公司评级	增持（首次）
报告日期	2025 年 04 月 11 日

基础数据

4 月 9 日收盘价（美元）	378.01
总市值（亿美元）	936.99
总股本（亿股）	2.48

来源：wind，兴业证券经济与金融研究院整理

相关研究

分析师：洪嘉骏
S0190519080002
BPL829
hongjiajun@xyzq.com.cn

分析师：周路昀
S0190522070002
请注意：周路昀并非香港证券及期货事务监察委员会的注册持牌人，不可在香港从事受监管的活动。
zhouluyun@xyzq.com.cn

CrowdStrike Holdings, Inc.
Class A(CRWD.O)

美股

风险图谱构筑壁垒，轻量代理脱颖而出

投资要点：

- **营收稳步增长，Non-GAAP 净利润稳健提升。**CrowdStrike 是一家海外网络安全解决方案提供商，为企业提供终端、云工作负载、身份、数据等风险领域的保护服务。2025 财年公司实现营收 39.5 亿美元（YoY+29%），GAAP 净亏损 0.19 亿美元，GAAP 净利率-0.5%，同比-3.4pcts；Non-GAAP 净利润 9.9 亿美元（YoY+31%），净利率 25.0%，同比+0.4pct。

- **风险图数据库和云原生平台铸就差异化，与三大云厂商集成提高客户渗透率。**公司以平台化产品布局网络安全解决方案，横跨终端安全、云安全、威胁情报&狩猎、下一代 SIEM、身份保护、数据保护等细分赛道。

  - **性能优势：**公司基于自主研发的风险图数据库（Threat Graph）提供强大检测、分析、可见性和可扩展性功能；先后发布攻击指标（IoA，Indicator of Attack）及 AI 驱动的 IoA，进一步提升数据检测和分析能力。

  - **架构优势：**公司采用单一轻量级代理+单一控制台架构，提升效率，简化部署，实现低系统延迟。公司积极拓展 AI 产品，Charlotte AI 旨在提升效率，AI-SPM 和 AI 红队则丰富现有产品，收购的 Adaptive Shield 补强云安全功能，预计 2025 自然年 TAM 将达 400 亿美元（YoY+33%）。

  - **生态优势：**公司与微软、谷歌、Amazon 等云厂商持续深化合作，其中与微软内核模式兼容的战略选择以及后续与 Defender、Intune 和 EntraID 的协同将进一步扩大成长空间。

- **“产品+销售创新”驱动未来增长，云安全、身份保护和下一代 SIEM 有望成为发展引擎。**产品方面，公司自 2020 自然年始逐步通过“内部创新+外部收购+合作伙伴协同”实现关键模块功能整合，提供完整的云安全生态系统覆盖，预计云安全、身份保护和下一代 SIEM 模块 2028 自然年 TAM 分别达 310 亿美元（相较于 2025 自然年的 170 亿美元）、170 亿美元（相较于 2025 自然年的 100 亿美元）、160 亿美元，带来公司新的增长曲线。销售方面，719 事件后，公司推出 Falcon Flex 的灵活销售计划和客户承诺包等，修复短期客户留存率的同时有望加速推进客户多模块、跨模块采用，实现在 2031 财年前达到 100 亿美元 ARR 的长期增长目标。

- **投资建议：**719 事件负面影响我们预计将逐季消散，我们看好公司差异化产品质量、创新集成能力及灵活销售体系在网络安全行业新趋势中的长期价值。预计公司 2026/2027/2028 财年营收分别为 47.75/58.56/72.36 亿美元，Non-GAAP 净利润分别为 9.06/12.75/18.23 亿美元，当前市值对应 FY2026/27/28 年 P/S 值分别为 19.6/16.0/12.9。首次覆盖，给予“增持”评级。

- 风险提示：企业安全支出不及预期；行业竞争加剧；公司创新速度放缓。

主要财务指标

会计年度	FY2025	FY2026E	FY2027E	FY2028E
营业总收入（百万美元）	3,954	4,775	5,856	7,236
同比增长	29.2%	20.8%	22.6%	23.6%
毛利率	78.1%	78.4%	78.9%	79.3%
Non-GAAP 净利润（百万美元）	988	906	1,275	1,823
Non-GAAP 净利润率	25.0%	19.0%	21.8%	25.2%
稀释 EPS（美元）	4.05	3.61	4.99	6.96

数据来源：wind，兴业证券经济与金融研究院整理
注：每股收益均按照新股本摊薄计算

Company Rating	Outperform(Initiate)
Report Date	April 11, 2025

Basic Data

Closing Price(USD)	378.01
Total market value(Mn)	936.99
Total Shares (Mn)	2.48

Related Report

Analyst：Jiajun HONG
SAC：S0190519080002
SFC：BPL829
hongjiajun@xyzq.com.cn

Analyst：Luyun ZHOU
SAC：S0190522070002
zhouluyun@xyzq.com.cn

Please note： Luyun ZHOU is not a registered licensee of the Securities and Futures Commission of Hong Kong and is not allowed to engage in regulated activities in Hong Kong

