques, such as penetration testing, debriefing after security incidents, to improve our security and responses, and regular briefing of our directors and officers on our cybersecurity risks, preparedness, and management, will be effective in protecting us from such attacks.

It is virtually impossible for us to entirely eliminate the risk of such attacks, compromises, interruptions in service, or other security incidents affecting our internal systems or data, or that of our third-party service providers and vendors. Organizations are subject to a wide variety of attacks on their supply chain, networks, systems, and endpoints, and techniques used to sabotage or to obtain unauthorized access to networks in which data is stored or through which data is transmitted change frequently. Furthermore, employee error or malicious activity could compromise our systems. As a result, we may be unable to anticipate these techniques or implement adequate measures to prevent an intrusion into our networks, which could result in unauthorized access to customer data, intellectual property including access to our source code, and information about vulnerabilities in our product, which in turn, could reduce the effectiveness of our solutions, or lead to cyberattacks or other intrusions of our customers' networks, litigation, governmental audits and investigations and significant legal fees, any or all of which could damage our relationships with our existing customers and could have a negative effect on our ability to attract and retain new customers. We have expended, and anticipate continuing to expend, significant resources in an effort to prevent security breaches and other security incidents impacting our systems and data. Since our business is focused on providing reliable security services to our customers, we believe that an actual or perceived security incident affecting our internal systems or data or data of our customers would be especially detrimental to our reputation, customer confidence in our solution, and our business.

In addition, while we maintain insurance policies that may cover certain liabilities in connection with a cybersecurity incident, we cannot be certain that our insurance coverage will be adequate for liabilities actually incurred, that insurance will continue to be available to us on commercially reasonable terms, or at all, or that any insurer will not deny coverage as to any future claim. The successful assertion of one or more large claims against us that exceed available insurance coverage, or the occurrence of changes in our insurance policies, including premium increases or the imposition of large deductible or co-insurance requirements, could have a material adverse effect on our business, including our financial condition, results of operations and reputation.

We rely on third-party data centers, such as Amazon Web Services, and our own colocation data centers to host and operate our Falcon platform, and any disruption of or interference with our use of these facilities may negatively affect our ability to maintain the performance and reliability of our Falcon platform which could cause our business to suffer.

Our customers depend on the continuous availability of our Falcon platform. We currently host our Falcon platform and serve our customers using a mix of third-party data centers, primarily Amazon Web Services, Inc., or AWS, and our data centers, hosted in colocation facilities. Consequently, we may be subject to service disruptions as well as failures to provide adequate support for reasons that are outside of our direct control. We have experienced, and expect that in the future we may experience interruptions, delays and outages in service and availability from time to time due to a variety of factors, including infrastructure changes, human or software errors, website hosting disruptions and capacity constraints.

The following factors, many of which are beyond our control, can affect the delivery, availability, and the performance of our Falcon platform:

- the development and maintenance of the infrastructure of the internet;
- the performance and availability of third-party providers of cloud infrastructure services, such as AWS, with the necessary speed, data capacity and security for providing reliable internet access and services;
- decisions by the owners and operators of the data centers where our cloud infrastructure is deployed to terminate our contracts, discontinue services to us, shut down operations or facilities, increase prices, change service levels, limit bandwidth, declare bankruptcy or prioritize the traffic of other parties;
- physical or electronic break-ins, acts of war or terrorism, human error or interference (including by disgruntled employees, former employees or contractors) and other catastrophic events;
- cyberattacks, including denial of service attacks, targeted at us, our data centers, or the infrastructure of the internet;
- failure by us to maintain and update our cloud infrastructure to meet our data capacity requirements;
- errors, defects or performance problems in our software, including third-party software incorporated in our software;

- improper deployment or configuration of our solutions;
- the failure of our redundancy systems, in the event of a service disruption at one of our data centers, to provide failover to other data centers in our data center network; and
- the failure of our disaster recovery and business continuity arrangements.

The adverse effects of any service interruptions on our reputation, results of operations, and financial condition may be disproportionately heightened due to the nature of our business and the fact that our customers have a low tolerance for interruptions of any duration. Interruptions or failures in our service delivery could result in a cyberattack or other security threat to us or to one of our customers during such periods of interruption or failure. Additionally, interruptions or failures in our service could cause customers to terminate their subscriptions with us, adversely affect our renewal rates, and harm our ability to attract new customers. Our business would also be harmed if our customers believe that a cloud-based SaaS-delivered endpoint security solution is unreliable. We have experienced, and may in the future experience, service interruptions and other performance problems due to a variety of factors. The occurrence of any of these factors, or if we are unable to rapidly and cost-effectively fix such errors or other problems that may be identified, could damage our reputation, negatively affect our relationship with our customers or otherwise harm our business, results of operations and financial condition.

We rely on our key technical, sales and management personnel to grow our business, and the loss of one or more key employees could harm our business.

Our future success is substantially dependent on our ability to attract, retain, and motivate the members of our management team and other key employees throughout our organization. In particular, we are highly dependent on the services of George Kurtz, our President and Chief Executive Officer, who is critical to our future vision and strategic direction. We rely on our leadership team in the areas of operations, security, research and development, marketing, sales, support and general and administrative functions. Although we have entered into employment agreements with our key personnel, our employees, including our executive officers, work for us on an “at-will” basis, which means they may terminate their employment with us at any time. Leadership transitions can be inherently difficult to manage. In particular, they can cause operational and administrative inefficiencies, and could impact relationships with key customers and vendors. If Mr. Kurtz, or one or more of our key employees, or members of our management team resigns or otherwise ceases to provide us with their service, our business could be harmed.

If we are unable to attract and retain qualified personnel, our business could be harmed.

There is significant competition for personnel with the skills and technical knowledge that we require across our technology, cyber, sales, professional services, and administrative support functions. Competition for these personnel is intense, especially for experienced sales professionals and for engineers experienced in designing and developing cloud applications and security software. We have from time to time experienced, and we expect to continue to experience, difficulty in hiring and retaining employees with appropriate qualifications. For example, in recent years, recruiting, hiring and retaining employees with expertise in the cybersecurity industry has become increasingly difficult as the demand for cybersecurity professionals has increased as a result of the recent cybersecurity attacks on global corporations and governments. Additionally, our incident response and proactive services team is small and comprised of personnel with highly technical skills and experience, who are in high demand, and who would be difficult to replace. More generally, the technology industry is subject to substantial and continuous competition for engineers with high levels of experience in designing, developing and managing software and Internet-related services. Many of the companies with which we compete for experienced personnel have greater resources than we have. Our competitors also may be successful in recruiting and hiring members of our management team or other key employees, and it may be difficult for us to find suitable replacements on a timely basis, on competitive terms, or at all. We have in the past, and may in the future, be subject to allegations that employees we hire have been improperly solicited, or that they have divulged proprietary or other confidential information or that their former employers own such employees’ inventions or other work product, or that they have been hired in violation of non-compete provisions or non-solicitation provisions.

In addition, job candidates and existing employees often consider the value of the equity awards they receive in connection with their employment. Therefore, volatility or lack of performance in our stock price could affect our ability to attract and retain our key employees. Also, many of our employees have become, or will soon become, vested in a substantial amount of equity awards, which may give them a substantial amount of personal wealth. This may make it more difficult for us to retain and motivate these employees, and this wealth could affect their decision about whether or not they continue to work for us. Any failure to successfully attract, integrate or retain qualified personnel to fulfill our current or future needs could adversely affect our business, results of operations and financial condition.

If we do not effectively expand and train our direct sales force, we may be unable to add new customers or increase sales to our existing customers, and our business will be adversely affected.

We depend on our direct sales force to obtain new customers and increase sales with existing customers. Our ability to achieve significant revenue growth will depend, in large part, on our success in recruiting, training and retaining sufficient numbers of sales personnel, particularly in international markets. We have expanded our sales organization significantly in recent periods and expect to continue to add additional sales capabilities in the near term. There is significant competition for sales personnel with the skills and technical knowledge that we require. New hires require significant training and may take significant time before they achieve full productivity, and this delay is accentuated by our long sales cycles. Our recent hires and planned hires may not become productive as quickly as we expect, and we may be unable to hire or retain sufficient numbers of qualified individuals in the markets where we do business or plan to do business. In addition, a large percentage of our sales force is new to our company and selling our solutions, and therefore this team may be less effective than our more seasoned sales personnel. Furthermore, hiring sales personnel in new countries, or expanding our existing presence, requires upfront and ongoing expenditures that we may not recover if the sales personnel fail to achieve full productivity. We cannot predict whether, or to what extent, our sales will increase as we expand our sales force or how long it will take for sales personnel to become productive. If we are unable to hire and train a sufficient number of effective sales personnel, or the sales personnel we hire are not successful in obtaining new customers or increasing sales to our existing customer base, our business and results of operations will be adversely affected.

Because we recognize revenue from subscriptions to our platform over the term of the subscription, downturns or upturns in new business will not be immediately reflected in our results of operations.

We generally recognize revenue from customers ratably over the terms of their subscription, which is generally one to three years. As a result, a substantial portion of the revenue we report in each period is attributable to the recognition of deferred revenue relating to agreements that we entered into during previous periods. Consequently, any increase or decline in new sales or renewals in any one period will not be immediately reflected in our revenue for that period. Any such change, however, would affect our revenue in future periods. In addition, subscription commencement dates may be impacted by a number of factors, some of which we may exercise varying degrees of control over, including terms negotiated with our customers and our internal review, approval and provisioning processes. As a result, the impact of new subscriptions may not be immediately reflected in our results of operations. Moreover, the effect of downturns or upturns in new sales and potential changes in our rate of renewals, including as a result of the July 19 Incident, may not be fully reflected in our results of operations until future periods. In addition, customer commitment packages introduced following the July 19 Incident that extend subscription periods will lengthen the applicable term over which we recognize revenue, which has adversely affected, and is expected to continue to adversely affect, our results. We may also be unable to timely reduce our cost structure in line with a significant deterioration in sales or renewals that would adversely affect our results of operations and financial condition.

Our results of operations may fluctuate significantly, which could make our future results difficult to predict and could cause our results of operations to fall below expectations.

Our results of operations may vary significantly from period to period, which could adversely affect our business, financial condition and results of operations. Our results of operations have varied significantly from period to period, and we expect that our results of operations will continue to vary as a result of a number of factors, many of which are outside of our control and may be difficult to predict, including:

- our ability to attract new and retain existing customers;
- the budgeting cycles, seasonal buying patterns, and purchasing practices of customers;

- economic difficulties confronting our customers, which may impact the number of modules or endpoint deployments they are willing or able to purchase;
- insolvency or credit difficulties confronting our customers, affecting their ability to purchase or pay for our solutions, including in connection with our customer and end-user financing arrangements;
- the timing and length of our sales cycles;
- changes in customer or channel partner requirements or market needs;
- any disruption in our relationship with channel partners;
- changes in the growth rate of the cloud-based SaaS-delivered endpoint security solutions market;
- the timing and success of new product and service introductions by us or our competitors or any other competitive developments, including consolidation among our customers or competitors;
- decisions by organizations to purchase security solutions from larger, more established security vendors or from their primary IT equipment vendors;
- changes in our pricing policies or those of our competitors;
- the level of awareness of cybersecurity threats, particularly advanced cyberattacks, and the market adoption of our Falcon platform;
- significant security breaches of, technical difficulties with or interruptions to, the use of our Falcon platform;
- the impact to our business from the July 19 Incident;
- negative media coverage or publicity;
- our ability to successfully expand our business domestically and internationally;
- the amount and timing of operating costs (including new hires), tightening of labor markets and capital expenditures related to the expansion of our business;
- extraordinary expenses such as litigation, regulatory or other dispute-related settlement payments or outcomes;
- increases or decreases in our expenses caused by fluctuations in foreign currency exchange rates;
- future accounting pronouncements or changes in our accounting policies or practices;
- developments relating to our valuation allowances for our deferred tax assets;
- deteriorating or volatile conditions in the global economy and financial markets, including as a result of weak or negative gross domestic product growth, uncertainty or disruptions in the capital and credit markets, changing interest rates, inflation, bank failures or adverse conditions impacting financial institutions, and supply-chain disruptions; and
- political events, geopolitical unrest or tension, acts of war and terrorism.

In addition, we experience seasonal fluctuations in our financial results as we typically receive a higher percentage of our annual orders from new customers, as well as renewal orders from existing customers, in the second half of the fiscal year as compared to the first half of the year due to the annual budget approval processes of many of our customers. In addition, we also experience seasonality in our operating margin, typically with a lower margin in the first half of our fiscal year. Any of the above factors, individually or in the aggregate, may result in significant fluctuations in our financial and other results of operations from period to period. As a result of this variability, our historical results of operations should not be relied upon as an indication of future performance. Moreover, this variability and unpredictability could result in our failure to meet our operating plan or the expectations of investors or analysts for any period. If we fail to meet such expectations for these or other reasons, our stock price could fall substantially, and we could face costly lawsuits, including securities class action suits. For example, we are currently party to securities litigation brought in connection with the July 19 Incident on behalf of certain purchasers of our common stock.

If we are not able to maintain and enhance our CrowdStrike and Falcon brands and our reputation as a provider of high-efficacy security solutions, our business and results of operations may be adversely affected.

We believe that maintaining and enhancing our CrowdStrike and Falcon brands and our reputation as a provider of high-efficacy security solutions is critical to our relationship with our existing customers, channel partners, and technology alliance partners and our ability to attract new customers and partners. The successful promotion of our CrowdStrike and Falcon brands depends on a number of factors, including our marketing efforts, our ability to continue to develop additional cloud modules and features for our Falcon platform, our ability to successfully differentiate our Falcon platform from competitive cloud-based or legacy security solutions and, ultimately, our ability to detect and stop breaches. Although we believe it is important for our growth, our brand promotion activities may not be successful or yield increased revenue.

In addition, independent industry or financial analysts and research firms often test our solutions and provide reviews of our Falcon platform, as well as the products of our competitors, and perception of our Falcon platform in the marketplace may be significantly influenced by these reviews. If these reviews are negative, or less positive as compared to those of our competitors' products, our brand may be adversely affected. Our solutions may fail to detect or prevent threats in any particular test for a number of reasons that may or may not be related to the efficacy of our solutions in real world environments. To the extent potential customers, industry analysts or testing firms believe that the occurrence of a failure to detect or prevent any particular threat is a flaw or indicates that our solutions or services do not provide significant value, we may lose customers, and our reputation, financial condition and business would be harmed. Additionally, the performance of our channel partners and technology alliance partners may affect our brand and reputation if customers do not have a positive experience with these partners. In addition, we have in the past worked, and continue to work, with high profile private and public customers as well as assist in analyzing and remediating high profile cyberattacks, which sometimes involve nation-state actors. Our work with such customers has exposed us to publicity and media coverage. Changing political environments in the United States and abroad may amplify the media and political scrutiny we face. Negative publicity about us, including about our management, the efficacy and reliability of our Falcon platform, our products offerings, our professional services, and the customers we work with, even if inaccurate, has in the past adversely affected, and may in the future adversely affect, our reputation and brand. For example, the July 19 Incident, which received significant media attention and negative publicity, harmed our reputation and brand.

If we are unable to maintain successful relationships with our channel partners and technology alliance partners, or if our channel partners or technology alliance partners fail to perform, our ability to market, sell and distribute our Falcon platform will be limited, and our business, financial position and results of operations will be harmed.

In addition to our direct sales force, we rely on our channel partners to sell and support our Falcon platform. The vast majority of sales of our Falcon platform flow through our channel partners, and we expect this to continue for the foreseeable future. Additionally, we have entered, and intend to continue to enter, into technology alliance partnerships with third parties to support our future growth plans. The loss of a substantial number of our channel partners or technology alliance partners, or the failure to recruit additional partners, could adversely affect our results of operations. Our ability to achieve revenue growth in the future will depend in part on our success in maintaining successful relationships with our channel partners and in training our channel partners to independently sell and deploy our Falcon platform. If we fail to effectively manage our existing sales channels, or if our channel partners are unsuccessful in fulfilling the orders for our solutions, or if we are unable to enter into arrangements with, and retain a sufficient number of, high quality channel partners in each of the regions in which we sell solutions and keep them motivated to sell our products, our ability to sell our products and results of operations will be harmed.

Our international operations and plans for future international expansion expose us to significant risks, and failure to manage those risks could adversely impact our business.

We derived approximately 32%, 32%, and 30% of our total revenue from our international customers for fiscal 2025, fiscal 2024, and fiscal 2023, respectively. We are continuing to adapt to and develop strategies to address international markets and our growth strategy includes expansion into target geographies, but there is no guarantee that such efforts will be successful. We expect that our international activities will continue to grow in the future, as we continue to pursue opportunities in international markets. These international operations will require significant management attention and financial resources and are subject to substantial risks, including:

- greater difficulty in negotiating contracts with standard terms, enforcing contracts and managing collections, and longer collection periods;
- higher costs of doing business internationally, including costs incurred in establishing and maintaining office space and equipment for our international operations;
- management communication and integration problems resulting from cultural and geographic dispersion;
- risks associated with trade restrictions and foreign legal requirements, including any importation, certification, and localization of our Falcon platform that may be required in foreign countries;
- greater risk of unexpected changes in regulatory practices, tariffs, and tax laws and treaties;
- compliance with anti-bribery laws, including, without limitation, compliance with the U.S. Foreign Corrupt Practices Act of 1977, as amended, or FCPA, the U.S. Travel Act and the U.K. Bribery Act 2010, or Bribery Act, violations of which could lead to significant fines, penalties, and collateral consequences for our company;
- heightened risk of unfair or corrupt business practices in certain geographies and of improper or fraudulent sales arrangements that may impact financial results and result in restatements of, or irregularities in, financial statements;
- the uncertainty of protection for intellectual property rights in some countries;
- general economic and political conditions in these foreign markets;
- foreign exchange controls or tax regulations that might prevent us from repatriating cash earned outside the United States;
- political and economic instability in some countries;
- double taxation of our international earnings and potentially adverse tax consequences due to changes in the tax laws of the United States or the foreign jurisdictions in which we operate;
- unexpected costs for the localization of our services, including translation into foreign languages and adaptation for local practices and regulatory requirements (including, but not limited to data localization requirements);
- requirements to comply with foreign privacy, data protection, and information security laws and regulations and the risks and costs of noncompliance;
- greater difficulty in identifying, attracting and retaining local qualified personnel, and the costs and expenses associated with such activities;
- greater difficulty identifying qualified channel partners and maintaining successful relationships with such partners;
- differing employment practices and labor relations issues; and

- difficulties in managing and staffing international offices and increased travel, infrastructure, and legal compliance costs associated with multiple international locations.

Additionally, nearly all of our sales contracts are currently denominated in U.S. dollars. However, a strengthening of the U.S. dollar could increase the cost of our solutions to our international customers, which could adversely affect our business and results of operations. In addition, an increasing portion of our operating expenses is incurred outside the United States; is denominated in foreign currencies, such as the Australian Dollar, British Pound, Canadian Dollar, Euro, Indian Rupee, and Japanese Yen; and is subject to fluctuations due to changes in foreign currency exchange rates. If we become more exposed to currency fluctuations and are not able to successfully hedge against the risks associated with currency fluctuations, our results of operations could be adversely affected.

As we continue to develop and grow our business globally, our success will depend in large part on our ability to anticipate and effectively manage these risks. The expansion of our existing international operations and entry into additional international markets will require significant management attention and financial resources. Our failure to successfully manage our international operations and the associated risks could limit the future growth of our business.

Our business depends, in part, on sales to government organizations, and significant changes in the contracting or fiscal policies of such government organizations could have an adverse effect on our business and results of operations.

Our future growth depends, in part, on increasing sales to government organizations. Demand from government organizations is often unpredictable, subject to budgetary uncertainty and typically involves long sales cycles. We have made significant investment to address the government sector, but we cannot assure you that these investments will be successful, or that we will be able to maintain or grow our revenue from the government sector. U.S. federal, state and local government sales as well as foreign government sales are subject to a number of challenges and risks that may adversely impact our business.

Sales to such government entities include, but are not limited to, the following risks:

- selling to governmental agencies can be highly competitive, expensive and time consuming, often requiring significant upfront time and expense without any assurance that such efforts will generate a sale;
- we may be required to obtain personnel security clearances and facility clearances to perform on classified contracts for government agencies, and there is no guarantee that we will be able to obtain or maintain such clearances;
- government certification, software supply chain, or source code transparency requirements applicable to us or our products are constantly evolving and, in doing so, restrict our ability to sell to certain government customers until we have attained the new or revised certification or meet other applicable requirements, which we are not guaranteed to do. For example, although we are currently certified under the U.S. Federal Risk and Authorization Management Program, or FedRAMP, such certification is costly to maintain and if we lose our certification it would restrict our ability to sell to government customers;
- government product requirements are often technically complex and assessors may require us to make costly changes to our products to meet such requirements without any assurance that such changes will generate a sale or improve the efficacy of our products;
- government demand and payment for our Falcon platform may be impacted by public sector budgetary cycles and funding authorizations, with funding reductions or delays in the government appropriations or procurement processes adversely affecting public sector demand for our Falcon platform, including as a result of abrupt events such as war, incidents of terrorism, natural disasters, and public health concerns or epidemics;
- government attitudes towards us as a company, our platform or the capabilities that we offer as a viable software solution may change, and reduce interest in our products and services as acceptable solutions;
- changes in the political environment, including before or after a change to the leadership within the government administration, can create uncertainty or changes in policy or priorities and reduce available funding for our products and services;

- third parties may compete intensely with us on pending, new or existing contracts with government products, which can also lead to appeals, disputes, or litigation relating to government procurement, including but not limited to bid protests by unsuccessful bidders on potential or actual awards of contracts to us or our partners by the government;
- even if we are awarded a sale, the terms of such contracts may be unusually burdensome;
- governments routinely investigate and audit government contractors' administrative processes, and any unfavorable audit could result in the government refusing to continue buying our Falcon platform, which would adversely impact our revenue and results of operations, or institute fines or civil or criminal liability if the audit were to uncover improper or illegal activities; and
- governments may require certain products to be manufactured, hosted, or accessed solely in their country or in other relatively high-cost manufacturing locations, and we may not manufacture all products in locations that meet these requirements, affecting our ability to sell these products to governmental agencies.

The occurrence of any of the foregoing risks could cause governments and governmental agencies to delay or refrain from purchasing our solutions in the future or otherwise have an adverse effect on our business and results of operations.

We may not timely and cost-effectively scale and adapt our existing technology to meet our customers' performance and other requirements.

Our future growth is dependent upon our ability to continue to meet the needs of new customers and the expanding needs of our existing customers as their use of our solutions grow. As our customers gain more experience with our solutions, the number of endpoints and events, the amount of data transferred, processed and stored by us, the number of locations where our platform and services are being accessed, have in the past, and may in the future, expand rapidly. In order to meet the performance and other requirements of our customers, we intend to continue to make significant investments to increase capacity and to develop and implement new technologies in our service and cloud infrastructure operations. These technologies, which include databases, applications and server optimizations, network and hosting strategies, and automation, are often advanced, complex, new and untested. We may not be successful in developing or implementing these technologies. In addition, as our business grows, we must continue to improve and expand our information technology infrastructure. It takes a significant amount of time to plan, develop and test improvements to our technologies and infrastructure, and we may not be able to accurately forecast demand or predict the results we will realize from such improvements. We rely on external ecosystems, such as operating systems, to operate and make our products and services available to customers. If we are unable to adapt to product or policy changes in such ecosystems, or if we do not effectively operate with such ecosystems, demand for and availability of our products or services could decline. To the extent that we do not effectively scale our operations and infrastructure to meet the needs of our business, our growing customer base and to maintain performance as our customers expand their use of our solutions, we may not be able to grow as quickly as we anticipate, our customers may reduce or cancel use of our solutions and we may be unable to compete as effectively and our business and results of operations may be harmed.

Additionally, we have and will continue to make substantial investments to support growth at our data centers and improve the profitability of our cloud platform. For example, because of the importance of AWS' services to our business and AWS' position in the cloud-based server industry, any renegotiation or renewal of our agreement with AWS may be on terms that are significantly less favorable to us than our current agreement. If our cloud-based server costs were to increase, our business, results of operations and financial condition may be adversely affected. Although we expect that we could receive similar services from other third parties, if any of our arrangements with AWS are terminated, we could experience interruptions on our Falcon platform and in our ability to make our solutions available to customers, as well as delays and additional expenses in arranging alternative cloud infrastructure services. Ongoing improvements to cloud infrastructure may be more expensive than we anticipate, and may not yield the expected savings in operating costs or the expected performance benefits. In addition, we may be required to re-invest any cost savings achieved from prior cloud infrastructure improvements in future infrastructure projects to maintain the levels of service required by our customers. We may not be able to maintain or achieve cost savings from our investments, which could harm our financial results.

Our ability to maintain customer satisfaction depends in part on the quality of our customer support.

Once our Falcon platform is deployed within our customers' networks, our customers depend on our customer support services to resolve any issues relating to the implementation and maintenance of our Falcon platform. If we do not provide effective ongoing support, customer renewals and our ability to sell additional modules as part of our Falcon platform to existing customers could be adversely affected and our reputation with potential customers could be damaged. Many of our larger organizational customers have more complex networks and require higher levels of support than smaller customers and we offer premium services for these customers. Failure to maintain high-quality customer support could have a material adverse effect on our business, results of operations, and financial condition.

We may need to raise additional capital to expand our operations and invest in new solutions, which capital may not be available on terms acceptable to us, or at all, and which could reduce our ability to compete and could harm our business.

We expect that the combination of our existing cash and cash equivalents, cash flows from operations, and our revolving facility will be sufficient to meet our anticipated cash needs for working capital and capital expenditures for at least the next 12 months. Retaining or expanding our current levels of personnel and product and service offerings may require additional funds to respond to business challenges, including the need to develop new products or services and enhancements to our Falcon platform, improve our operating infrastructure, or acquire complementary businesses and technologies. Our failure to raise additional capital or generate the significant capital necessary to expand our operations and invest in new products or services could reduce our ability to compete and could harm our business. Accordingly, we may need to engage in additional equity or debt financings to secure additional funds. If we raise additional equity financing, our stockholders may experience significant dilution of their ownership interests and the market price of our common stock could decline. If we engage in additional debt financing, the holders of such debt would have priority over the holders of our common stock, and we may be required to accept terms that further restrict our operations or our ability to incur additional indebtedness or to take other actions that would otherwise be in the interests of the debt holders. Any of the above could harm our business, results of operations, and financial condition.

If we cannot maintain our company culture as we grow, we could lose the innovation, teamwork, passion, and focus on execution that we believe contribute to our success and our business may be harmed.

We believe that our corporate culture has been a contributor to our success, which we believe fosters innovation, teamwork, passion and focus on building and marketing our Falcon platform. As we grow, we may find it difficult to maintain our corporate culture. Any failure to preserve our culture could harm our future success, including our ability to retain and recruit personnel, innovate and operate effectively and execute on our business strategy. Additionally, our productivity and the quality of our solutions may be adversely affected if we do not integrate and train our new employees quickly and effectively. If we experience any of these effects in connection with future growth, it could impair our ability to attract new customers, retain existing customers and expand their use of our Falcon platform, all of which would adversely affect our business, financial condition and results of operations.

We rely on a limited number of suppliers for certain components of the equipment we use to operate our cloud platform. Supply chain disruptions could delay our ability to expand or increase the capacity of our global data center network, replace defective equipment in our existing data centers and impact our operating costs.

We rely on a limited number of suppliers for several components of the equipment we use to operate our cloud platform and provide services to our customers. We generally purchase these components on a purchase order basis, and do not have long-term contracts guaranteeing supply. Our reliance on these suppliers exposes us to risks, including reduced control over production costs and constraints based on the then current availability, terms and pricing of these components. If we experience disruption or delay from our suppliers, we may not be able to obtain supplies or components from alternative suppliers on a timely basis or on terms that are favorable to us, if at all. The technology industry has experienced widespread component shortages and delivery delays, including as a result of geopolitical tensions, public health crises and natural disasters. While we have taken steps to mitigate our supply chain risk, supply chain disruptions and delays could nevertheless adversely impact our operations by, among other things, causing us to delay opening new data centers, delay increasing capacity or replacing defective equipment at existing data centers, and experience increased operating costs.

We are exposed to the credit risks of certain of our customers and end-users, which could adversely impact our business, financial condition or results of operations.

We provide financing arrangements for certain of our customers and end-users to purchase our products and services. Such financing activities expose us to the credit risks of our customers and end-users and these risks may be more pronounced if our customers and end-users are negatively impacted by a global economic downturn or periods of economic uncertainty. There can be no assurance that our efforts to monitor and mitigate these credit risks will be effective. If we are unable to adequately control these risks, our business, financial condition or results of operations could be harmed.

Risks Related to Intellectual Property, Legal, and Regulatory Matters

The success of our business depends in part on our ability to protect and enforce our intellectual property rights.

We believe our intellectual property is an essential asset of our business, and our success and ability to compete depend in part upon protection of our intellectual property rights. We rely on a combination of patent, copyright, trademark and trade secret laws, as well as confidentiality procedures and contractual provisions, to establish and protect our intellectual property rights in the United States and abroad, all of which provide only limited protection. The efforts we have taken to protect our intellectual property may not be sufficient or effective, and our trademarks, copyrights and patents may be held invalid or unenforceable. Moreover, we cannot assure you that any patents will be issued with respect to our currently pending patent applications in a manner that gives us adequate defensive protection or competitive advantages, or that any patents issued to us will not be challenged, invalidated or circumvented. We have filed for patents in the United States and in certain non-U.S. jurisdictions, but such protections may not be available in all countries in which we operate or in which we seek to enforce our intellectual property rights, or may be difficult to enforce in practice. For example, many foreign countries have compulsory licensing laws under which a patent owner must grant licenses to third parties. In addition, many countries limit the enforceability of patents against certain third parties, including government agencies or government contractors. In these countries, patents may provide limited or no benefit. Moreover, we may need to expend additional resources to defend our intellectual property rights in these countries, and our inability to do so could impair our business or adversely affect our international expansion. Our currently issued patents and any patents that may be issued in the future with respect to pending or future patent applications may not provide sufficiently broad protection or they may not prove to be enforceable in actions against alleged infringers.

We may not be effective in policing unauthorized use of our intellectual property, and even if we do detect violations, litigation or technical changes to our products may be necessary to enforce our intellectual property rights. Protecting against the unauthorized use of our intellectual property rights, technology and other proprietary rights is expensive and difficult, particularly outside of the United States. Any enforcement efforts we undertake, including litigation, could be time-consuming and expensive and could divert management's attention, which could harm our business and results of operations. Further, attempts to enforce our rights against third parties could also provoke these third parties to assert their own intellectual property or other rights against us, or result in a holding that invalidates or narrows the scope of our rights, in whole or in part. The inability to adequately protect and enforce our intellectual property and other proprietary rights could seriously harm our business, results of operations and financial condition. Even if we are able to secure our intellectual property rights, we cannot assure you that such rights will provide us with competitive advantages or distinguish our services from those of our competitors or that our competitors will not independently develop similar technology, duplicate any of our technology, or design around our patents.

Claims by others that we infringe their proprietary technology or other intellectual property rights could result in significant costs and substantially harm our business, financial condition, results of operations, and prospects.

Claims by others that we infringe their proprietary technology or other intellectual property rights could harm our business. A number of companies in our industry hold a large number of patents and also protect their copyright, trade secret and other intellectual property rights, and companies in the networking and security industry frequently enter into litigation based on allegations of patent infringement or other violations of intellectual property rights. As we face increasing competition and grow, the possibility of intellectual property rights claims against us also grows. In addition, to the extent we hire personnel from competitors, we may be subject to allegations that such personnel have divulged proprietary or other confidential information to us. From time to time, third parties have in the past and may in the future assert claims of infringement of intellectual property rights against us.

Third parties may in the future also assert claims against our customers or channel partners, whom our standard license and other agreements obligate us to indemnify against claims that our solutions infringe the intellectual property rights of third parties. As the number of products and competitors in the security and IT operations market increases and overlaps occur, claims of infringement, misappropriation, and other violations of intellectual property rights may increase. While we intend to increase the size of our patent portfolio, many of our competitors and others may now and in the future have significantly larger and more mature patent portfolios than we have. In addition, future litigation may involve non-practicing entities, companies or other patent owners who have no relevant product offerings or revenue and against whom our own patents may therefore provide little or no deterrence or protection. Any claim of intellectual property infringement by a third party, even a claim without merit, could cause us to incur substantial costs defending against such claim, could distract our management from our business and could require us to cease use of such intellectual property.

Additionally, our insurance may not cover intellectual property rights infringement claims that may be made. In the event that we fail to successfully defend ourselves against an infringement claim, a successful claimant could secure a judgment or otherwise require payment of legal fees, settlement payments, ongoing royalties or other costs or damages; or we may agree to a settlement that prevents us from offering certain services or features; or we may be required to obtain a license, which may not be available on reasonable terms, or at all, to use the relevant technology. If we are prevented from using certain technology or intellectual property, we may be required to develop alternative, non-infringing technology, which could require significant time, effort and expense and may ultimately not be successful. Additionally, we may be unable to continue to offer our affected services or features while developing such technology.

Although third parties may offer a license to their technology or other intellectual property, the terms of any offered license may not be acceptable, and the failure to obtain a license or the costs associated with any license could cause our business, financial condition and results of operations to be adversely affected. In addition, some licenses may be nonexclusive, and therefore our competitors may have access to the same technology licensed to us. If a third party does not offer us a license to its technology or other intellectual property on reasonable terms, or at all, we could be enjoined from continued use of such intellectual property. As a result, we may be required to develop alternative, non-infringing technology, which could require significant time, effort and expense and may ultimately not be successful. Additionally, we may be unable to continue to offer our affected products, subscriptions or services, while developing such technology. Furthermore, a successful claimant could secure a judgment or we may agree to a settlement that prevents us from distributing certain products, providing certain subscriptions or performing certain services. Any such judgment or settlement could also require us to pay substantial damages, royalties or other fees. Any of these events could harm our business, financial condition and results of operations.

We license technology from third parties, and our inability to maintain those licenses could harm our business.

We currently incorporate, and will in the future incorporate, technology that we license from third parties, including software, into our solutions. We cannot be certain that our licensors do not or will not infringe on the intellectual property rights of third parties or that our licensors have or will have sufficient rights to the licensed intellectual property in all jurisdictions in which we may sell our Falcon platform. Some of our agreements with our licensors may be terminated by them for convenience, or otherwise provide for a limited term. If we are unable to continue to license technology because of intellectual property infringement claims brought by third parties against our licensors or against us, or if we are unable to continue our license agreements or enter into new licenses on commercially reasonable terms, our ability to develop and sell solutions and services containing or dependent on that technology would be limited, and our business could be harmed. Additionally, if we are unable to license technology from third parties, we may be forced to acquire or develop alternative technology, which we may be unable to do in a commercially feasible manner or at all, and may require us to use alternative technology of lower quality or performance standards. This could limit or delay our ability to offer new or competitive solutions and increase our costs. As a result, our margins, market share, and results of operations could be significantly harmed.

We are required to comply with stringent, complex and evolving laws, rules, regulations and standards in many jurisdictions, as well as contractual obligations, relating to data privacy and security. Any actual or perceived failure to comply with these requirements could have a material adverse effect on our business.

We are required to comply with stringent, complex and evolving laws, rules, regulations and standards in many jurisdictions, as well as contractual obligations, relating to data privacy and security. Ensuring compliance with such requirements may increase operating costs, impact our data processing practices and policies and the development of new products or services, and reduce operational efficiency, any of which could adversely affect our business and operations.

In the United States, there are numerous federal, state and local data privacy and security laws, rules, and regulations governing the collection, sharing, use, retention, disclosure, security, transfer, storage and other processing of personal information, including federal and state data privacy and security laws, data breach notification laws, and data disposal laws. For example, at the federal level, we are subject to, among other laws and regulations, the rules and regulations promulgated under the authority of the Federal Trade Commission (which has the authority to regulate and enforce against unfair or deceptive acts or practices in or affecting commerce, including acts and practices with respect to data privacy and security), as well as the Electronic Communication Privacy Act, the Computer Fraud and Abuse Act, the Health Insurance Portability and Accountability Act, and the Gramm Leach Bliley Act. The United States Congress also has considered, is currently considering, and may in the future consider, various proposals for comprehensive federal data privacy and security legislation, to which we may become subject if passed.

At the state level, we are subject to laws and regulations such as the California Consumer Privacy Act, as amended by the California Privacy Rights Act (collectively, the “CCPA”). The CCPA broadly defines personal information and gives California residents expanded privacy rights and protections, such as affording them the right to access and request deletion of their information and to opt out of certain sharing and sales of personal information. The CCPA provides for severe civil penalties and statutory damages for violations and a private right of action for certain data breaches that result in the loss of unencrypted personal information. This private right of action is expected to increase the likelihood of, and risks associated with, data breach litigation. Numerous other states have also enacted, or are in the process of enacting or considering, comprehensive state-level data privacy and security laws, rules, and regulations that share similarities with the CCPA. Moreover, laws in all 50 U.S. states require businesses to provide notice under certain circumstances to consumers whose personal information has been disclosed as a result of a data breach.