CrowdStrike Holdings, Inc. Class A（CRWD.O） Nasdaq

Threat Graph Fortifies Defenses, Lightweight Agent Reigns Supreme

Investment Highlights:

- **Revenue Steady Growth, Non-GAAP Net Profit keeps improving**：CrowdStrike is an overseas cybersecurity solutions provider offering protection services for enterprises in risk areas such as endpoints, cloud workloads, identity, and data. In fiscal year 2025, the company achieved revenue of 3.95 billion (YoY+29%) and GAAP net loss of 19 million, with GAAP net profit margin of -0.5% (down 3.4 percentage points YoY). Non-GAAP net profit reached $988 million (YoY+31%), with a net profit margin of 25.0% (up 0.4 percentage point YoY).
- **Threat Graph Database and Cloud-Native Platform Create Differentiation, Integration with Major Cloud Providers Boosts Customer Penetration:**The company adopts a platform-based strategy for cybersecurity solutions, spanning segments such as endpoint security, cloud security, threat intelligence & hunting, next-gen SIEM, identity protection, and data protection.
- **Performance Advantages:** Leveraging its self-developed Threat Graph database, the company delivers robust detection, analysis, visibility, and scalability. The introduction of Indicators of Attack (IoA) and AI-driven IoA, synergized with the Threat Graph database, further enhances data detection and analysis capabilities.
- **Architectural Advantages:** The single lightweight agent + single console architecture improves efficiency, simplifies deployment, and ensures low system latency. The company actively expands AI products: Charlotte AI boosts efficiency, AI-SPM and AI Red Team enrich existing offerings, and the acquisition of Adaptive Shield enhances cloud security capabilities. The cybersecurity AI TAM is expected to reach $40 billion by calendar year 2025 (YoY +33%).
- **Ecosystem Advantages:** Continued collaboration with cloud providers like Microsoft, Google, and Amazon, particularly strategic compatibility with Microsoft's kernel mode and integration with Defender, Intune, and Entra ID, will further expand growth opportunities.
- **"Product + Sales Innovation" Drives Future Growth; Cloud Security, Identity Protection, and Next-Gen SIEM to Fuel Expansion: Product Strategy:** Since calendar year 2020, the company has integrated key module functionalities through "internal innovation + external acquisitions + partner collaboration," offering the industry's most comprehensive cloud security ecosystem. Cloud security, identity protection, and next-gen SIEM are projected to achieve TAMs of 31 billion (vs.17 billion in calendar year 2025),17 billion (vs.10 billion in calendar year 2025), and 16 billion, respectively, by calendar year 2028, driving new growth curves. **Sales Strategy:** Post the "719incident," the company introduced flexible sales plans like Falcon Flex and customer commitment packages to stabilize short-term retention while accelerating multi-module and cross-module adoption, fueling to achieve the long-term goal of 10 billion in Annual Recurring Revenue (ARR) by fiscal year 2031.
- **Investment Recommendation:**We expect the negative impact of the "719 incident" to diminish quarterly. Long-term, we remain optimistic about the company's differentiated product quality, innovative integration capabilities, and flexible sales system in the evolving cybersecurity landscape. We forecast fiscal year 2026 /2027 /2028 revenue of 4.775 billion, 5.856 billion, and 7.236 billion, with Non-GAAP net profits of 906 million, 1.275 billion and 1.823 billion, and the current market capitalization corresponds to P/S values of 19.6, 16.0, and 12.9 for fiscal year 2026 /2027 /2028, respectively. Initiating coverage with an "Overweight" rating.
- **Potential risks**：Enterprise security spending falls short of expectations; Intensified industry competition; Slowed pace of company innovation.

Key Financial Indicators

FY	FY2025	FY2026E	FY2027E	FY2028E
Revenue (USD/Mn)	3,954	4,775	5,856	7,236
YoY	29.2%	20.8%	22.6%	23.6%
Gross Margin	78.1%	78.4%	78.9%	79.3%
Non-GAAP Net Income (USD/Mn)	988	906	1,275	1,823
Non-GAAP Net Profit Margin	25.0%	19.0%	21.8%	25.2%
EPS (USD)	4.05	3.61	4.99	6.96

Source: Company Disclosure, Industrial Securities Research Institute
Notes: The EPS was diluted based on the current outstanding shares

目录

图目录

表目录

一、公司基本情况

（一）CrowdStrike 是海外地区网络安全服务公司

CrowdStrike 由 George Kurtz 创立，专注于终端和云工作负载、身份、数据等风险领域的保护服务，提供云原生、平台化的网络安全解决方案。

- **起步阶段（2011 年-2017 年）：建立平台，初步定型商业模式。**CrowdStrike 由 George Kurtz 成立于 2011 年，致力于提供云时代安全解决方案。2012 年 7 月，CrowdStrike 推出威胁情报模块，13 年 6 月推出终端检测和响应模块，8 月推出托管威胁狩猎模块。2016 年 11 月，CrowdStrike Falcon 平台被认证为传统防病毒软件（AV）的替代方案，**在单一平台上创造性地整合了防病毒、EDR 和威胁情报狩猎服务功能，构筑平台产品核心优势。**2017 年 1 月，CrowdStrike 推出漏洞管理模块，进一步降低安全风险。
- **扩张阶段（2018 年-2021 年）：全球扩张，丰富产品设计+深耕解决方案。**2018 年 4 月，CrowdStrike 推出托管检测与响应（MDR）服务，提升组织对复杂网络威胁的检测能力和响应效率，同年 8 月推出设备控制模块。9 月，CrowdStrike 获得了联邦风险与授权管理计划（FedRAMP）认证，进一步在政府和公共部门应用中扩张。2019 年 3 月，CrowdStrike 推出增强型检测与响应（EDR）模块，提供更深入的威胁检测和响应能力。**19 年 6 月，CrowdStrike 在纳斯达克上市，股票代码“CRWD”。**11 月，推出防火墙管理模块，进一步强化网络安全领域产品线。2020 年 2 月，CrowdStrike 推出保护云工作负载模块和终端恢复服务。2021 年 1 月，CrowdStrike 收购 Humio，提升其在数据收集、存储和分析方面的能力。5 月，推出安全编排、自动化和响应框架（SOAR），以提高对安全事件的响应速度和效率。7 月，CrowdStrike 引入托管威胁情报服务，为企业提供专业的威胁情报分析和支持。10 月，CrowdStrike 发布开放协作平台 Crowd XDR Alliance，通过扩展检测和响应（XDR）提升网络安全防护能力。11 月，CrowdStrike 收购专注于数据保护和访问控制的供应商 Secure Circle。
- **成熟阶段（2022 至今）：构建平台，覆盖云生态系统+加入 AI 引擎。**2022 年 2 月，CrowdStrike 推出扩展检测和响应解决方案 Falcon XDR，3 月推出托管身份威胁保护服务。4 月，CrowdStrike 引入云原生应用保护平台能力，提供行业完整的 CNAPP 服务，6 月推出 CrowdStrike Asset Graph 提供全面的资产管理和安全态势视图，7 月推出云威胁狩猎服务，主动监测识别云环

境中的潜在威胁。8 月，CrowdStrike 推出行业首个 AI 驱动的攻击指标，使用 AI 技术识别分析攻击模式。9 月，CrowdStrike 允许所有 EDR 客户访问 XDR 功能。2023 年 4 月，CrowdStrike 推出全球首个针对物联网的 XDR，同时发布 Falcon Complete XDR，为企业提供一体化的安全保护。5 月，CrowdStrike 获得针对处理敏感政府数据的云服务 IL5 安全认证。9 月，CrowdStrike 收购业界完整的代码到运行时保护应用程序的网络安全平台 Bionic，推出无代码应用开发平台 Falcon Foundry。2024 年 2 月，CrowdStrike 正式推出 Charlotte AI，同时推出 Falcon for IT，提供与 IT 基础设施的无缝集成。3 月，CrowdStrike 收购 Flow Security，进一步扩展云安全和应用程序安全领域服务能力。2024 年 11 月，CrowdStrike 宣布收购 SaaS 安全领域供应商 Adaptive Shield，将成为唯一提供针对身份攻击的统一端到端保护的网络安全供应商，覆盖整个现代云生态系统。

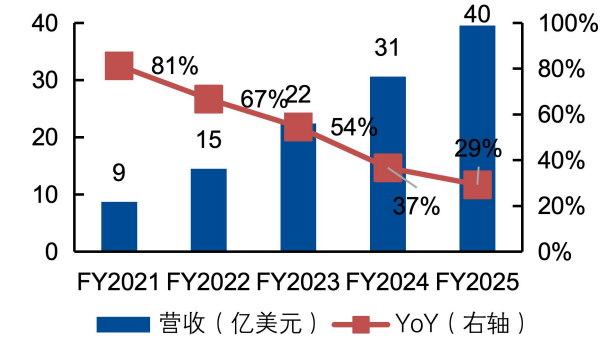
图 1、CrowdStrike 发展历程

数据来源：公司官网，兴业证券经济与金融研究院整理
注：图中年度数据以自然年为统一标准

（二）订阅服务为基，盈利能力持续改善

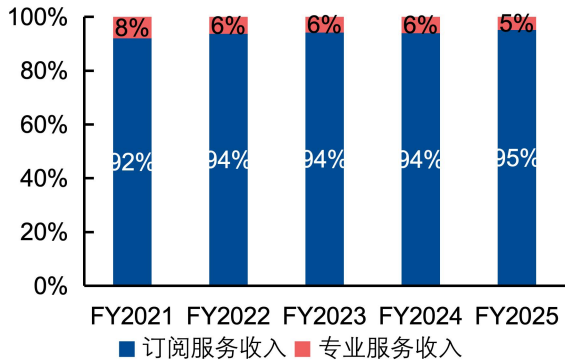
- **收入：同比高增速，订阅服务占比提升。** 2025 财年公司实现营收 39.5 亿美元，同比增长 29.2%，高同比基数下保持高增速，主要得益于公司高效的业务执行以及对创新引擎的持续投资。分业务板块来看，订阅服务收入 37.6 亿美元（YoY+31.1%），营收占比为 95%（同比+1pct）；专业服务收入达 1.9 亿美元（YoY+3.9%），营收占比 5%（同比-1pct）。