Internationally, virtually every jurisdiction in which we operate has established its own data privacy and security legal framework with which we must comply. For example, we are required to comply with the European Union (“EU”) General Data Protection Regulation (“GDPR”) and its equivalent in the U.K. (“U.K. GDPR”), which impose stringent obligations regarding the collection, control, use, sharing, disclosure and other processing of personal data and create mandatory breach notification requirements under certain circumstances. While the GDPR and U.K. GDPR remain substantially similar for the time being, the U.K. government has announced plans and introduced legislative proposals to chart its own path on data protection and reform its relevant laws, including in ways that may differ from the GDPR. While these developments increase uncertainty with regard to data protection regulation in the U.K., even in their current, substantially similar form, the GDPR and U.K. GDPR can expose businesses to divergent parallel regimes that may be subject to potentially different interpretations and enforcement actions for certain violations and related uncertainty. Failure to comply with the GDPR or the U.K. GDPR can result in significant fines and other liability, including, under the GDPR, fines of up to EUR 20 million (or GBP 17.5 million under the U.K. GDPR) or four percent (4%) of annual global revenue, whichever is greater. European data protection authorities have already imposed fines for GDPR violations of up to, in some cases, hundreds of millions of Euros.

Legal developments in the European Economic Area (“EEA”) have created complexity and uncertainty regarding processing and transfers of personal data from the EEA to the United States and other so-called third countries outside the EEA, including in the context of website cookies. Similar complexities and uncertainties also apply to transfers from the U.K. to third countries. While we have taken steps to mitigate the impact on us, such as implementing the European Commission’s standard contractual clauses (“SCCs”) and the U.K.’s international Data Transfer Agreement (or the U.K.’s international data transfer addendum that can be used with the SCCs), the efficacy and longevity of these mechanisms remains uncertain. On July 10, 2023, the European Commission adopted an adequacy decision concluding that the U.S. ensures an adequate level of protection for personal data transferred from the EU to the U.S. under the recently adopted EU-U.S. Data Privacy Framework (followed on October 12, 2023 with the adoption of an adequacy decision in the U.K. for the U.K.-U.S. Data Bridge); however, such new adequacy decision has been challenged in EU courts, and is likely to face additional challenges. Moreover, although the U.K. currently has an adequacy decision from the European Commission, such that SCCs are not required for the transfer of personal data from the EEA to the U.K., that decision will sunset in June 2025 unless extended and it may be revoked in the future by the European Commission if the U.K. data protection regime is reformed in ways that deviate substantially from the GDPR. The EU has also proposed legislation that would regulate non-personal data and establish new cybersecurity standards, and other countries, including the U.K., may similarly do so in the future. If we are otherwise unable to transfer data, including personal data, between and among countries and regions in which we operate, it could affect the manner in which we provide our services, the geographical location or segregation of our relevant systems and operations, and could adversely affect our financial results. While we have implemented new controls and procedures designed to comply with the requirements of the GDPR, U.K. GDPR and the data privacy and security laws of other jurisdictions in which we operate, such procedures and controls may not be effective in ensuring compliance or preventing unauthorized transfers of personal data.

Moreover, while we strive to publish and prominently display privacy policies that are accurate, comprehensive, and compliant with applicable laws, rules regulations and industry standards, we cannot ensure that our privacy policies and other statements regarding our practices will be sufficient to protect us from claims, proceedings, liability or adverse publicity relating to data privacy and security. Although we endeavor to comply with our privacy policies, we may at times fail to do so or be alleged to have failed to do so. If our public statements about our use, collection, disclosure and other processing of personal information, whether made through our privacy policies, information provided on our website, press statements or otherwise, are alleged to be deceptive, unfair or misrepresentative of our actual practices, we may be subject to potential government or legal investigation or action, including by the Federal Trade Commission or applicable state attorneys general.

Our compliance efforts are further complicated by the fact that data privacy and security laws, rules, regulations and standards around the world are rapidly evolving, may be subject to uncertain or inconsistent interpretations and enforcement, and may conflict among various jurisdictions. In many jurisdictions, enforcement actions and consequences for non-compliance with data privacy and security laws, rules, regulations, standards, certifications, contractual requirements or other obligations are rising. Data subjects may also have a private right of action, as well as support from consumer privacy advocates or organizations, to lodge complaints with supervisory authorities, seek judicial remedies and obtain compensation for damages resulting from violations of applicable data privacy and security laws, rules and regulations. In addition, privacy advocates and industry groups have proposed, and may propose in the future, self-regulatory standards that may legally or contractually apply to us or be alleged to apply to us. Any failure or perceived failure by us or any third parties with which we do business to comply with applicable privacy policies, data privacy or security laws, rules, regulations, standards, certifications or contractual obligations, or any compromise of security that results in unauthorized access to, or unauthorized loss, destruction, use, modification, acquisition, disclosure, release, transfer or other processing of personal information, may result in requirements to modify or cease certain operations or practices, the expenditure of substantial costs, time and other resources, proceedings or actions against us, legal liability, governmental investigations, enforcement actions, claims, fines, judgments, awards, penalties, sanctions and costly litigation (including class actions). There also has been increased regulatory scrutiny from the SEC with respect to adequately disclosing risks concerning cybersecurity and data privacy. Such scrutiny from the SEC increases the risk of investigations into the cybersecurity practices, and related disclosures, of companies within its jurisdiction. Any of the foregoing could harm our reputation, distract our management and technical personnel, increase our costs of doing business, adversely affect the demand for our products and services, and ultimately result in the imposition of liability, any of which could have a material adverse effect on our business, financial condition and results of operations.

Failure to comply with laws and regulations applicable to our business could subject us to fines and penalties and could also cause us to lose customers or negatively impact our ability to contract with customers, including those in the public sector.

Our business is subject to regulation by various federal, state, local and foreign governmental agencies, including agencies responsible for monitoring and enforcing data privacy and security laws and regulations, employment and labor laws, workplace safety, product safety, environmental laws, consumer protection laws, anti-bribery laws, import and export controls, federal securities laws and tax laws and regulations. In certain jurisdictions, these regulatory requirements may be more stringent than in the United States. Increased scrutiny may also lead to new laws and regulations, or new applications of existing laws and regulations, that target topics such as AI, critical infrastructure software resiliency and concentration risk. Noncompliance by us, our employees, representatives, contractors, channel partners, agents, intermediaries, or other third parties with applicable regulations or requirements could subject us to:

- investigations, enforcement actions and sanctions;
- mandatory changes to our Falcon platform;
- disgorgement of profits, fines and damages;
- civil and criminal penalties or injunctions;
- claims for damages by our customers or channel partners;
- termination of contracts;
- loss of intellectual property rights;
- loss of our license to do business in the jurisdictions in which we operate; or

- temporary or permanent debarment from sales to government organizations.

If any governmental sanctions are imposed, or if we do not prevail in any possible civil or criminal litigation, our business, results of operations and financial condition could be adversely affected. In addition, responding to any action will likely result in a significant diversion of management's attention and resources and an increase in professional fees. Enforcement actions and sanctions could harm our business, results of operations and financial condition.

We endeavor to properly classify employees as exempt versus non-exempt under applicable law. Although there are no pending or threatened material claims or investigations against us asserting that some employees are improperly classified as exempt, the possibility exists that some of our current or former employees could have been incorrectly classified as exempt employees.

These laws and regulations impose added costs on our business, and failure by us, our employees, representatives, contractors, channel partners, agents, intermediaries, or other third parties to comply with these or other applicable regulations and requirements could lead to claims for damages, penalties, termination of contracts, loss of exclusive rights in our intellectual property and temporary suspension or permanent debarment from government contracting. Any such damages, penalties, disruptions or limitations in our ability to do business with customers, including those in the public sector, could result in reduced sales of our products or services, substantial product inventory write-offs, reputational damage, penalties, and other sanctions, any of which could harm our business, reputation, and results of operations.

We are subject to governmental export controls and economic sanctions laws that could impair our ability to compete in international markets and subject us to liability if we are not in full compliance with applicable laws.

Our products, services and business activities, including our collection of information about cyber threats, are subject to various restrictions under U.S. export controls and trade and economic sanctions laws, including the U.S. Commerce Department's Export Administration Regulations and economic and trade sanctions regulations maintained by the U.S. Treasury Department's Office of Foreign Assets Control. The U.S. export control laws and U.S. economic sanctions laws include prohibitions on the sale or supply of certain products and services to U.S. embargoed or sanctioned countries, governments, persons and entities and also require authorization for the export of encryption items. In addition, various countries regulate the import of certain encryption technology, including through import and licensing requirements, and have enacted laws that could limit our ability to distribute our products or service or could limit our customers' ability to implement our service in those countries. Changes in our products or services or changes in these laws and regulations may create delays in the introduction of our products or services into international markets, prevent our customers with international operations from deploying our products or services globally or, in some cases, prevent the export or import of our products or services to certain countries, governments or persons altogether. Any decreased use of our products or services or limitation on our ability to export to or sell our products or services in international markets would likely adversely affect our business, financial condition, and operating results. Obtaining the necessary authorizations, including any required license, for a particular transaction may be time-consuming, is not guaranteed, and may result in the delay or loss of sales opportunities. If we fail to comply with these laws and regulations, we and certain of our employees could be subject to civil or criminal penalties, including the possible loss of export privileges and monetary penalties. Although we take precautions to prevent our products or services from being provided in violation of such laws, our products or services may have been in the past, and could in the future be, provided in violation of such laws, despite the precautions we take. This could result in negative consequences to us, including government investigations, penalties and harm to our reputation.

We are subject to anti-corruption, anti-bribery and similar laws, and non-compliance with such laws can subject us to criminal penalties or significant fines and harm our business and reputation.

We are subject to the U.S. Foreign Corrupt Practices Act of 1977, as amended ("FCPA"), the U.K. Bribery Act 2010 and other anti-corruption, anti-bribery, anti-money laundering and similar laws in the United States and other countries in which we conduct activities. Anti-corruption and anti-bribery laws have been enforced aggressively in recent years and are interpreted broadly and prohibit companies and their employees and agents from promising, authorizing, making or offering improper payments or other benefits to government officials and others in the private sector. As we increase our international sales and business, our risks under these laws may increase.

In addition, we use channel partners, agents and other third-parties to sell our products or conduct business on our behalf. We or such third parties may have direct or indirect interactions with officials and employees of government agencies or state-owned or affiliated entities and under certain circumstances we could be held liable for the corrupt or other illegal activities of such partners, and our employees, representatives, contractors, partners, and agents, even if we do not explicitly authorize such activities. We have implemented an anti-corruption compliance program but cannot ensure that all our employees and agents, as well as those companies to which we outsource certain of our business operations, will not take actions in violation of our policies and applicable law, for which we may be ultimately held responsible.

Noncompliance with the FCPA, other applicable anti-corruption, anti-bribery, or anti-money laundering laws could subject us to investigations, whistleblower complaints, sanctions, settlements, prosecution, and other enforcement actions within the U.S. and internationally. Any violation of these laws could result in disgorgement of profits, significant fines, damages, other civil and criminal penalties or injunctions, adverse media coverage, loss of export privileges, severe criminal or civil sanctions, suspension or debarment from U.S. government contracts and other consequences, any of which could have a material adverse effect on our reputation, business, results of operations, and financial condition.

Some of our technology incorporates “open source” software, which could negatively affect our ability to sell our Falcon platform and subject us to possible litigation.

Our products and subscriptions contain third-party open source software components, and failure to comply with the terms of the underlying open source software licenses could restrict our ability to sell our products and subscriptions. The use and distribution of open source software may entail greater risks than the use of third-party commercial software, as open source licensors generally do not provide warranties or other contractual protections regarding infringement claims or the quality of the code and they can change the license terms on which they offer the open source software. Many of the risks associated with use of open source software cannot be eliminated and could negatively affect our business. In addition, the wide availability of source code used in our solutions could expose us to security vulnerabilities.

Some open source licenses contain requirements that we make available source code for modifications or derivative works we create based upon the type of open source software we use. If we combine our proprietary software with open source software in a certain manner, we could, under certain open source licenses, be required to release the source code of our proprietary software to the public, including authorizing further modification and redistribution, or otherwise be limited in the licensing of our services, each of which could provide an advantage to our competitors or other entrants to the market, create security vulnerabilities in our solutions, require us to re-engineer all or a portion of our Falcon platform, and could reduce or eliminate the value of our services. This would allow our competitors to create similar products with lower development effort and time and ultimately could result in a loss of sales for us.

The terms of many open source licenses have not been interpreted by U.S. courts, and there is a risk that these licenses could be construed in ways that could impose unanticipated conditions or restrictions on our ability to commercialize products and subscriptions incorporating such software. Moreover, we cannot assure you that our processes for controlling our use of open source software in our products and subscriptions will be effective. From time to time, we may face claims from third parties asserting ownership of, or demanding release of, the open source software or derivative works that we developed using such software (which could include our proprietary source code), or otherwise seeking to enforce the terms of the applicable open source license. These claims could result in litigation. Litigation could be costly for us to defend, have a negative effect on our results of operations and financial condition or require us to devote additional research and development resources to change our solutions. Responding to any infringement or noncompliance claim by an open source vendor, regardless of its validity, discovering certain open source software code in our Falcon platform, or a finding that we have breached the terms of an open source software license, could harm our business, results of operations and financial condition, by, among other things:

- resulting in time-consuming and costly litigation;
- diverting management’s time and attention from developing our business;
- requiring us to pay monetary damages or enter into royalty and licensing agreements that we would not normally find acceptable;
- causing delays in the deployment of our Falcon platform or service offerings to our customers;
- requiring us to stop offering certain services or features of our Falcon platform;

- requiring us to redesign certain components of our Falcon platform using alternative non-infringing or non-open source technology, which could require significant effort and expense;
- requiring us to disclose our software source code and the detailed program commands for our software; and
- requiring us to satisfy indemnification obligations to our customers.

We utilize AI, which could expose us to liability or adversely affect our business.

We incorporate novel uses of AI technologies, including generative AI, into our products and operations, such as our Falcon platform. AI is complex and rapidly evolving, and we face significant competition from other companies who may incorporate AI into their products more quickly or more successfully than us, as well as an evolving regulatory landscape. The introduction of AI, and particularly generative AI, a relatively new and emerging technology in the early stages of commercial use, into new or existing products, and our operations, may result in new or enhanced governmental or regulatory scrutiny, litigation, confidentiality, ethical concerns, or other complications that could adversely affect our business, reputation, or financial results. For example, generative AI has been known to produce a false or “hallucinatory” interferences or output, and certain generative AI uses machine learning and predictive analytics, which may be flawed, insufficient, of poor quality, reflect unwanted forms of bias, or contain other errors or inadequacies, any of which may not be easily detectable. Our customers or others may rely on or use this flawed content to their detriment, which may expose us to brand or reputational harm, competitive harm, and/or legal liability. In addition, the use of AI by other companies has resulted in, and may in the future result in, data breaches and cybersecurity incidents that implicate the personal information of AI users. Further, the use of AI presents emerging ethical and social issues, and if we enable or offer solutions that draw scrutiny or controversy due to their perceived or actual impact on customers or on society as a whole, we may experience brand or reputational harm, competitive harm, and/or legal liability.

The technologies underlying AI and its uses are subject to a variety of laws and regulations, including intellectual property, privacy, data protection, cybersecurity, consumer protection, competition, and equal opportunity laws and regulations, and are expected to be subject to new laws and regulations or new applications of existing laws and regulations. AI is the subject of ongoing review by various U.S. governmental and regulatory agencies, and various U.S. states and other foreign jurisdictions are applying, or are considering applying, their cybersecurity and data protection laws to AI or are considering general legal frameworks for AI. For example, in Europe, the EU’s AI Act was published in the Official Journal of the EU on July 12, 2024 and entered into force on August 1, 2024. The AI Act establishes, among other things, a risk-based governance framework for regulating AI systems in the EU by categorizing AI systems, based on the risks associated with such AI systems’ intended purposes, as creating unacceptable or high risks, with all other AI systems being considered low risk. This regulatory framework is expected to have a material impact on the way AI is regulated in the EU and beyond. As further indication of a trend in increased regulatory and legislative oversight of the use and development of AI, in 2024, California enacted a range of laws regulating the use and development of AI, which generally relate to transparency, privacy and fairness, among other concerns.

As a fast-evolving and complicated technology subject to significant government attention, AI-related legislation and regulation may be developed and apply to AI in unexpected ways. We may not be able to anticipate how to respond to or comply with these rapidly evolving frameworks, and we may need to expend resources to adjust our offerings in certain jurisdictions if the legal frameworks are inconsistent across jurisdictions. The cost to comply with such frameworks could be significant and may increase our operating expenses. Additionally, if we do not have sufficient rights to use the data or other material or content on which our AI technologies rely, we may incur liability through the violation of applicable laws or regulations, third-party intellectual property, privacy or other rights, or contracts to which we are a party. Further, any content or other output created by our use of AI-powered tools may not be subject to copyright protection, which may adversely affect our ability to enforce our intellectual property rights. Because AI technology itself is highly complex and rapidly developing, it is not possible to predict all of the legal, operational or technological risks that may arise relating to the use of AI.

We provide service level commitments under some of our customer contracts. If we fail to meet these contractual commitments, we could be obligated to provide credits for future service and our business could suffer.

Certain of our customer agreements contain service level commitments, which contain specifications regarding the availability and performance of our Falcon platform. Any failure of or disruption to our infrastructure could impact the performance of our Falcon platform and the availability of services to customers. To the extent we are unable to meet our stated service level commitments or to the extent we suffer extended periods of poor performance or unavailability of our Falcon platform, we may be contractually obligated to provide affected customers with service credits for future subscriptions, and, in certain cases, refunds. To date, there has not been a material failure to meet our service level commitments, and we do not currently have any material liabilities accrued on our balance sheets for such commitments. Our revenue, other results of operations and financial condition could be harmed to the extent we suffer performance issues or downtime that exceeds the service level commitments under our agreements with our customers.

We are currently, and may in the future become, involved in litigation that may adversely affect us.

We are regularly subject to claims, suits, and government investigations and other proceedings including patent, product liability, class action, whistleblower, personal injury, property damage, labor and employment (including allegations of wage and hour violations), commercial disputes, securities litigation, compliance with laws and regulatory requirements and other matters, and we may become subject to additional types of claims, suits, investigations and proceedings as our business develops or in connection with the July 19 Incident. Such claims, suits, and government investigations and proceedings are inherently uncertain and their results cannot be predicted with certainty. Regardless of the outcome, any of these types of legal proceedings can have an adverse impact on us because of legal costs and diversion of management attention and resources, and could cause us to incur significant expenses or liability, adversely affect our brand recognition, and/or require us to change our business practices. The expense of litigation and the timing of this expense from period to period are difficult to estimate, subject to change and could adversely affect our results of operations. It is possible that a resolution of one or more such proceedings could result in substantial damages, settlement costs, fines and penalties that could adversely affect our business, consolidated financial position, results of operations, or cash flows in a particular period. These proceedings could also result in reputational harm, sanctions, consent decrees, or orders requiring a change in our business practices. Because of the potential risks, expenses and uncertainties of litigation, we may, from time to time, settle disputes, even where we have meritorious claims or defenses, by agreeing to settlement agreements. Because litigation is inherently unpredictable, we cannot assure you that the results of any of these actions will not have a material adverse effect on our business, financial condition, results of operations, and prospects. Any of these consequences could adversely affect our business and results of operations.

We have in the past experienced, and may in the future experience, warranty claims, product returns, and claims related to product liability and product defects from real or perceived defects in our solutions or their misuse by our customers or third parties and indemnity provisions in various agreements potentially expose us to substantial liability for intellectual property infringement and other losses.

We may be subject to liability claims for damages related to errors or defects in our solutions, and we are currently subject to claims, and may in the future become subject to additional claims, arising out of the July 19 Incident. A material liability claim or other occurrence that harms our reputation or decreases market acceptance of our products may harm our business and results of operations. Although we generally have limitation of liability provisions in our terms and conditions of sale, these provisions may not cover all of our indemnification obligations and they may not fully or effectively protect us from claims as a result of federal, state, or local laws or ordinances, or unfavorable judicial decisions in the United States or other countries. The sale and support of our products also entail the risk of product liability claims.

Additionally, our agreements with customers and other third parties typically include indemnification or other provisions under which we agree to indemnify or otherwise be liable to them for losses suffered or incurred as a result of claims regarding intellectual property infringement, breach of agreement, including confidentiality, privacy and security obligations, violation of applicable laws, damages caused by failures of our solutions or to property or persons, or other liabilities relating to or arising from our products and services, or other acts or omissions. These contractual provisions often survive termination or expiration of the applicable agreement. We have received, and may continue to receive, claims in connection with the July 19 Incident.

If our customers or other third parties we do business with make intellectual property rights or other indemnification claims against us, we will incur significant legal expenses and may have to pay damages, license fees, and/or stop using technology found to be in violation of the third party's rights. We may also have to seek a license for the technology. Such license may not be available on reasonable terms, if at all, and may significantly increase our operating expenses or may require us to restrict our business activities and limit our ability to deliver certain solutions or features. We may also be required to develop alternative non-infringing technology, which could require significant effort and expense and/or cause us to alter our products and services, which could harm our business. Large indemnity obligations, whether for intellectual property or other claims, could harm our business, results of operations, and financial condition.

Additionally, our Falcon platform may be used by our customers and other third parties who obtain access to our solutions for purposes other than for which our platform was intended. For example, our Falcon platform might be misused by a customer to monitor its employee's activities in a manner that violates the employee's privacy rights under applicable law.

During the course of performing certain solution-related services and our professional services, our teams may have significant access to our customers' networks. We cannot be sure that an employee may not take advantage of such access which may make our customers vulnerable to malicious activity by such employee. Any such misuse of our Falcon platform could result in negative press coverage and negatively affect our reputation, which could result in harm to our business, reputation, and results of operations.

We maintain insurance to mitigate potential losses arising from certain claims associated with the use of our products, but our insurance coverage may not adequately cover all claims asserted against us, including our liability related to the July 19 Incident. In addition, even claims that ultimately are unsuccessful could result in our expenditure of funds in litigation, divert management's time and other resources, and harm our business and reputation. We offer our Falcon Complete customers a limited warranty, subject to certain conditions. While we maintain insurance relating to our warranty, we cannot be certain that our insurance coverage will be adequate to cover such claims, that such insurance will continue to be available to us on commercially reasonable terms, or at all, or that any insurer will not deny coverage as to any claim. Any failure or refusal of our insurance providers to provide the expected insurance benefits to us after we have paid the warranty claims would cause us to incur significant expense or cause us to cease offering this warranty which could damage our reputation, cause us to lose customers, expose us to liability claims by our customers, negatively impact our sales and marketing efforts, and have an adverse effect on our business, financial condition and results of operations.

Risks Related to Ownership of Our Common Stock

The market price of our common stock may be volatile regardless of our operating performance, and you could lose all or part of your investment.

We cannot predict the prices at which our common stock will trade. The market price of our common stock depends on a number of factors, including those described in this "Risk Factors" section, many of which are beyond our control and may not be related to our operating performance. These fluctuations could cause you to lose all or part of your investment in our common stock. Factors that could cause fluctuations in the market price of our common stock include the following:

- actual or anticipated changes or fluctuations in our results of operations;
- the financial projections we may provide to the public, any changes in these projections or our failure to meet these projections;
- announcements by us or our competitors of new products or services or new or terminated significant contracts, commercial relationships or capital commitments;
- industry or financial analyst or investor reaction to our press releases, other public announcements and filings with the SEC;
- rumors and market speculation involving us or other companies in our industry;
- price and volume fluctuations in the overall stock market from time to time;

- changes in operating performance and stock market valuations of other technology companies generally, or those in our industry in particular;
- failure of industry or financial analysts to maintain coverage of us, changes in financial estimates by any analysts who follow our company, or our failure to meet these estimates or the expectations of investors;
- actual or anticipated developments in our business or our competitors' businesses or the competitive landscape generally;
- litigation involving us, our industry or both, or investigations by regulators into our operations or those of our competitors;
- developments or disputes concerning our intellectual property rights or our solutions, or third-party proprietary rights;
- announced or completed acquisitions of businesses or technologies by us or our competitors;
- new laws or regulations or new interpretations of existing laws or regulations applicable to our business;
- any major changes in our management or our board of directors, particularly with respect to Mr. Kurtz;
- effects of public health crises, pandemics and epidemics;
- the emergence of new or different information relating to the impact of the July 19 Incident;
- general economic conditions and slow or negative growth of our markets; and
- other events or factors, including those resulting from war, incidents of terrorism or responses to these events.

In addition, the stock market in general, and the market for technology companies in particular, has experienced extreme price and volume fluctuations that have often been unrelated or disproportionate to the operating performance of those companies. Broad market and industry factors may seriously affect the market price of our common stock, regardless of our actual operating performance. In addition, in the past, following periods of volatility in the overall market and the market prices of a particular company's securities, securities class action litigation has often been instituted against that company. We are currently party to securities litigation asserted against us arising out of the July 19 Incident. Any securities litigation could result in substantial costs and divert our management's attention and resources from our business. This could have an adverse effect on our business, results of operations and financial condition.

Sales of substantial amounts of our common stock in the public markets, or the perception that they might occur, could reduce the price that our common stock might otherwise attain and may dilute your voting power and your ownership interest in us.

Sales of a substantial number of shares of our common stock in the public market, particularly sales by our directors, executive officers and significant stockholders, or the perception that these sales could occur, could adversely affect the market price of our common stock. As of February 28, 2025, we had 247,873,415 shares of common stock outstanding.

We may also issue our shares of common stock or securities convertible into shares of our common stock from time to time in connection with a financing, acquisition, investments or otherwise. Any such issuance could result in substantial dilution to our existing stockholders and cause the market price of our common stock to decline.

If industry or financial analysts do not publish research or reports about our business, or if they issue inaccurate or unfavorable research regarding our common stock, our stock price and trading volume could decline.

The trading market for our common stock will be influenced by the research and reports that industry or financial analysts publish about us or our business. We do not control these analysts or the content and opinions included in their reports. If any of the analysts who cover us issues an inaccurate or unfavorable opinion regarding our stock price, our stock price would likely decline. In addition, the stock prices of many companies in the technology industry have declined significantly after those companies have failed to meet, or significantly exceed, the financial guidance publicly announced by the companies or the expectations of analysts. If our financial results fail to meet, or significantly exceed, our announced guidance or the expectations of analysts or public investors, analysts could downgrade our common stock or publish unfavorable research about us. If one or more of these analysts cease coverage of our company or fail to publish reports on us regularly, our visibility in the financial markets could decrease, which in turn could cause our stock price or trading volume to decline.

We do not intend to pay dividends in the foreseeable future. As a result, your ability to achieve a return on your investment will depend on appreciation in the price of our common stock.

We have never declared or paid any cash dividends on our capital stock. We currently intend to retain all available funds and any future earnings for use in the operation of our business and do not anticipate paying any dividends in the foreseeable future. Any determination to pay dividends in the future will be at the discretion of our board of directors. Additionally, our ability to pay dividends is limited by restrictions on our ability to pay dividends or make distributions under the terms of our credit facility. Accordingly, investors must rely on sales of their common stock after price appreciation, which may never occur, as the only way to realize any future gains on their investments.

Certain provisions in our charter documents and under Delaware law could make an acquisition of our company more difficult, limit attempts by our stockholders to replace or remove members of our board of directors or current management, and may adversely affect the market price of our common stock.

Our amended and restated certificate of incorporation and amended and restated bylaws contain provisions that could delay or prevent a change in control of our company. These provisions could also make it difficult for stockholders to elect directors that are not nominated by the current members of our board of directors or take other corporate actions, including effecting changes in our management. These provisions include:

- a classified board of directors with three-year staggered terms, which could delay the ability of stockholders to change the membership of a majority of our board of directors;
- the ability of our board of directors to issue shares of preferred stock and to determine the price and other terms of those shares, including preferences and voting rights, without stockholder approval, which could be used to significantly dilute the ownership of a hostile acquirer;
- the exclusive right of our board of directors to elect a director to fill a vacancy created by the expansion of our board of directors or the resignation, death or removal of a director, which prevents stockholders from being able to fill vacancies on our board of directors;
- a prohibition on stockholder action by written consent, which forces stockholder action to be taken at an annual or special meeting of our stockholders;
- the requirement that a special meeting of stockholders may be called only by the chairperson of our board of directors, chief executive officer or by the board of directors acting pursuant to a resolution adopted by a majority of our board of directors, which could delay the ability of our stockholders to force consideration of a proposal or to take action, including the removal of directors;
- certain amendments to our amended and restated certificate of incorporation require the approval of two-thirds of the then-outstanding voting power of our capital stock; and

- advance notice procedures with which stockholders must comply to nominate candidates to our board of directors or to propose matters to be acted upon at a stockholders' meeting, which may discourage or deter a potential acquirer from conducting a solicitation of proxies to elect the acquirer's own slate of directors or otherwise attempting to obtain control of us.

These provisions may prohibit large stockholders, in particular those owning 15% or more of our outstanding voting stock, from merging or combining with us for a certain period of time.

Our amended and restated bylaws provide that the Court of Chancery of the State of Delaware, and to the extent enforceable, the federal district courts of the United States, will be the exclusive forum for certain disputes between us and our stockholders, which could limit our stockholders' ability to obtain a favorable judicial forum for disputes with us or our directors, officers or employees.

Our amended and restated bylaws provide that the Court of Chancery of the State of Delaware is the exclusive forum for:

- any derivative action or proceeding brought on our behalf;
- any action asserting a breach of fiduciary duty;
- any action asserting a claim against us arising under the Delaware General Corporation Law, our amended and restated certificate of incorporation or our amended and restated bylaws;
- any action to interpret, apply, enforce or determine the validity of our amended and restated certificate of incorporation or our amended and restated bylaws; and
- any action asserting a claim against us that is governed by the internal-affairs doctrine.

However, this exclusive forum provision does not apply to suits brought to enforce a duty or liability created by the Exchange Act. In addition, our amended and restated bylaws provide that the federal district courts of the United States will be the exclusive forum for resolving any complaint asserting a cause of action arising under the Securities Act, subject to and contingent upon a final adjudication in the State of Delaware of the enforceability of such exclusive forum provision.

These exclusive-forum provisions may limit a stockholder's ability to bring a claim in a judicial forum that it finds favorable for disputes with us or our directors, officers or other employees, which may discourage lawsuits against us and our directors, officers and other employees.

Risks Related to our Indebtedness

Our indebtedness could adversely affect our financial condition.

As of January 31, 2025, we had \$750.0 million principal amount of indebtedness outstanding (excluding intercompany indebtedness), and there is additional availability under our revolving facility of up to \$750.0 million (excluding issued but undrawn letters of credit). Our indebtedness could have important consequences, including:

- limiting our ability to obtain additional financing to fund future working capital, capital expenditures, acquisitions or other general corporate requirements;
- requiring a portion of our cash flows to be dedicated to debt service payments instead of other purposes, thereby reducing the amount of cash flows available for working capital, capital expenditures, acquisitions and other general corporate purposes;
- increasing our vulnerability to adverse changes in general economic, industry and competitive conditions; and
- exposing us to the risk of increased interest rates as certain of our borrowings, including borrowings under our revolving facility, are at variable rates of interest; and increasing our cost of borrowing.

We may not be able to generate sufficient cash to service all of our indebtedness, including the notes, and may be forced to take other actions to satisfy our obligations under our indebtedness, which may not be successful.

Our ability to make scheduled payments on or to refinance our debt obligations, including the Senior Notes, depends on our financial condition and results of operations, which in turn are subject to prevailing economic and competitive conditions and to certain financial, business and other factors beyond our control. We may not be able to maintain a level of cash flows from operating activities sufficient to permit us to pay the principal, premium, if any, and interest on our indebtedness, including the notes.

If our cash flows and capital resources are insufficient to fund our debt service obligations, we could face substantial liquidity problems and may be forced to reduce or delay investments and capital expenditures, or to sell assets, seek additional capital or restructure or refinance our indebtedness, including the Senior Notes. Our ability to restructure or refinance our debt will depend on, among other things, the condition of the capital markets and our financial condition at such time. Any refinancing of our debt could be at higher interest rates and may require us to comply with more onerous covenants, which could further restrict our business operations. The terms of existing or future debt instruments and the indenture that governs the Senior Notes may restrict us from adopting some of these alternatives. In addition, any failure to make payments of interest and principal on our outstanding indebtedness on a timely basis would likely result in a reduction of our credit rating, which could harm our ability to incur additional indebtedness. In the absence of such cash flows and resources, we could face substantial liquidity problems and might be required to dispose of material assets or operations to meet our debt service and other obligations.

Further, our credit agreement contains provisions that restrict our ability to dispose of assets and use the proceeds from any such disposition. We may not be able to consummate those dispositions or to obtain the proceeds that we could realize from them and these proceeds may not be adequate to meet any debt service obligations then due. These alternative measures may not be successful and may not permit us to meet our scheduled debt service obligations.

If we cannot make scheduled payments on our indebtedness, we will be in default and holders of our Senior Notes could declare all outstanding principal and interest to be due and payable, the lenders under our revolving facility could terminate their commitments to loan money, our secured lenders could foreclose against the assets securing their borrowings and we could be forced into bankruptcy or liquidation. If we breach the covenants under our debt instruments, we would be in default under such instruments. The holders of such indebtedness could exercise their rights, as described above, and we could be forced into bankruptcy or liquidation.

Our revolving facility and the indenture that governs our Senior Notes contain terms which restrict our current and future operations, particularly our ability to respond to changes or to take certain actions.

Our revolving facility and the indenture that governs our Senior Notes contain a number of restrictive covenants that impose significant operating and financial restrictions on us and may limit our ability to engage in acts that may be in our long-term best interest, including, among other things, restrictions on our ability to:

- incur additional indebtedness and guarantee indebtedness;
- prepay, redeem or repurchase certain indebtedness;
- sell or otherwise dispose of assets;
- incur liens;
- enter into transactions with affiliates;
- alter the businesses we conduct;
- enter into agreements restricting our subsidiaries' ability to pay dividends; and
- consolidate, merge with, or sell all or substantially all of our assets to, another person.

The covenants in the indenture and supplemental indenture that govern the Senior Notes are subject to exceptions and qualifications.

In addition, the restrictive covenants in the credit agreement governing our revolving facility require us to maintain specified financial ratios and satisfy other financial condition tests. Our ability to meet those financial ratios and tests can be affected by events beyond our control, and we may not be able to meet them. These restrictive covenants could adversely affect our ability to:

- finance our operations;
- make needed capital expenditures;
- make strategic acquisitions or investments or enter into joint ventures;
- withstand a future downturn in our business, the industry or the economy in general;
- engage in business activities, including future opportunities, that may be in our best interest; and
- plan for or react to market conditions or otherwise execute our business strategies.

These restrictions may affect our ability to expand our business, which could have a material adverse effect on our business, financial condition and results of operations.

As a result of these restrictions, we will be limited as to how we conduct our business and we may be unable to raise additional debt or equity financing to compete effectively or to take advantage of new business opportunities. The terms of any future indebtedness we may incur could include more restrictive covenants. We cannot assure you that we will be able to maintain compliance with these covenants in the future and, if we fail to do so, that we will be able to obtain waivers from the lenders and/or amend the covenants.

Our failure to comply with the restrictive covenants described above and/or the terms of any future indebtedness from time to time could result in an event of default, which, if not cured or waived, could result in our being required to repay these borrowings before their due date. If we are forced to refinance these borrowings on less favorable terms or cannot refinance these borrowings, our business, financial condition and results of operations could be adversely affected.

Our revolving facility and the indenture that governs our Senior Notes contain cross-default provisions that could result in the acceleration of all of our indebtedness.

A breach of the covenants under our revolving facility or the indenture that governs our Senior Notes could result in an event of default under the applicable indebtedness. Such a default may allow the creditors to accelerate the related indebtedness and may result in the acceleration of any other indebtedness to which a cross-acceleration or cross-default provision applies. In addition, an event of default under the credit agreement governing our revolving facility would permit the lenders under our revolving facility to terminate all commitments to extend further credit under that facility. Furthermore, if we were unable to repay amounts due and payable under our revolving facility, those lenders could proceed against the collateral granted to them to secure that indebtedness. In the event our lenders or noteholders accelerate the repayment of our borrowings, we and our guarantors may not have sufficient assets to repay that indebtedness. Additionally, we may not be able to borrow money from other lenders to enable us to refinance our indebtedness.

General Risk Factors

If we fail to maintain an effective system of internal controls, our ability to produce timely and accurate financial statements or comply with applicable regulations could be impaired.

We are subject to the reporting requirements of the Exchange Act, the Sarbanes-Oxley Act of 2002 (“Sarbanes-Oxley Act”), the rules and regulations of Nasdaq, and other securities rules and regulations that impose various requirements on public companies. Our management and other personnel devote substantial time and resources to comply with these rules and regulations. Such compliance has increased, and will continue to increase our legal, accounting and financial compliance costs; make some activities more difficult, time-consuming and costly, and place significant strain on our personnel, systems and resources. The Sarbanes-Oxley Act requires, among other things, that we maintain effective disclosure controls and procedures and internal control over financial reporting. We are continuing to develop and refine our disclosure controls, internal control over financial reporting and other procedures that are designed to ensure information required to be disclosed by us in our consolidated financial statements and in the reports that we file with the SEC is recorded, processed, summarized and reported within the time periods specified in SEC rules and forms, and information required to be disclosed in reports under the Exchange Act is accumulated and communicated to our principal executive and financial officers.