图 2、FY2021-2025 公司营收及增速



数据来源：公司季度报，兴业证券经济与金融研究院整理
注：FY2025 期间为 2024.2.1-2025.1.31

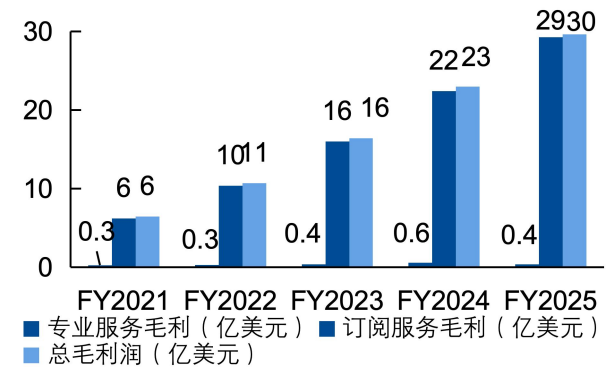
图 3、FY2021-2025 公司营收结构



数据来源：公司季度报，兴业证券经济与金融研究院整理
注：FY2025 期间为 2024.2.1-2025.1.31

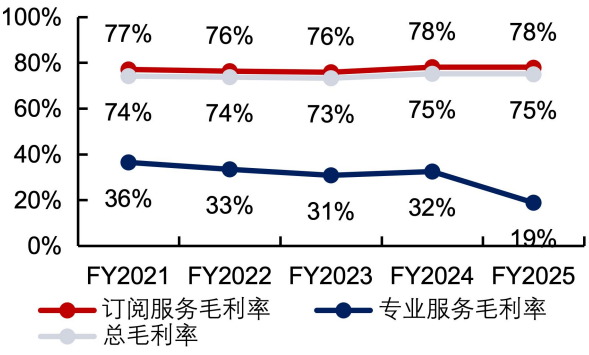
- **利润：毛利率持续改善，费用结构优化释放盈利能力。**得益于 Falcon 平台提供的卓越客户价值，以及公司在数据中心和工作负载优化方面的持续投资，FY25 公司 GAAP 整体毛利润达 29.6 亿美元，GAAP 毛利率 75%（同比持平），Non-GAAP 毛利润达 30.9 亿美元，Non-GAAP 毛利润率 78%（同比持平），主要受到专业服务毛利率较低影响。GAAP 总费用率 78.0%（YoY+2.8pcts），费用结构进一步优化：其中 GAAP 营销费用为 15.2 亿美元（YoY+33.6%），营销费用率 38.5%，同比+1.3pcts；GAAP 研发费用 10.8 亿美元（YoY+40.1%），研发费用率 27.2%，同比+2.1pcts；GAAP 管理费用 4.8 亿美元（YoY+22.8%），管理费用率 12.2%，同比-0.6pct。

图 4、FY2021-2025 年公司订阅服务和专业服务 GAAP 毛利润



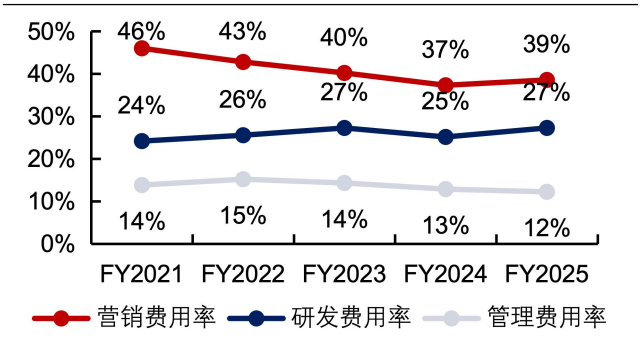
数据来源：公司季度报，兴业证券经济与金融研究院整理
注：FY2025 期间为 2024.2.1-2025.1.31

图 5、FY2021-2025 年公司 GAAP 毛利率



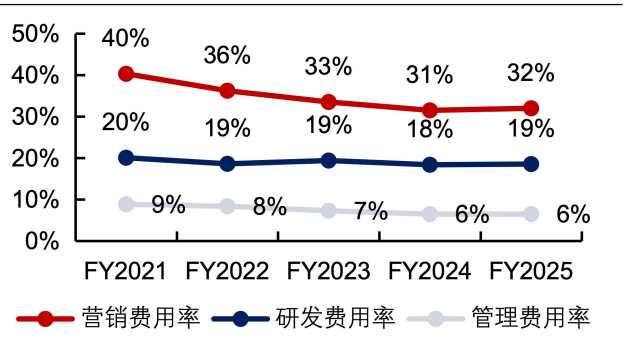
数据来源：公司季度报，兴业证券经济与金融研究院整理
注：FY2025 期间为 2024.2.1-2025.1.31

图 6、FY2021-2025 年公司 GAAP 费用率



数据来源：公司季度报，兴业证券经济与金融研究院整理
注：FY2025 期间为 2024.2.1-2025.1.31

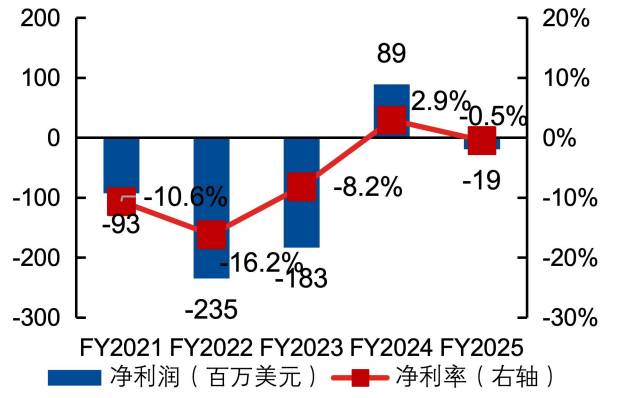
图 7、FY2021-2025 年公司 Non-GAAP 费用率



数据来源：公司季度报，兴业证券经济与金融研究院整理
注：FY2025 期间为 2024.2.1-2025.1.31

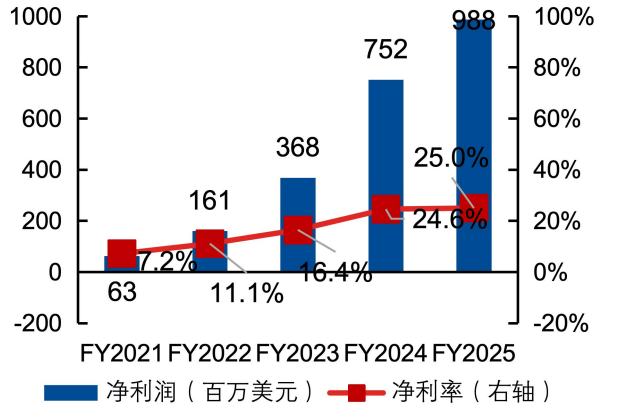
- 净利润及净利率：Non-GAAP 净利润稳健提升。FY25 公司 GAAP 净亏损 0.19 亿美元，GAAP 净利润率为-0.5%，同比-3.4pcts，主要受到收购 Adaptive Shield 的 0.50 亿美元税费和 719 事件相关的 0.21 亿美元费用影响。Non-GAAP 净利润 9.9 亿美元，Non-GAAP 净利润率为 25.0%，同比+0.4pct。

图 8、FY2021-2025 年公司 GAAP 净利润



数据来源：公司季度报，兴业证券经济与金融研究院整理
注：FY2025 期间为 2024.2.1-2025.1.31

图 9、FY2021-2025 年公司 Non-GAAP 净利润



数据来源：公司季度报，兴业证券经济与金融研究院整理
注：FY2025 期间为 2024.2.1-2025.1.31

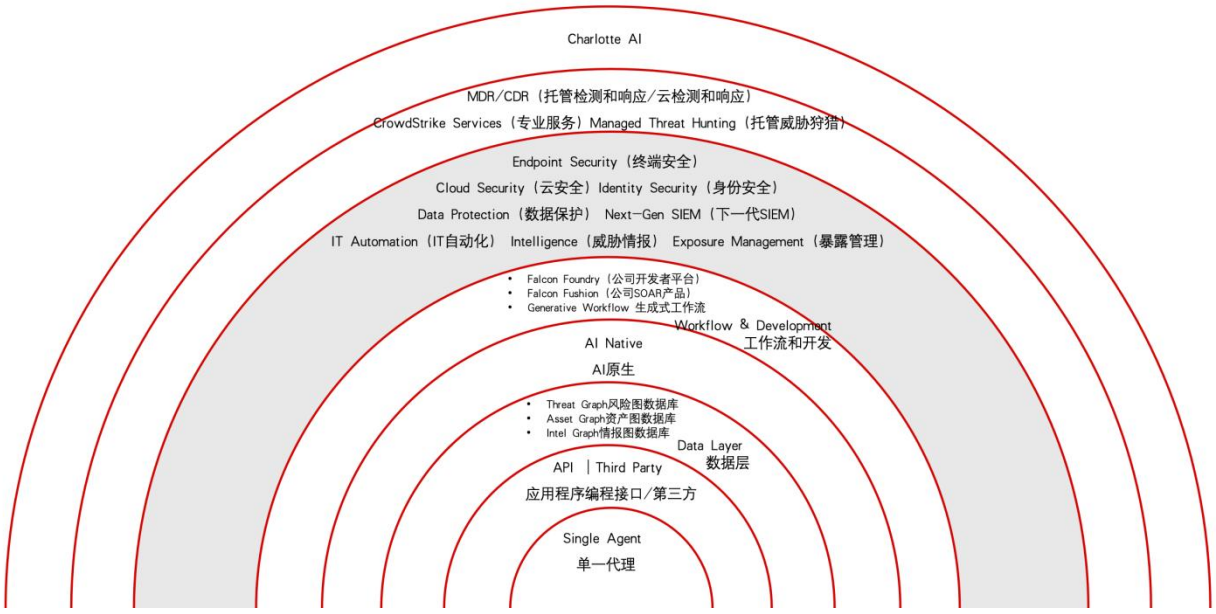
二、公司分析：整合安全服务，Threat Graph 和 AI 驱动平台铸就差异化