Our current controls and any new controls we develop may become inadequate because of changes in conditions in our business. Additionally, to the extent we acquire other businesses, the acquired company may not have a sufficiently robust system of internal controls and we may uncover new deficiencies. Weaknesses in our internal controls may be discovered in the future. Any failure to develop or maintain effective controls, or any difficulties encountered in their implementation or improvement, could harm our results of operations, may result in a restatement of our consolidated financial statements for prior periods, cause us to fail to meet our reporting obligations, and could result in an adverse opinion regarding our internal control over financial reporting from our independent registered public accounting firm, and lead to investigations or sanctions by regulatory authorities.

Section 404 of the Sarbanes-Oxley Act requires our management to certify financial and other information in our quarterly and annual reports and provide an annual management report on the effectiveness of our internal control over financial reporting. We are also required to have our independent registered public accounting firm attest to, and issue an opinion on, the effectiveness of our internal control over financial reporting. If we are unable to assert that our internal control over financial reporting is effective, or if, when required, our independent registered public accounting firm is unable to express an opinion on the effectiveness of our internal control over financial reporting, we could lose investor confidence in the accuracy and completeness of our financial reports, which would cause the price of our common stock to decline.

Any failure to maintain effective disclosure controls and internal control over financial reporting could have a material and adverse effect on our business and results of operations and could cause a decline in the price of our stock.

Future acquisitions, strategic investments, partnerships, or alliances could be difficult to identify and integrate, divert the attention of key management personnel, disrupt our business, dilute stockholder value and adversely affect our business, financial condition, and results of operations.

As part of our business strategy, we have in the past made and expect to continue to make investments in and/or acquire complementary companies, services or technologies. Our ability as an organization to acquire and integrate other companies, services or technologies in a successful manner in the future is not guaranteed. We may not be able to find suitable acquisition candidates, and we may not be able to complete such acquisitions on favorable terms, if at all. If we do complete acquisitions, we may not ultimately strengthen our competitive position or ability to achieve our business objectives, and any acquisitions we complete could be viewed negatively by our end-customers or investors. In addition, our due diligence may fail to identify all of the problems, liabilities or other shortcomings or challenges of an acquired business, product or technology, including issues related to intellectual property, product quality or product architecture, regulatory compliance practices, revenue recognition or other accounting practices or issues with employees or customers. If we are unsuccessful at integrating such acquisitions, or the technologies associated with such acquisitions, into our company, the revenue and results of operations of the combined company could be adversely affected. Any integration process may require significant time and resources, and we may not be able to manage the process successfully. We may not successfully evaluate or utilize the acquired technology or personnel, or accurately forecast the financial impact of an acquisition transaction, causing unanticipated write-offs or accounting charges. We may have to pay cash, incur debt or issue equity securities to pay for any such acquisition, each of which could adversely affect our financial condition and the market price of our common stock. The sale of equity or issuance of debt to finance any

such acquisitions could result in dilution to our stockholders. The incurrence of indebtedness would result in increased fixed obligations and could also include covenants or other restrictions that would impede our ability to manage our operations.

Additional risks we may face in connection with acquisitions include:

- diversion of management time and focus from operating our business to addressing acquisition integration challenges;
- coordination of research and development and sales and marketing functions;
- integration of administrative systems, employee, product and service offerings;
- retention of key employees from the acquired company;
- changes in relationships with strategic partners as a result of product acquisitions or strategic positioning resulting from the acquisition;
- the need to implement or improve controls, procedures, and policies at a business that prior to the acquisition may have lacked sufficiently effective controls, procedures and policies;
- additional legal, regulatory or compliance requirements;
- financial reporting, revenue recognition or other financial or control deficiencies of the acquired company that we do not adequately address and that cause our reported results to be incorrect;
- liability for activities of the acquired company before the acquisition, including intellectual property infringement claims, violations of laws, commercial disputes, tax liabilities and other known and unknown liabilities; and
- litigation or other claims in connection with the acquired company, including claims from terminated employees, customers, former stockholders or other third parties.

Our failure to address these risks or other problems encountered in connection with acquisitions and investments could cause us to fail to realize the anticipated benefits of these acquisitions or investments, cause us to incur unanticipated liabilities, and harm our business generally.

Our corporate structure and intercompany arrangements are subject to the tax laws of various jurisdictions, and we could be obligated to pay additional taxes, which would harm our results of operations.

We are expanding our international operations and staff to support our business in international markets. We generally conduct our international operations through wholly-owned subsidiaries and are or may be required to report our taxable income in various jurisdictions worldwide based upon our business operations in those jurisdictions. Our intercompany relationships are subject to complex transfer pricing regulations administered by taxing authorities in various jurisdictions. The amount of taxes we pay in different jurisdictions may depend on the application of the tax laws of the various jurisdictions, including the United States, to our international business activities, changes in tax rates, new or revised tax laws or interpretations of existing tax laws and policies, and our ability to operate our business in a manner consistent with our corporate structure and intercompany arrangements. The relevant taxing authorities may disagree with our determinations as to the income and expenses attributable to specific jurisdictions. If such a disagreement were to occur, and our position was not sustained, we could be required to pay additional taxes, interest and penalties, which could result in one-time tax charges, higher effective tax rates, reduced cash flows and lower overall profitability of our operations.

We are subject to federal, state, and local income, sales, and other taxes in the United States and income, withholding, transaction, and other taxes in numerous foreign jurisdictions. Significant judgment is required in evaluating our tax positions and our worldwide provision for taxes. During the ordinary course of business, there are many activities and transactions for which the ultimate tax determination may be uncertain. In addition, our tax obligations and effective tax rates could be adversely affected, among other things, by (i) changes in the relevant tax, accounting and other laws, regulations, principles and interpretations, including increases in corporate tax rates and greater taxation of international income and changes relating to income tax nexus, (ii) recognizing tax losses or lower than anticipated earnings in jurisdictions where we have lower statutory

rates and higher than anticipated earnings in jurisdictions where we have higher statutory rates, (iii) changes in foreign currency exchange rates, or (iv) changes in the valuation of our deferred tax assets and liabilities. We may be audited in various jurisdictions, and such jurisdictions may assess additional taxes, sales taxes and value added taxes against us. Although we believe our tax estimates are reasonable, the final determination of any tax audits or litigation could be materially different from our historical tax provisions and accruals, which could have an adverse effect on our results of operations or cash flows in the period or periods for which a determination is made.

In addition, the Organization for Economic Cooperation and Development (“OECD”) has published proposals covering a number of issues, including country-by-country reporting, permanent establishment rules, transfer pricing rules, tax treaties and taxation of the digital economy. On October 8, 2021, the OECD/G20 inclusive framework on Base Erosion and Profit Shifting (the “Inclusive Framework”) published a statement updating and finalizing the key components of a two-pillar plan on global tax reform originally agreed on July 1, 2021, and a timetable for implementation by 2023. The timetable for implementation has since been extended to 2024 and, with respect to certain components of the plan, to 2025. Under Pillar Two, the Inclusive Framework has agreed on a global minimum corporate tax rate of 15% for companies with revenue above €750 million, calculated on a jurisdictional basis. While substantial work remains to be completed by the OECD and national governments on the implementation of these proposals, future tax reform resulting from these developments may result in changes to long-standing tax principles, which could adversely affect our effective tax rate or result in higher cash tax liabilities. On February 1, 2023, the U.S. Financial Accounting Standards Board (“FASB”) indicated that they believe the minimum tax imposed under Pillar Two is an alternative minimum tax, and, accordingly, deferred tax assets and liabilities associated with the minimum tax would not be recognized or adjusted for the estimated future effects of the minimum tax but would be recognized in the period incurred. In addition, the OECD’s proposed solution envisages new international tax rules and the removal of all Digital Services Taxes (“DST”). Notwithstanding this, some countries, in the European Union and beyond, continue to operate existing DST regimes to capture tax revenue on digital services more immediately. Such laws may increase our tax obligations in those countries or change the manner in which we operate our business.

Our ability to use our net operating loss carryforwards and certain other tax attributes may be limited.

As of January 31, 2025, we had aggregate U.S federal and California net operating loss carryforwards of \$1.4 billion and \$307.9 million, respectively, which may be available to offset future taxable income for income tax purposes. The federal net operating losses are carried forward indefinitely, and California net operating loss carryforwards begin to expire in fiscal 2034 through fiscal 2045. As of January 31, 2025, net operating loss carryforwards for other states totaled \$716.0 million, which begin to expire in fiscal 2026 through fiscal 2045. As of January 31, 2025, net operating loss carryforwards for the U.K. totaled \$78.0 million, which are carried forward indefinitely, and net operating loss carryforwards totaled immaterial amounts in certain foreign jurisdictions. As of January 31, 2025, we had U.S federal and California research and development (“R&D”) credit carryforwards of \$165.1 million and \$39.6 million, respectively. The federal R&D credit carryforwards begin to expire in fiscal 2037 through fiscal 2045. The California R&D credits are carried forward indefinitely. Realization of these net operating loss and R&D credit carryforwards depends on future income, and there is a risk that our existing carryforwards could expire unused and be unavailable to offset future income tax liabilities, which could adversely affect our results of operations.

In addition, under Sections 382 and 383 of the Internal Revenue Code, if a corporation undergoes an “ownership change,” generally defined as a greater than 50% change (by value) in ownership by “5 percent shareholders” over a rolling three-year period, the corporation’s ability to use its pre-change net operating loss carryovers and other pre-change tax attributes, such as R&D credits, to offset its post-change income or taxes may be limited. We may experience ownership changes in the future as a result of shifts in our stock ownership. As a result, if we earn net taxable income, our ability to use our pre-change net operating loss carryforwards to offset U.S. federal taxable income may be subject to limitations, which could potentially result in increased future tax liability to us.

Taxing authorities may successfully assert that we should have collected or in the future should collect sales and use, value added or similar taxes, and we could be subject to liability with respect to past or future sales, which could adversely affect our results of operations.

We do not collect sales and use, value added or similar taxes in all jurisdictions in which we have sales because we have been advised that such taxes are not applicable to our services in certain jurisdictions. Sales and use, value added, and similar tax laws and rates vary greatly by jurisdiction. Certain jurisdictions in which we do not collect such taxes may assert that such taxes are applicable, which could result in tax assessments, penalties and interest, to us or our customers for the past amounts, and we may be required to collect such taxes in the future. If we are unsuccessful in collecting such taxes from our customers, we could be held liable for such costs, which may adversely affect our results of operations.

If our estimates or judgments relating to our critical accounting policies prove to be incorrect or financial reporting standards or interpretations change, our results of operations could be adversely affected.

The preparation of financial statements in conformity with U.S. GAAP requires management to make estimates and assumptions that affect the amounts reported in our consolidated financial statements and accompanying notes. We base our estimates on historical experience and on various other assumptions that we believe to be reasonable under the circumstances, as discussed in the section titled “Management’s Discussion and Analysis of Financial Condition and Results of Operations.” The results of these estimates form the basis for making judgments about the carrying values of assets, liabilities and equity, and the amount of revenue and expenses that are not readily apparent from other sources. Significant assumptions and estimates used in preparing our consolidated financial statements include those related to revenue recognition; allowance for credit losses; valuation of common stock and redeemable convertible preferred stock warrants; carrying value and useful lives of long-lived assets; loss contingencies; and the provision for income taxes and related deferred taxes. Our results of operations may be adversely affected if our assumptions change or if actual circumstances differ from those in our assumptions, which could cause our results of operations to fall below the expectations of industry or financial analysts and investors, resulting in a decline in the market price of our common stock.

Additionally, we regularly monitor our compliance with applicable financial reporting standards and review new pronouncements and drafts thereof that are relevant to us. As a result of new standards, changes to existing standards and changes in their interpretation, we might be required to change our accounting policies, alter our operational policies and implement new or enhance existing systems so that they reflect new or amended financial reporting standards, or we may be required to restate our published financial statements. Such changes to existing standards or changes in their interpretation may have an adverse effect on our reputation, business, financial position and profit, or cause an adverse deviation from our revenue and operating profit target, which may negatively impact our financial results.

We are subject to risks associated with our equity investments, including partial or complete loss of invested capital, and significant changes in the fair value of this portfolio could adversely impact our financial results.

Through our Falcon Funds, we invest in early to late stage private companies, and we may not realize a return on our equity investments. Many such companies generate net losses and the market for their products, services, or technologies may be slow to develop or never materialize. These companies are often dependent on the availability of later rounds of financing from banks or investors on favorable terms to continue their operations. The financial success of our investment in any company is typically dependent on a liquidity event, such as a public offering, acquisition, or other favorable market event reflecting appreciation to the cost of our initial investment. The capital markets for public offerings and acquisitions are dynamic and the likelihood of liquidity events for the companies in which we have invested could deteriorate, which could result in a loss of all or a substantial part of our investment in these companies. In addition, our ability to realize gains on investments may be impacted by our contractual obligations to hold securities for a set period of time. For example, to the extent a company we have invested in undergoes an initial public offering, we may be subject to a lock-up agreement that restricts our ability to sell our securities for a period of time after the public offering or otherwise impedes our ability to mitigate market volatility in such securities.

Further, valuations of non-marketable equity investments are inherently complex due to the lack of readily available market data. In addition, we may experience additional volatility to our statements of operations due to changes in market prices of our marketable equity investments, the valuation and timing of observable price changes or impairments of our non-marketable equity investments, and changes in the proportionate share of earnings and losses or impairment of our equity investments accounted for under the equity method. This volatility could be material to our results in any given quarter and may cause our stock price to decline.

Expectations of our performance relating to environmental, social and governance factors may impose additional costs and expose us to new risks.

There is an increasing focus from regulators, certain investors, and other stakeholders concerning environmental, social and governance (“ESG”) matters, both in the United States and internationally. We have undertaken and expect to continue to undertake certain ESG-related initiatives, goals and commitments, which we have communicated on our website, in our SEC filings and elsewhere. These initiatives, goals, or commitments could be difficult to achieve and costly to implement. We could fail to achieve, or be perceived to fail to achieve, our ESG-related initiatives, goals, or commitments. In addition, we could be criticized for the timing, scope or nature of these initiatives, goals, or commitments, or for any revisions to them. Stakeholders could also challenge the accuracy, adequacy, or completeness of our ESG-related disclosures. Our actual or perceived failure to achieve some or all of our ESG-related initiatives, goals, or commitments or maintain ESG practices that meet evolving stakeholder expectations or regulatory requirements could harm our reputation, adversely impact our ability to attract and retain employees or customers and expose us to increased scrutiny from ESG-focused investors, regulatory authorities and others, or subject us to liability. Damage to our reputation or reduced demand for our products may adversely impact our business, financial condition, or results of operations.

Our business is subject to the risks of catastrophic events, including, but not limited to, natural events such as earthquakes, fire, floods, and the outbreak of diseases, as well as man-made problems such as power disruptions, computer viruses or data security breaches.

Our principal executive offices are located in Austin, Texas, and we also maintain other office locations around the world, including in California and India, that are prone to natural disasters including severe weather and seismic activity. A significant natural disaster, such as an earthquake, a fire, a flood, or significant power outage and other catastrophic events, including the occurrence of a contagious disease or illness, such as COVID-19, could have a material adverse impact on our business, results of operations, and financial condition. Natural disasters and other catastrophic events such as public health crises, could affect our personnel, recovery of our assets, data centers, supply chain, manufacturing vendors, or logistics providers’ ability to provide materials and perform services such as manufacturing products or assisting with shipments on a timely basis. In addition, climate change could result in an increase in the frequency or severity of natural disasters. If our or our service providers’ information technology systems or manufacturing or logistics abilities are hindered by any of the events discussed above, shipments could be delayed, resulting in missed financial targets, such as revenue and shipment targets, for a particular quarter. In addition, computer malware, viruses and computer hacking, fraudulent use attempts, and phishing attacks have become more prevalent in our industry and may be further enhanced in frequency or effectiveness through threat actors’ use of AI, and our internal systems may be victimized by such attacks. Although we maintain incident management and disaster response plans, in the event of a major disruption caused by a catastrophic event, such as a natural disaster, or man-made problem, we may be unable to continue our operations and may endure system interruptions, reputational harm, delays in our development activities, lengthy interruptions in service, breaches of data security and loss of critical data, and our insurance may not cover such events or may be insufficient to compensate us for the potentially significant losses we may incur. All of the aforementioned risks may be further increased if the disaster recovery plans for us and our suppliers prove to be inadequate. To the extent that any of the above should result in delays or cancellations of customer orders, delays in the manufacture, deployment or shipment of our products, or delays in the rendering of our services, our business, financial condition and results of operations would be adversely affected.

ITEM 1B. UNRESOLVED STAFF COMMENTS

None.

ITEM 1C. CYBERSECURITY

Cybersecurity Risk Management and Strategy

As a provider of cybersecurity solutions, we are passionate about cybersecurity risk management. At CrowdStrike, cybersecurity risk management is an integral part of our overall enterprise risk management program.

Our cybersecurity risk management program, which includes data privacy, product security, and information security, is designed to align with our industry's best practices. Our program provides a framework for identifying, monitoring, evaluating, and responding to cybersecurity threats and incidents, including those associated with our use of software, applications, services, and cloud infrastructure developed or provided by third-party vendors and service providers. This framework includes steps for identifying the source of a cybersecurity threat or incident, including whether such cybersecurity threat or incident is associated with a third-party vendor or service provider, assessing the severity and risk of a cybersecurity threat or incident, implementing cybersecurity countermeasures and mitigation or remediation strategies, and informing management and the audit committee of our Board of Directors (the "Audit Committee") of material cybersecurity threats and incidents.

Our cybersecurity team is responsible for assessing our cybersecurity risk management program and our incident response plan, which we regularly test through table-top exercises, and testing of our security protocols through additional techniques, such as penetration testing. In addition, we regularly engage independent third-party auditors to evaluate our compliance with various security compliance standards. We also conduct internal annual assessments of our cybersecurity risk management program. We review or update our cybersecurity policies, standards and procedures annually, or more frequently as needed, to account for changes in the threat landscape, as well as in response to legal and regulatory developments. Our cybersecurity efforts also include mandatory training for all employees and contractors on CrowdStrike's security and privacy policies. We also have a clearly defined acceptable use policy, and we require employees to certify to it. We also require employees to certify their adherence to our code of conduct. We also periodically send our employees simulated phishing emails to test their compliance with our policies. Although we have continued to invest in our diligence, onboarding, and monitoring capabilities over our critical third parties, including our third-party vendors and service providers, our control over the security posture of our critical third parties is limited, and there can be no assurance that we can prevent or mitigate the risk of any compromise or failure in the information assets owned or controlled by such third parties.

A cross-functional incident response team, comprised of representatives from information technology, information security, product security, engineering, privacy and legal, is responsible for the monitoring and disposition of potential occurrences such as data breaches, intrusions, and other security incidents and implementing our detailed incident response plan. Our incident response plan includes processes and procedures for assessing potential internal and external threats, activation and notification, crisis management, and post-incident recovery designed to safeguard the confidentiality, availability, and integrity of our information assets.

In fiscal 2025, we did not identify any cybersecurity threats or incidents that have materially affected or are reasonably likely to materially affect our business strategy, results of operations, or financial condition. However, despite our efforts, we cannot eliminate all risks from cybersecurity threats or incidents or provide assurances that we have not experienced an undetected cybersecurity incident. For more information about these risks, please see "Risk Factors—Risks Related to Our Business and Industry" in this annual report on Form 10-K.

Cybersecurity Governance

Our Board of Directors has oversight responsibility for our overall enterprise risk management, and has delegated cybersecurity risk management oversight to the Audit Committee. The Audit Committee is responsible for ensuring that management (i) has policies, processes, and procedures designed to identify, monitor, evaluate, and respond to cybersecurity risks to which the company is exposed and (ii) takes steps to mitigate or remediate cybersecurity risks, threats and incidents, including monitoring the activities of the cybersecurity team and reviewing and updating our cybersecurity policies, processes and procedures. The Audit Committee also reports material cybersecurity incidents to our full Board of Directors.

Management is responsible for day-to-day risk management activities, including identifying and assessing cybersecurity risks, establishing processes to ensure that potential cybersecurity risk exposures are monitored, implementing appropriate mitigation or remediation measures and maintaining cybersecurity programs. Our cybersecurity programs are under the direction of our Chief Information Security Officer ("CISO"). Our CISO and dedicated personnel are certified and experienced

information systems security professionals and information security managers with many years of experience across a variety of technology sub-specialties.

Our CISO receives reports from our cybersecurity team and monitors the prevention, detection, and mitigation or remediation of cybersecurity risks. Management, including the CISO, regularly updates the Audit Committee and the Board of Directors on the Company's cybersecurity programs, material cybersecurity risks, and mitigation or remediation strategies.

ITEM 2. PROPERTIES

Our principal executive offices occupy approximately 47,618 square feet in Austin, Texas under a lease that expires in 2030. We also lease office space for our operations in various locations throughout the United States as well as office space in a number of countries in Europe, the Middle East, and the Asia-Pacific region.

We believe that our existing facilities are sufficient for our current needs. In the future, we may need to add new facilities and expand our existing facilities as we add employees, grow our infrastructure and evolve our business. We believe that suitable additional or substitute space will be available on commercially reasonable terms to meet our future needs.

ITEM 3. LEGAL PROCEEDINGS

We are currently a party to, and may from time to time in the future be involved in, various litigation matters and subject to claims that arise in the ordinary course of business, including claims asserted by third parties in the form of letters and other communications. For information regarding legal proceedings and other claims asserted against us, including in relation to the July 19 Incident, see Note 10, Commitments and Contingencies, in Part II, Item 8 of this Annual Report on Form 10-K.

For any claims for which we believe a liability is both probable and reasonably estimable, we record a liability in the period in which we make this determination. Other than as disclosed in Note 10, there is no pending or threatened legal proceeding to which we are a party that, in our opinion, is likely to have a material adverse effect on our business and our consolidated financial statements; however, the results of legal proceedings and claims are inherently unpredictable. Regardless of the outcome, litigation can have an adverse impact on our business because of defense and settlement costs, diversion of management resources, and other factors. In addition, the expense of litigation and the timing of this expense from period to period are difficult to estimate, subject to change, and could adversely affect our consolidated financial statements.

ITEM 4. MINE SAFETY DISCLOSURES

Not applicable.

Part II

ITEM 5. MARKET FOR REGISTRANT'S COMMON EQUITY, RELATED STOCKHOLDER MATTERS AND ISSUER PURCHASES OF EQUITY SECURITIES

Market Information for Common Stock

Our Class A common stock has been listed and traded on the Nasdaq Global Select Market under the symbol "CRWD" since June 12, 2019. Prior to that date, there was no public market for our Class A common stock. There is no public market for our Class B common stock. On December 11, 2024, all of our outstanding shares of Class B common stock automatically converted into an equal number of shares of Class A common stock pursuant to the provisions of the Amended and Restated Certificate of Incorporation.

Holders of Record

As of January 31, 2025, we had 95 holders of record of our Class A common stock and zero holders of record of our Class B common stock. The actual number of stockholders is greater than this number of record holders and includes stockholders who are beneficial owners but whose shares are held in street name by brokers and other nominees.

Dividend Policy

We have never declared or paid any cash dividends on our capital stock. We currently intend to retain all available funds and any future earnings for use in the operation of our business and do not expect to pay any dividends on our capital stock in the foreseeable future. Additionally, our ability to pay dividends is limited by restrictions on our ability to pay dividends or make distributions under the terms of our credit facility. Any future determination to declare dividends will be made at the discretion of our board of directors, subject to applicable laws, and will depend on a number of factors, including our financial condition, results of operations, capital requirements, contractual restrictions, general business conditions, and other factors that our board of directors may deem relevant.

Securities Authorized for Issuance under Equity Compensation Plans

The information required by this item with respect to our equity compensation plans is incorporated by reference to our Proxy Statement for the 2025 Annual Meeting of Stockholders to be filed with the Securities and Exchange Commission within 120 days of the fiscal year ended January 31, 2025.

Recent Sales of Unregistered Equity Securities and Use of Proceeds

(a) Sale of Unregistered Equity Securities

On November 20, 2024, we issued approximately \$22.8 million of shares of our Class A common stock, subject to service-based vesting and other conditions, to certain stockholders of Adaptive Shield in connection with our acquisition of Adaptive Shield. The transaction was exempt from registration under Section 4(a)(2) of the Securities Act.

(b) Use of Proceeds from Public Offering of Common Stock

None.

Issuer Purchases of Equity Securities

None.

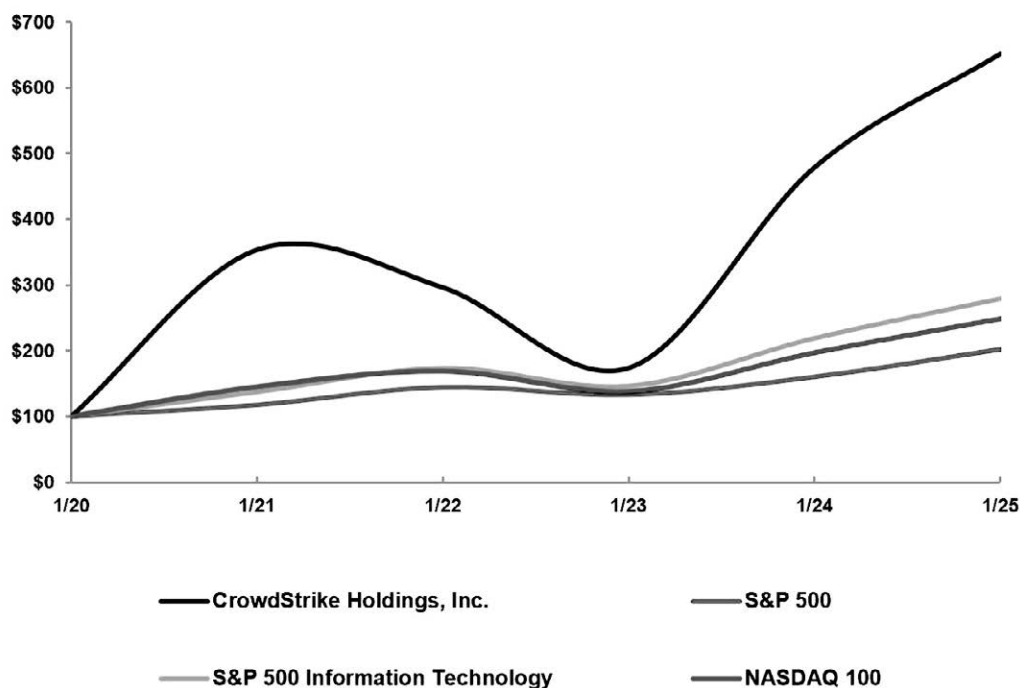
Stock Performance Graph

This performance graph shall not be deemed “soliciting material” or to be “filed” with the SEC for purposes of Section 18 of the Exchange Act, or otherwise subject to the liabilities under that Section, and shall not be deemed to be incorporated by reference into any filing of CrowdStrike Holdings, Inc. under the Securities Act or the Exchange Act.

We have presented below the cumulative total return to our stockholders for the five years ended January 31, 2025 in comparison to the Standard & Poor’s 500 Index, Standard & Poor Information Technology Index, and the Nasdaq 100 Index. All values assume a \$100 initial investment and data for the Standard & Poor’s 500 Index, Standard & Poor Information Technology Index and the Nasdaq 100 Index assume reinvestment of dividends. The comparisons are based on historical data and are not indicative of, nor intended to forecast, the future performance of our common stock.

COMPARISON OF 5 YEAR CUMULATIVE TOTAL RETURN*

Among CrowdStrike Holdings, Inc., the S&P 500 Index, the S&P 500 Information Technology Index and the NASDAQ 100 Index



*\$100 invested on 1/31/20 in stock or index, including reinvestment of dividends.
Fiscal year ending January 31.

Copyright© 2025 Standard & Poor's, a division of S&P Global. All rights reserved.

| Company/ Index | Base period | | | | | |
|----------------------------|-------------|-----------|-----------|-----------|-----------|-----------|
| | 1/31/20 | 1/31/21 | 1/31/22 | 1/31/23 | 1/31/24 | 1/31/25 |
| CrowdStrike Holdings, Inc. | \$ 100.00 | \$ 353.25 | \$ 295.69 | \$ 173.35 | \$ 478.80 | \$ 651.61 |
| S&P 500 | \$ 100.00 | \$ 117.25 | \$ 144.56 | \$ 132.68 | \$ 160.30 | \$ 202.59 |
| S&P Information Technology | \$ 100.00 | \$ 137.13 | \$ 173.37 | \$ 146.16 | \$ 219.37 | \$ 279.92 |
| Nasdaq 100 | \$ 100.00 | \$ 145.00 | \$ 168.64 | \$ 137.90 | \$ 196.96 | \$ 248.82 |

ITEM 6. [RESERVED]

ITEM 7. MANAGEMENT'S DISCUSSION AND ANALYSIS OF FINANCIAL CONDITION AND RESULTS OF OPERATIONS

The following discussion and analysis of our financial condition and results of operations should be read in conjunction with the consolidated financial statements and related notes thereto included in Item 8 "Financial Statements and Supplementary Data" in this Annual Report on Form 10-K. This section of this Form 10-K generally discusses fiscal 2025 and 2024 items and year-over-year comparisons between fiscal 2025 and 2024. Discussions of fiscal 2023 items and year-over-year comparisons between fiscal 2024 and 2023 are not included in this Form 10-K, and can be found in "Management's Discussion and Analysis of Financial Condition and Results of Operations" in Part II, Item 7 of our Annual Report on Form 10-K for the fiscal year ended January 31, 2024. Some of the information contained in this discussion and analysis or set forth elsewhere in this Annual Report on Form 10-K, including information with respect to our plans and strategy for our business, includes forward-looking statements that involve risks and uncertainties, including those described under the heading "Special Note Regarding Forward-Looking Statements." You should review the disclosure under Part I, Item 1A, "Risk Factors" in this Annual Report on Form 10-K for a discussion of important factors that could cause actual results to differ materially from the results described in or implied by the forward-looking statements contained in the following discussion and analysis. Our fiscal years ended January 31, 2025, January 31, 2024, and January 31, 2023, are referred to herein as fiscal 2025, fiscal 2024, and fiscal 2023, respectively.

Overview

Founded in 2011, CrowdStrike reinvented cybersecurity for the cloud era and transformed the way cybersecurity is delivered and experienced by customers. When we started CrowdStrike, cyberattackers had an asymmetric advantage over legacy cybersecurity products that could not keep pace with the rapid changes in adversary tactics. We took a fundamentally different approach to solve this problem with the AI-native CrowdStrike Falcon platform – the first, true cloud-native unified platform built with AI at the core, capable of harnessing vast amounts of security and enterprise data to deliver highly modular solutions through a single lightweight agent.

We believe our approach has defined a new category called the Security Cloud, which has transformed the cybersecurity industry the same way the cloud has transformed the customer relationship management, human resources, and service management industries. Using cloud-scale AI, our Security Cloud enriches and correlates trillions of cybersecurity events per week with indicators of attack, threat intelligence, and enterprise data (including data from across endpoints, workloads, identities, DevOps, IT assets, and configurations) to create actionable data, identify shifts in adversary tactics, and automatically prevent threats in real-time across our customer base. The more data that is fed into our Falcon platform, the more intelligent our Security Cloud becomes, and the more our customers benefit, creating a powerful network effect that increases the overall value we provide.

Our Go-To-Market Strategy

We sell subscriptions to our Falcon platform and cloud modules to organizations across multiple industries. We primarily sell subscriptions to our Falcon platform and cloud modules through our direct sales team that leverages our network of channel partners. Our direct sales team is comprised of field sales and inside sales professionals who are segmented by a customer's number of endpoints.

We have a low friction land-and-expand sales strategy. When customers deploy our Falcon platform, they can start with any number of cloud modules and easily add additional cloud modules. Once customers experience the benefits of our Falcon platform, they often expand their adoption over time by adding more endpoints or purchasing additional modules. We also use our sales team to identify current customers who may be interested in free trials of additional cloud modules, which serves as a powerful driver of our land-and-expand model. By segmenting our sales teams, we can deploy a low-touch sales model that efficiently identifies prospective customers.

We began as a solution for large enterprises, but the flexibility and scalability of our Falcon platform has enabled us to seamlessly offer our solution to customers of any size. We have expanded our sales focus to include any sized organization without the need to modify our Falcon platform for small and medium sized businesses.

A substantial majority of our customers purchase subscriptions with a term over one year. Our subscriptions are generally priced on a per-endpoint and per-module basis. We recognize revenue from our subscriptions ratably over the term of the subscription. We also generate revenue from our incident response and proactive professional services, which are generally priced on a time and materials basis. We view our professional services business primarily as an opportunity to cross-sell subscriptions to our Falcon platform and cloud modules.

Certain Factors Affecting Our Performance

Adoption of Our Solutions. We believe our future success depends in large part on the growth in the market for cloud-based SaaS-delivered endpoint security solutions. Many organizations have not yet abandoned the on-premise legacy products in which they have invested substantial personnel and financial resources to design and maintain. As a result, it is difficult to predict customer adoption rates and demand for our cloud-based solutions.

New Customer Acquisition. Our future growth depends in large part on our ability to acquire new customers. If our efforts to attract new customers are not successful, our revenue and rate of revenue growth may decline. We believe that our go-to-market strategy and the flexibility and scalability of our Falcon platform allow us to rapidly expand our customer base. Our incident response and proactive services also help drive new customer acquisitions, as many of these professional services customers subsequently purchase subscriptions to our Falcon platform. Many organizations have not yet adopted cloud-based security solutions, and since our Falcon platform has offerings for organizations of all sizes, worldwide, and across industries, we believe this presents a significant opportunity for growth.

Maintain Customer Retention and Increase Sales. Our ability to increase revenue depends in large part on our ability to retain our existing customers and increase the size of their subscriptions. We focus on increasing sales to our existing customers by expanding their deployments to more endpoints and selling additional cloud modules for increased functionality. Over time we have transitioned our platform from a single offering into highly-integrated offerings of multiple cloud modules.

Invest in Growth. We believe that our market opportunity is large and requires us to continue to invest significantly in sales and marketing efforts to further grow our customer base, both domestically and internationally. Our open cloud architecture and single data model have allowed us to rapidly build and deploy new cloud modules, and we expect to continue investing in those efforts to further enhance our technology platform and product functionality. In addition to our ongoing investment in research and development, we may also pursue acquisitions of businesses, technologies, and assets that complement and expand the functionality of our Falcon platform, add to our technology or security expertise, or bolster our leadership position by gaining access to new customers or markets. Furthermore, we expect our general and administrative expenses to increase in dollar amount for the foreseeable future given the additional expenses for accounting, compliance, and investor relations as we grow as a public company.

July 19 Incident. On July 19, 2024, we released a content configuration update for our Falcon sensor that resulted in system crashes for certain Windows systems (the “July 19 Incident”). As a result of the July 19 Incident, we are subject to lawsuits, claims and inquiries as described in Note 10, Commitments and Contingencies, in Part II, Item 8 of this Annual Report on Form 10-K. We have incurred, and expect to continue to incur, significant legal and professional services and other general and administrative expenses associated with the July 19 Incident in future periods. It is not reasonably possible to quantify the precise impact of the July 19 Incident, but the incident has adversely affected our results of operations, and we currently expect a number of factors relating to the incident to adversely affect our key metrics and results of operations in future periods. While we have maintained high dollar-based gross retention rates following the incident, we have experienced delays in creating sales opportunities and longer sales cycles, including delays in customer purchasing decisions. We expect sales cycles to continue to be elongated in future periods. In addition, because our customers typically sign contracts with terms of twelve months or longer, customer churn and any corresponding impact to our key metrics and revenue may occur in future periods. Customer commitment packages introduced following the July 19 Incident have included discounting, additional modules, professional services, flexible payment terms or subscription period extensions. Our customer commitment packages have resulted, and are expected to continue to result, in increased contraction, due to elongated subscription terms, and decreased upsell dollar values.

Key Metrics

We monitor the following key metrics to help us evaluate our business, identify trends affecting our business, formulate business plans, and make strategic decisions.

Annual Recurring Revenue (“ARR”)

ARR is calculated as the annualized value of our customer subscription contracts as of the measurement date, assuming any contract that expires during the next 12 months is renewed on its existing terms. To the extent that we are negotiating a renewal with a customer after the expiration of the subscription, we continue to include that revenue in ARR if we are actively in discussion with such organization for a new subscription or renewal, or until such organization notifies us that it is not renewing its subscription.