（一）云原生平台为基，集成全面的安全服务

CrowdStrike 在成立之初是基于风险图数据库（Threat Graph）构建网络安全平台的供应商。公司基于风险图数据库和 AI 驱动，在单一平台+单一代理上创造性

地整合了防病毒、EDR 和威胁情报狩猎服务功能。目前，公司主要产品为 Falcon 平台，包含 Falcon Insight、Falcon Prevent、Falcon Forensics 等细分产品，提供终端安全、云安全、身份保护、数据安全、威胁情报识别与猎杀、下一代 SIEM、SaaS 安全、暴露管理、IT 自动化、网络安全生成式 AI 等领域的订阅产品，同时包括不按订阅收费的专业服务（包括事件响应和主动服务、取证和恶意软件分析、归因分析）。

图 10、Falcon 平台架构



数据来源：公司投资者 PPT，兴业证券经济与金融研究院整理

1. 终端安全：CrowdStrike 广泛功能融合提升整体 MDR 能力

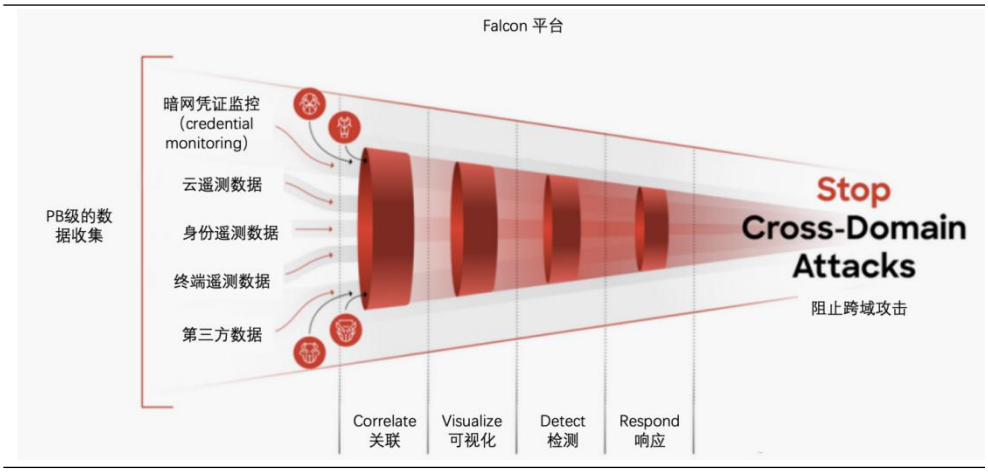
托管检测和响应（MDR，Managed Detection and Response）主要包括终端检测和响应（EDR，Endpoint Detection and Response）和安全信息与事件管理（SIEM，Security Information and Event Management）能力。此外，XDR（扩展检测与响应）通常被视为 EDR 的演进，它通过集成身份、云和 IT 数据等原生或第一方数据来扩展传统的终端可见性，为增强 MDR 提供了新的机会。然而，XDR 对原生数据的关注可能会带来安全漏洞，尤其是在缺乏第三方数据的情况下。此外，各种用例（如审计、合规性和取证调查）需要强大的日志管理（Log Management）功能，而这些功能超出了 XDR 的范围，因此 CrowdStrike 选择通过下一代 SIEM 增强 XDR。根据 IDC，CrowdStrike 的 Falcon 平台内置广泛的能力（如云工作负载保护和身份保护），提供对每个系统中每个身份和账户的细粒度实时可见性，缩小攻击面，同时启用强大的控制措施以防止被盗凭证的滥用，为 MDR 服务提供强大的技术支持。