The following table sets forth our ARR as of the dates presented (dollars in thousands):

| | As of January 31, | |
|--------------------------|--------------------------|--------------|
| | 2025 | 2024 |
| Annual recurring revenue | \$ 4,241,838 | \$ 3,435,150 |
| Year-over-year growth | 23 % | 34 % |

ARR increased 23% year-over-year and grew to \$4.2 billion as of January 31, 2025, of which \$806.7 million was net new ARR added during fiscal 2025. ARR increased 34% year-over-year and grew to \$3.4 billion as of January 31, 2024, of which \$875.5 million was net new ARR added during fiscal 2024.

Dollar-Based Net Retention Rate

Our dollar-based net retention rate compares our ARR from a set of subscription customers against the same metric for those subscription customers from the prior year. Our dollar-based net retention rate reflects customer renewals, expansion, contraction, and churn, and excludes revenue from our incident response and proactive services. We calculate our dollar-based net retention rate as of period end by starting with the ARR from all subscription customers as of 12 months prior to such period end, or Prior Period ARR. We then calculate the ARR from these same subscription customers as of the current period end, or Current Period ARR. Current Period ARR includes any expansion and is net of contraction or churn over the trailing 12 months but excludes revenue from new subscription customers in the current period. We then divide the Current Period ARR by the Prior Period ARR to arrive at our dollar-based net retention rate. For the purposes of calculating our dollar-based net retention rate, we define a subscription customer as a separate legal entity that has entered into a distinct subscription agreement for access to our Falcon platform for which the term has not ended or with which we are negotiating a renewal contract. We do not consider our channel partners as customers, and we treat managed service security providers, who may purchase our products on behalf of multiple companies, as a single customer.

Our dollar-based net retention rate can fluctuate from period to period due to large customer contracts in a given period and incentives provided, which may reduce our dollar-based net retention rate in subsequent periods. In addition, if our customers are not able to fully utilize their product subscriptions (including in connection with our flexible subscription offering), we may experience increased contraction as such customers may elect to renew with shorter subscription periods, fewer cloud modules, fewer endpoints or smaller contract values, which may reduce our dollar-based net retention rate.

| | As of January 31, | |
|---------------------------------|--------------------------|-------------|
| | 2025 | 2024 |
| Dollar-based net retention rate | 112 % | 119 % |

Components of Our Results of Operations

Revenue

Subscription Revenue. Subscription revenue primarily consists of subscription fees for our Falcon platform and additional cloud modules that are supported by our cloud-based platform. Subscription revenue is driven primarily by the number of subscription customers, the number of endpoints per customer, and the number of cloud modules included in the subscription. We recognize subscription revenue ratably over the term of the agreement, which is generally one to three years. We generally invoice our subscription customers at the beginning of the subscription term, or in some instances, such as in multi-year arrangements, in installments. Consequently, a substantial portion of the revenue that we report in each period is attributable to the recognition of deferred revenue relating to subscriptions that we entered into during previous periods.

Professional Services Revenue. Professional services revenue includes incident response and proactive services, forensic and malware analysis, attribution analysis, operationalizing the Falcon Platform, residency program, and active defense services. Professional services are generally sold separately from subscriptions to our Falcon platform, although customers frequently enter into a separate arrangement to purchase subscriptions to our Falcon platform at the conclusion of a professional services arrangement. Professional services are available through hourly rate and fixed fee contracts, one-time and ongoing engagements, and retainer-based agreements. For time and materials and retainer-based arrangements, revenue is recognized as services are performed. Fixed fee contracts account for an immaterial portion of our revenue.

Cost of Revenue

Subscription Cost of Revenue. Subscription cost of revenue consists primarily of costs related to hosting our cloud-based Falcon platform in data centers, amortization of our capitalized internal-use software, employee-related costs such as salaries and bonuses, stock-based compensation expense, benefits costs associated with our operations and support personnel, software license fees, property and equipment depreciation, amortization of acquired intangibles, and an allocated portion of facilities and administrative costs.

As new customers subscribe to our platform and existing subscription customers increase the number of endpoints on our Falcon platform, our cost of revenue will increase due to greater cloud hosting costs related to powering new cloud modules and the incremental costs for storing additional data collected for such cloud modules and employee-related costs. We intend to continue to invest additional resources in our cloud platform and our customer support organizations as we grow our business. The level and timing of investment in these areas could affect our cost of revenue in the future.

Professional Services Cost of Revenue. Professional services cost of revenue consists primarily of employee-related costs, such as salaries and bonuses, stock-based compensation expense, consulting expense, and an allocated portion of facilities and administrative costs.

Gross Profit and Gross Margin

Gross profit and gross margin have been and will continue to be affected by various factors, including the timing of our acquisition of new subscription customers, renewals from existing subscription customers, sales of additional modules to existing subscription customers, the data center and bandwidth costs associated with operating our cloud platform, the extent to which we expand our customer support and cloud operations organizations, and the extent to which we can increase the efficiency of our technology, infrastructure, and data centers through technological improvements. We expect our gross profit to increase in dollar amount and our gross margin to increase modestly over the long term as we grow our business, although our gross margin could fluctuate from period to period depending on the interplay of these factors. Demand for our incident response services is driven by the number of breaches experienced by non-customers. Also, we view our professional services solutions in the context of our larger business and as a significant lead generator for new subscriptions. Because of these factors, our services revenue and gross margin may fluctuate over time.

Operating Expenses

Our operating expenses consist of sales and marketing, research and development, and general administrative expenses. For each of these categories of expense, employee-related expenses are the most significant component, which include salaries, employee bonuses, sales commissions, and employer payroll tax. Operating expenses also include an allocated portion of overhead costs for facilities and other administrative functions.

Sales and Marketing. Sales and marketing expenses primarily consist of employee-related expenses such as salaries, commissions, and bonuses. Sales and marketing expenses also include stock-based compensation; expenses related to our marketing programs; and an allocated portion of facilities and administrative expenses. Sales and marketing expenses also include the amortization of deferred contract acquisition costs, which includes commissions and any other incremental payments made upon the initial acquisition of a subscription or upsells to existing customers, which are capitalized and amortized over the estimated customer life. We also capitalize and amortize any such expenses paid for the renewal of a subscription over the term of the renewal.

We expect sales and marketing expenses to increase in dollar amount as we continue to make significant investments in our sales and marketing organization to drive additional revenue, further penetrate the market, and expand our global customer base. However, we anticipate sales and marketing expenses to decrease as a percentage of our total revenue over time as we grow our business, although our sales and marketing expenses may fluctuate as a percentage of our total revenue from period to period depending on the timing of these expenses.

Research and Development. Research and development expenses primarily consist of employee-related expenses such as salaries and bonuses; stock-based compensation; cloud hosting and related costs; and an allocated portion of facilities and administrative expenses. Our cloud platform is software-driven, and our research and development teams employ software engineers in the design, and the related development, testing, certification, and support of these solutions.

We expect research and development expenses to increase in dollar amount as we continue to increase investments in our technology architecture and software platform. However, we anticipate research and development expenses to decrease as a percentage of our total revenue over time as we grow our business, although our research and development expenses may fluctuate as a percentage of our total revenue from period to period depending on the timing of these expenses.

General and Administrative. General and administrative expenses consist of employee-related expenses such as salaries and bonuses; stock-based compensation; and related expenses for our executive, finance, human resources, and legal organizations. In addition, general and administrative expenses include outside legal, accounting, and other professional fees; and an allocated portion of facilities and administrative expenses.

We expect general and administrative expenses to increase in dollar amount over time. We expect to incur significant legal and professional services and other expenses associated with the July 19 Incident in future periods. General and administrative expenses may fluctuate as a percentage of our total revenue from period to period depending on the timing of these expenses.

Interest Expense. Interest expense consists primarily of amortization of debt issuance costs, contractual interest expense for our Senior Notes issued in January 2021, and amortization of debt issuance costs on our secured revolving credit facility (“Revolving Facility”).

Interest Income. Interest income consists primarily of income earned on our cash, cash equivalents, and short-term investments.

Other Income, Net. Other income, net consists primarily of gains and losses on strategic investments and foreign currency transaction gains and losses.

Provision for Income Taxes. Provision for income taxes consists of state income taxes in the United States, foreign income taxes, and withholding taxes related to customer payments in certain foreign jurisdictions in which we conduct business. We maintain a full valuation allowance on our U.S. federal and state and certain foreign deferred tax assets, including net operating loss carryforwards and tax credits, which we have determined are not realizable on a more-likely-than-not basis. We regularly evaluate the need for a valuation allowance.

Net Income Attributable to Non-controlling Interest. Net income attributable to non-controlling interest consists of the Falcon Funds' non-controlling interest share of gains and losses and interest income from our strategic investments.

Results of Operations

The following tables set forth our consolidated statements of operations for each period presented (in thousands, except percentages):

| | Year Ended January 31, | | |
|---|------------------------|------------------|---------------------|
| | 2025 | 2024 | 2023 |
| Revenue | | | |
| Subscription | \$ 3,761,480 | \$ 2,870,557 | \$ 2,111,660 |
| Professional services | 192,144 | 184,998 | 129,576 |
| Total revenue | 3,953,624 | 3,055,555 | 2,241,236 |
| Cost of revenue | | | |
| Subscription | 835,509 | 630,745 | 511,684 |
| Professional services | 155,972 | 124,978 | 89,547 |
| Total cost of revenue | 991,481 | 755,723 | 601,231 |
| Gross profit | 2,962,143 | 2,299,832 | 1,640,005 |
| Operating expenses | | | |
| Sales and marketing | 1,523,356 | 1,140,566 | 904,409 |
| Research and development | 1,076,901 | 768,497 | 608,364 |
| General and administrative | 482,316 | 392,764 | 317,344 |
| Total operating expenses | 3,082,573 | 2,301,827 | 1,830,117 |
| Loss from operations | (120,430) | (1,995) | (190,112) |
| Interest expense | (26,311) | (25,756) | (25,319) |
| Interest income | 196,174 | 148,930 | 52,495 |
| Other income, net | 5,101 | 1,638 | 3,053 |
| Income (loss) before provision for income taxes | 54,534 | 122,817 | (159,883) |
| Provision for income taxes | 71,130 | 32,232 | 22,402 |
| Net income (loss) | (16,596) | 90,585 | (182,285) |
| Net income attributable to non-controlling interest | 2,675 | 1,258 | 960 |
| Net income (loss) attributable to CrowdStrike | <u>\$ (19,271)</u> | <u>\$ 89,327</u> | <u>\$ (183,245)</u> |

The following table presents the components of our consolidated statements of operations as a percentage of total revenue for the periods presented:

| | Year Ended January 31, | | |
|---|------------------------|-------|-------|
| | 2025 | 2024 | 2023 |
| | % | % | % |
| Revenue | | | |
| Subscription | 95 % | 94 % | 94 % |
| Professional services | 5 % | 6 % | 6 % |
| Total revenue | 100 % | 100 % | 100 % |
| Cost of revenue | | | |
| Subscription | 21 % | 21 % | 23 % |
| Professional services | 4 % | 4 % | 4 % |
| Total cost of revenue | 25 % | 25 % | 27 % |
| Gross profit | 75 % | 75 % | 73 % |
| Operating expenses | | | |
| Sales and marketing | 39 % | 37 % | 40 % |
| Research and development | 27 % | 25 % | 27 % |
| General and administrative | 12 % | 13 % | 14 % |
| Total operating expenses | 78 % | 75 % | 82 % |
| Loss from operations | (3)% | — % | (8)% |
| Interest expense | (1)% | (1)% | (1)% |
| Interest income | 5 % | 5 % | 2 % |
| Other income, net | — % | — % | — % |
| Income (loss) before provision for income taxes | 1 % | 4 % | (7)% |
| Provision for income taxes | 2 % | 1 % | 1 % |
| Net income (loss) | — % | 3 % | (8)% |
| Net income attributable to non-controlling interest | — % | — % | — % |
| Net income (loss) attributable to CrowdStrike | — % | 3 % | (8)% |

Comparison of Fiscal 2025 and Fiscal 2024

Revenue

The following shows total revenue from subscriptions and professional services for fiscal 2025, as compared to fiscal 2024 (in thousands, except percentages):

| | | | Change | |
|-----------------------|---------------------|---------------------|-------------------|------|
| | 2025 | 2024 | \$ | % |
| Subscription | \$ 3,761,480 | \$ 2,870,557 | \$ 890,923 | 31 % |
| Professional services | 192,144 | 184,998 | 7,146 | 4 % |
| Total revenue | <u>\$ 3,953,624</u> | <u>\$ 3,055,555</u> | <u>\$ 898,069</u> | 29 % |

Total revenue increased by \$898.1 million, or 29%, in fiscal 2025, compared to fiscal 2024. Subscription revenue accounted for 95% and 94% of our total revenue in fiscal 2025 and fiscal 2024, respectively. Professional services revenue accounted for 5% and 6% of our total revenue in fiscal 2025 and fiscal 2024, respectively.

Subscription revenue increased by \$890.9 million, or 31% in fiscal 2025, compared to fiscal 2024, which was primarily driven by a combination of the addition of new customers and the sale of additional sensors and modules to existing customers.

Professional services revenue increased by \$7.1 million, or 4%, in fiscal 2025, compared to fiscal 2024, which was primarily attributable to an increase in the number of professional service hours.

Cost of Revenue, Gross Profit, and Gross Margin

The following shows cost of revenue related to subscriptions and professional services for fiscal 2025, as compared to fiscal 2024 (in thousands, except percentages):

| | | | Change | |
|-----------------------|-------------------|-------------------|-------------------|----------|
| | 2025 | 2024 | \$ | % |
| Subscription | \$ 835,509 | \$ 630,745 | \$ 204,764 | 32 % |
| Professional services | 155,972 | 124,978 | 30,994 | 25 % |
| Total cost of revenue | <u>\$ 991,481</u> | <u>\$ 755,723</u> | <u>\$ 235,758</u> | 31 % |

Total cost of revenue increased by \$235.8 million, or 31%, in fiscal 2025, compared to fiscal 2024. Subscription cost of revenue increased by \$204.8 million, or 32%, in fiscal 2025, compared to fiscal 2024. The increase in subscription cost of revenue was primarily due to an increase in employee-related expenses of \$55.6 million driven by a 28% increase in average headcount, an increase in depreciation of data center equipment of \$38.4 million, an increase in stock-based compensation expense of \$29.7 million, an increase in cloud hosting and related services costs of \$28.5 million, an increase in allocated overhead costs of \$20.3 million, an increase in amortization of internal-use software of \$17.6 million, an increase in hardware maintenance costs of \$5.4 million, and an increase in employee benefits of \$4.2 million.

Professional services cost of revenue increased by \$31.0 million, or 25%, in fiscal 2025, compared to fiscal 2024. The increase in professional services cost of revenue was primarily due to an increase in employee-related expenses of \$13.1 million driven by an 20% increase in average headcount, an increase in stock-based compensation expense of \$8.8 million, an increase in allocated overhead costs of \$5.0 million, an increase in consulting expense of \$2.2 million, and an increase in employee benefits of \$1.0 million.

The following shows gross profit and gross margin for subscriptions and professional services for fiscal 2025, as compared to fiscal 2024 (in thousands, except percentages):

| | | | Change | |
|------------------------------------|---------------------|---------------------|-------------------|----------|
| | 2025 | 2024 | \$ | % |
| Subscription gross profit | \$ 2,925,971 | \$ 2,239,812 | \$ 686,159 | 31 % |
| Professional services gross profit | 36,172 | 60,020 | (23,848) | (40)% |
| Total gross profit | <u>\$ 2,962,143</u> | <u>\$ 2,299,832</u> | <u>\$ 662,311</u> | 29 % |

| | 2025 | 2024 | Change |
|------------------------------------|-------------|-------------|---------------|
| Subscription gross margin | 78 % | 78 % | — % |
| Professional services gross margin | 19 % | 32 % | (13)% |
| Total gross margin | 75 % | 75 % | — % |

Subscription gross margin was flat in fiscal 2025, compared to fiscal 2024.

Professional services gross margin decreased by 13% in fiscal 2025, compared to fiscal 2024. The decrease in professional services gross margin was primarily due to an increase in consulting expense and decreased utilization during fiscal 2025 compared to fiscal 2024.

Operating Expenses

Sales and Marketing

The following shows sales and marketing expenses for fiscal 2025, as compared to fiscal 2024 (in thousands, except percentages):

| | | | Change | |
|------------------------------|--------------|--------------|---------------|----------|
| | 2025 | 2024 | \$ | % |
| Sales and marketing expenses | \$ 1,523,356 | \$ 1,140,566 | \$ 382,790 | 34 % |

Sales and marketing expenses increased by \$382.8 million, or 34%, in fiscal 2025, compared to fiscal 2024. The increase in sales and marketing expenses was primarily due to an increase in employee-related expenses of \$159.0 million driven by a 14% increase in average headcount, an increase in stock-based compensation expense of \$59.7 million, an increase in marketing programs of \$55.5 million, an increase in allocated overhead costs of \$28.4 million, \$21.4 million of expenses relating to the July 19 Incident, an increase in travel expenses of \$13.1 million, an increase in company events expenses of \$8.6 million, an increase in employee benefits of \$6.3 million, an increase in term-based software licenses of \$5.4 million, an increase in cloud hosting and related costs of \$4.2 million, an increase in other labor expenses of \$2.8 million, and an increase in consulting expense of \$2.5 million.

Research and Development

The following shows research and development expenses for fiscal 2025, as compared to fiscal 2024 (in thousands, except percentages):

| | | | Change | |
|-----------------------------------|--------------|-------------|---------------|----------|
| | 2025 | 2024 | \$ | % |
| Research and development expenses | \$ 1,076,901 | \$ 768,497 | \$ 308,404 | 40 % |

Research and development expenses increased by \$308.4 million, or 40% in fiscal 2025, compared to fiscal 2024. This increase was primarily due to an increase in stock-based compensation expense of \$131.7 million, an increase in employee-related expenses of \$119.3 million driven by a 18% increase in average headcount, an increase in cloud hosting and related costs of \$64.2 million, \$6.8 million of expenses relating to the July 19 Incident, an increase in term-based software licenses of \$6.4 million, an increase in employee benefits of \$5.1 million, an increase in travel expenses of \$3.2 million, and an increase in consulting expense of \$1.7 million, partially offset by a decrease in allocated engineering and overhead costs of \$27.5 million, an increase in software capitalization of \$11.4 million, and a decrease in other labor expenses of \$9.7 million.

General and Administrative

The following shows general and administrative expenses for fiscal 2025, as compared to fiscal 2024 (in thousands, except percentages):

| | | | Change | |
|-------------------------------------|-------------|-------------|---------------|----------|
| | 2025 | 2024 | \$ | % |
| General and administrative expenses | \$ 482,316 | \$ 392,764 | \$ 89,552 | 23 % |

General and administrative expenses increased by \$89.6 million, or 23%, in fiscal 2025, compared to fiscal 2024. The increase in general and administrative expenses was primarily due to \$31.9 million of expenses relating to the July 19 Incident, an increase in employee-related expenses of \$27.2 million driven by a 19% increase in average headcount, an increase in allocated overhead costs of \$6.3 million, an increase in consulting expense of \$5.0 million, an increase in leased airfare costs of \$4.5 million, an increase in stock-based compensation expense of \$4.0 million, an increase in travel expenses of \$2.3 million, an increase in company events expenses of \$2.1 million, an increase in term-based software licenses of \$2.1 million, an increase in taxes and licenses expenses of \$2.0 million, an increase in employee related programs of \$1.8 million, and an increase in other labor expenses of \$1.7 million, partially offset by a decrease in legal expense of \$7.5 million unrelated to the July 19 Incident.

Interest Expense, Interest Income and Other Income, Net

The following shows interest expense, interest income, and other income, net, for fiscal 2025, as compared to fiscal 2024 (in thousands, except percentages):

| | | | Change | |
|-------------------|-------------|-------------|-----------|-------|
| | 2025 | 2024 | \$ | % |
| Interest expense | \$ (26,311) | \$ (25,756) | \$ (555) | 2 % |
| Interest income | \$ 196,174 | \$ 148,930 | \$ 47,244 | 32 % |
| Other income, net | \$ 5,101 | \$ 1,638 | \$ 3,463 | 211 % |

Interest expense consists primarily of amortization of debt issuance costs, contractual interest expense, accretion of debt discount for our Senior Notes issued in January 2021, and amortization of debt issuance costs on our Revolving Facility.

The increase in interest income during fiscal 2025 compared to fiscal 2024 was driven by an increase in our cash and cash equivalents.

The increase in other income, net during fiscal 2025 compared to fiscal 2024 was primarily due to an increase in gains on our strategic investments of \$2.4 million, a decrease in downward mark to market adjustments of \$0.5 million on our strategic investments, and gains on deferred compensation assets of \$0.4 million.

Provision for Income Taxes

The following shows the provision for income taxes for fiscal 2025, as compared to fiscal 2024 (in thousands, except percentages):

| | | | Change | |
|----------------------------|-----------|-----------|-----------|-------|
| | 2025 | 2024 | \$ | % |
| Provision for income taxes | \$ 71,130 | \$ 32,232 | \$ 38,898 | 121 % |

The increase in provision for income taxes during fiscal 2025 compared to fiscal 2024 was primarily attributable to intercompany sales of intellectual property from acquired entities, pre-tax foreign earnings, withholding taxes related to customer payments in certain foreign jurisdictions, and change in the realizability of deferred tax assets in certain foreign jurisdictions.

Liquidity and Capital Resources

Our primary sources of liquidity as of January 31, 2025, consisted of: (i) \$4.3 billion in cash and cash equivalents, which mainly consists of cash on hand and highly liquid investments in money market funds and U.S. Treasury bills, (ii) cash we expect to generate from operations, and (iii) available capacity under our \$750.0 million Revolving Facility. It is not currently possible to reasonably estimate the amount of loss or range of possible loss that might result from adverse judgments, settlements, penalties, or other resolution of proceedings resulting from the July 19 Incident. However, despite such uncertainties, we expect that the combination of our existing cash and cash equivalents, cash flows from operations, and the Revolving Facility will be sufficient to meet our anticipated cash needs for working capital and capital expenditures for at least the next 12 months. Our Revolving Facility matures on January 2, 2026.

Our short-term and long-term liquidity requirements primarily arise from: (i) business acquisitions and investments we may make from time to time, (ii) working capital requirements, (iii) interest and principal payments related to our outstanding indebtedness, (iv) research and development and capital expenditure needs, and (v) license and service arrangements integral to our business operations. Our ability to fund these requirements will depend, in part, on our future cash flows, which are determined by our future operating performance and, therefore, subject to prevailing global macroeconomic conditions and financial, business, and other factors, some of which are beyond our control.

We have historically generated operating losses prior to fiscal 2024 and during fiscal 2025, as reflected in our accumulated deficit of \$1.1 billion as of January 31, 2025. We expect to continue to make investments, particularly in sales and marketing and research and development. As a result, we may require additional capital resources in the future to execute strategic initiatives to grow our business.

We generally invoice our subscription customers at the beginning of the subscription term, or in some instances, such as in multi-year arrangements, in installments. Therefore, a substantial source of our cash is from such prepayments, which are included on our consolidated balance sheets as deferred revenue. Deferred revenue primarily consists of billed fees for our subscriptions, prior to satisfying the criteria for revenue recognition, which are subsequently recognized as revenue in accordance with our revenue recognition policy. As of January 31, 2025, we had deferred revenue of \$3.7 billion, of which \$2.7 billion was recorded as a current liability and is expected to be recorded as revenue in the next 12 months, provided all other revenue recognition criteria have been met.

We do not have any relationships with unconsolidated entities or financial partnerships, such as entities often referred to as structured finance or special purpose entities. We do not have any outstanding derivative financial instruments, off-balance sheet guarantees, interest rate swap transactions, or foreign currency forward contracts.

Cash Flows

The following table summarizes our cash flows for the periods presented (in thousands):

| | Year Ended January 31, | | |
|--|-------------------------------|--------------|-------------|
| | 2025 | 2024 | 2023 |
| Net cash provided by operating activities | \$ 1,381,727 | \$ 1,166,207 | \$ 941,007 |
| Net cash used in investing activities | (536,588) | (340,650) | (556,658) |
| Net cash provided by financing activities | 107,208 | 93,158 | 77,437 |
| Net change in cash, cash equivalents and restricted cash | 947,069 | 920,673 | 460,291 |

Operating Activities

Net cash provided by operating activities during fiscal 2025 was \$1.4 billion, which resulted from net loss of \$16.6 million, adjusted for non-cash charges of \$1.4 billion and net cash outflow of \$6.0 million from changes in operating assets and liabilities. Non-cash charges primarily consisted of \$865.4 million in stock-based compensation expense, \$318.8 million of amortization of deferred contract acquisition costs, \$188.0 million of depreciation and amortization, \$26.0 million of amortization of intangibles assets, \$15.3 million of non-cash operating lease costs, \$3.8 million of non-cash interest expense, and \$2.3 million of accretion of short-term investments purchased at a discount, partially offset by \$9.9 million of deferred income taxes and \$6.3 million of realized gains on strategic investments. The net cash outflow from changes in operating assets and liabilities was primarily due to a \$584.5 million increase in deferred contract acquisition costs, a \$274.2 million increase in accounts receivable, net, a \$190.2 million increase in prepaid expenses and other assets, and a \$15.7 million decrease in operating lease liabilities, partially offset by a \$669.3 million increase in deferred revenue, a \$218.5 million increase in accrued expenses and other liabilities, an \$85.9 million increase in accrued payroll and benefits, and an \$84.9 million increase in accounts payable.

Net cash provided by operating activities during fiscal 2024 was \$1.2 billion, which resulted from net income of \$90.6 million, adjusted for non-cash charges of \$1.0 billion and net cash inflow of \$51.5 million from changes in operating assets and liabilities. Non-cash charges primarily consisted of \$631.5 million in stock-based compensation expense, \$238.9 million of amortization of deferred contract acquisition costs, \$126.8 million of depreciation and amortization, \$18.4 million of amortization of intangibles assets, \$13.4 million of non-cash operating lease costs, and \$3.2 million of non-cash interest expense, partially offset by \$3.9 million of realized gains on strategic investments and a \$3.4 million change in deferred income taxes. The net cash inflow from changes in operating assets and liabilities was primarily due to a \$696.6 million increase in deferred revenue, a \$65.1 million increase in accrued payroll and benefits, a \$14.6 million increase in accrued expenses and other liabilities, partially offset by a \$371.6 million increase in deferred contract acquisition costs, a \$217.7 million increase in accounts receivable, net, a \$102.5 million increase in prepaid expenses and other assets, a \$18.9 million decrease in accounts payable, and a \$14.0 million decrease in operating lease liabilities.

Investing Activities

Net cash used in investing activities during fiscal 2025 of \$536.6 million was primarily due to business acquisitions, net of cash acquired, of \$310.3 million, which was related to the Flow Security and Adaptive Shield acquisitions, purchases of property and equipment of \$254.9 million, capitalized internal-use software and website development costs of \$59.0 million, purchases of strategic investments of \$19.7 million, and purchases of deferred compensation investments of \$2.7 million, partially offset by proceeds from maturities of short-term investments of \$97.3 million and proceeds from sales of strategic investments of \$12.5 million.

Net cash used in investing activities during fiscal 2024 of \$340.7 million was primarily due to business acquisitions, net of cash acquired, of \$239.0 million, which was related to the Bionic acquisition, purchases of short-term investments of \$195.6 million, purchases of property and equipment of \$176.5 million, capitalized internal-use software and website development costs of \$49.5 million, purchases of strategic investments of \$17.2 million, purchases of intangible assets of \$11.1 million, and purchases of deferred compensation investments of \$2.0 million, partially offset by proceeds from maturities and sales of short-term investments of \$348.3 million, and proceeds from sales of strategic investments of \$2.0 million.

Financing Activities

Net cash provided by financing activities of \$107.2 million during fiscal 2025 was primarily due to proceeds from our employee stock purchase plan of \$99.6 million, capital contributions from non-controlling interest holders of \$8.5 million, and proceeds from the exercise of stock options of \$4.0 million, partially offset by distributions to non-controlling interest holders of \$4.9 million.

Net cash provided by financing activities of \$93.2 million during fiscal 2024 was primarily due to proceeds from our employee stock purchase plan of \$76.4 million, proceeds from the exercise of stock options of \$8.7 million, and capital contributions from non-controlling interests of \$8.1 million.

Supplemental Guarantor Financial Information

Our Senior Notes are guaranteed on a senior, unsecured basis by CrowdStrike, Inc. and CrowdStrike Financial Services, Inc., wholly owned subsidiaries of CrowdStrike Holdings, Inc. (the “subsidiary guarantors,” and together with CrowdStrike Holdings, Inc., the “Obligor Group”). The guarantee is full and unconditional and is subject to certain conditions for release. See Note 5, Debt, in Part II, Item 8 of this Annual Report on Form 10-K, for a brief description of the Senior Notes.

We conduct our operations almost entirely through our subsidiaries. Accordingly, the Obligor Group’s cash flows and ability to service the notes will depend on the earnings of our subsidiaries and the distribution of those earnings to the Obligor Group, whether by dividends, loans, or otherwise. Holders of the guaranteed registered debt securities will have a direct claim only against the Obligor Group.

Summarized financial information is presented below for the Obligor Group on a combined basis after elimination of intercompany transactions and balances within the Obligor Group and equity in the earnings from and investments in any non-guarantor subsidiary. The revenue amounts presented in the summarized financial information include substantially all of our consolidated revenue, and there is no intercompany revenue from the non-guarantor subsidiaries. This summarized financial information has been prepared and presented pursuant to Regulation S-X Rule 13-01, “Financial Disclosures about Guarantors and Issuers of Guaranteed Securities” and is not intended to present the financial position or results of operations of the Obligor Group in accordance with U.S. GAAP.

| Statement of Operations | Year Ended January 31, 2025 |
|--------------------------------------|--|
| | (in thousands) |
| Revenue | \$ 3,948,062 |
| Cost of revenue | 1,022,627 |
| Operating expenses | 3,063,076 |
| Loss from operations | (137,641) |
| Net loss | (36,365) |
| Net loss attributable to CrowdStrike | (36,365) |

| Balance Sheet | January 31, 2025 |
|---|-------------------------|
| | (in thousands) |
| Current assets (excluding current intercompany receivables from non-Guarantors) | \$ 5,922,562 |
| Current intercompany receivables from non-Guarantors | 49,417 |
| Noncurrent assets (excluding noncurrent intercompany receivables from non-Guarantors) | 2,316,545 |
| Noncurrent intercompany receivables from non-Guarantors | 613,732 |
| Current liabilities (excluding current intercompany payables to non-Guarantors) | 3,331,647 |
| Current intercompany payables to non-Guarantors | 31,092 |
| Noncurrent liabilities (excluding noncurrent intercompany payables to non-Guarantors) | 1,897,235 |
| Noncurrent intercompany payables to non-Guarantors | 234,643 |

Strategic Investments

In July 2019, we agreed to commit up to \$10.0 million to a newly formed entity, CrowdStrike Falcon Fund LLC (the “Original Falcon Fund”) in exchange for 50% of the sharing percentage of any distribution by the Original Falcon Fund. In December 2021, we agreed to commit an additional \$50.0 million to a newly formed entity, CrowdStrike Falcon Fund II LLC (“Falcon Fund II”) in exchange for 50% of the sharing percentage of any distribution by Falcon Fund II. Further, entities associated with Accel also agreed to commit up to \$10.0 million and \$50.0 million, respectively, to the Original Falcon Fund and Falcon Fund II (collectively, the “Falcon Funds”), and collectively own the remaining 50% of the sharing percentage of the Falcon Funds. Both Falcon Funds are in the business of purchasing, selling, and investing in minority equity and convertible debt securities of privately-held companies that develop applications that have potential for substantial contribution to us and our platform. We are the manager of the Falcon Funds and control their investment decisions and day-to-day operations and accordingly have consolidated each of the Falcon Funds. Each Falcon Fund has a duration of ten years and may be extended for three additional years. At dissolution, the Falcon Funds will be liquidated, and the remaining assets will be distributed to the investors based on their respective sharing percentage.

Contractual Obligations and Commitments

Our commitments consist of obligations under non-cancellable real estate arrangements on an undiscounted basis, of which \$14.1 million is due in the next 12 months and \$35.6 million is due thereafter. In addition, we have debt obligations related to \$750.0 million aggregate principal amount of the Senior Notes due in fiscal 2030 and the interest payments associated with the Senior Notes of \$22.5 million due in the next 12 months and \$78.8 million due thereafter. We have non-cancellable purchase commitments with various parties to purchase products and services entered in the normal course of business totaling \$2.7 billion as of January 31, 2025, with remaining terms in excess of 12 months. We expect to fund these obligations with cash flows from operations and cash on our balance sheet.

As of January 31, 2025, our unrecognized tax benefits included \$53.1 million, which were classified as long-term liabilities due to the inherent uncertainty with respect to the timing of future cash outflows associated with our unrecognized tax benefits.

As of January 31, 2025, we had non-cancellable unfunded commitments from our financing arrangements totaling approximately \$94.2 million.

Critical Accounting Policies and Estimates

Our management's discussion and analysis of financial condition and results of operations is based upon our consolidated financial statements and notes to our consolidated financial statements, which were prepared in accordance with U.S. GAAP. The preparation of the consolidated financial statements requires our management to make estimates and assumptions that affect the amounts reported in the consolidated financial statements and accompanying notes. See Note 1, Description of Business and Significant Accounting Policies to our consolidated financial statements included in Item 8, Financial Statements and Supplementary Data of this Annual Report on Form 10-K. We base our estimates and judgments on our historical experience, knowledge of factors affecting our business, and our belief as to what could occur in the future considering available information and assumptions that are believed to be reasonable under the circumstances.

The accounting estimates we use in the preparation of our consolidated financial statements will change as new events occur, more experience is acquired, additional information is obtained, and our operating environment changes. Changes in estimates are made when circumstances warrant. Such changes in estimates and refinements in estimation methodologies are reflected in our reported results of operations and, if material, the effects of changes in estimates are disclosed in the notes to our consolidated financial statements. By their nature, these estimates and judgments are subject to an inherent degree of uncertainty and actual results could differ materially from the amounts reported based on these estimates.

The critical accounting estimates, assumptions, and judgments that we believe have the most significant impact on our consolidated financial statements are described below.

Revenue Recognition

We derive our revenue predominately from subscription revenue, which is primarily based on the solutions subscribed to by the customer. We recognize subscription revenue ratably over the contract term. Our professional services are available through time and material and fixed fee agreements. Revenue from professional services is recognized as services are performed.

We enter into revenue contracts with multiple performance obligations in which a customer may purchase combinations of subscriptions, support, training, and consulting service. Judgment is required when considering the terms and conditions of these contracts. The transaction price for these contracts is allocated to the separate performance obligations on a relative standalone selling price ("SSP") basis. The SSP is the price at which we would sell promised subscription or professional services separately to a customer.

Business Combinations

We allocate the purchase price of acquired companies to the tangible and intangible assets acquired and liabilities assumed based on their estimated fair values at the acquisition date. The excess of the fair value of purchase consideration over the fair values of these identifiable assets and liabilities is recorded as goodwill. The purchase price allocation process requires management to make significant estimates and assumptions with respect to intangible assets. Although we believe the assumptions and estimates we have made are reasonable, they are based in part on historical experience, market conditions, and information obtained from management of the acquired companies and are inherently uncertain. Examples of judgments used to estimate the fair value of intangibles assets include, but are not limited to, future expected cash flows, expected customer attrition rates, estimated obsolescence rates, and discount rates. These estimates are inherently uncertain and unpredictable and, as a result, actual results may differ from estimates.

Income Taxes

We account for income taxes using the asset and liability method. Under this method, deferred tax assets and liabilities are determined based on differences between the financial statement and tax basis of assets and liabilities and net operating loss and credit carryforwards using enacted tax rates in effect for the year in which the differences are expected to reverse. Valuation allowances are established when necessary to reduce deferred tax assets to the amounts expected to be realized.

We account for unrecognized tax benefits using a more-likely-than-not threshold for financial statement recognition and measurement of tax positions taken or expected to be taken in a tax return. We establish a liability for tax-related uncertainties based on estimates of whether, and the extent to which, additional taxes will be due. Our assumptions, judgments, and estimates relative to the current provision for income taxes take into account current tax laws, our interpretation of current tax laws, and possible outcomes of current and future audits conducted by foreign and domestic tax authorities. We have established reserves for income taxes to address potential exposures involving tax positions that could be challenged by tax authorities. In addition, we are subject to the continual examination of our income tax returns by the U.S. Internal Revenue Service (“IRS”) and other domestic and foreign tax authorities. We regularly assess the likelihood of outcomes resulting from these examinations to determine the adequacy of our provision for income taxes and have reserved for potential adjustments that may result from such examinations. We believe such estimates to be reasonable; however, the final determination of any of these examinations could significantly impact the amounts provided for income taxes in our consolidated financial statements.

Recently Issued Accounting Pronouncements

See Note 1, Description of Business and Significant Accounting Policies, included in Part II, Item 8 of this Annual Report on Form 10-K for more information about the impact of certain recent accounting pronouncements on our consolidated financial statements.

ITEM 7A. QUANTITATIVE AND QUALITATIVE DISCLOSURES ABOUT MARKET RISK

We have operations in the United States and internationally, and we are exposed to market risk in the ordinary course of business.

Interest Rate Risk

Our cash and cash equivalents primarily consist of cash on hand and highly liquid investments in money market funds, U.S. Treasury bills, and time deposits. Our short-term investments consist of U.S. Treasury bills and time deposits. Our investments do not have significant interest rate risk, as the yields on our investments are fixed rates. As of January 31, 2025, we had cash and cash equivalents of \$4.3 billion. As of January 31, 2024, we had cash and cash equivalents of \$3.4 billion and short-term investments of \$99.6 million. The primary objectives of our investment activities are the preservation of capital, the fulfillment of liquidity needs, and the fiduciary control of cash and investments. We do not enter into investments for trading or speculative purposes. The effect of a hypothetical 100 basis point change in interest rates would not have had a material effect on the fair market value of our portfolio as of January 31, 2025 or January 31, 2024. We therefore do not expect our results of operations or cash flows to be materially affected by a sudden change in market interest rates.

Our debt obligations consist of a variety of financial instruments that expose us to interest rate risk, including, but not limited to our revolving credit facility and the Senior Notes. The interest on the revolving credit facility is tied to short-term interest rate benchmarks including the Term SOFR. The interest rate on the Senior Notes is fixed.

Foreign Currency Risk

To date, nearly all of our sales contracts have been denominated in U.S. dollars. A portion of our operating expenses are incurred outside the United States, denominated in foreign currencies, and subject to fluctuations due to changes in foreign currency exchange rates, particularly changes in the British Pound, Australian Dollar, and Euro. The functional currencies of our foreign subsidiaries are generally the country's local currency. Foreign currency transaction gains and losses are recorded to other income (expense), net. A hypothetical 10% adverse change in the U.S. dollar against other currencies would have resulted in an increase in operating loss of approximately \$108.3 million, \$75.8 million and \$55.5 million for the fiscal years ended January 31, 2025, January 31, 2024 and January 31, 2023 respectively. We have not entered into derivative or hedging transactions, but we may do so in the future if our exposure to foreign currency becomes more significant.

Inflation Rate Risk

We do not believe that inflation had a material effect on our business, financial condition, or results of operations during the fiscal years ended January 31, 2025, January 31, 2024, or January 31, 2023. If our costs were to become subject to significant inflationary pressures, we may not be able to fully offset such higher costs through price increases. Our inability or failure to do so could harm our business, financial condition, and results of operations.

ITEM 8. FINANCIAL STATEMENTS AND SUPPLEMENTARY DATA

Index to Consolidated Financial Statements

| | Page |
|--|-------------|
| Report of Independent Registered Public Accounting Firm (PCAOB ID 238) | 78 |
| Consolidated Financial Statements | |
| Consolidated Balance Sheets as of January 31, 2025 and 2024 | 80 |
| Consolidated Statements of Operations for the years ended January 31, 2025, 2024 and 2023 | 81 |
| Consolidated Statements of Comprehensive Income (Loss) for the years ended January 31, 2025, 2024 and 2023 | 82 |
| Consolidated Statements of Stockholders' Equity for the years ended January 31, 2025, 2024 and 2023 | 83 |
| Consolidated Statements of Cash Flows for the years ended January 31, 2025, 2024 and 2023 | 84 |
| Notes to Consolidated Financial Statements | 86 |

Report of Independent Registered Public Accounting Firm

To the Board of Directors and Stockholders of CrowdStrike Holdings, Inc.

Opinions on the Financial Statements and Internal Control over Financial Reporting

We have audited the accompanying consolidated balance sheets of CrowdStrike Holdings, Inc. and its subsidiaries (the "Company") as of January 31, 2025 and 2024, and the related consolidated statements of operations, of comprehensive income (loss), of stockholders' equity and of cash flows for each of the three years in the period ended January 31, 2025, including the related notes (collectively referred to as the "consolidated financial statements"). We also have audited the Company's internal control over financial reporting as of January 31, 2025, based on criteria established in Internal Control - Integrated Framework (2013) issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

In our opinion, the consolidated financial statements referred to above present fairly, in all material respects, the financial position of the Company as of January 31, 2025 and 2024, and the results of its operations and its cash flows for each of the three years in the period ended January 31, 2025 in conformity with accounting principles generally accepted in the United States of America. Also in our opinion, the Company maintained, in all material respects, effective internal control over financial reporting as of January 31, 2025, based on criteria established in Internal Control - Integrated Framework (2013) issued by the COSO.

Basis for Opinions

The Company's management is responsible for these consolidated financial statements, for maintaining effective internal control over financial reporting, and for its assessment of the effectiveness of internal control over financial reporting, included in Management's Report on Internal Control over Financial Reporting appearing under Item 9A. Our responsibility is to express opinions on the Company's consolidated financial statements and on the Company's internal control over financial reporting based on our audits. We are a public accounting firm registered with the Public Company Accounting Oversight Board (United States) (PCAOB) and are required to be independent with respect to the Company in accordance with the U.S. federal securities laws and the applicable rules and regulations of the Securities and Exchange Commission and the PCAOB.

We conducted our audits in accordance with the standards of the PCAOB. Those standards require that we plan and perform the audits to obtain reasonable assurance about whether the consolidated financial statements are free of material misstatement, whether due to error or fraud, and whether effective internal control over financial reporting was maintained in all material respects.

Our audits of the consolidated financial statements included performing procedures to assess the risks of material misstatement of the consolidated financial statements, whether due to error or fraud, and performing procedures that respond to those risks. Such procedures included examining, on a test basis, evidence regarding the amounts and disclosures in the consolidated financial statements. Our audits also included evaluating the accounting principles used and significant estimates made by management, as well as evaluating the overall presentation of the consolidated financial statements. Our audit of internal control over financial reporting included obtaining an understanding of internal control over financial reporting, assessing the risk that a material weakness exists, and testing and evaluating the design and operating effectiveness of internal control based on the assessed risk. Our audits also included performing such other procedures as we considered necessary in the circumstances. We believe that our audits provide a reasonable basis for our opinions.

Definition and Limitations of Internal Control over Financial Reporting

A company's internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles. A company's internal control over financial reporting includes those policies and procedures that (i) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company; (ii) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company; and (iii) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the company's assets that could have a material effect on the financial statements.

Because of its inherent limitations, internal control over financial reporting may not prevent or detect misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

Critical Audit Matters

The critical audit matter communicated below is a matter arising from the current period audit of the consolidated financial statements that was communicated or required to be communicated to the audit committee and that (i) relates to accounts or disclosures that are material to the consolidated financial statements and (ii) involved our especially challenging, subjective, or complex judgments. The communication of critical audit matters does not alter in any way our opinion on the consolidated financial statements, taken as a whole, and we are not, by communicating the critical audit matter below, providing a separate opinion on the critical audit matter or on the accounts or disclosures to which it relates.

Revenue Recognition – Subscription Revenue

As described in Note 1 to the consolidated financial statements, subscription revenues are primarily comprised of fees that give customers access to the ordered service, related support and updates, if any, during the subscription term. The Company initially records the subscription fees as deferred revenue and recognizes revenue on a straight-line basis over the term of the agreement. The Company recognized consolidated subscription revenue of \$3,761.5 million for the year ended January 31, 2025.

The principal consideration for our determination that performing procedures relating to revenue recognition for subscription revenue is a critical audit matter is a high degree of auditor effort in performing procedures relating to the Company's subscription revenue recognition.

Addressing the matter involved performing procedures and evaluating audit evidence in connection with forming our overall opinion on the consolidated financial statements. These procedures included testing the effectiveness of controls relating to the subscription revenue recognition process. These procedures also included, among others (i) testing subscription revenue recognized for a sample of revenue transactions by obtaining and inspecting source documents, such as agreements, evidence of delivery of the service, invoices, and receipt of payment and (ii) confirming a sample of outstanding customer invoice balances as of January 31, 2025 and, for confirmations not returned, obtaining and inspecting source documents, such as agreements, evidence of delivery of the service, invoices, and subsequent receipt of payment.

/s/ PricewaterhouseCoopers LLP
San Jose, California
March 10, 2025

CrowdStrike Holdings, Inc.
Consolidated Balance Sheets
(in thousands, except per share data)

| | January 31, | |
|--|---------------------|---------------------|
| | 2025 | 2024 |
| Assets | | |
| Current assets: | | |
| Cash and cash equivalents | \$ 4,323,295 | \$ 3,375,069 |
| Short-term investments | — | 99,591 |
| Accounts receivable, net of allowance for credit losses of \$2.8 million and \$2.2 million as of January 31, 2025 and January 31, 2024, respectively | 1,128,564 | 853,105 |
| Deferred contract acquisition costs, current | 347,042 | 246,370 |
| Prepaid expenses and other current assets | 314,444 | 183,172 |
| Total current assets | 6,113,345 | 4,757,307 |
| Strategic investments | 72,544 | 56,244 |
| Property and equipment, net | 788,640 | 620,172 |
| Operating lease right-of-use assets | 42,763 | 48,211 |
| Deferred contract acquisition costs, noncurrent | 500,908 | 335,933 |
| Goodwill | 912,805 | 638,041 |
| Intangible assets, net | 133,114 | 114,518 |
| Other long-term assets | 137,459 | 76,094 |
| Total assets | <u>\$ 8,701,578</u> | <u>\$ 6,646,520</u> |
| Liabilities and Stockholders' Equity | | |
| Current liabilities: | | |
| Accounts payable | \$ 130,887 | \$ 28,180 |
| Accrued expenses | 191,349 | 125,896 |
| Accrued payroll and benefits | 319,243 | 234,624 |
| Operating lease liabilities, current | 13,811 | 14,150 |
| Deferred revenue | 2,733,005 | 2,270,757 |
| Other current liabilities | 72,755 | 23,672 |
| Total current liabilities | 3,461,050 | 2,697,279 |
| Long-term debt | 743,983 | 742,494 |
| Deferred revenue, noncurrent | 995,672 | 783,342 |
| Operating lease liabilities, noncurrent | 31,107 | 36,230 |
| Other liabilities, noncurrent | 150,849 | 50,086 |
| Total liabilities | 5,382,661 | 4,309,431 |
| Commitments and contingencies (Note 10) | | |
| Stockholders' Equity | | |
| Preferred stock, \$0.0005 par value; 100,000 shares authorized as of January 31, 2025 and January 31, 2024; no shares issued and outstanding as of January 31, 2025 and January 31, 2024. | — | — |
| Class A common stock, \$0.0005 par value; 2,000,000 shares authorized as of January 31, 2025 and January 31, 2024; 247,872 shares, and 229,380 shares issued and outstanding as of January 31, 2025 and January 31, 2024, respectively; Class B common stock, \$0.0005 par value; 92,364 shares and 300,000 shares authorized as of January 31, 2025 and January 31, 2024, respectively; 0 shares, and 12,485 shares issued and outstanding as of January 31, 2025 and January 31, 2024, respectively. | 124 | 121 |
| Additional paid-in capital | 4,367,070 | 3,364,328 |
| Accumulated deficit | (1,078,107) | (1,058,836) |
| Accumulated other comprehensive loss | (9,593) | (1,663) |
| Total CrowdStrike Holdings, Inc. stockholders' equity | 3,279,494 | 2,303,950 |
| Non-controlling interest | 39,423 | 33,139 |
| Total stockholders' equity | 3,318,917 | 2,337,089 |
| Total liabilities and stockholders' equity | <u>\$ 8,701,578</u> | <u>\$ 6,646,520</u> |

The accompanying notes are an integral part of these consolidated financial statements.

CrowdStrike Holdings, Inc.
Consolidated Statements of Operations
(in thousands, except per share data)

| | Year Ended January 31, | | |
|--|-------------------------------|------------------|---------------------|
| | 2025 | 2024 | 2023 |
| Revenue | | | |
| Subscription | \$ 3,761,480 | \$ 2,870,557 | \$ 2,111,660 |
| Professional services | 192,144 | 184,998 | 129,576 |
| Total revenue | 3,953,624 | 3,055,555 | 2,241,236 |
| Cost of revenue | | | |
| Subscription | 835,509 | 630,745 | 511,684 |
| Professional services | 155,972 | 124,978 | 89,547 |
| Total cost of revenue | 991,481 | 755,723 | 601,231 |
| Gross profit | 2,962,143 | 2,299,832 | 1,640,005 |
| Operating expenses | | | |
| Sales and marketing | 1,523,356 | 1,140,566 | 904,409 |
| Research and development | 1,076,901 | 768,497 | 608,364 |
| General and administrative | 482,316 | 392,764 | 317,344 |
| Total operating expenses | 3,082,573 | 2,301,827 | 1,830,117 |
| Loss from operations | (120,430) | (1,995) | (190,112) |
| Interest expense | (26,311) | (25,756) | (25,319) |
| Interest income | 196,174 | 148,930 | 52,495 |
| Other income, net | 5,101 | 1,638 | 3,053 |
| Income (loss) before provision for income taxes | 54,534 | 122,817 | (159,883) |
| Provision for income taxes | 71,130 | 32,232 | 22,402 |
| Net income (loss) | (16,596) | 90,585 | (182,285) |
| Net income attributable to non-controlling interest | 2,675 | 1,258 | 960 |
| Net income (loss) attributable to CrowdStrike | <u>\$ (19,271)</u> | <u>\$ 89,327</u> | <u>\$ (183,245)</u> |
| Net income (loss) per share attributable to CrowdStrike common stockholders: | | | |
| Basic | <u>\$ (0.08)</u> | <u>\$ 0.37</u> | <u>\$ (0.79)</u> |
| Diluted | <u>\$ (0.08)</u> | <u>\$ 0.37</u> | <u>\$ (0.79)</u> |
| Weighted-average shares used in computing net income (loss) per share attributable to CrowdStrike common stockholders: | | | |
| Basic | <u>244,750</u> | <u>238,637</u> | <u>233,139</u> |
| Diluted | <u>244,750</u> | <u>243,635</u> | <u>233,139</u> |

The accompanying notes are an integral part of these consolidated financial statements.

CrowdStrike Holdings, Inc.
Consolidated Statements of Comprehensive Income (Loss)
(in thousands)

| | Year Ended January 31, | | |
|---|-------------------------------|------------------|---------------------|
| | 2025 | 2024 | 2023 |
| Net income (loss) | \$ (16,596) | \$ 90,585 | \$ (182,285) |
| Other comprehensive income (loss): | | | |
| Foreign currency translation adjustments | (8,631) | (594) | 221 |
| Unrealized gain (loss) on cash equivalents and short-term investments, net of tax | 701 | (50) | — |
| Other comprehensive income (loss) | (7,930) | (644) | 221 |
| Less: Comprehensive income attributable to non-controlling interest | 2,675 | 1,258 | 960 |
| Total comprehensive income (loss) attributable to CrowdStrike | <u>\$ (27,201)</u> | <u>\$ 88,683</u> | <u>\$ (183,024)</u> |

The accompanying notes are an integral part of these consolidated financial statements.

CrowdStrike Holdings, Inc.
Consolidated Statements of Stockholders' Equity
(in thousands)

| | Common Stock | | Additional | Accumulated | Other | Non- | Total |
|---|----------------|---------------|---------------------|-----------------------|-------------------|------------------|---------------------|
| | Shares | Amount | Paid-in | Deficit | Comprehensive | controlling | Stockholders' |
| | | | Capital | | Income (Loss) | Interest | Equity |
| Balances at January 31, 2022 | 230,706 | \$ 115 | \$ 1,991,807 | \$ (964,918) | \$ (1,240) | \$ 11,879 | \$ 1,037,643 |
| Issuance of common stock upon exercise of options | 1,032 | 3 | 8,652 | — | — | — | 8,655 |
| Issuance of common stock under RSU and PSU release | 3,444 | — | — | — | — | — | — |
| Issuance of common stock under employee stock purchase plan | 517 | — | 59,419 | — | — | — | 59,419 |
| Issuance of common stock for restricted stock awards | 6 | — | — | — | — | — | — |
| Vesting of early exercised options | — | — | 2,204 | — | — | — | 2,204 |
| Issuance of common stock for founders holdbacks related to acquisitions | 72 | — | 10,645 | — | — | — | 10,645 |
| Stock-based compensation expense, net of founder revest | — | — | 519,735 | — | — | — | 519,735 |
| Capitalized stock-based compensation | — | — | 20,193 | — | — | — | 20,193 |
| Fair value of replacement equity awards attributable to pre-acquisition service | — | — | 50 | — | — | — | 50 |
| Net income (loss) | — | — | — | (183,245) | — | 960 | (182,285) |
| Non-controlling interest | — | — | — | — | — | 10,954 | 10,954 |
| Other comprehensive income | — | — | — | — | 221 | — | 221 |
| Balances at January 31, 2023 | 235,777 | \$ 118 | \$ 2,612,705 | \$ (1,148,163) | \$ (1,019) | \$ 23,793 | \$ 1,487,434 |
| Issuance of common stock upon exercise of options | 1,146 | 2 | 8,693 | — | — | — | 8,695 |
| Issuance of common stock under RSU and PSU release | 4,041 | — | — | — | — | — | — |
| Issuance of common stock under employee stock purchase plan | 747 | 1 | 76,374 | — | — | — | 76,375 |
| Issuance of common stock for restricted stock awards | 125 | — | — | — | — | — | — |
| Issuance of common stock for founders holdbacks related to acquisitions | 27 | — | 4,314 | — | — | — | 4,314 |
| Issuance of common stock for payment of board of director fees | 2 | — | 344 | — | — | — | 344 |
| Stock-based compensation expense, net of founder revest | — | — | 626,861 | — | — | — | 626,861 |
| Capitalized stock-based compensation | — | — | 34,385 | — | — | — | 34,385 |
| Fair value of replacement equity awards attributable to pre-acquisition service | — | — | 652 | — | — | — | 652 |
| Net income | — | — | — | 89,327 | — | 1,258 | 90,585 |
| Non-controlling interest | — | — | — | — | — | 8,088 | 8,088 |
| Other comprehensive loss | — | — | — | — | (644) | — | (644) |
| Balances at January 31, 2024 | 241,865 | \$ 121 | \$ 3,364,328 | \$ (1,058,836) | \$ (1,663) | \$ 33,139 | \$ 2,337,089 |
| Issuance of common stock upon exercise of options | 514 | — | 3,983 | — | — | — | 3,983 |
| Issuance of common stock under RSU and PSU release | 4,552 | 3 | (3) | — | — | — | — |
| Issuance of common stock under employee stock purchase plan | 858 | — | 99,616 | — | — | — | 99,616 |
| Issuance of common stock for restricted stock awards | 72 | — | — | — | — | — | — |
| Issuance of common stock for founders holdbacks related to acquisitions | 11 | — | 3,555 | — | — | — | 3,555 |
| Issuance of common stock for payment of board of director fees | — | — | 348 | — | — | — | 348 |
| Stock-based compensation expense, net of founder revest | — | — | 857,129 | — | — | — | 857,129 |
| Capitalized stock-based compensation | — | — | 36,959 | — | — | — | 36,959 |
| Fair value of replacement equity awards attributable to pre-acquisition service | — | — | 1,155 | — | — | — | 1,155 |
| Net income (loss) | — | — | — | (19,271) | — | 2,675 | (16,596) |
| Non-controlling interest | — | — | — | — | — | 3,609 | 3,609 |
| Other comprehensive loss | — | — | — | — | (7,930) | — | (7,930) |
| Balances at January 31, 2025 | 247,872 | \$ 124 | \$ 4,367,070 | \$ (1,078,107) | \$ (9,593) | \$ 39,423 | \$ 3,318,917 |

The accompanying notes are an integral part of these consolidated financial statements.

CrowdStrike Holdings, Inc.
Consolidated Statements of Cash Flows
(in thousands)

| | Year Ended January 31, | | |
|--|------------------------|--------------|--------------|
| | 2025 | 2024 | 2023 |
| Operating activities | | | |
| Net income (loss) | \$ (16,596) | \$ 90,585 | \$ (182,285) |
| Adjustments to reconcile net income (loss) to net cash provided by operating activities: | | | |
| Depreciation and amortization | 187,952 | 126,838 | 77,245 |
| Amortization of intangible assets | 26,004 | 18,416 | 16,565 |
| Amortization of deferred contract acquisition costs | 318,837 | 238,901 | 170,808 |
| Non-cash operating lease cost | 15,283 | 13,398 | 9,440 |
| Stock-based compensation expense | 865,421 | 631,519 | 526,504 |
| Deferred income taxes | (9,903) | (3,387) | 1,306 |
| Realized gains on strategic investments | (6,321) | (3,936) | — |
| Accretion of short-term investments purchased at a discount | 2,285 | (2,285) | — |
| Non-cash interest expense | 3,763 | 3,173 | 2,813 |
| Change in fair value of strategic investments | 1,000 | 1,459 | (1,830) |
| Changes in operating assets and liabilities, net of impact of acquisitions | | | |
| Accounts receivable, net | (274,219) | (217,699) | (258,109) |
| Deferred contract acquisition costs | (584,484) | (371,649) | (298,716) |
| Prepaid expenses and other assets | (190,232) | (102,520) | (46,807) |
| Accounts payable | 84,939 | (18,898) | (15,463) |
| Accrued expenses and other liabilities | 218,518 | 14,586 | 58,923 |
| Accrued payroll and benefits | 85,873 | 65,102 | 65,226 |
| Operating lease liabilities | (15,657) | (14,035) | (10,364) |
| Deferred revenue | 669,264 | 696,639 | 825,751 |
| Net cash provided by operating activities | 1,381,727 | 1,166,207 | 941,007 |
| Investing activities | | | |
| Purchases of property and equipment | (254,852) | (176,529) | (235,019) |
| Capitalized internal-use software and website development costs | (58,969) | (49,457) | (29,095) |
| Purchases of strategic investments | (19,702) | (17,177) | (21,808) |
| Proceeds from sales of strategic investments | 12,507 | 2,000 | — |
| Business acquisitions, net of cash acquired | (310,257) | (239,030) | (18,349) |
| Purchases of intangible assets | — | (11,126) | (2,323) |
| Purchases of short-term investments | — | (195,581) | (250,000) |
| Proceeds from maturities and sales of short-term investments | 97,300 | 348,281 | — |
| Purchases of deferred compensation investments | (2,721) | (2,031) | (64) |
| Proceeds from the sale of deferred compensation investments | 106 | — | — |
| Net cash used in investing activities | (536,588) | (340,650) | (556,658) |
| Financing activities | | | |
| Repayment of loan payable | — | — | (1,591) |
| Proceeds from issuance of common stock upon exercise of stock options | 3,983 | 8,695 | 8,655 |
| Proceeds from issuance of common stock under the employee stock purchase plan | 99,616 | 76,375 | 59,419 |
| Distributions to non-controlling interest holders | (4,891) | — | — |
| Capital contributions from non-controlling interest holders | 8,500 | 8,088 | 10,954 |
| Net cash provided by financing activities | 107,208 | 93,158 | 77,437 |
| Effect of foreign exchange rates on cash, cash equivalents and restricted cash | (5,278) | 1,958 | (1,495) |
| Net increase in cash, cash equivalents and restricted cash | 947,069 | 920,673 | 460,291 |
| Cash, cash equivalents and restricted cash at beginning of period | 3,377,597 | 2,456,924 | 1,996,633 |
| Cash, cash equivalents and restricted cash at end of period | \$ 4,324,666 | \$ 3,377,597 | \$ 2,456,924 |
| Cash, cash equivalents and restricted cash at the end of period: | | | |
| Cash and cash equivalents | 4,323,295 | 3,375,069 | 2,455,369 |

| | | | |
|---|-----------|------------|-----------|
| Restricted cash included in prepaid expenses and other assets | 1,371 | 2,528 | 1,555 |
| Total cash, cash equivalents and restricted cash shown in the consolidated statements of cash flows | 4,324,666 | 3,377,597 | 2,456,924 |
| Supplemental disclosure of cash flow information: | | | |
| Interest paid | \$ 22,500 | \$ 22,500 | \$ 22,551 |
| Income taxes paid, net of refunds received | \$ 19,022 | \$ 22,608 | \$ 11,943 |
| Supplemental disclosure of non-cash investing and financing activities: | | | |
| Net increase (decrease) in property and equipment included in accounts payable and accrued expenses | \$ 9,452 | \$ (3,081) | \$ 22,421 |
| Vesting of early exercised stock options | \$ — | \$ — | \$ 2,204 |
| Equity consideration for acquisitions | \$ 1,155 | \$ 652 | \$ 50 |
| Operating lease liabilities arising from obtaining operating right of-use assets | \$ 6,821 | \$ 16,445 | \$ 18,464 |
| Proceeds from sales of strategic investments not yet received | \$ 4,992 | \$ 8,774 | \$ — |
| Stock-based compensation included in capitalized software development costs and fixed assets | \$ 36,959 | \$ 31,919 | \$ 20,193 |
| Noncash consideration for the purchase of strategic investments | \$ 3,319 | \$ — | \$ — |
| Noncash consideration received from sales of strategic investments | \$ 3,319 | \$ — | \$ — |

The accompanying notes are an integral part of these consolidated financial statements.

1. Description of Business and Significant Accounting Policies

Business

CrowdStrike Holdings, Inc. (and/or its subsidiaries, as applicable, the “Company”) was formed on November 7, 2011. The Company is a global cybersecurity leader that delivers cybersecurity’s AI-native platform for the XDR era, purpose-built to stop breaches. The Company’s unified platform provides cloud-delivered protection of endpoints, cloud workloads, identity, and data via a software as a service (“SaaS”) subscription-based model that spans multiple large security markets, including corporate endpoint security, security and IT operations, managed security services, next-gen SIEM, cloud security, identity protection, threat intelligence, data protection, exposure management and cybersecurity generative AI. The Company conducts its business in the United States, as well as locations internationally, including in Australia, Germany, India, Israel, Japan, Romania, and the United Kingdom.

Basis of Presentation

The accompanying consolidated financial statements have been prepared in conformity with U.S. generally accepted accounting principles (“U.S. GAAP”). Certain prior year information has been reclassified to conform to the current year presentation. These reclassifications had no effect on previously reported results of operations or accumulated deficit.

Principles of Consolidation

The consolidated financial statements include the accounts of the Company and its wholly owned subsidiaries. All intercompany balances and transactions have been eliminated in consolidation.

Use of Estimates

The preparation of financial statements in conformity with U.S. GAAP requires management to make estimates and assumptions that affect the amounts reported and disclosed in the Company’s consolidated financial statements and accompanying notes. These estimates are based on information available as of the date of the consolidated financial statements. On a regular basis, management evaluates these estimates and assumptions. Actual results may differ from these estimates and such differences could be material to the Company’s consolidated financial statements.

Estimates and assumptions used by management include, but are not limited to, revenue recognition, the allowance for credit losses, the useful lives of long-lived assets, the fair values of strategic investments, the period of benefit for deferred contract acquisition costs, the discount rate used for operating leases, the recognition and disclosure of contingent liabilities, income taxes, stock-based compensation, and the fair value of assets acquired and liabilities assumed in business combinations.

Concentration of Credit Risk and Geographic Information

The Company generates revenue from the sale of subscriptions to access its cloud platform and professional services. The Company’s sales team, along with its channel partner network of system integrators and value-added resellers (collectively, “channel partners”), sells the Company’s services worldwide to organizations of all sizes.

Financial instruments that potentially subject the Company to concentrations of credit risk consist of cash, cash equivalents, accounts receivable, financing receivables, and strategic investments. The Company’s cash is placed with high-credit-quality financial institutions and issuers, and at times exceeds federally insured limits. The Company has not experienced any credit loss relating to its cash, cash equivalents, short-term investments, or strategic investments. The Company performs periodic credit evaluations of its customers and generally does not require collateral.

There were no channel partners or direct customers who represented 10% or more of the Company’s accounts receivable as of January 31, 2025 and January 31, 2024.

CrowdStrike Holdings, Inc.
Notes to Consolidated Financial Statements

There were two end users who represented 10% or more of the Company's financing receivables as of January 31, 2025 representing 41% and 37%, respectively.

There were no channel partners or direct customers who represented 10% or more of the Company's total revenue during the fiscal years ended January 31, 2025, January 31, 2024, and January 31, 2023.

Fair Value of Financial Instruments

The Company's financial instruments consist of cash equivalents, short-term investments, strategic investments, accounts receivable, financing receivables, accounts payable, accrued expenses, the Senior Notes, and investments for the Company's deferred compensation plan. The carrying values of cash equivalents, short-term investments, accounts receivable, financing receivables, accounts payable, and accrued expenses approximate fair value. If these financial instruments were measured at fair value in the consolidated financial statements, money market funds, accounts receivable, accounts payable, accrued expenses, and investments for the Company's deferred compensation plan would be classified as Level 1, U.S. treasury securities included in cash equivalents and short-term investments would be classified as Level 2, and financing receivables would be classified as Level 3. The Senior Notes are carried at the initially allocated liability value less unamortized debt discount and issuance costs on the Company's consolidated balance sheets. The Company discloses the fair value of the Senior Notes at each reporting period for disclosure purposes only. The Company's investments related to the deferred compensation plan are invested within a Rabbi Trust. Participants in the deferred compensation plan may select the securities in which their compensation deferrals are invested within the confines of the Rabbi Trust. These securities are marked-to-market each reporting period. Refer to Note 2, Investments and Fair Value Measurements, regarding the fair value of the Company's financial instruments, and Note 5, Debt, for the fair value of the Company's Senior Notes.

Cash Equivalents and Short-term Investments

The Company considers all highly liquid investments with original maturities of three months or less at the date of purchase to be cash equivalents. Cash equivalents are mainly comprised of money market funds, U.S. Treasury bills, and time deposits. The Company had \$4.0 billion and \$3.1 billion of cash equivalents as of January 31, 2025 and January 31, 2024, respectively.

Short-term investments consist of U.S. Treasury bills and time deposits with original maturities greater than three months but less than one year. The Company had no short-term investments as of January 31, 2025, and \$99.6 million of short-term investments as of January 31, 2024. The Company classifies investments in U.S. Treasury bills as available-for-sale securities at the time of purchase and re-evaluates the designations as of each balance sheet date. The Company classifies its available-for-sale securities as short-term investments based on their nature and their availability for use in current operations. Available-for-sale securities are carried at fair value with unrealized gains and losses, if any, included in accumulated other comprehensive income (loss). Unrealized losses are recorded in other income, net, for declines in fair value below the cost of an individual investment that is deemed to be other-than-temporary. The Company did not identify any available-for-sale securities as other-than-temporarily impaired as of January 31, 2025 and January 31, 2024. Realized gains and losses from the sale of available-for-sale securities are determined based on a specific identification method and are recorded in other income, net.

Accounts Receivable

Accounts receivable are recorded at the invoiced amount and are non-interest bearing. Accounts receivable are stated at their net realizable value, net of the allowance for credit losses. The Company has a well-established collections history from its customers. Credit is extended to customers based on an evaluation of their financial condition and other factors. The Company generally does not require collateral from its customers; however, the Company may require payment prior to commencing service in certain instances to limit credit risk. The Company regularly reviews the adequacy of the allowance for credit losses by considering various factors including the age of each outstanding invoice, each customer's expected ability to pay, historical loss rates, and expectations of forward-looking loss estimates to determine whether the allowance is appropriate. Amounts deemed uncollectible are written off against the allowance for credit losses.

CrowdStrike Holdings, Inc.
Notes to Consolidated Financial Statements

Financing Receivables

The Company provides financing arrangements for certain qualified end-users to purchase its products and services. Payment terms on these financing arrangements are generally up to five years. Financing receivables are recorded at amortized cost, which approximates fair value. Financing receivables, with contractual maturities of one year or less, are included in prepaid expenses and other current assets, while those with contractual terms exceeding one year are included in other long-term assets on the consolidated balance sheets.

The Company evaluates the allowance for credit losses by assessing the risks and losses inherent in the financing receivables on either an individual or a collective basis. The Company's assessment considers various factors, including lifetime expected losses determined using customer risk profile, current economic conditions that may affect a customer's ability to pay, and forward-looking economic considerations. Financing receivables deemed uncollectible are charged against the allowance for credit losses.

The allowance for credit losses on off-balance sheet credit exposure is estimated at each reporting period based on the contractual period over which the Company is exposed to credit risk via a contractual obligation to extend credit, unless that obligation is unconditionally cancellable by the Company. The portion of the allowance for credit losses related to future disbursements is shown as a liability on the consolidated balance sheets, and the related expense for credit losses is reflected in the consolidated statements of operations.

Strategic Investments

In July 2019, the Company agreed to commit up to \$10.0 million to a newly formed entity, CrowdStrike Falcon Fund LLC (the "Original Falcon Fund") in exchange for 50% of the sharing percentage of any distributions by the Original Falcon Fund. In December 2021, the Company agreed to commit an additional \$50.0 million to a newly formed entity, CrowdStrike Falcon Fund II LLC ("Falcon Fund II") in exchange for 50% of the sharing percentage of any distributions by Falcon Fund II. Further, entities associated with Accel also agreed to commit up to \$10.0 million and \$50.0 million, respectively, to the Original Falcon Fund and Falcon Fund II (collectively, the "Falcon Funds"), and collectively own the remaining 50% of the sharing percentage of the Falcon Funds. Both Falcon Funds are in the business of purchasing, selling, and investing in minority equity and convertible debt securities of privately-held companies that develop applications that have potential for substantial contribution to CrowdStrike and its platform. The Company is the manager of the Falcon Funds and controls the investment decisions and day-to-day operations and accordingly has consolidated each of the Falcon Funds. Each Falcon Fund has a duration of ten years and may be extended for three additional years. At dissolution, the Falcon Funds will be liquidated, and the remaining assets will be distributed to the investors based on their respective sharing percentage.

The Company elected the measurement alternative for the non-marketable equity investments of the Falcon Funds where eligible. Under the measurement alternative, the non-marketable equity investments are measured at cost, less any impairment, plus or minus adjustments resulting from price changes from observable transactions of identical or similar securities of the same issuer. All gains and losses on strategic investments, realized and unrealized, are recognized in other income (expense), net. Strategic investments are classified within Level 3 in the fair value hierarchy as these investments do not have readily determinable market values. The carrying amount of strategic investments is adjusted based on observable price changes from observable transactions of identical or similar securities of the same issuer and other unobservable inputs including volatility, rights, and obligations of the investments, or by impairments when identified events and circumstances indicate a decline in value has occurred. The Company classifies the investments in the Falcon Funds as a non-current asset called strategic investments on the consolidated balance sheets.

Business Combinations

The Company allocates the purchase price of acquired companies to the tangible and intangible assets acquired and liabilities assumed based on their estimated fair values at the acquisition date. The excess of the fair value of purchase consideration over the fair values of these identifiable assets and liabilities is recorded as goodwill. The purchase price allocation process requires management to make significant estimates and assumptions with respect to intangible assets. Although the Company believes the assumptions and estimates it has made are reasonable, they are based in part on historical experience, market conditions, and information obtained from management of the acquired companies and are inherently uncertain. Examples of judgments used to estimate the fair value of intangibles assets include, but are not limited to, future expected cash flows, expected customer attrition rates, estimated obsolescence rates, and discount rates. These estimates are

CrowdStrike Holdings, Inc.
Notes to Consolidated Financial Statements

inherently uncertain and unpredictable and, as a result, actual results may differ from estimates. During the measurement period, which is one year from the acquisition date, the Company may record adjustments to the assets acquired and liabilities assumed, with the corresponding offset to goodwill. Upon the conclusion of the measurement period, any subsequent adjustments are recorded in the consolidated statements of operations.

Goodwill and Intangible Assets

The Company evaluates and tests goodwill for impairment at least annually, on January 31, or more frequently if circumstances indicate that goodwill may not be recoverable. A qualitative assessment is performed to determine whether the existence of events or circumstances leads to a determination that it is more likely than not that the fair value of its one reporting unit is less than its carrying value. In assessing the qualitative factors, the Company considers the impact of certain key factors including macroeconomic conditions, industry and market considerations, management turnover, changes in regulation, litigation matters, changes in enterprise value, and overall financial performance. If the Company determines it is more likely than not that the fair value of its one reporting unit is less than its carrying value, a quantitative test is performed by estimating the fair value of its reporting unit, including goodwill, and comparing it to its carrying value. If the fair value is lower than the carrying value, the excess is recognized as an impairment loss. No impairment losses were recorded during the fiscal years ended January 31, 2025, January 31, 2024, or January 31, 2023. See Note 4, Balance Sheet Components, and Note 12, Acquisitions, to the consolidated financial statements for more information.

Acquired intangible assets mainly consisting of developed technology, customer relationships, intellectual property and other acquired intangible assets are stated at fair value at the acquisition date and are amortized on a straight-line basis over their estimated economic lives, which are generally one to 20 years. The Company reviews the carrying amounts of intangible assets for impairment whenever events or changes in circumstances indicate that the carrying amount of the assets may not be recoverable. The impairment to be recognized equals the amount by which the carrying value of the asset exceeds its fair value. No impairment indicators were identified by the Company, and no impairment losses were recorded by the Company during the fiscal years ended January 31, 2025, January 31, 2024, and January 31, 2023.