表 1、CrowdStrike MDR 技术产品组件

板块	作用	公司产品	CrowdStrike 产品特殊性
XDR	跨平台检测安全数据-->利用机器学习和行为分析,识别复杂攻击模式+结合遥测数据源提高检测能力-->自动化响应	Falcon Insight XDR	● 利用 Charlotte AI 驱动的 EDR+威胁情报和专家见解； ● 提供实时响应（RTR，Real Time Response），通过 Falcon Fusion SOAR 简化、自动化大规模复杂任务； ● 通过原生扩展检测与响应（XDR，Extended Detection and Response）扩展控制，结合身份、云、移动和数据保护模块的上下文，可视化和响应事件；
		Falcon Insight for IoT	● 基于 CrowdStrike 的专业知识提供全天候 MDR ● 利用深度威胁情报，量身定制威胁预防策略和 AI 驱动的检测； ● 不干扰客户业务运营； ● 可利用 Falcon Fusion 或第三方 SOAR 工具自动化重复性任务 ● 无需读取或扫描内容实现检测；
		Falcon for Mobile	● 协同 Falcon® Fusion，内置恶意 IP 黑名单； ● 允许客户利用其现有的统一终端管理和移动设备管理工具（MDM，Mobile Device Management ）部署，同时保护个人隐私； ● 通过统一的平台控制每台设备，监控实时事件，避免静默故障
下一代防病毒（Next-Gen Antivirus）	识别程序行为-->实时分析威胁检测-->监控和保护系统内存-->自动隔离/修复受影响的文件	Falcon Prevent	● 与 AI、威胁情报、行为分析、高性能内存扫描和漏洞缓解协同工作； ● 涵盖 Windows、macOS 和 Linux 等主要操作系统； ● 结合上下文分析网络威胁情报，将对手行为映射到熟悉的 MITRE 对抗技术、战术和程序框架
设备管理（Device Control）	管控制对外部设备（如 USB 驱动器）的访问-->实时监控设备-->实施安全策略，限制使用或访问权限	Falcon Device Control	● 允许客户查看全面的文件元数据和 USB 活动上下文，进行主动防御； ● 通过机器学习检测源代码的移动； ● 实施细致的访问权限，允许客户在执行之前测试 USB 访问规则影响
防火墙管理	流量监控-->配置和管理防火墙规则-->入侵防御	Falcon Firewall Management	● 允许客户使用自己或 CrowdStrike 提供的模板管理防火墙政策； ● 可在几分钟内部署+投入运行； ● 提供防火墙可视化服务； ● 客户可轻松启用或禁用特定防火墙规则、组或政策
数据丰富、收集、关联	从各种来源收集安全数据-->添加上下文信息-->关联不同来源的数据识别潜在的安全事件和攻击模式	Falcon Forensics	● 通过直观的仪表板展示历史和实时数据中的活动和趋势； ● 自动化数据收集、丰富和与威胁情报的关联简化工作流程； ● 覆盖 Windows、macOS 和 Linux 操作系统，支持调查不同数据类型
MDR	事件调查-->制定+实施事件响应计划-->提供安全报告，满足合规要求	Falcon Complete	● 结合 MDR、Adversary OverWatch 和 AI 驱动的智能威胁猎捕； ● 提供 24/7 全天候覆盖，使客户组织无需承受内部构建程序的困难、负担和成本，弥补客户组织面临的技能差距； ● 4 分钟内实现高级威胁检测
下一代 SIEM	数据收集、存储-->事件关联、上下文分析-->警报通知、事件响应-->提供可视化界面，生成合规报告	Falcon Next-Gen SIEM	● 每天免费处理 10GB 的数据摄取； ● 开箱即用，简化设置； ● 使用实时、精准的攻击指标（IoA）阻止数据泄露； ● 提供可视化图表，协助客户了解攻击的根本原因，搜索性能比遗留 SIEM 快 150 倍； ● 利用 Fusion SOAR 进行无代码工作流自动化，协调端点和第三方工具的行动，限制横向移动； ● 结合 Charlotte AI 和 CrowdStrike 威胁情报中的 230+对手及其战术，提升决策速度

数据来源：公司风险图谱白皮书，兴业证券经济与金融研究院整理

图 11、Falcon 平台工作流程示意图



数据来源：公司官网，兴业证券经济与金融研究院整理

2. 云安全：提供全面的 CNAPP

CrowdStrike 云原生应用程序保护平台（CNAPP，Cloud Native Application Protection Platform）Falcon Cloud Security 通过统一集成平台，提供全面一致的覆盖和构建到运行/代码到云的上下文，帮助用户组织识别、关联、分类、优先处理和修复整个应用和云生命周期中的漏洞和安全风险，降低使用复杂性；同时支持无代理和有代理扫描，提供即时可见性和快速云环境评估，为工作负载和应用提供动态运行时的保护能力。此外，公司 CNAPP 平台与专用于云安全的云检测和响应（CDR, Cloud Detection & Response，侧重于威胁检测、即时事件响应和云服务集成）、XDR 和 MDR 服务无缝集成，提供跨所有层（包括云、终端和身份）的端到端可见性和保护，并与 AWS、GCP、Azure 等云管理平台实现协同。