Property and Equipment, Net

Property and equipment, net, is stated at historical cost less accumulated depreciation and amortization. Depreciation and amortization are calculated using the straight-line method over the estimated useful lives of the assets as follows:

| | |
|---|--|
| Data center and other computer equipment | 3 – 5 years |
| Furniture and equipment | 5 years |
| Purchased software | 3 – 5 years |
| Capitalized internal-use software and website development | 3 years |
| Leasehold improvements | Estimated useful life or term of the lease, whichever is shorter |

Expenditures for routine maintenance and repairs are charged to operating expense as incurred. Major renewals and improvements are capitalized and depreciated over their estimated useful lives.

The Company reviews for impairment of long-lived assets whenever events or changes in circumstances indicate that the carrying amount of the asset (or asset group) may not be recoverable. Events and changes in circumstances considered by the Company in determining whether the carrying value of long-lived assets may not be recoverable, include, but are not limited to, significant changes in performance relative to expected operating results, significant changes in the use of the assets, significant negative industry or economic trends, and changes in the Company's business strategy. Impairment testing is performed at an asset level that represents the lowest level for which identifiable cash flows are largely independent of the cash flows of other assets and liabilities (an "asset group"). An impairment loss would be recognized when estimated future cash flows expected to result from the use of the asset (or asset group) and its eventual disposition are less than its carrying amount. No impairment indicators were identified by the Company, and no impairment losses were recorded by the Company during the fiscal years ended January 31, 2025, January 31, 2024, and January 31, 2023.

Capitalized Internal-Use Software and Website Development Costs

The Company capitalizes certain development costs incurred in connection with its internal-use software and website development. These capitalized costs are primarily related to the Company's cybersecurity platform, as well as redefining, redesigning, and rebuilding crowdstrike.com. Costs incurred in the preliminary stages of development are expensed as incurred. Once an application has reached the development stage, internal and external costs, if direct, are capitalized until the internal-use software and website are substantially complete and ready for their intended use. The Company contracts with third party information technology providers for various service arrangements including software, platform, and information technology infrastructure. The Company capitalizes the implementation costs incurred to develop or obtain internal-use software in such arrangements, which are recorded as part of property and equipment, net in the consolidated balance sheets. All capitalized implementation costs are amortized over the term of the arrangement, which includes reasonably certain renewals. Costs incurred during the preliminary project and post-implementation stages are expensed as the activities are performed.

Capitalization ceases upon completion of all substantial testing. The Company also capitalizes costs related to specific upgrades and enhancements when it is probable the expenditures will result in additional functionality. Capitalized costs are recorded as property and equipment, net. Maintenance and training costs are expensed as incurred. Internal-use software and website development costs are amortized to cost of revenue on a straight-line basis over its estimated useful life of three years. Management evaluates the useful lives of these assets on an annual basis and tests for impairment whenever events or changes in circumstances occur that could impact the recoverability of these assets.

Deferred Contract Acquisition Costs

Under ASC 340-40, Other Assets and Deferred Costs - Contracts with Customers, the Company capitalizes contract acquisition costs that are incremental to the acquisition of customer contracts. Contract acquisition costs are accrued and capitalized upon execution of the sales contract by the customer. Sales commissions for renewal of a contract are not considered commensurate with the commissions paid for the acquisition of the initial contract or follow-on upsell given the substantive difference in commission rates in proportion to their respective contract values. Commissions, including referral fees paid to referral partners, earned upon the initial acquisition of a contract or subsequent upsell are amortized over an estimated period of benefit of four years, while commissions earned for renewal contracts are amortized over the contractual term of the renewals. Sales commissions associated with professional service contracts are amortized ratably over an estimated period of benefit of five months.

Deferred Revenue

The deferred revenue balance consists of subscription and professional services, which have been invoiced upfront, and are recognized as revenue only when the revenue recognition criteria are met. The Company's subscription contracts are typically invoiced to its customers at the beginning of the term, or in some instances, such as in multi-year arrangements, in installments. Professional services are invoiced upfront, invoiced in installments, or invoiced as the services are performed. Accordingly, the Company's deferred revenue balance does not include revenue for future years of multi-year non-cancellable contracts that have not yet been billed.

The Company recognizes subscription revenue ratably over the contract term beginning on the commencement date of each contract, the date that services are made available to customers. The Company recognizes professional services revenue as services are delivered. Once services are available to customers, the Company records amounts due in accounts receivable and in deferred revenue. To the extent the Company bills customers in advance of the contract commencement date, the accounts receivable and corresponding deferred revenue amounts are netted to zero on the consolidated balance sheets, unless such amounts have been paid as of the balance sheet date.

Revenue Recognition

In accordance with ASU 2014-09, Revenue from Contracts with Customers ("ASC 606"), revenue is recognized when a customer obtains control of promised services. The amount of revenue recognized reflects the consideration that the Company expects to be entitled to receive in exchange for these services. To achieve the core principle of this standard, the Company applies the following five steps:

- (1) Identify the contract with a customer

CrowdStrike Holdings, Inc.
Notes to Consolidated Financial Statements

The Company considers the terms and conditions of contracts with customers and its customary business practices in identifying contracts under ASC 606. The Company determines it has a contract with a customer when the contract is approved, each party's rights regarding the services to be transferred can be identified, payment terms for the services can be identified, it has been determined that the customer has the ability and intent to pay, and the contract has commercial substance. The Company applies judgment in determining the customer's ability and intent to pay, which is based on a variety of factors, including the customer's historical payment experience or, in the case of a new customer, credit and financial information pertaining to the customer.

(2) Identify the performance obligations in the contract

Performance obligations promised in a contract are identified based on the services that will be transferred to the customer that are both capable of being distinct, whereby the customer can benefit from the service either on its own or together with other resources that are readily available from the Company or from third parties, and are distinct in the context of the contract, whereby the transfer of the services is separately identifiable from other promises in the contract. The Company's performance obligations consist of (i) subscriptions and (ii) professional services.

(3) Determine the transaction price

The transaction price is determined based on the consideration to which the Company is expected to be entitled in exchange for transferring services to the customer. Variable consideration is included in the transaction price if it is probable that a significant future reversal of cumulative revenue under the contract will not occur. None of the Company's contracts contain a significant financing component.

(4) Allocate the transaction price to performance obligations in the contract

If the contract contains a single performance obligation, the entire transaction price is allocated to the single performance obligation. Contracts that contain multiple performance obligations require an allocation of the transaction price to each performance obligation based on a relative standalone selling price ("SSP").

(5) Recognize revenue when or as performance obligations are satisfied

Revenue is recognized at the time the related performance obligation is satisfied by transferring the promised service to the customer. Revenue is recognized when control of the services is transferred to the customer, in an amount that reflects the consideration expected to be received in exchange for those services. The Company generates all its revenue from contracts with customers.

Subscription Revenue

The Company's Falcon Platform technology solutions are subscription SaaS offerings designed to continuously monitor, share, and mitigate risks from determined attackers. Subscription revenues are primarily comprised of fees that give customers access to the ordered service, related support, and updates, if any, during the subscription term. Customers do not have the right to take possession of the cloud-based software platform. Fees are based on several factors, including the solutions subscribed for by the customer and the number of endpoints purchased by the customer. The subscription fees are typically payable within 30 to 60 days after the execution of the arrangement, and thereafter upon renewal or subsequent installment. The Company initially records the subscription fees as deferred revenue and recognizes revenue on a straight-line basis over the term of the agreement.

The typical subscription term is one to three years. The Company's contracts with customers typically include a fixed amount of consideration and are generally non-cancellable and without any refund-type provisions. Customers typically have the right to terminate their contracts for cause if the Company fails to perform in accordance with the contractual terms. Some customers have the option to purchase additional subscription at a stated price. These options generally do not provide a material right as they are priced at the Company's SSP.

CrowdStrike Holdings, Inc.
Notes to Consolidated Financial Statements

Professional Services Revenue

The Company offers several types of professional services including incident response and forensic services, surge forensic and malware analysis, and attribution analysis, which are focused on responding to imminent and direct threats, assessing vulnerabilities, and recommending solutions. These services are distinct from subscription services. Professional services do not result in significant customization of the subscription service. The Company's professional services are available through time and material and fixed fee agreements. Revenue for time and material agreements is recognized as services are performed. Fixed fee contracts account for an immaterial portion of the Company's revenue.

Contracts with Multiple Performance Obligations

Some contracts with customers contain multiple promised services consisting of subscription and professional services that are distinct and accounted for separately. The transaction price is allocated to the separate performance obligations on a relative SSP basis. The SSP is the price at which the Company would sell promised subscription or professional services separately to a customer. Judgment is required to determine the SSP for each distinct performance obligation. The Company determines SSP based on its overall pricing objectives, taking into consideration the type of subscription or professional service and the number of endpoints.

Variable Consideration

Revenue from sales is recorded at the net sales price, which is the transaction price, and may include estimates of variable consideration. The amount of variable consideration that is included in the transaction price is constrained and is included in the net sales price only to the extent that it is probable that a significant reversal in the amount of the cumulative revenue will not occur when the uncertainty is resolved.

If subscriptions do not meet certain service level commitments, the Company's customers are entitled to receive service credits, and in certain cases, refunds, each representing a form of variable consideration. The Company has historically not experienced any significant incidents affecting the defined levels of reliability and performance as required by its subscription contracts. Accordingly, any estimated refunds related to these agreements in the consolidated financial statements is not material during the periods presented.

The Company provides rebates and other credits within its contracts with certain resellers, which are estimated based on the expected value to be earned or claimed on the related sales transaction. Overall, the transaction price is reduced to reflect the Company's estimate of the amount of consideration to which it is entitled based on the terms of the contract. Estimated rebates and other credits were not material during the periods presented.

Research and Development Expense

Research and development costs are expensed when incurred, except for certain internal-use software development costs, which may be capitalized as noted above. Research and development expenses consist primarily of personnel and related headcount costs, stock-based compensation expenses, costs of professional services associated with the ongoing development of the Company's technology, and allocated overhead.

Advertising

Most advertising costs are expensed as incurred, except for certain production costs that are deferred and expensed at the time the advertising first takes place. The Company incurred \$118.1 million, \$79.9 million, and \$53.8 million of advertising costs during the fiscal years ended January 31, 2025, January 31, 2024, and January 31, 2023, respectively.

Stock-Based Compensation

Compensation related to stock-based awards to employees and directors is measured and recognized in the Company's consolidated statements of operations based on the fair value of the awards granted. The Company estimates the fair value of its stock options using the Black-Scholes option-pricing model. The stock-based compensation expense relating to stock options is recognized on a straight-line basis over the period during which the employee or director is required to provide service in exchange for the award, usually the vesting period, which is generally four years.

CrowdStrike Holdings, Inc.
Notes to Consolidated Financial Statements

Restricted stock units (“RSUs”) are generally subject to a service-based vesting condition. The service-based vesting condition is generally four years. The valuation of these RSUs is based solely on the Company’s stock price on the date of grant, and the corresponding compensation expense is amortized on a straight-line basis.

Performance-based stock units (“PSUs”) are generally subject to both a service-based vesting condition and a performance-based vesting condition. The fair value of the award is equal to the Company’s stock price on the date of grant. PSUs generally vest over a four-year period, subject to continued service through the applicable vesting dates. The stock-based compensation expense relating to PSUs is recognized using the accelerated attribution method over the requisite service period when it is probable that the performance condition will be satisfied.

The Special PSU Awards are subject to the Company’s achievement of specified stock price hurdles and a service-based vesting condition. The Company measured the fair value of the Special PSU Awards using a Monte Carlo simulation valuation model. The stock-based compensation expense relating to the Special PSU Awards is recognized using the accelerated attribution method over the longer of the derived service period and the explicit service period.

Employee Stock Purchase Plan (“ESPP”) grants are measured based on the fair value at grant date using the Black-Scholes option-pricing model. The resulting stock-based compensation expense is recognized using the accelerated attribution method over a two-year offering period and is accounted for as having four separate tranches starting on the same initial enrollment date. The requisite service periods for the four tranches are approximately 6, 12, 18, and 24 months.

The Company accounts for forfeitures as they occur for all stock-based awards.

Deferred Compensation

In December 2022, the board of directors approved the CrowdStrike Inc. Deferred Compensation Plan (the “Plan”), effective January 1, 2023. The Plan is a non-qualified, deferred compensation arrangement that permits eligible employees to make 100% vested salary and incentive compensation deferrals within established limits. The Company does not make contributions to the Plan.

The Plan’s assets consist of marketable securities held in a Rabbi Trust and are included in other long-term assets in the consolidated balance sheets because they are intended to fund the Plan’s long-term liabilities. They are not available for use in the Company’s daily operations and are not intended to be sold within a short period of time after purchase. The marketable securities were recorded at fair value based on quoted market prices and were \$5.5 million and \$2.3 million as of January 31, 2025 and January 31, 2024, respectively. The deferred compensation liability was \$5.5 million and \$2.3 million as of January 31, 2025 and January 31, 2024, respectively, and is included in other liabilities, noncurrent in the consolidated balance sheets. Gains and losses on deferred compensation investments are included in other income (expense), net, and corresponding changes in the deferred compensation liability are included in operating expenses and cost of revenue. Changes in the fair value of the deferred compensation asset and liability were immaterial for the fiscal years ended January 31, 2025 and January 31, 2024.

Operating Leases

The Company enters into operating lease arrangements for real estate assets related to office space. The Company determines if an arrangement is or contains a lease at inception by evaluating various factors, including whether a vendor’s right to substitute an identified asset is substantive. Lease classification is determined at the lease commencement date, which is the date the leased assets are made available for use. Operating leases are included in operating lease right-of-use assets, operating lease liabilities, current, and operating lease liabilities, noncurrent in the consolidated balance sheets. The Company did not have any financing leases in any of the periods presented.

Operating lease right-of-use assets and lease liabilities are recognized at the lease commencement date based on the present value of lease payments over the lease term. Lease payments consist of the fixed payments under the arrangement, less any lease incentives, such as tenant improvement allowances. Variable costs, such as maintenance and utilities based on actual usage, are not included in the measurement of right-to-use (“ROU”) assets and lease liabilities but are expensed when the event determining the amount of variable consideration to be paid occurs. As the implicit rate of the leases is not determinable, the Company uses an incremental borrowing rate (“IBR”) based on the information available at the lease commencement date in determining the present value of lease payments. Lease expenses are recognized on a straight-line basis over the lease term.

CrowdStrike Holdings, Inc.
Notes to Consolidated Financial Statements

The Company uses the non-cancellable lease term when recognizing the ROU assets and lease liabilities, unless it is reasonably certain that a renewal or termination option will be exercised. The Company accounts for the lease and non-lease components as a single lease component.

Leases with a term of twelve months or less are not recognized on the consolidated balance sheets but are recognized as expense on a straight-line basis over the term of the lease.

Debt Issuance Costs

Debt issuance costs incurred in connection with securing the Company's financing arrangements are generally presented in the consolidated balance sheets as a direct deduction from the carrying amount of the outstanding borrowings, consistent with debt discounts. However, the Company has chosen to present debt issuance costs under other long-term assets for its revolving credit facility on the consolidated balance sheets regardless of whether the Company has any outstanding borrowings on the revolving credit facility. Debt issuance costs, net of accumulated amortization, were \$2.9 million and \$4.0 million as of January 31, 2025 and January 31, 2024, respectively. Debt issuance costs associated with the Senior Notes are recorded as a reduction to the carrying value of the Senior Notes on the consolidated balance sheets. The unamortized issuance costs relating to the Senior Notes were \$1.3 million and \$1.6 million as of January 31, 2025 and January 31, 2024, respectively.

All deferred financing costs are amortized to interest expense. The effective interest method is used for debt issuance costs related to the Senior Notes. Debt issuance costs related to the revolving credit facility are amortized over the term of the financing arrangement under the straight-line method. The Company's amortization of these costs was \$2.2 million, \$1.6 million, and \$1.3 million for the fiscal years ended January 31, 2025, January 31, 2024, and January 31, 2023, respectively.

Foreign Currency Translation and Transactions

The functional currencies of the Company's foreign subsidiaries are generally the country's local currency. Assets and liabilities of the subsidiaries are translated into U.S. Dollars at exchange rates in effect at the reporting date. Amounts classified in stockholders' equity (deficit) are translated at historical exchange rates. Revenue and expenses are translated at the average exchange rates during the period. The resulting translation adjustments are recorded in accumulated other comprehensive income (loss). Foreign currency transaction gains or losses, whether realized or unrealized, are reflected in the consolidated statements of operations within other income (expense), net, and have not been material for all periods presented.

Income Taxes

The Company accounts for income taxes using the asset and liability method. Under this method, deferred tax assets and liabilities are determined based on differences between the financial statement and tax basis of assets and liabilities and net operating loss and credit carryforwards using enacted tax rates in effect for the year in which the differences are expected to reverse. Valuation allowances are established when necessary to reduce deferred tax assets to the amounts expected to be realized.

The Company accounts for unrecognized tax benefits using a more-likely-than-not threshold for financial statement recognition and measurement of tax positions taken or expected to be taken in a tax return. The Company establishes a liability for tax-related uncertainties based on estimates of whether, and the extent to which, additional taxes will be due. The Company's assumptions, judgments, and estimates relative to the current provision for income taxes take into account current tax laws, the Company's interpretation of current tax laws, and possible outcomes of current and future audits conducted by foreign and domestic tax authorities. The Company has established reserves for income taxes to address potential exposures involving tax positions that could be challenged by tax authorities. In addition, the Company is subject to the continual examination of its income tax returns by the U.S. Internal Revenue Service ("IRS") and other domestic and foreign tax authorities. The Company regularly assesses the likelihood of outcomes resulting from these examinations to determine the adequacy of its provision for income taxes and have reserved for potential adjustments that may result from such examinations. The Company believes such estimates to be reasonable; however, the final determination of any of these examinations could significantly impact the amounts provided for income taxes in the Company's consolidated financial statements.

CrowdStrike Holdings, Inc.
Notes to Consolidated Financial Statements

Net Income (Loss) per Share

The Company computes basic and diluted net income (loss) per share attributable to common stockholders for Class A and Class B common stock using the two-class method required for participating securities. Under the two-class method, basic net income (loss) per share attributable to common stockholders is computed by dividing the net income (loss) attributable to common stockholders by the weighted-average number of shares of common stock outstanding during the period. On December 11, 2024, all of the Company's outstanding shares of Class B common stock were automatically converted into an equal number of shares of Class A common stock pursuant to the provisions of the Amended and Restated Certificate of Incorporation.

Diluted earnings per share attributable to common stockholders adjusts basic earnings per share for the potentially dilutive impact of outstanding stock options, RSUs, PSUs, Special PSUs, ESPP obligations, and founder holdbacks. The dilutive potential shares are computed using the treasury stock method. The effects of the outstanding stock options, RSUs, PSUs, Special PSUs, ESPP obligations, and founders holdbacks are excluded from the computation of the diluted earnings per share in periods in which the effect would be anti-dilutive.

Recently Adopted Accounting Pronouncements

In November 2023, the FASB issued ASU 2023-07, Segment Reporting (Topic 280): Improvements to Reportable Segment Disclosures. The standard requires disclosure of significant segment expenses that are regularly provided to the Chief Operating Decision Maker ("CODM") and included within each reported measure of segment profit or loss, an amount for other segment items required to reconcile the difference between segment revenue and segment expenses to segment profit or loss along with a description of their composition, and the title and position of the entity's CODM. The update also expands interim segment disclosure requirements. The new standard is effective for annual periods beginning after December 15, 2023, and interim periods within fiscal years beginning after December 15, 2024. The Company adopted this guidance during the year ended January 31, 2025. See Note 14, Segment Information for further details.

Recently Issued Accounting Pronouncements

In November 2024, the FASB issued ASU 2024-03, Income Statement—Reporting Comprehensive Income—Expense Disaggregation Disclosures. The standard requires additional disclosure of specific expense categories included in the expense captions presented on the statements of operations. The new standard can be applied either prospectively or retrospectively, and is effective for annual periods beginning after December 15, 2026 and interim reporting periods within annual reporting periods beginning after December 15, 2027. Early adoption is permitted. The Company is currently evaluating the impact of this new guidance on its disclosures within the consolidated financial statements.

In December 2023, the FASB issued ASU 2023-09, Improvements to Income Tax Disclosures, a final standard on improvements to income tax disclosures. The standard requires disaggregated information about a reporting entity's effective tax rate reconciliation, as well as information on income taxes paid. The standard is intended to benefit investors by providing more detailed income tax disclosures that would be useful in making capital allocation decisions and applies to all entities subject to income taxes. The new standard is effective for annual periods beginning after December 15, 2024. The Company does not expect the adoption of this new guidance to have a material impact on its disclosures within the consolidated financial statements.

2. Investments and Fair Value Measurements

The Company follows ASC 820, Fair Value Measurements, with respect to cash equivalents, short-term investments, and deferred compensation investments that are measured at fair value on a recurring basis. Under the standard, fair value is defined as the exit price, or the amount that would be received to sell an asset or a liability in an orderly transaction between market participants as of the measurement date. The standard also establishes a hierarchy for inputs used in measuring fair value that maximizes the use of observable inputs and minimizes the use of unobservable inputs by requiring that the most observable inputs be used when available. Observable inputs are inputs market participants would use in valuing the asset or liability based on market data obtained from sources independent of the Company. Unobservable inputs are inputs that reflect the Company's assumptions about the factors market participants would use in valuing the asset or liability based upon the best information available in the circumstances.

CrowdStrike Holdings, Inc.
Notes to Consolidated Financial Statements

The hierarchy is broken down into three levels as follows:

- Level 1 Assets and liabilities whose values are based on unadjusted quoted market prices for identical assets and liabilities in active markets
- Level 2 Assets and liabilities whose values are based on quoted prices in markets that are not active or inputs that are observable for substantially the full term of the asset or liability
- Level 3 Assets and liabilities whose values are based on prices or valuation techniques that require inputs that are both unobservable and significant to the overall fair value measurement

Categorization within the valuation hierarchy is based upon the lowest level of input that is significant to the fair value measurement.

The Company's fair value hierarchy for its financial assets and liabilities that are measured at fair value on a recurring basis are as follows (in thousands):

| | January 31, 2025 | | | | January 31, 2024 | | | |
|-----------------------------------|--------------------|--------------------|-------------|--------------------|--------------------|-------------------|-------------|--------------------|
| | Level 1 | Level 2 | Level 3 | Total | Level 1 | Level 2 | Level 3 | Total |
| Assets | | | | | | | | |
| Cash equivalents | | | | | | | | |
| Money market funds | \$1,470,040 | \$ — | \$ — | \$1,470,040 | \$2,360,173 | \$ — | \$ — | \$2,360,173 |
| U.S. Treasury securities | — | 2,490,097 | — | 2,490,097 | — | 693,599 | — | 693,599 |
| Short-term investments | | | | | | | | |
| U.S. Treasury securities | — | — | — | — | — | 99,591 | — | 99,591 |
| Other assets | | | | | | | | |
| Deferred compensation investments | 5,496 | — | — | 5,496 | 2,271 | — | — | 2,271 |
| Total assets | <u>\$1,475,536</u> | <u>\$2,490,097</u> | <u>\$ —</u> | <u>\$3,965,633</u> | <u>\$2,362,444</u> | <u>\$ 793,190</u> | <u>\$ —</u> | <u>\$3,155,634</u> |

There were no transfers between the levels of the fair value hierarchy during the periods presented.

As of January 31, 2025, and January 31, 2024, the Company's U.S. Treasury securities are carried at fair value, and there were no material realized or unrealized gains or losses, either individually or in aggregate.

The total estimated fair value of the Company's financing receivables approximates their carrying amounts as of January 31, 2025. The fair value of the Company's financing receivables is considered to be a Level 3 measurement as unobservable inputs are used in determining discounted cash flows to estimate fair value.

Strategic Investments

The Company's investments in privately held securities as of January 31, 2025, consisted of the following (in thousands):

| | Privately held equity securities | Privately held debt and other securities | Total |
|--------------------------------|----------------------------------|--|------------------|
| Initial total cost | \$ 68,140 | \$ 1,000 | \$ 69,140 |
| Cumulative net gains | 3,404 | — | 3,404 |
| Carrying amount, end of period | <u>\$ 71,544</u> | <u>\$ 1,000</u> | <u>\$ 72,544</u> |

The Company's investments in privately held securities as of January 31, 2024, consisted of the following (in thousands):

CrowdStrike Holdings, Inc.
Notes to Consolidated Financial Statements

| | Privately held equity securities | Privately held debt and other securities | Total |
|--------------------------------|-------------------------------------|--|------------------|
| Initial total cost | \$ 50,373 | \$ 1,000 | \$ 51,373 |
| Cumulative net gains | 4,871 | — | 4,871 |
| Carrying amount, end of period | <u>\$ 55,244</u> | <u>\$ 1,000</u> | <u>\$ 56,244</u> |

As of January 31, 2025, the cumulative net gains of 3.4 million are comprised of upward adjustments of 7.3 million, less downward adjustments and impairment of 3.9 million. As of January 31, 2024, the cumulative net gains of \$4.9 million are comprised of upward adjustments of \$9.3 million, less downward adjustments and impairment of \$4.4 million.

Gains and Losses on Strategic Investments

The components of gains and losses on strategic investments were as follows (in thousands):

| | Year Ended January 31, | | |
|---|------------------------|-----------------|-----------------|
| | 2025 | 2024 | 2023 |
| Unrealized gains recognized on privately held equity securities | \$ — | \$ — | \$ 4,758 |
| Unrealized losses recognized on privately held equity securities including impairment | (1,000) | (1,459) | (2,928) |
| Unrealized gains (losses), net | (1,000) | (1,459) | 1,830 |
| Realized gains recognized on sales of privately held equity securities | 6,975 | 3,936 | — |
| Realized losses recognized on sales of privately held equity securities | (654) | — | — |
| Realized gains, net | 6,321 | 3,936 | — |
| Gains on strategic investments, net | <u>\$ 5,321</u> | <u>\$ 2,477</u> | <u>\$ 1,830</u> |
| Unrealized gains (losses) recognized during the reporting period on privately held equity securities still held at the reporting date | \$ (1,000) | \$ (1,459) | \$ 1,830 |

Unrealized gains recognized on privately held equity securities includes upward adjustments from equity securities accounted for under the measurement alternative while unrealized losses recognized on privately held equity securities includes downward adjustments and impairment.

Realized gains and losses recognized on sales of privately held equity securities reflects the difference between the sale proceeds and the carrying value of the security at the beginning of the period or the purchase date, if later.

3. Financing Receivables

The Company's short-term and long-term financing receivables were as follows (in thousands):

| | January 31, 2025 |
|---|------------------|
| Short-term financing receivables, gross | \$ 9,579 |
| Unearned income | (2,339) |
| Allowance for credit losses | (76) |
| Short-term financing receivables, net | <u>\$ 7,164</u> |
| Long-term financing receivables, gross | \$ 43,235 |
| Unearned income | (5,051) |
| Allowance for credit losses | (342) |
| Long-term financing receivables, net | <u>\$ 37,842</u> |

CrowdStrike Holdings, Inc.
Notes to Consolidated Financial Statements

The Company's amortized cost basis of financing receivables categorized by internal risk rating and year of origination was as follows (in thousands):

| Internal Risk Rating ⁽¹⁾ | Year Ended January 31, 2025 |
|---|--------------------------------|
| 1 to 4 | \$ 18,413 |
| 5 to 6 | 27,011 |
| 7 to 9 | — |
| Amortized cost basis of financing receivables | <u>\$ 45,424</u> |

⁽¹⁾ Internal risk ratings are determined based on the end-user's financial condition and are categorized as 1 through 9, with the lowest rating representing the highest quality.

There were no financing receivables prior to fiscal year ended January 31, 2025.

There was no significant activity in allowance for credit losses during the year ended January 31, 2025. Past due amounts on financing receivables were not material as of January 31, 2025.

4. Balance Sheet Components

Prepaid Expenses and Other Current Assets

Prepaid expenses were 247.3 million and 144.9 million as of January 31, 2025 and January 31, 2024, respectively. Other current assets were 67.1 million and 38.3 million as of January 31, 2025 and January 31, 2024, respectively.

Property and Equipment, Net

Property and equipment, net consisted of the following (in thousands):

| | January 31, | |
|---|-------------------|-------------------|
| | 2025 | 2024 |
| Data center and other computer equipment | \$ 755,728 | \$ 525,890 |
| Capitalized internal-use software and website development costs | 265,987 | 183,117 |
| Leasehold improvements | 42,230 | 39,168 |
| Purchased software | 15,876 | 10,907 |
| Furniture and equipment | 10,485 | 8,524 |
| Construction in progress | 220,088 | 190,832 |
| | <u>1,310,394</u> | <u>958,438</u> |
| Less: Accumulated depreciation and amortization | (521,754) | (338,266) |
| Property and equipment, net | <u>\$ 788,640</u> | <u>\$ 620,172</u> |

Construction in progress primarily includes data center equipment purchased that has not yet been placed in service. Data center equipment that was purchased but not yet been placed into service was \$180.1 million and \$167.5 million as of January 31, 2025 and January 31, 2024, respectively.

Depreciation and amortization expense of property and equipment was \$188.0 million, \$126.8 million, and \$77.2 million, during the fiscal years ended January 31, 2025, January 31, 2024, and January 31, 2023, respectively.

The Company capitalized \$91.9 million, \$77.9 million, and \$49.3 million in internal-use software and website development costs during the fiscal years ended January 31, 2025, January 31, 2024, and January 31, 2023, respectively. Amortization expense associated with internal-use software and website development costs totaled \$54.8 million, \$37.3 million, and \$21.5 million during the fiscal years ended January 31, 2025, January 31, 2024, and January 31, 2023, respectively. The net book

CrowdStrike Holdings, Inc.
Notes to Consolidated Financial Statements

value of capitalized internal-use software and website development costs was \$144.0 million and \$106.9 million as of January 31, 2025 and January 31, 2024, respectively.

Intangible Assets, Net

Total intangible assets, net consisted of the following (dollars in thousands):

| | January 31, 2025 | | | Weighted-Average Remaining Useful Life (in months) |
|--|------------------------------|---------------------------------|-------------------|---|
| | Gross Carrying Amount | Accumulated Amortization | Net Amount | |
| Developed technology | \$ 168,416 | \$ 63,783 | \$ 104,633 | 55 |
| Customer relationships | 24,502 | 8,454 | 16,048 | 65 |
| Intellectual property and other acquired intangible assets | 15,837 | 3,404 | 12,433 | 112 |
| Total | <u>\$ 208,755</u> | <u>\$ 75,641</u> | <u>\$ 133,114</u> | |

| | January 31, 2024 | | | Weighted-Average Remaining Useful Life (in months) |
|--|------------------------------|---------------------------------|-------------------|---|
| | Gross Carrying Amount | Accumulated Amortization | Net Amount | |
| Developed technology | \$ 131,346 | \$ 41,854 | \$ 89,492 | 60 |
| Customer relationships | 17,027 | 5,825 | 11,202 | 68 |
| Intellectual property and other acquired intangible assets | 15,842 | 2,018 | 13,824 | 123 |
| Total | <u>\$ 164,215</u> | <u>\$ 49,697</u> | <u>\$ 114,518</u> | |

Amortization expense of intangible assets was \$26.0 million, \$18.4 million, and \$16.6 million, during the fiscal years ended January 31, 2025, January 31, 2024, and January 31, 2023, respectively.

The estimated aggregate future amortization expense of intangible assets as of January 31, 2025 was as follows (in thousands):

| | Total |
|----------------------------|-------------------|
| Fiscal 2026 | \$ 29,423 |
| Fiscal 2027 | 27,248 |
| Fiscal 2028 | 26,735 |
| Fiscal 2029 | 23,982 |
| Fiscal 2030 | 14,605 |
| Thereafter | 11,121 |
| Total amortization expense | <u>\$ 133,114</u> |

CrowdStrike Holdings, Inc.
Notes to Consolidated Financial Statements

Goodwill

The change in goodwill during the fiscal year ended January 31, 2025 consisted of the following (in thousands):

| | Amounts |
|----------------------------------|-------------------|
| Goodwill as of January 31, 2024 | \$ 638,041 |
| Goodwill acquired ⁽¹⁾ | 274,981 |
| Foreign currency translation | (217) |
| Goodwill as of January 31, 2025 | <u>\$ 912,805</u> |

(1) Goodwill acquired resulted from the acquisitions of Flow Security and A.S. Adaptive Shield Ltd. Refer to Note 12 for additional information.

Accrued Payroll and Benefits

Accrued payroll and benefits consisted of the following (in thousands):

| | January 31, | |
|--------------------------------------|--------------------|-------------------|
| | 2025 | 2024 |
| Accrued commissions | \$ 174,322 | \$ 116,870 |
| Accrued payroll and related expenses | 69,197 | 58,579 |
| Accrued bonuses | 42,510 | 36,860 |
| Employee stock purchase plan | 33,214 | 22,315 |
| Accrued payroll and benefits | <u>\$ 319,243</u> | <u>\$ 234,624</u> |

5. Debt

Secured Revolving Credit Facility

In April 2019, the Company entered into a Credit Agreement with Silicon Valley Bank and other lenders, to provide a revolving line of credit of up to \$150.0 million, including a letter of credit sub-facility in the aggregate amount of \$10.0 million, and a swingline sub-facility in the aggregate amount of \$10.0 million.

On January 4, 2021, the Company amended and restated its existing credit agreement (the “A&R Credit Agreement” and the facility thereunder the “Revolving Facility”) among CrowdStrike, Inc., as borrower, CrowdStrike Holdings, Inc., as guarantor, and Silicon Valley Bank and the other lenders party thereto, providing the Company with a revolving line of credit of up to \$750.0 million, including a letter of credit sub-facility in the aggregate amount of \$100.0 million, and a swingline sub-facility in the aggregate amount of \$50.0 million. The Company also has the option to request an incremental facility of up to an additional \$250.0 million from one or more of the lenders under the A&R Credit Agreement. The A&R Credit Agreement is guaranteed by all of the Company’s material domestic subsidiaries. The A&R Credit Agreement extended the maturity date of April 19, 2022 to January 2, 2026.

On January 6, 2022, the Company modified the A&R Credit Agreement (the “Amended A&R Credit Agreement”) among CrowdStrike, Inc., as borrower, CrowdStrike Holdings, Inc., as guarantor, and Silicon Valley Bank and the other lenders party thereto. There were no changes to the borrowing amounts or maturity date. Under the Amended A&R Credit Agreement, revolving loans are Alternate Base Rate (“ABR”) Loans. Outstanding ABR Loans incur interest at the highest of (a) the Prime Rate, as published by the Wall Street Journal, (b) the federal funds rate in effect on such day plus 0.50%, and (c) the Term Secured Overnight Finance Rate (the “Term SOFR”) for a one-month tenor in effect on such day plus 1.00%, in each case plus a margin between (0.25)% and 0.25%, depending on the senior secured leverage ratio. The Company will be charged a commitment fee of 0.15% to 0.25% per year for committed but unused amounts, depending on the senior secured leverage ratio. The financial covenants require the Company to maintain a minimum consolidated interest coverage ratio of 3.00:1.00 and a maximum total leverage ratio of 5.50:1.00 stepping down to 3.50:1.00 over time. The Company was in compliance with all of its financial covenants as of January 31, 2025.

CrowdStrike Holdings, Inc.
Notes to Consolidated Financial Statements

The Amended A&R Credit Agreement is secured by substantially all of the Company's current and future consolidated assets, property and rights, including, but not limited to, intellectual property, cash, goods, equipment, contractual rights, financial assets, and intangible assets of the Company and certain of its subsidiaries. The Amended A&R Credit Agreement contains customary covenants limiting the Company's ability and the ability of its subsidiaries to, among other things, dispose of assets, undergo a change in control, merge or consolidate, make acquisitions, incur debt, incur liens, pay dividends, repurchase stock, and make investments, in each case subject to certain exceptions.

No amounts were outstanding under the Amended A&R Credit Agreement as of January 31, 2025.

Senior Notes

On January 20, 2021, the Company issued \$750.0 million in aggregate principal amount of 3.00% Senior Notes maturing in February 2029 (the "Senior Notes"). The Senior Notes are guaranteed by the Company's subsidiaries, CrowdStrike, Inc. and CrowdStrike Financial Services, Inc., and will be guaranteed by each of the Company's existing and future domestic subsidiaries that becomes a borrower or guarantor under the A&R Credit Agreement. The Senior Notes were issued at par and bear interest at a rate of 3.00% per annum. Interest payments are payable semiannually on February 15 and August 15 of each year, commencing on August 15, 2021. The Company may voluntarily redeem the Senior Notes, in whole or in part, 1) at any time prior to February 15, 2024 at (a) 100.00% of their principal amount, plus a "make whole" premium or (b) with the net cash proceeds received from an equity offering at a redemption price equal to 103.00% of the principal amount, provided the aggregate principal amount of all such redemptions does not exceed 40% of the original aggregate principal amount of the Senior Notes; 2) at any time on or after February 15, 2024 at a prepayment price equal to 101.50% of the principal amount; 3) at any time on or after February 15, 2025 at a prepayment price equal to 100.75% of the principal amount; and 4) at any time on or after February 15, 2026 at a prepayment price equal to 100.00% of the principal amount; in each case, plus accrued and unpaid interest, if any, to but excluding, the date of redemption.

The net proceeds from the debt offering were \$738.0 million after deducting the underwriting commissions of \$9.4 million and \$2.6 million of issuance costs. The debt issuance costs are being amortized to interest expense using the effective interest method over the term of the Senior Notes. Interest expense related to contractual interest expense, amortization of debt issuance costs, and accretion of debt discount was \$24.0 million during both fiscal years ended January 31, 2025 and January 31, 2024.

In certain circumstances involving a change of control event, the Company will be required to make an offer to repurchase all or, at the holder's option, any part, of each holder's notes of that series at 101% of the aggregate principal amount thereof, plus accrued and unpaid interest, if any, to, but excluding, the repurchase date.

The indenture governing the Senior Notes (the "Indenture") contains covenants limiting the Company's ability and the ability of its subsidiaries to create liens on certain assets to secure debt; grant a subsidiary guarantee of certain debt without also providing a guarantee of the Senior Notes; declare dividends; and consolidate or merge with or into, or sell or otherwise dispose of all or substantially all of its assets to, another person. These covenants are subject to a number of limitations and exceptions. Certain of these covenants will not apply during any period in which the notes are rated investment grade by Fitch Ratings, Inc. ("Fitch"), Moody's Investors Service, Inc. ("Moody's"), and Standard & Poor's Ratings Services ("S&P").

As of January 31, 2025, the Company was in compliance with all of its financial covenants under the Indenture associated with the Senior Notes.

Based on the trading prices of the Senior Notes, the fair value of the Senior Notes was approximately \$688.4 million and \$671.2 million as of January 31, 2025 and January 31, 2024, respectively. While the Senior Notes are recorded at cost, the fair value of the Senior Notes was determined based on quoted prices in markets that are not active; accordingly, the Senior Notes are categorized as Level 2 for purposes of the fair value measurement hierarchy.

CrowdStrike Holdings, Inc.
Notes to Consolidated Financial Statements

6. Income Taxes

The Company's geographical breakdown of its income (loss) before provision for income taxes for the fiscal years ended January 31, 2025, January 31, 2024, and January 31, 2023 is as follows (in thousands):

| | Year Ended January 31, | | |
|---|------------------------|-------------------|---------------------|
| | 2025 | 2024 | 2023 |
| Domestic | \$ 62,385 | \$ 99,241 | \$ (195,042) |
| International | (7,851) | 23,576 | 35,159 |
| Income (loss) before provision for income taxes | <u>\$ 54,534</u> | <u>\$ 122,817</u> | <u>\$ (159,883)</u> |

The components of the provision for income taxes during the fiscal years ended January 31, 2025, January 31, 2024, and January 31, 2023 are as follows (in thousands):

| | Year Ended January 31, | | |
|----------------------------|------------------------|------------------|------------------|
| | 2025 | 2024 | 2023 |
| Current | | | |
| Federal | \$ 431 | \$ 272 | \$ — |
| State | 2,493 | 4,462 | 855 |
| Foreign | 78,109 | 30,885 | 20,241 |
| Total current | <u>81,033</u> | <u>35,619</u> | <u>21,096</u> |
| Deferred | | | |
| Federal | 323 | (307) | 135 |
| State | (204) | (343) | 89 |
| Foreign | (10,022) | (2,737) | 1,082 |
| Total deferred | <u>(9,903)</u> | <u>(3,387)</u> | <u>1,306</u> |
| Provision for income taxes | <u>\$ 71,130</u> | <u>\$ 32,232</u> | <u>\$ 22,402</u> |

The following table provides a reconciliation between income taxes computed at the federal statutory rate and the provision for income taxes during the fiscal years ended January 31, 2025, January 31, 2024, and January 31, 2023 (in thousands):

| | As of January 31, | | |
|--|-------------------|------------------|------------------|
| | 2025 | 2024 | 2023 |
| Provision for income taxes at statutory rate | \$ 11,452 | \$ 25,527 | \$ (33,777) |
| State income taxes, net of federal benefits | 2,289 | 4,118 | 944 |
| Effects of foreign operations | 10,236 | 22,425 | 11,003 |
| Research and other credits | (36,669) | (21,182) | (19,465) |
| Stock-based compensation | (125,590) | (31,852) | (47,335) |
| Non-deductible expenses | 6,904 | 4,604 | 2,800 |
| Change in valuation allowance | 152,608 | 28,810 | 102,892 |
| Tax impact of foreign transactions | 49,883 | — | 5,340 |
| Other | 17 | (218) | — |
| Provision for income taxes | <u>\$ 71,130</u> | <u>\$ 32,232</u> | <u>\$ 22,402</u> |

CrowdStrike Holdings, Inc.
Notes to Consolidated Financial Statements

The Company recognized income tax expense of \$71.1 million, \$32.2 million, and \$22.4 million for the fiscal years January 31, 2025, January 31, 2024 and January 31, 2023, respectively. The tax expense for the fiscal year ended January 31, 2025 was primarily attributable to pre-tax foreign earnings, withholding taxes related to customer payments in certain foreign jurisdictions, intercompany sale of intellectual property from acquired entities and change in the realizability of deferred tax assets in certain foreign jurisdictions. The Company transferred acquired intellectual property from foreign subsidiaries to the U.S. Although the transfer of the intellectual property between consolidated entities did not result in any gain in the consolidated statement of operations, such transactions were taxable for tax purposes. The tax expense for the fiscal years ended January 31, 2024 and January 31, 2023 was primarily attributable to pre-tax foreign earnings and withholding taxes related to customer payments in certain foreign jurisdictions and intercompany sales of intellectual property from acquisitions.

Deferred income taxes reflect the net tax effects of temporary differences between the carrying amount of assets and liabilities for financial reporting purposes and the amounts used for income tax purposes.

Significant components of the Company's deferred tax assets and liabilities as of January 31, 2025 and January 31, 2024 are as follows (in thousands):

| | As of January 31, | |
|---|--------------------------|-------------|
| | 2025 | 2024 |
| Deferred tax assets | | |
| Net operating loss carryforwards | \$ 400,277 | \$ 420,803 |
| Research and other credit carryforwards | 144,068 | 100,002 |
| Intangible assets | 117,620 | 81,551 |
| Stock-based compensation | 60,290 | 33,885 |
| Deferred revenue | 209,357 | 169,777 |
| Accrued expenses | 29,833 | 23,956 |
| Operating lease liabilities | 17,418 | 20,613 |
| Capitalized research and development | 473,889 | 320,708 |
| Other, net | 13,898 | — |
| Gross deferred assets | 1,466,650 | 1,171,295 |
| Less: Valuation allowance | (1,192,366) | (957,710) |
| Total deferred tax assets | 274,284 | 213,585 |
| Deferred tax liabilities | | |
| Property and equipment, net | (64,576) | (51,335) |
| Capitalized commissions | (171,349) | (128,302) |
| Intangible assets | (6,921) | (6,489) |
| Operating right-of-use assets | (16,853) | (19,956) |
| Other, net | — | (277) |
| Total deferred tax liabilities | (259,699) | (206,359) |
| Net deferred tax assets | \$ 14,585 | \$ 7,226 |

The Company maintains a full valuation allowance on U.S. federal and state and certain foreign deferred tax assets, including net operating loss carryforwards and tax credits, which the Company has determined are not realizable on a more-likely-than-not basis. In completing the assessment of the continued need for valuation allowance, we analyzed various factors including, but not limited to, cumulative pre-tax losses, excess tax benefits related to stock-based compensation, future reversal of existing temporary differences and tax planning strategies that are prudent and feasible. During the fiscal years ended January 31, 2025, January 31, 2024, and January 31, 2023, the valuation allowance increased by \$234.7 million, \$47.6 million, and \$139.2 million, respectively. The increases in the valuation allowance during the fiscal years ended January 31, 2025 and January 31, 2024 were primarily driven by U.S. operations. As of January 31, 2025, January 31, 2024, and January 31, 2023 the valuation allowance for deferred taxes was \$1.2 billion, \$957.7 million, and \$910.1 million, respectively.

CrowdStrike Holdings, Inc.
Notes to Consolidated Financial Statements

As of January 31, 2025, the Company had aggregate federal and California net operating loss carryforwards of \$1.4 billion and \$307.9 million, respectively, which may be available to offset future taxable income for income tax purposes. The federal net operating losses are carried forward indefinitely, and California net operating loss carryforwards begin to expire in fiscal 2034 through fiscal 2045. As of January 31, 2025, net operating loss carryforwards for other states totaled \$716.0 million, which begin to expire in fiscal 2026 through fiscal 2045. As of January 31, 2025, net operating loss carryforwards for the U.K. totaled \$78.0 million, which are carried forward indefinitely, and net operating loss carryforwards totaled immaterial amounts in certain foreign jurisdictions.

As of January 31, 2025, the Company had federal and California research and development (“R&D”) credit carryforwards of \$165.1 million and \$39.6 million, respectively. The federal R&D credit carryforwards begin to expire in fiscal 2037 through fiscal 2045. The California R&D credits are carried forward indefinitely.

The Internal Revenue Code imposes limitations on a corporation’s ability to utilize net operating loss (“NOLs”) and credit carryovers if it experiences an ownership change as defined in Section 382. In general terms, an ownership change may result from transactions increasing the ownership of certain stockholders in the stock of a corporation by more than 50% over a three-year period. If an ownership change has occurred, or were to occur, utilization of the Company’s NOLs and credit carryovers could be restricted. The Company’s net operating losses and credit carryovers are not currently subject to a limitation due to an ownership change.

Total gross unrecognized tax benefits as of January 31, 2025, January 31, 2024, and January 31, 2023 were \$117.5 million, \$58.9 million, and \$36.9 million, respectively. As of January 31, 2025, the Company had \$54.8 million of unrecognized tax benefits, which, if recognized, would affect the Company’s effective tax rate due to the full valuation allowance. The Company’s policy is to classify interest and penalties related to unrecognized tax benefits as part of the income tax provision in the consolidated statements of operations. Cumulatively, the Company had incurred \$3.0 million of interest and penalties related to unrecognized tax benefits as of January 31, 2025, and \$1.4 million and an insignificant amount of interest and penalties related to unrecognized tax benefits as of January 31, 2024, and January 31, 2023, respectively. During the fiscal year ended January 31, 2025, the net increase in unrecognized tax benefits was a result of certain taxable foreign transactions and R&D credits. During the fiscal year ended January 31, 2024, and January 31, 2023 the net increase in unrecognized tax benefits was a result of R&D credits. The potential change in unrecognized tax benefits during the next 12 months is not expected to be material.

The following is a rollforward of the total gross unrecognized tax benefits for the fiscal years ended January 31, 2025, January 31, 2024, and January 31, 2023 (in thousands):

| | |
|---|-------------------|
| Balance as of February 1, 2022 | \$ 26,324 |
| Decreases in prior period tax positions | (2,122) |
| Increases in current period tax positions | 12,699 |
| Balance as of January 31, 2023 | 36,901 |
| Increases in prior period tax positions | 4,757 |
| Decreases in prior period tax positions | (1,321) |
| Increases in current period tax positions | 18,538 |
| Balance as of January 31, 2024 | 58,875 |
| Increases in current period tax positions | 66,354 |
| Increases in prior period tax positions | 890 |
| Decreases in prior period tax positions | (5,285) |
| Settlements with taxing authorities | (2,882) |
| Statute of limitations expirations | (151) |
| Impact from currency fluctuations | (261) |
| Balance as of January 31, 2025 | <u>\$ 117,540</u> |

The Company files income tax returns in the U.S. federal, foreign, and various state jurisdictions. Tax years 2011 and onwards remain subject to examination by taxing authorities.

CrowdStrike Holdings, Inc.
Notes to Consolidated Financial Statements

The Company does not provide for federal and state income taxes on the undistributed earnings of its foreign subsidiaries as such earnings are to be reinvested offshore indefinitely. If the Company repatriated these earnings, the tax impact of future distributions of foreign earnings would generally be limited to withholding tax from foreign jurisdictions, and the resulting income tax liability would be insignificant.

7. Leases

Operating Leases

The Company has entered into non-cancellable operating lease agreements with various expiration dates through fiscal 2033. Certain lease agreements include options to renew or terminate the lease, which are not reasonably certain to be exercised and therefore are not factored into the determination of lease payments.

Cash paid for amounts included in the measurement of operating lease liabilities was \$19.5 million, \$15.4 million, and \$12.0 million for the fiscal years ended January 31, 2025, January 31, 2024, and January 31, 2023, respectively. Operating lease liabilities arising from obtaining operating right-of-use assets were \$6.8 million and \$16.4 million for the fiscal years ended January 31, 2025 and January 31, 2024, respectively.

The weighted-average remaining lease terms were 2.9 years and 3.7 years as of January 31, 2025 and January 31, 2024, respectively. The weighted-average discount rates were 5.5% and 5.7% as of January 31, 2025 and January 31, 2024, respectively.

The components of lease costs were as follows (in thousands):

| | Year Ended January 31, | | |
|-------------------------|------------------------|------------------|------------------|
| | 2025 | 2024 | 2023 |
| Lease cost | | | |
| Operating lease cost | \$ 17,326 | \$ 15,510 | \$ 11,084 |
| Short-term lease cost | 3,519 | 3,664 | 2,344 |
| Variable lease cost | 11,526 | 8,480 | 8,279 |
| Total lease cost | \$ 32,371 | \$ 27,654 | \$ 21,707 |

Sublease income for the fiscal years ended January 31, 2025 and January 31, 2024 was immaterial. There was no sublease income for the fiscal year ended January 31, 2023. As of January 31, 2025, the Company has not entered into non-cancellable operating leases with terms greater than 12 months that have not yet commenced.

The maturities of the Company's non-cancellable operating lease liabilities are as follows (in thousands):

| | January 31, 2025 |
|--|------------------|
| Fiscal 2026 | \$ 14,135 |
| Fiscal 2027 | 11,269 |
| Fiscal 2028 | 10,794 |
| Fiscal 2029 | 6,042 |
| Fiscal 2030 | 3,787 |
| Thereafter | 3,717 |
| Total operating lease payments | 49,744 |
| Less: imputed interest | (4,826) |
| Present value of operating lease liabilities | \$ 44,918 |

8. Stock-Based Compensation

Stock Incentive Plan

In May 2019, the Company's board of directors adopted, and the stockholders approved the CrowdStrike Holdings, Inc. 2019 Equity Incentive Plan (the "2019 Plan") with the purpose of granting stock-based awards to employees, directors, officers, and consultants, including stock options, restricted stock awards, restricted stock units ("RSUs"), and performance-based restricted stock units ("PSUs"). A total of 8,750,000 shares of Class A common stock were initially available for issuance under the 2019 Plan. The Company's compensation committee administers the 2019 Plan. The number of shares of the Company's common stock available for issuance under the 2019 Plan is subject to an annual increase on the first day of each fiscal year beginning on February 1, 2020, equal to the lesser of: (i) two percent (2%) of outstanding shares of the Company's capital stock as of the last day of the immediately preceding fiscal year or (ii) such other amount as the Company's board of directors may determine.

The 2011 Plan was terminated on June 10, 2019, which was the business day prior to the effectiveness of the Company's registration statement on Form S-1 used in connection with the Company's IPO, and stock-based awards are no longer granted under the 2011 Plan. Any shares underlying stock options that expire, terminate, or are forfeited or repurchased under the 2011 Plan will be automatically transferred to the 2019 Plan.

Stock Options

The Company records compensation expense for employee stock options based on the estimated fair value of the options on the date of grant using the Black-Scholes option-pricing model.

Stock options granted during both fiscal years ended January 31, 2025 and January 31, 2024 were immaterial.

The following table is a summary of stock option activity for the fiscal year ended January 31, 2025:

| | Number of Shares | Weighted- Average Exercise Price Per Share |
|--|-----------------------------|---|
| | (in thousands) | |
| Options outstanding at January 31, 2024 | 1,754 | \$ 9.37 |
| Granted | 30 | \$ 18.06 |
| Exercised | (514) | \$ 7.75 |
| Canceled | (19) | \$ 12.69 |
| Options outstanding at January 31, 2025 | <u>1,251</u> | \$ 10.23 |
| Options vested and expected to vest at January 31, 2025 | <u>1,251</u> | \$ 10.23 |
| Options exercisable at January 31, 2025 | <u>1,217</u> | \$ 9.93 |

There were no options that were unvested and exercisable as of January 31, 2025.

The aggregate intrinsic value of options vested and exercisable was \$472.3 million, \$451.0 million, and \$247.2 million as of January 31, 2025, January 31, 2024, and January 31, 2023, respectively. The weighted-average remaining contractual term of options vested and exercisable was 3.5 years, 4.2 years, and 4.8 years as of January 31, 2025, January 31, 2024, and January 31, 2023, respectively.

The weighted-average grant date fair values of all options granted was \$321.98, \$126.16, and \$116.26 per share during the fiscal years ended January 31, 2025, January 31, 2024, and January 31, 2023, respectively. The total intrinsic value of all options exercised was \$170.4 million, \$190.1 million, and \$166.8 million during the fiscal years ended January 31, 2025, January 31, 2024, and January 31, 2023, respectively.

CrowdStrike Holdings, Inc.
Notes to Consolidated Financial Statements

The aggregate intrinsic value of stock options outstanding as of January 31, 2025, January 31, 2024, and January 31, 2023 was \$485.3 million, \$496.7 million, and \$279.4 million, respectively, which represents the excess of the fair value of the Company's common stock over the exercise price of the options, multiplied by the number of options outstanding. The weighted-average remaining contractual term of stock options outstanding was 3.6 years, 4.3 years, and 5.0 years as of January 31, 2025, January 31, 2024, and January 31, 2023, respectively.

Total unrecognized stock-based compensation expense related to unvested options was \$8.0 million as of January 31, 2025. This expense is expected to be amortized over a weighted-average vesting period of 1.8 years.

Restricted Stock Units

RSUs granted under the 2019 Plan are generally subject to only a service-based vesting condition. The service-based vesting condition is generally satisfied based on one of the following vesting schedules: (i) vesting of one-fourth of the RSUs on the first "Company vest date" (defined as March 20, June 20, September 20, or December 20) on or following the one-year anniversary of the vesting commencement date, with the remainder of the RSUs vesting in twelve equal quarterly installments thereafter, subject to continued service, (ii) vesting in sixteen equal quarterly installments, subject to continued service, or (iii) vesting in sixteen quarterly installments with 10% in the first year, 15% in the second year, 25% in the third year, and 50% in the fourth year, subject to continued service. The valuation of these RSUs is based solely on the fair value of the Company's stock on the date of grant.

Total unrecognized stock-based compensation expense related to unvested RSUs was \$2.1 billion as of January 31, 2025. This expense is expected to be amortized over a weighted-average vesting period of 2.7 years.

Performance-based Stock Units

PSUs granted under the 2019 Plan are generally subject to both a service-based vesting condition and a performance-based vesting condition. PSUs will vest upon the achievement of specified performance targets and subject to continued service through the applicable vesting dates. The stock-based compensation expense relating to PSUs is recognized using the accelerated attribution method over the requisite service period when it is probable that the performance condition will be satisfied.

Total unrecognized stock-based compensation expense related to unvested PSUs was \$61.0 million as of January 31, 2025, which reflects the Company's updated assessment of the likelihood of satisfying the performance conditions. This expense is expected to be amortized over a weighted-average vesting period of 1.1 years.

Special PSU Awards

In fiscal 2022 the Company's board of directors granted 655,000 performance stock units (the "Special PSU Awards") to certain executives under the 2019 Plan. The Special PSU Awards vest upon the satisfaction of the Company's achievement of specified stock price hurdles, which are based on the average of the closing stock price per share of the Company's Class A common stock during any 45 consecutive trading day period during the applicable performance period, and a service-based vesting condition. The service condition applicable to each tranche of the Special PSU Awards will be satisfied in installments as follows, subject to continued employment with the Company through each applicable vesting date: (i) 50% of the Special PSU Awards underlying the applicable tranche will service vest on the first anniversary of the vesting commencement date applicable to such tranche of the Special PSU Awards (i.e., February 1, 2022, February 1, 2023, February 1, 2024, and February 1, 2025) and (ii) the remaining PSUs with respect to such tranche will thereafter service vest in four equal quarterly installments of 12.5%.

The Company measured the fair value of the Special PSU Awards on the grant date using a Monte Carlo simulation valuation model. The risk-free interest rates used were 0.85% - 1.51%, which were based on the zero-coupon-risk-free interest rate derived from the Treasury Constant Maturities yield curve for the expected term of the award on the grant date. The expected volatility was a blended volatility rate of 54.89% - 55.36%, which includes 50% weight on the Company's historical volatility calculated from daily stock returns over a 2.21 - 2.58 year look-back from the grant date and 50% weight based on the Company's implied volatility as of the grant date.

CrowdStrike Holdings, Inc.
Notes to Consolidated Financial Statements

Total unrecognized stock-based compensation expense related to the unvested portion of the Special PSU Awards was \$11.2 million as of January 31, 2025. This expense is expected to be amortized over a weighted-average vesting period of 1.1 years.

The following table is a summary of RSUs, PSUs, and the Special PSU Awards activities for the fiscal year ended January 31, 2025:

| | Number of Shares | Weighted- Average Grant Date Fair Value Per Share |
|---|---------------------|---|
| | (in thousands) | |
| RSUs and PSUs outstanding at January 31, 2024 | 10,968 | \$ 167.84 |
| Granted | 5,122 | \$ 306.50 |
| Released | (4,552) | \$ 171.25 |
| Performance adjustment ⁽¹⁾ | 245 | \$ 132.83 |
| Forfeited | (759) | \$ 205.25 |
| RSUs and PSUs outstanding at January 31, 2025 | 11,024 | \$ 227.55 |
| RSUs and PSUs expected to vest at January 31, 2025⁽²⁾ | 10,454 | \$ 228.49 |

(1) The performance adjustment represents adjustments in shares outstanding due to the actual achievement of performance-based awards, the achievement of which was based upon pre-defined financial performance targets.

(2) Excludes in progress PSUs and Special PSUs where pre-defined targets have not yet been achieved.

Employee Stock Purchase Plan

In May 2019, the board of directors adopted, and the stockholders approved, the CrowdStrike Holdings, Inc. 2019 Employee Stock Purchase Plan (“ESPP”), which became effective on June 10, 2019, which was the business day prior to the effectiveness of the Company’s registration statement on Form S-1 used in connection with the Company’s IPO. A total of 3,500,000 shares of Class A common stock were initially reserved for issuance under the ESPP. The Company’s compensation committee administers the ESPP. The number of shares of common stock available for issuance under the ESPP is subject to an annual increase on the first day of each fiscal year beginning on February 1, 2020, equal to the lesser of: (i) one percent (1%) of the outstanding shares of the Company’s capital stock as of the last day of the immediately preceding fiscal year or (ii) such other amount as its board of directors may determine. In May 2021, the Company’s compensation committee adopted an amendment and restatement of the ESPP, which was approved by the Company’s stockholders in June 2021. The amended and restated ESPP clarified the original intent that the annual increase will in no event exceed 5,000,000 shares of the Company’s Class A common stock in any year.

The ESPP provides for consecutive offering periods that will typically have a duration of approximately 24 months in length and are comprised of four purchase periods of approximately six months in length. The offering periods are scheduled to start on the first trading day on or after June 11 and December 11 of each year. The first offering period commenced on June 11, 2019 and ended on June 10, 2021.

The ESPP provides eligible employees with an opportunity to purchase shares of the Company’s Class A common stock through payroll deductions of up to 15% of their eligible compensation. A participant may purchase a maximum of 2,500 shares of common stock during a purchase period. Amounts deducted and accumulated by the participant are used to purchase shares of common stock at the end of each six-month purchase period. The purchase price of the shares is 85% of the lower of the fair market value of the Class A common stock on (i) the first trading day of the applicable offering period and (ii) the last trading day of each purchase period in the related offering period. Participants may end their participation at any time during an offering period and will be paid their accrued contributions that have not yet been used to purchase shares of common stock. Participation ends automatically upon termination of employment. The ESPP allows for up to one increase in contribution during each purchase period. If an employee elects to increase his or her contribution, the Company treats this as an accounting modification. The ESPP also offers a two-year look-back feature, as well as a rollover feature that provides for an offering period to be rolled over to a new lower-priced offering if the offering price of the new offering period is less than that of the

CrowdStrike Holdings, Inc.
Notes to Consolidated Financial Statements

current offering period. During the fiscal years ended January 31, 2025 and January 31, 2023, there were ESPP rollovers because the Company's closing stock price on the purchase date was lower than the Company's closing stock price on the first day of the offering periods. As a result, these offering dates were rolled over to new 24-month offering periods through December 10, 2026, and December 12, 2024, respectively. These rollovers were accounted for as a modification to the original offerings. The total incremental expense as a result of the rollover and contribution modifications was \$12.4 million and \$58.6 million, respectively, which will be recognized over the new or remaining offering periods. There were no ESPP rollovers during the fiscal year ended January 31, 2024. Total incremental expense as a result of contribution modifications during the fiscal year ended January 31, 2024 was \$7.3 million, which will be recognized over the remaining offering periods.

Employee payroll contributions ultimately used to purchase shares are reclassified to stockholders' equity on the purchase date. ESPP employee payroll contributions accrued as of January 31, 2025 and January 31, 2024 totaled \$33.2 million and \$22.3 million, respectively, and are included within accrued payroll and benefits in the consolidated balance sheets.

The following table summarizes the assumptions used in the Black-Scholes option-pricing model to determine the fair value of employee stock purchase rights granted under the Company's ESPP:

| | Year Ended January 31, | | |
|---------------------------------|------------------------|---------------|---------------|
| | 2025 | 2024 | 2023 |
| Expected term (in years) | 0.5 – 2.0 | 0.5 – 2.0 | 0.5 – 2.0 |
| Risk-free interest rate | 3.4% – 5.3% | 0.2% – 5.3% | 0.1% – 4.7% |
| Expected stock price volatility | 40.8% – 59.8% | 40.8% – 61.2% | 39.6% – 67.4% |
| Dividend yield | — % | — % | — % |

Stock-Based Compensation Expense

Stock-based compensation expense included in the consolidated statements of operations is as follows (in thousands):

| | Year Ended January 31, | | |
|--|------------------------|-------------------|-------------------|
| | 2025 | 2024 | 2023 |
| Subscription cost of revenue | \$ 73,592 | \$ 43,886 | \$ 32,091 |
| Professional services cost of revenue | 31,126 | 22,302 | 15,692 |
| Sales and marketing | 235,499 | 175,808 | 151,919 |
| Research and development | 337,620 | 205,896 | 174,711 |
| General and administrative | 187,584 | 183,627 | 152,091 |
| Total stock-based compensation expense | <u>\$ 865,421</u> | <u>\$ 631,519</u> | <u>\$ 526,504</u> |

9. Revenue, Deferred Revenue and Remaining Performance Obligations

The following table summarizes revenue by region based on the shipping address of customers who have contracted to use the Company's platform or service (in thousands, except percentages):

| | Year Ended January 31, | | | | | |
|---------------------------------|------------------------|--------------|---------------------|--------------|---------------------|--------------|
| | 2025 | | 2024 | | 2023 | |
| | Amount | % Revenue | Amount | % Revenue | Amount | % Revenue |
| United States | \$ 2,682,942 | 68 % | \$ 2,088,054 | 68 % | \$ 1,563,567 | 70 % |
| Europe, Middle East, and Africa | 619,483 | 16 % | 467,928 | 15 % | 327,929 | 15 % |
| Asia Pacific | 402,453 | 10 % | 315,524 | 10 % | 228,124 | 10 % |
| Other | 248,746 | 6 % | 184,049 | 7 % | 121,616 | 5 % |
| Total revenue | <u>\$ 3,953,624</u> | <u>100 %</u> | <u>\$ 3,055,555</u> | <u>100 %</u> | <u>\$ 2,241,236</u> | <u>100 %</u> |

No single country other than the United States represented 10% or more of the Company's total revenue during the fiscal years ended January 31, 2025, January 31, 2024, and January 31, 2023.

CrowdStrike Holdings, Inc.
Notes to Consolidated Financial Statements

Contract Balances

Contract liabilities consist of deferred revenue and include payments received in advance of performance under the contract. Such amounts are recognized as revenue over the contractual period. The Company recognized revenue of \$2,251.3 million and \$1,718.5 million for the fiscal years ended January 31, 2025 and January 31, 2024, respectively, which was included in the corresponding contract liability balance at the beginning of the period.

The Company receives payments from customers based upon contractual billing schedules. Accounts receivable are recorded when the right to consideration becomes unconditional. Payment terms on invoiced amounts are typically 30 – 60 days. Contract assets include amounts related to the contractual right to consideration for both completed and partially completed performance obligations that may not have been invoiced.

Changes in deferred revenue were as follows (in thousands):

| | Year Ended January 31, | |
|---------------------------------|-------------------------------|---------------------|
| | 2025 | 2024 |
| Beginning balance | \$ 3,054,099 | \$ 2,355,113 |
| Additions to deferred revenue | 4,628,202 | 3,754,541 |
| Recognition of deferred revenue | (3,953,624) | (3,055,555) |
| Ending balance | <u>\$ 3,728,677</u> | <u>\$ 3,054,099</u> |

Remaining Performance Obligations

The Company's subscription contracts with its customers have a typical term of one to three years, and most subscription contracts are non-cancellable. Customers generally have the right to terminate their contracts for cause as a result of the Company's failure to perform. As of January 31, 2025, the aggregate amount of the transaction price allocated to remaining performance obligations was \$6.5 billion. The Company expects to recognize approximately 53% of the remaining performance obligations in the 12 months following January 31, 2025 and 42% of the remaining performance obligations between 13 to 36 months, with the remainder to be recognized thereafter.

Costs to Obtain and Fulfill a Contract

The Company capitalizes referral fees paid to partners and sales commissions and associated payroll taxes paid to internal sales personnel, contractors, or sales agents that are incremental to the acquisition of channel partner and direct customer contracts and would not have occurred absent the customer contract. These costs are recorded as deferred contract acquisition costs, current and deferred contract acquisition costs, noncurrent on the consolidated balance sheets.

Sales commissions for renewal of a contract are not considered commensurate with the commissions paid for the acquisition of the initial contract or follow-on upsell given the substantive difference in commission rates in proportion to their respective contract values. Commissions, including referral fees paid to referral partners, earned upon the initial acquisition of a contract or subsequent upsell are amortized over an estimated period of benefit of four years, while commissions earned for renewal contracts are amortized over the contractual term of the renewals. Sales commissions associated with professional service contracts are amortized ratably over an estimated period of benefit of five months. Commissions are included in sales and marketing expense in the consolidated statements of operations. In determining the period of benefit for commissions paid for the acquisition of the initial contract, the Company took into consideration the expected subscription term and expected renewals of customer contracts, the historical duration of relationships with customers, customer retention data, and the life of the developed technology. The Company periodically reviews the carrying amount of deferred contract acquisition costs to determine whether events or changes in circumstances have occurred that could impact the period of benefit of these deferred costs. The Company did not recognize any material impairment losses of deferred contract acquisition costs during the year ended January 31, 2025.

CrowdStrike Holdings, Inc.
Notes to Consolidated Financial Statements

The following table summarizes the activity of deferred contract acquisition costs (in thousands):

| | Year Ended January 31, | |
|---|-------------------------------|-------------------|
| | 2025 | 2024 |
| Beginning balance | \$ 582,303 | \$ 447,088 |
| Capitalization of contract acquisition costs | 584,484 | 374,116 |
| Amortization of deferred contract acquisition costs | (318,837) | (238,901) |
| Ending balance | <u>\$ 847,950</u> | <u>\$ 582,303</u> |
| Deferred contract acquisition costs, current | \$ 347,042 | \$ 246,370 |
| Deferred contract acquisition costs, noncurrent | 500,908 | 335,933 |
| Total deferred contract acquisition costs | <u>\$ 847,950</u> | <u>\$ 582,303</u> |

10. Commitments and Contingencies

July 19 Incident

On July 19, 2024, the Company released a content configuration update for its Falcon sensor that resulted in system crashes for certain Windows systems (the “July 19 Incident”). The Company is subject to a number of legal proceedings in connection with the July 19 Incident, including:

- On July 30, 2024, a putative class action lawsuit was filed against the Company and certain of the Company’s officers in federal court in the Western District of Texas alleging violations of federal securities laws, including that the defendants made false or misleading statements. The complainants seek certification of a class of all persons who purchased or otherwise acquired the Company’s securities during specified periods of time and are seeking unspecified monetary damages, costs and attorneys’ fees. On January 21, 2025, an amended complaint was filed.
- On August 5, 2024, a putative class action lawsuit was filed against CrowdStrike, Inc. in federal court in the Western District of Texas alleging, among other things, negligence and violations of the California Unfair Competition Law. The complainants seek certification of a nationwide class, as well as sub-classes of certain California, Ohio, and Pennsylvania citizens, who had a flight delayed or canceled during a specified period of time and are seeking unspecified monetary damages, certain injunctive relief, costs and attorneys’ fees. On November 6, 2024, this lawsuit was consolidated with the August 19, 2024 lawsuit described below, and interim class counsel was appointed. On December 6, 2024, a consolidated class action complaint was filed. On February 4, 2025, CrowdStrike, Inc. filed a motion to dismiss the complaint.
- On August 19, 2024, a putative class action lawsuit was filed against the Company and CrowdStrike, Inc. in federal court in the Western District of Texas alleging, among other things, negligence in the design and testing of the Falcon sensor and tortious interference between certain airline customers and their airline. The complainants seek certification of a nationwide class (or alternatively a class of Iowa citizens) who had a flight delayed or canceled on a specified airline during a specific period of time and are seeking unspecified monetary damages, costs and attorneys’ fees. On November 6, 2024, this lawsuit was consolidated with the lawsuit filed on August 5, 2024 described above and was administratively closed.
- On September 4, September 11, and September 20, 2024, three derivative lawsuits were filed against certain of the Company’s officers and directors, and against the Company as nominal defendant, in federal court in the Western District of Texas alleging breach of fiduciary duty under Delaware law and violations of federal securities laws, including that the defendants made false or misleading statements in violation of Sections 10(b) and 14(a) of the Exchange Act and SEC Rules 10b-5 and 14a-9. One of the lawsuits also brings a claim against certain of the defendants for contribution under Sections 10(b) and 21D of the Exchange Act. The complainants seek monetary and non-monetary relief purportedly on behalf of the Company. On November 21, 2024, all three cases were consolidated and stayed pending resolution of the putative securities class action described above.

CrowdStrike Holdings, Inc.
Notes to Consolidated Financial Statements

- On October 25, 2024, Delta Airlines, Inc. (“Delta”) filed a complaint against CrowdStrike, Inc. in the Superior Court for Fulton County, Georgia, alleging, among other things, computer trespass, trespass to personality, breach of contract, intentional misrepresentation/fraud by omission, strict-liability product defect, gross negligence, and deceptive and unfair business practices. Delta is seeking unspecified monetary damages, attorneys’ fees and unspecified punitive damages. The matter has been transferred to the Metro Atlanta Business Case Division. On December 16, 2024, CrowdStrike, Inc. filed a motion to dismiss.

Additionally, some customers and third parties have asserted claims or publicly threatened litigation against the Company. The Company has also received inquiries from governmental authorities and other third parties related to the July 19 Incident. The Company is cooperating and providing information in connection with these inquiries.

For any claims and legal proceedings for which the Company believes a liability is both probable and reasonably estimable, the Company records a liability in the period for which it makes this determination. For claims and legal proceedings where a loss may be reasonably possible, but not probable, or is probable but not reasonably estimable, no accrual is established. While the Company believes it is reasonably possible that it could incur losses associated with the claims, proceedings and inquiries described above, it is not possible to estimate the amount of any loss or range of possible loss that might result from adverse judgments, settlements, penalties or other resolutions of these claims, proceedings and inquiries based on their early stage, and the lack of resolution on significant factual and legal issues. Because the final outcome of any of these matters cannot be predicted with certainty, unfavorable or unexpected developments or outcomes could result in a material impact to the Company’s results of operations.

The Company expects to incur significant legal and professional services and other expenses associated with the July 19 Incident in future periods. These expenses will be recognized as incurred. Certain costs may be recoverable under the Company’s insurance policies in effect at the date of the July 19 Incident. Any amounts recoverable under such policies will be reflected in future periods in which recovery is considered probable.

Amounts accrued and expenses incurred, net of insurance receivable recorded, relating to the July 19 Incident during fiscal years ended January 31, 2025 were as follows (in thousands):

| | Amounts |
|--|------------------|
| Balance at January 31, 2024 | \$ — |
| Expenses incurred, net of insurance receivable recorded ⁽¹⁾ | 60,062 |
| Payments made / cash received | (38,917) |
| Balance at January 31, 2025 | <u>\$ 21,145</u> |

- (1) These expenses were included in the Company’s consolidated statements of operations as sales and marketing expenses, research and development expenses, and general and administrative expenses. Accruals were recorded in accrued expenses in the Company’s consolidated balance sheets. Insurance receivable was recorded in prepaid expenses and other current assets in the Company’s consolidated balance sheets.

In addition to customer commitment packages, the Company has made an immaterial amount of settlement offers to certain customers in response to the July 19 Incident. These amounts are, or will be, entirely offset by recoveries under the Company’s insurance policies. Accordingly, there is no impact on the Company’s consolidated statement of operations for the fiscal year ended January 31, 2025. The customer payables and insurance receivables were recorded as accrued expenses and as prepaid expenses and other current assets in the Company’s consolidated balance sheet as of January 31, 2025, respectively.

Other Legal Proceedings

In March 2022, Webroot, Inc. and Open Text, Inc. (collectively, “Webroot”) filed a lawsuit against the Company and CrowdStrike, Inc. in federal court in the Western District of Texas alleging that certain of the Company’s products infringe six patents held by them. In the complaint, Webroot sought unspecified damages, attorneys’ fees and a permanent injunction. In May 2022, CrowdStrike, Inc. asserted counterclaims alleging that certain of Webroot’s products infringe two of its patents. In the filing, CrowdStrike, Inc. sought unspecified damages, reasonable fees and costs, and a permanent injunction. In September 2022, Webroot amended its complaint to assert six additional patents. In November 2023, CrowdStrike, Inc. entered into an

CrowdStrike Holdings, Inc.
Notes to Consolidated Financial Statements

agreement that provided for, among other things, the settlement and dismissal of the parties' claims and filed for dismissal. The amount attributable to the settlement was not material.

In addition, the Company is involved in various other legal proceedings and subject to claims that arise in the ordinary course of business. For any claims for which the Company believes a liability is both probable and reasonably estimable, the Company records a liability in the period for which it makes this determination. Other than as discussed above, there is no pending or threatened legal proceeding to which the Company is a party that, in the Company's opinion, is reasonably possible to have a material effect on its consolidated financial statements; however, the results of litigation and claims are inherently unpredictable. Regardless of the outcome, litigation can have an adverse impact on the Company's business because of defense and settlement costs, diversion of management resources, and other factors. In addition, the costs of litigation and the timing of these costs from period to period are difficult to estimate, subject to change and could adversely affect the Company's consolidated financial statements.

Purchase Obligations

In the normal course of business, the Company enters into non-cancellable purchase commitments with various parties to purchase products and services such as data center capacity, advertising, technology, equipment, office renovations, corporate events, and consulting services. A summary of non-cancellable purchase obligations in excess of one year as of January 31, 2025, with expected date of payment is as follows (in thousands):

| | Total Commitments |
|----------------------------|------------------------------|
| Fiscal 2026 | \$ 491,027 |
| Fiscal 2027 | 541,433 |
| Fiscal 2028 | 558,559 |
| Fiscal 2029 | 581,474 |
| Fiscal 2030 | 432,481 |
| Thereafter | 87,058 |
| Total purchase commitments | <u>\$ 2,692,032</u> |

Unfunded Loan Commitments

The Company provides financing arrangements for certain qualified end-users to purchase its products and services. When the Company enters into these financing arrangements with the end-users, the funds provided by the Company for the sales transactions do not always occur immediately upon signing, depending on the terms of the arrangements. The Company estimates an allowance for credit losses on these off-balance sheet credit exposures at each reporting period on the contractual period over which the Company is exposed to credit risk via a contractual obligation to extend credit, unless that obligation is unconditionally cancellable by the Company. As of January 31, 2025, the Company had non-cancellable unfunded commitments totaling approximately \$94.2 million.

Warranties and Indemnification

The Company's cloud computing services are typically warranted to perform in a manner consistent with general industry standards that are reasonably applicable and materially in accordance with the Company's online help documentation under normal use and circumstances. In addition, for its Falcon Complete customers, the Company offers a limited warranty, subject to certain conditions, to cover certain costs incurred by the customer in case of a cybersecurity breach. The Company has entered into an insurance policy to reduce its potential liability arising from such limited warranty arrangements. The Company's customer arrangements generally include certain provisions for indemnifying customers against losses suffered or incurred as a result of third-party claims that the Company's products or services infringe a third party's intellectual property rights. From time to time, the Company has also agreed to certain other indemnifications and warranties. The Company has not incurred any material costs because of such obligations and has not accrued any liabilities related to such obligations in the consolidated financial statements as of January 31, 2025 or January 31, 2024.

CrowdStrike Holdings, Inc.
Notes to Consolidated Financial Statements

The Company has also agreed to indemnify its directors and certain executive officers for costs associated with any fees, expenses, judgments, fines, and settlement amounts incurred by any of these persons in any action or proceeding to which any of those persons is, or is threatened to be, made a party by reason of the person's service as a director or officer, including any action by the Company, arising out of that person's services as the Company's director or officer or that person's services provided to any other company or enterprise at the Company's request. The Company maintains director and officer insurance coverage that would generally enable the Company to recover a portion of any future amounts paid. The Company may also be subject to indemnification obligations by law with respect to the actions of its employees under certain circumstances and in certain jurisdictions. No liabilities have been accrued associated with this indemnification provision as of January 31, 2025 or January 31, 2024.

11. Geographic Information

The Company's property and equipment, net and operating lease right-of-use assets, are summarized by geographic area as follows (in thousands):

| | January 31, | |
|---|--------------------|-------------------|
| | 2025 | 2024 |
| United States | \$ 688,766 | \$ 539,580 |
| Germany | 88,443 | 84,488 |
| Other countries | 54,194 | 44,315 |
| Total property and equipment, net and operating lease right-of-use assets | <u>\$ 831,403</u> | <u>\$ 668,383</u> |

12. Acquisitions

Adaptive Shield

On November 20, 2024, the Company acquired 100% of the equity interest of A.S. Adaptive Shield Ltd. ("Adaptive Shield"), a SaaS-based cybersecurity company that offers customers comprehensive SaaS security posture management solutions.

The acquisition has been accounted for as a business combination. The total consideration transferred consisted of \$213.7 million in cash, net of \$13.7 million of cash acquired, and \$0.7 million representing the fair value of replacement equity awards attributable to pre-acquisition service. The remaining fair value of these replacement awards attributed to post-combination service was excluded from the purchase price. The purchase price was allocated on a preliminary basis, subject to working capital adjustment and continuing management analysis, to identifiable intangible assets, which include developed technology and customer relationships of \$31.1 million, net tangible liabilities acquired of \$7.7 million, and goodwill of \$191.0 million, which was allocated to the Company's one reporting unit and represents the excess of the purchase price over the fair value of net tangible and intangible assets acquired. The goodwill was primarily attributable to the assembled workforce of Adaptive Shield, planned growth in new markets, and synergies expected to be achieved from the integration of Adaptive Shield. Goodwill is not deductible for income tax purposes.

Per the terms of the share purchase agreement with Adaptive Shield, certain unvested stock options held by Adaptive Shield employees were canceled and exchanged for replacement stock options under the 2019 Plan. Additionally, certain shares of Adaptive Shield stock held by Adaptive Shield employees were exchanged for shares of the Company's common stock, subject to service-based vesting and other conditions. Further, the Company granted RSUs and PSUs under the 2019 Plan to certain continuing employees. The awards that are subject to continued service are recognized ratably as stock-based compensation cost over the requisite service period. The awards that are subject to both continued service and specified performance targets are recognized over the requisite service period when it is probable that the performance condition will be satisfied.

CrowdStrike Holdings, Inc.
Notes to Consolidated Financial Statements

The following table sets forth the components of identifiable intangible assets acquired and their estimated useful lives as of the date of acquisition (dollars in thousands):

| | <u>Fair Value</u> | <u>Useful Life</u> (in months) |
|----------------------------------|-------------------|-----------------------------------|
| Developed technology | \$ 23,600 | 72 |
| Customer relationships | 7,500 | 72 |
| Total intangible assets acquired | <u>\$ 31,100</u> | |

Acquisition costs incurred during the fiscal year ended January 31, 2025 were \$2.7 million and are recorded in general and administrative expenses on the Company's consolidated statements of operations.

The results of operations for the acquisition have been included in the Company's consolidated financial statements from the date of acquisition. The acquisition of Adaptive Shield did not have a material impact on the Company's consolidated financial statements, and therefore historical and pro forma disclosures have not been presented.

Flow Security

On March 26, 2024, the Company acquired 100% of the equity interest of Flow Security Ltd. ("Flow Security"), a leading provider of data security solutions.

The acquisition has been accounted for as a business combination. The total consideration transferred consisted of \$96.4 million in cash, net of \$0.8 million of cash acquired, and \$0.5 million representing the fair value of replacement equity awards attributable to pre-acquisition service. The remaining fair value of these replacement awards attributed to post-combination service was excluded from the purchase price. The purchase price was allocated on a preliminary basis, subject to working capital adjustment and continuing management analysis, to developed technology of \$13.5 million with a useful life of 72 months, net tangible liabilities acquired of \$0.6 million, and goodwill of \$84.0 million, which was allocated to the Company's one reporting unit and represents the excess of the purchase price over the fair value of net tangible and intangible assets acquired. The goodwill was primarily attributable to the assembled workforce of Flow Security, planned growth in new markets, and synergies expected to be achieved from the integration of Flow Security. Goodwill is not deductible for income tax purposes.

Per the terms of the share purchase agreement with Flow Security, certain unvested stock options held by Flow Security employees were canceled and exchanged for replacement stock options under the 2019 Plan. Additionally, certain shares of Flow Security stock held by Flow Security employees were exchanged for the right to receive shares of the Company's common stock, subject to service-based vesting and other conditions. Further, the Company granted RSUs and PSUs under the 2019 Plan to certain continuing employees. The awards that are subject to continued service are recognized ratably as stock-based compensation cost over the requisite service period. The awards that are subject to both continued service and specified performance targets are recognized over the requisite service period when it is probable that the performance condition will be satisfied.

Acquisition costs incurred during the fiscal year ended January 31, 2025 were \$3.2 million and are primarily recorded in general and administrative expenses on the Company's consolidated statements of operations.

The results of operations for the acquisition have been included in the Company's consolidated financial statements from the date of acquisition. The acquisition of Flow Security did not have a material impact on the Company's consolidated financial statements, and therefore historical and pro forma disclosures have not been presented.

Bionic

On September 28, 2023, the Company acquired 100% of the equity interest of Bionic Stork, Ltd. ("Bionic"), a privately-held company that provides an Application Security Posture Management platform designed to proactively reduce and mitigate security, data privacy, and operational risks by analyzing application architecture and dependencies that run in production.

CrowdStrike Holdings, Inc.
Notes to Consolidated Financial Statements

The acquisition has been accounted for as a business combination. The total consideration transferred consisted of \$239.0 million in cash, net of \$25.7 million of cash acquired, and \$0.7 million representing the fair value of replacement equity awards attributable to pre-acquisition service. The remaining fair value of these replacement awards attributed to post-combination service was excluded from the purchase price. The purchase price was allocated to identified intangible assets, which include developed technology and customer relationships of \$34.9 million, net tangible liabilities acquired of \$2.7 million, and goodwill of \$207.5 million, which was allocated to the Company's one reporting unit and represents the excess of the purchase price over the fair value of net tangible and intangible assets acquired. The goodwill was primarily attributable to the assembled workforce of Bionic, planned growth in new markets, and synergies expected to be achieved from the integration of Bionic. Goodwill is not deductible for income tax purposes.

Per the terms of the share purchase agreement with Bionic, certain unvested stock options held by Bionic employees were canceled and exchanged for replacement stock options under the 2019 Plan. Additionally, certain shares of Bionic stock held by Bionic employees were exchanged for shares of the Company's common stock, subject to service-based vesting and other conditions. Further, the Company granted RSUs and PSUs under the 2019 Plan to certain continuing employees. The awards that are subject to continued service are recognized ratably as stock-based compensation expense over the requisite service period. The awards that are subject to both continued service and specified performance targets are recognized over the requisite service period when it is probable that the performance condition will be satisfied.

The following table sets forth the components of identifiable intangible assets acquired and their estimated useful lives as of the date of acquisition (dollars in thousands):

| | <u>Fair Value</u> | <u>Useful Life</u> (in months) |
|----------------------------------|-------------------|-----------------------------------|
| Developed technology | \$ 29,900 | 72 |
| Customer relationships | 5,000 | 96 |
| Total intangible assets acquired | <u>\$ 34,900</u> | |

Acquisition costs incurred during the fiscal year ended January 31, 2025 were immaterial.

The results of operations for the acquisition have been included in the Company's consolidated financial statements from the date of acquisition. The acquisition of Bionic did not have a material impact on the Company's consolidated financial statements, and therefore historical and pro forma disclosures have not been presented.

13. Net Income (Loss) Per Share Attributable to Common Stockholders

Basic and diluted net income (loss) per share attributable to CrowdStrike's common stockholders is computed in conformity with the two-class method required for participating securities. Basic net income (loss) per share attributable to CrowdStrike common stockholders is computed by dividing the net income (loss) attributable to CrowdStrike by the weighted-average number of shares of common stock outstanding during the period. Diluted net income per share attributable to CrowdStrike common stockholders is calculated by dividing net income by the combination of the weighted-average number of common shares outstanding and the effect of the weighted-average number of dilutive common share equivalents during the period. The dilutive potential shares of common stock are comprised of outstanding stock options, RSUs, PSUs, Special PSUs, ESPP obligations, and founders' holdbacks, and are computed using the treasury stock method. The effects of the outstanding stock options, RSUs, PSUs, Special PSUs, ESPP obligations, and founders holdbacks are excluded from the computation of the diluted net income per share in periods in which the effect would be anti-dilutive. Diluted net loss per share is the same as basic net loss per share for the fiscal year ended January 31, 2025 and January 31, 2023 because the effects of potentially dilutive items were antidilutive given the Company's net loss position during fiscal year ended January 31, 2025 and January 31, 2023.

The rights of the holders of Class A and Class B common stock are identical, except with the respect to voting and conversion rights. As such, the undistributed earnings are allocated equally to each share of common stock without class distinction and the resulting basic and diluted net income (loss) per share attributable to CrowdStrike common stockholders are the same for shares of Class A and Class B common stock. On December 11, 2024, all of the Company's outstanding shares of Class B common stock were automatically converted into an equal number of shares of Class A common stock pursuant to the provisions of the Amended and Restated Certificate of Incorporation.

CrowdStrike Holdings, Inc.
Notes to Consolidated Financial Statements

The following table sets forth the computation of basic and diluted net income (loss) per share attributable to CrowdStrike common stockholders (in thousands, except per share data):

| | Year Ended January 31, | | |
|---|------------------------|----------------|------------------|
| | 2025 | 2024 | 2023 |
| Numerator: | | | |
| Net income (loss) attributable to CrowdStrike | \$ (19,271) | \$ 89,327 | \$ (183,245) |
| Denominator: | | | |
| Weighted-average shares used in computing net income (loss) per share attributable to CrowdStrike common stockholders, basic | 244,750 | 238,637 | 233,139 |
| Dilutive effect of common stock equivalents | — | 4,998 | — |
| Weighted-average shares used in computing net income (loss) per share attributable to CrowdStrike common stockholders, dilutive | 244,750 | 243,635 | 233,139 |
| Net income (loss) per share attributable to CrowdStrike common stockholders, basic | <u>\$ (0.08)</u> | <u>\$ 0.37</u> | <u>\$ (0.79)</u> |
| Net income (loss) per share attributable to CrowdStrike common stockholders, diluted | <u>\$ (0.08)</u> | <u>\$ 0.37</u> | <u>\$ (0.79)</u> |

The potential shares of common stock that were excluded from the computation of diluted net income (loss) per share attributable to common stockholders for the periods presented because including them would have been antidilutive are as follows (in thousands):

| | Year Ended January 31, | | |
|---|------------------------|--------------|---------------|
| | 2025 | 2024 | 2023 |
| RSUs and PSUs subject to future vesting | 10,454 | 3,125 | 10,050 |
| Shares of common stock issuable from stock options | 1,217 | 1 | 2,869 |
| Share purchase rights under the Employee Stock Purchase Plan | 742 | 411 | 4,481 |
| Potential common shares excluded from diluted net income (loss) per share | <u>12,413</u> | <u>3,537</u> | <u>17,400</u> |

The above table excludes founder holdbacks related to business combinations where a variable number of shares will be issued upon vesting to settle a fixed monetary amount of \$18.4 million, contingent upon continued employment with the Company. The share price will be determined based on the Company's average stock price or the volume weighted average stock price five days prior to each vesting date. During the fiscal year ended January 31, 2025, 10,780 shares were issued to settle founder holdbacks at a weighted average price of \$329.82 per share.

As of January 31, 2025, the above table also excludes 575,747 outstanding shares of in progress PSUs and Special PSUs where pre-defined targets have not yet been achieved.

14. Segment Information

CrowdStrike's Chief Operating Decision Maker ("CODM"), the Chief Executive Officer, manages the Company's business activities as a single operating and reportable segment at the consolidated level. Accordingly, the CODM uses consolidated net income (loss) to measure segment profit or loss, evaluate financial performance, and allocate resources. Consolidated net income (loss) is evaluated on a monthly basis by comparing actual results against budgeted or forecasted net income (loss), facilitating the analysis of the Company's financial trends.

Significant expenses within net income (loss) include cost of revenue for subscription and professional services, sales and marketing expenses, research and development expenses, and general and administrative expenses. Other segment items within net income (loss) include interest expense, interest income, other income, net, and provision for income taxes, which are each separately disclosed and presented in the consolidated statements of operations.

See Note 9 for additional information about the Company's revenue by geographic region, and Note 11 for additional information about the Company's property and equipment, net and operating lease right-of-use assets by geographic region.

ITEM 9. CHANGES IN AND DISAGREEMENTS WITH ACCOUNTANTS ON ACCOUNTING AND FINANCIAL DISCLOSURE

None.

ITEM 9A. CONTROLS AND PROCEDURES

Evaluation of Disclosure Controls and Procedures

We maintain “disclosure controls and procedures,” as defined in Rule 13a–15(e) and Rule 15d–15(e) under the Exchange Act that are designed to provide reasonable assurance that information required to be disclosed by us in the reports that we file or submit under the Exchange Act is recorded, processed, summarized and reported, within the time periods specified in the SEC’s rules and forms. Disclosure controls and procedures include, without limitation, controls and procedures designed to provide reasonable assurance that information required to be disclosed by us in the reports that we file or submit under the Exchange Act is accumulated and communicated to our management, including our Chief Executive Officer and Chief Financial Officer, as appropriate to allow timely decisions regarding required disclosure.

Our management, with the participation of our Chief Executive Officer and Chief Financial Officer, has evaluated the effectiveness of our disclosure controls and procedures as of January 31, 2025. Based on such evaluation, our Chief Executive Officer and Chief Financial Officer have concluded that, as of such date, our disclosure controls and procedures were effective at the reasonable assurance level.

Management’s Report on Internal Control Over Financial Reporting

Our management is responsible for establishing and maintaining adequate “internal control over financial reporting,” as defined in Rule 13a-15(f) and Rule 15d-15(f) under the Exchange Act. Our management conducted an evaluation of the effectiveness of our internal control over financial reporting as of January 31, 2025 based on the criteria established in *Internal Control - Integrated Framework* (2013) issued by the Committee of Sponsoring Organizations of the Treadway Commission.

Based on the results of its evaluation, management concluded that our internal control over financial reporting was effective as of January 31, 2025. The effectiveness of our internal control over financial reporting as of January 31, 2025 has been audited by PricewaterhouseCoopers LLP, an independent registered public accounting firm, as stated in its report which is included in Part II, Item 8 of this Annual Report on Form 10-K.

Changes in Internal Control Over Financial Reporting

There was no change in our internal control over financial reporting identified in connection with the evaluation required by Rule 13a-15(d) and Rule 15d-15(d) of the Exchange Act that occurred during the fiscal quarter ended January 31, 2025 that has materially affected, or is reasonably likely to materially affect, our internal control over financial reporting.

Inherent Limitations on Effectiveness of Controls

Our management, including our Chief Executive Officer and Chief Financial Officer, believes that our disclosure controls and procedures and internal control over financial reporting are designed to provide reasonable assurance of achieving their objectives and are effective at the reasonable assurance level. However, our management does not expect that our disclosure controls and procedures or our internal control over financial reporting will prevent or detect all errors and all fraud. A control system, no matter how well conceived and operated, can provide only reasonable, not absolute, assurance that the objectives of the control system are met. Further, the design of a control system must reflect the fact that there are resource constraints, and the benefits of controls must be considered relative to their costs. Because of the inherent limitations in all control systems, no evaluation of controls can provide absolute assurance that all control issues and instances of fraud, if any, have been detected. These inherent limitations include the realities that judgments in decision making can be faulty, and that breakdowns can occur because of a simple error or mistake. Additionally, controls can be circumvented by the individual acts of some persons, by collusion of two or more people or by management override of the controls. The design of any system of controls also is based in part upon certain assumptions about the likelihood of future events, and there can be no assurance that any design will succeed in achieving its stated goals under all potential future conditions; over time, controls may become inadequate because

of changes in conditions, or the degree of compliance with policies or procedures may deteriorate. Because of the inherent limitations in a cost-effective control system, misstatements due to error or fraud may occur and not be detected.

ITEM 9B. OTHER INFORMATION

During the three months ended January 31, 2025, certain of our directors and officers (as defined in Rule 16a-1(f) under the Exchange Act) adopted a “Rule 10b5-1 trading arrangement” (as defined in Regulation S-K Item 408) for the sale of shares of our Class A common stock, as set forth below, in amounts and prices determined in accordance with a formula set forth in each such plan:

| Plans | | | | | | |
|-------------------------------------|----------|-------------------|----------------------------|--------------------------------|-----------------------------|--|
| Name and Title | Action | Date | Rule 10b5-1 ⁽¹⁾ | Non-Rule 10b5-1 ⁽²⁾ | Number of Shares to be Sold | Expiration ⁽⁴⁾ |
| Gerhard Watzinger, Chairman | Adoption | December 6, 2024 | X | | Up to 60,500 | Earlier of the date when all shares under the plan are sold and April 1, 2026. |
| Shawn Henry, Chief Security Officer | Adoption | December 18, 2024 | X | | Up to 54,333 ⁽³⁾ | Earlier of when all shares under the plan are sold and March 24, 2026. |
| Johanna Flower, Director | Adoption | January 16, 2025 | X | | Up to 10,394 | Earlier of when all shares under the plan are sold and April 17, 2026. |

(1) Intended to satisfy the affirmative defense conditions of Rule 10b5-1(c).

(2) Not intended to satisfy the affirmative defense conditions of Rule 10b5-1(c).

(3) Intended to permit Mr. Henry to sell (i) 21,330 shares subject to RSUs and (ii) 33,003 shares subject to PSUs. The actual number of shares subject to PSUs that may be sold is subject to the satisfaction of the applicable performance conditions and may be equal to, greater than or less than 33,003 shares.

(4) Each as subject to further early termination for certain specified events as set forth therein.

No other officers or directors, as defined in Rule 16a-1(f), adopted and/or terminated a “Rule 10b5-1 trading arrangement” or a “non-Rule 10b5-1 trading arrangement,” as defined in Regulation S-K Item 408, during the last fiscal quarter.

ITEM 9C. DISCLOSURE REGARDING FOREIGN JURISDICTIONS THAT PREVENT INSPECTIONS

Not applicable.

PART III

ITEM 10. DIRECTORS, EXECUTIVE OFFICERS AND CORPORATE GOVERNANCE

We have adopted a code of business conduct and ethics (the “Code of Conduct”) that applies to all of our employees, executive officers and directors. The full text of the Code of Conduct is available on our website at ir.crowdstrike.com. The nominating and corporate governance committee of our board of directors is responsible for overseeing the Code of Conduct and must approve any waivers of the Code of Conduct for employees, executive officers and directors. We expect that any amendments to the Code of Conduct, or any waivers of its requirements, will be disclosed on our website, as required by applicable law or the listing standards of The Nasdaq Global Select Market.

Certain information required by this Item with respect to our executive officers is set forth under Item 1 of Part I of this Annual Report on Form 10-K under the section entitled “Information about our Executive Officers.”

The information otherwise required by this Item will be included in our definitive proxy statement for our 2025 annual meeting of stockholders (the “2025 Proxy Statement”), which will be filed with the SEC within 120 days after the end of our fiscal year ended January 31, 2025, and is incorporated herein by reference.

ITEM 11. EXECUTIVE COMPENSATION

The information required by this item is incorporated herein by reference to our 2025 Proxy Statement.

ITEM 12. SECURITY OWNERSHIP OF CERTAIN BENEFICIAL OWNERS AND MANAGEMENT AND RELATED STOCKHOLDER MATTERS

The information required by this item is incorporated herein by reference to our 2025 Proxy Statement.

ITEM 13. CERTAIN RELATIONSHIPS AND RELATED TRANSACTIONS, AND DIRECTOR INDEPENDENCE

The information required by this item is incorporated herein by reference to our 2025 Proxy Statement.

ITEM 14. PRINCIPAL ACCOUNTANT FEES AND SERVICES

The information required by this item is incorporated herein by reference to our 2025 Proxy Statement.

PART IV

ITEM 15. EXHIBITS AND FINANCIAL STATEMENT SCHEDULES

(a)(1) Financial Statements

See Index to consolidated financial statements in Part II, Item 8 of this Annual Report on Form 10-K.

(a)(2) Financial Statement Schedule

All financial statement schedules have been omitted as the information is not required under the related instructions or is not applicable or because the information required is already included in the consolidated financial statements or the notes to those consolidated financial statements.

(a)(3) Exhibits

We have filed the exhibits listed on the accompanying Exhibit Index, which is incorporated herein by reference.

ITEM 16. FORM 10-K SUMMARY

None.

EXHIBIT INDEX

| Exhibit Number | Exhibit Description | Incorporated by Reference | | | | Filed Herewith |
|----------------|--|---------------------------|------------|---------|-------------------|----------------|
| | | Form | File No. | Exhibit | Filing Date | |
| 3.1 | Amended and Restated Certificate of Incorporation of the Registrant, as currently in effect. | 8-K | 001-38933 | 3.1 | June 14, 2019 | |
| 3.2 | Amended and Restated Bylaws of the Registrant, as currently in effect. | 10-Q | 001-38933 | 3.2 | November 27, 2024 | |
| 3.3 | Certificate of Retirement of Class B common stock. | 8-K | 001-38933 | 3.1 | December 13, 2024 | |
| 4.1 | Amended and Restated Stockholders Agreement among the Registrant and certain holders of its capital stock, dated as of June 21, 2018, as amended on September 25, 2018 and April 17, 2019. | S-1 | 333-231461 | 4.1 | May 14, 2019 | |
| 4.2 | Amended and Restated Registration Rights Agreement among the Registrant and certain holders of its capital stock, dated as of June 21, 2018. | S-1 | 333-231461 | 4.2 | May 14, 2019 | |
| 4.3 | Class A common stock certificate of the Registrant. | S-1/A | 333-231461 | 4.3 | May 29, 2019 | |
| 4.4 | Description of Registrant's securities. | | | | | X |
| 4.5 | Indenture dated as of January 20, 2021, between CrowdStrike Holdings, Inc. and U.S. Bank National Association, as trustee | 8-K | 001-38933 | 4.1 | January 20, 2021 | |
| 4.6 | First Supplemental Indenture, dated as of January 20, 2021, between CrowdStrike Holdings, Inc. and U.S. Bank National Association, as trustee | 8-K | 001-38933 | 4.2 | January 20, 2021 | |
| 4.7 | Form of 3.000% Senior Notes due 2029 (included in Exhibit 4.9) | 8-K | 001-38933 | 4.2 | January 20, 2021 | |
| 4.8 | Second Supplemental Indenture, dated as of January 10, 2025, by and among CrowdStrike Holdings, Inc., CrowdStrike Financial Services, Inc. and U.S. Bank Trust Company, National Association, as successor to U.S. Bank National Association, as trustee | | | | | X |
| 10.1† | Form of Indemnification Agreement between the Registrant and each of its directors and executive officers. | S-1 | 333-231461 | 10.1 | May 14, 2019 | |
| 10.2† | 2019 Equity Incentive Plan and related form agreement. | S-1/A | 333-231461 | 10.2 | May 29, 2019 | |
| 10.3† | Form of Global Restricted Stock Unit Agreement Outside Directors – Annual Grant under the Company's 2019 Equity Incentive Plan | 10-Q | 001-38933 | 10.1 | September 3, 2020 | |
| 10.4† | Form of Global Restricted Stock Unit Agreement Outside Directors – Initial Grant under the Company's 2019 Equity Incentive Plan | 10-K | 001-38933 | 10.4 | March 18, 2021 | |
| 10.5† | CrowdStrike Holdings, Inc. 2019 Equity Incentive Plan Global Performance Unit Agreement | 10-Q | 001-38933 | 10.1 | June 3, 2020 | |
| 10.6† | Amended and Restated 2011 Stock Incentive Plan and related form agreements. | S-1 | 333-231461 | 10.4 | May 14, 2019 | |
| 10.7† | Amended and Restated 2019 Employee Stock Purchase Plan and related form agreements. | 10-Q | 001-38933 | 10.2 | September 1, 2021 | |
| 10.8† | CrowdStrike Holdings, Inc. Corporate Incentive Plan. | 10-Q | 001-38933 | 10.1 | June 1, 2023 | |
| 10.9† | Outside Director Compensation Policy, as amended on June 19, 2024. | 10-Q | 001-38933 | 10.1 | August 29, 2024 | |
| 10.10† | Employment Agreement between the Registrant and George Kurtz, dated as of November 18, 2011. | S-1 | 333-231461 | 10.6 | May 14, 2019 | |
| 10.11† | Offer Letter between the Registrant and Burt W. Podbere, dated as of August 10, 2015. | S-1 | 333-231461 | 10.8 | May 14, 2019 | |
| 10.12 | Office Lease Agreement between EQC Capitol Tower Property LLC and CrowdStrike, Inc., dated April 20, 2018. | 10-K | 001-38933 | 10.18 | March 16, 2022 | |

| | | | | | | |
|---------|--|------|-----------|-------|-------------------|---|
| 10.13 | First Amendment to Office Lease Agreement between EQC Capitol Tower Property LLC and CrowdStrike, Inc., dated June 6, 2019. | 10-K | 001-38933 | 10.19 | March 16, 2022 | |
| 10.14 | Amended and Restated Credit Agreement dated as of January 4, 2021, as amended on January 6, 2022 among CrowdStrike Holdings, Inc., as guarantor, CrowdStrike, Inc. as borrower, and Silicon Valley Bank and the other lenders party thereto. | 10-K | 001-38933 | 10.20 | March 16, 2022 | |
| 10.15† | Amended and Restated Performance Unit Agreement with George Kurtz, dated September 1, 2021, under the CrowdStrike Holdings, Inc. 2019 Equity Incentive Plan. | 10-Q | 001-38933 | 10.4 | September 1, 2021 | |
| 10.16† | Change in Control and Severance Agreement, dated as of September 1, 2021, by and between CrowdStrike Holdings, Inc. and George Kurtz. | 10-Q | 001-38933 | 10.3 | September 1, 2021 | |
| 10.17† | Performance Unit Agreement with Burt Podbere, dated January 12, 2022, under the CrowdStrike Holdings, Inc. 2019 Equity Incentive Plan. | 8-K | 001-38933 | 10.1 | January 14, 2022 | |
| 10.18† | Offer Letter between the Registrant and Shawn Henry, dated as of March 4, 2012. | 10-Q | 001-38933 | 10.2 | June 4, 2021 | |
| 10.19 | Second Amendment to Office Lease between EQC Capitol Tower Property LLC and CrowdStrike, Inc., dated January 19, 2023 | 10-K | 001-38933 | 10.26 | March 9, 2023 | |
| 10.20† | CrowdStrike, Inc. Deferred Compensation Plan Adoption Agreement, dated May 4, 2023. | 10-K | 001-38933 | 10.20 | March 7, 2024 | |
| 10.21† | CrowdStrike, Inc. Deferred Compensation Plan, dated January 1, 2023. | 10-K | 001-38933 | 10.21 | March 7, 2024 | |
| 10.22† | Offer Letter between CrowdStrike, Inc. and Michael Sentonas, dated as of March 22, 2021. | 10-Q | 001-38933 | 10.1 | June 5, 2024 | |
| 19.1 | Insider Trading Policy | | | | | X |
| 21.1 | List of Subsidiaries of the Registrant. | | | | | X |
| 22.1 | List of Subsidiary Guarantors | | | | | X |
| 23.1 | Consent of PricewaterhouseCoopers LLC, independent registered public accounting firm. | | | | | X |
| 24.1 | Power of Attorney (reference is made to the signature page hereto). | | | | | X |
| 31.1 | Certification of the Principal Executive Officer pursuant to Exchange Act Rules 13a14(a) and 15d14(a), as adopted pursuant to Section 302 of the Sarbanes-Oxley Act of 2002. | | | | | X |
| 31.2 | Certification of the Principal Financial Officer pursuant to Exchange Act Rules 13a14(a) and 15d14(a), as adopted pursuant to Section 302 of the Sarbanes-Oxley Act of 2002. | | | | | X |
| 32.1* | Certification of the Principal Executive Officer and Principal Financial Officer pursuant to 18 U.S.C. Section 1350, as adopted pursuant to Section 906 of the Sarbanes-Oxley Act of 2002. | | | | | X |
| 97.1 | Compensation Recovery Policy | 10-K | 001-38933 | 97.1 | March 7, 2024 | |
| 101.INS | Inline XBRL Instance Document | | | | | X |
| 101.SCH | Inline XBRL Taxonomy Extension Schema Document | | | | | X |
| 101.CAL | Inline XBRL Taxonomy Extension Calculation Linkbase Document | | | | | X |
| 101.DEF | Inline XBRL Taxonomy Extension Definition Linkbase Document | | | | | X |
| 101.LAB | Inline XBRL Taxonomy Extension Label Linkbase Document | | | | | X |
| 101.PRE | Inline XBRL Taxonomy Extension Presentation Linkbase Document | | | | | X |

| | | |
|-----|---|---|
| 104 | Cover Page Interactive Data File – the cover page XBRL tags are embedded within the Inline Instance XBRL document | X |
|-----|---|---|

† Indicates management contract or compensatory plan, contract or agreement.

* The certifications furnished in Exhibit 32.1 hereto are deemed to accompany this Annual Report on Form 10-K and will not be deemed “filed” for purposes of Section 18 of the Securities Exchange Act of 1934, as amended, except to the extent that the registrant specifically incorporates it by reference.

SIGNATURES

Pursuant to the requirements of the Securities Act of 1934, the Registrant has duly caused this report to be signed on its behalf by the undersigned, thereunto duly authorized on the day of March 10, 2025.

CROWDSTRIKE HOLDINGS, INC.

By: /s/ George Kurtz

George Kurtz
*President, Chief Executive Officer and Director (Principal
Executive Officer)*

POWER OF ATTORNEY

KNOW ALL THESE PERSONS BY THESE PRESENTS, that each person whose signature appears below constitutes and appoints George Kurtz and Burt W. Podbere, and each of them, as his or her true and lawful attorney-in-fact and agent, with full power of substitution and resubstitution, for him or her and in his or her name, place and stead, in any and all capacities, to sign any and all amendments to this Annual Report on Form 10-K, and to file the same, with all exhibits thereto, and other documents in connection therewith, with the Securities and Exchange Commission, granting unto said attorneys-in-fact and agents, and each of them, full power and authority to do and perform each and every act and thing requisite and necessary to be done in connection therewith, as fully to all intents and purposes as he or she might or could do in person, hereby ratifying and confirming all that said attorneys-in-fact and agents, or any of them, or their, his or her substitutes, may lawfully do or cause to be done by virtue thereof.

Pursuant to the requirements of the Securities Exchange Act of 1934, this report has been signed below by the following persons on behalf of the Registrant and in the capacities and on the dates indicated.

| Signature | Title | Date |
|---|---|----------------|
| <u>/s/ George Kurtz</u> George Kurtz | President, Chief Executive Officer, and Director (Principal Executive Officer) | March 10, 2025 |
| <u>/s/ Burt W. Podbere</u> Burt W. Podbere | Chief Financial Officer (Principal Financial Officer) | March 10, 2025 |
| <u>/s/ Anurag Saha</u> Anurag Saha | Chief Accounting Officer (Principal Accounting Officer) | March 10, 2025 |
| <u>/s/ Gerhard Watzinger</u> Gerhard Watzinger | Chairman of the Board of Directors | March 10, 2025 |
| <u>/s/ Cary J. Davis</u> Cary J. Davis | Director | March 10, 2025 |
| <u>/s/ Denis J. O’Leary</u> Denis J. O’Leary | Director | March 10, 2025 |
| <u>/s/ Godfrey R. Sullivan</u> Godfrey R. Sullivan | Director | March 10, 2025 |
| <u>/s/ Johanna Flower</u> Johanna Flower | Director | March 10, 2025 |
| <u>/s/ Laura J. Schumacher</u> Laura J. Schumacher | Director | March 10, 2025 |
| <u>/s/ Roxanne S. Austin</u> Roxanne S. Austin | Director | March 10, 2025 |
| <u>/s/ Sameer K. Gandhi</u> Sameer K. Gandhi | Director | March 10, 2025 |