根据 Frost & Sullivan 2024 年 CNAPP 报告，CNAPP 主要用于满足企业组织从代码到云的可见性、安全态势和风险管理、运行时保护和威胁管理三方面需求。CrowdStrike CNAPP 平台完整覆盖从代码到云的可见性、安全态势和风险管理、运行时保护和威胁管理三个板块。相较于缺乏 DSPM、ASPM 的 SentinelOne，CDR、威胁情报&狩猎不完整的 Palo Alto Networks，ASPM、威胁狩猎&情报缺乏与 CDR 不完整的 Wiz（Alphabet），公司提供行业首个完全集成的云安全解决方案。

- **从代码到云的可见性**：具体包括云工作负载保护平台（CWPP，Cloud Workload Protection Platform）、云安全态势管理（CSPM，Cloud Security Posture Management）、漏洞管理（Vulnerability Management）、数据安全和保护管理（DSPM，Data Security Posture Management）、云身份和权限管理（CIEM，Cloud Infrastructure and Entitlement Management）等用例。

- **安全态势和风险管理**：主要涵盖基础设施即代码扫描（IaC Scanning）、软件物料清单（SBOM，Software Bill of Materials）、应用安全态势管理（ASPM，Application Security Posture Management）和 AI 安全态势管理（AI-SPM，AI Security Posture Management）等模块。
- **运行时保护和威胁管理**：包含云工作负载保护平台（CWPP，Cloud Workload Protection Platform），云检测和响应（CDR, Cloud Detection & Response），云安全态势管理（CSPM，Cloud Security Posture Management）和威胁狩猎与情报（Threat Hunting & Intelligence）模块。

表 2、SentinelOne、Palo Alto Networks、Wiz（Alphabet）和 CrowdStrike CNAPP 产品功能对比

板块	技术	SentinelOne	Palo Alto Networks	Wiz（Alphabet）	CrowdStrike
从代码到云的可见性	CWPP	☑	☑	☑	☑
	CSPM	☑	☑	☑	☑
	漏洞管理	☑	☑	☑	☑
	DSPM	缺乏	☑	☑	☑
	CIEM	☑	☑	☑	☑
安全态势和风险管理	IaC 扫描	☑	☑	☑	☑
	SBOM	☑	☑	☑	☑
	ASPM	缺乏	☑	缺乏	☑
	AI-SPM	☑	☑	☑	☑
运行时保护和威胁管理	CWPP	☑	☑	☑	☑
	CSPM	☑	☑	☑	☑
	CDR	☑	依赖静态行为为基线进行检测，导致客户在部署新工作负载时面临 24 小时的漏洞风险	缺乏内部管理服务、数字取证和事件响应（DFIR，Digital Forencis and Incident Response）、原生安全模块（如 EDR、身份保护、威胁情报、暴露管理）	☑
	威胁狩猎与情报	☑	缺乏对手档案；Autofocus 仅提供基本的对手归属信息	缺乏	☑

数据来源：各公司官网，Frost & Sullivan 2024 CNAPP 报告，兴业证券经济与金融研究院整理
注：2025 年 3 月 18 日，谷歌母公司 Alphabet 宣布将以 320 亿美元现金收购网络安全公司 Wiz

3. 身份安全：主动阻止基于身份的攻击

包含身份安全态势管理（ISPM，Identity Security Posture Management），身份威胁检测与响应（ITDR，Identity Threat Detection and Response），持续访问评估配置文件（CAEP，Continuous Access Evaluation Profile），用户和实体行为分析（User and Entity Behavior Analytics），零信任（Zero Trust），非人类身

份（Non-Human Identities）保护和可视化等技术组件，同时与 Falcon Complete 协同，提供主动的身份保护服务。此外，CrowdStrike 收购的 Adaptive Shield 业务将对在本地、SaaS 应用程序中或者超大规模基础设施中的身份提供全面保护。

4. 暴露管理：原生漏洞管理+集成的攻击面管理替代传统漏洞管理

Falcon Exposure Management：CrowdStrike 暴露管理为设备和应用程序提供原生漏洞管理，并结合集成的攻击面管理，这使得攻击路径分析等功能成为可能，并显著改善了漏洞优先级排序。根据公司业绩会公开信息，公司客户已经在规模化地替换传统的漏洞管理产品。CrowdStrike 暴露管理包含网络攻击资产管理（CAASM，Cyber Attack Asset Security Management)，风险优先级排序（Risk Prioritization），外部攻击面管理(EASM，External Attack Surface Management)，扩展物联网（xIoT），基于风险的漏洞管理(RBVM，Risk-Based Vulnerability Management)，网络漏洞评估(NVA，Network Vulnerability Assessment)，攻击路径分析(APA，Attack Path Analysis)，浏览器扩展评估（Browser Extension Assessment），漏洞情报（Vulnerability Intelligence），安全配置评估(SCA，Security Configuration Assessment)，文件完整性管理（FileVantage）等用例。

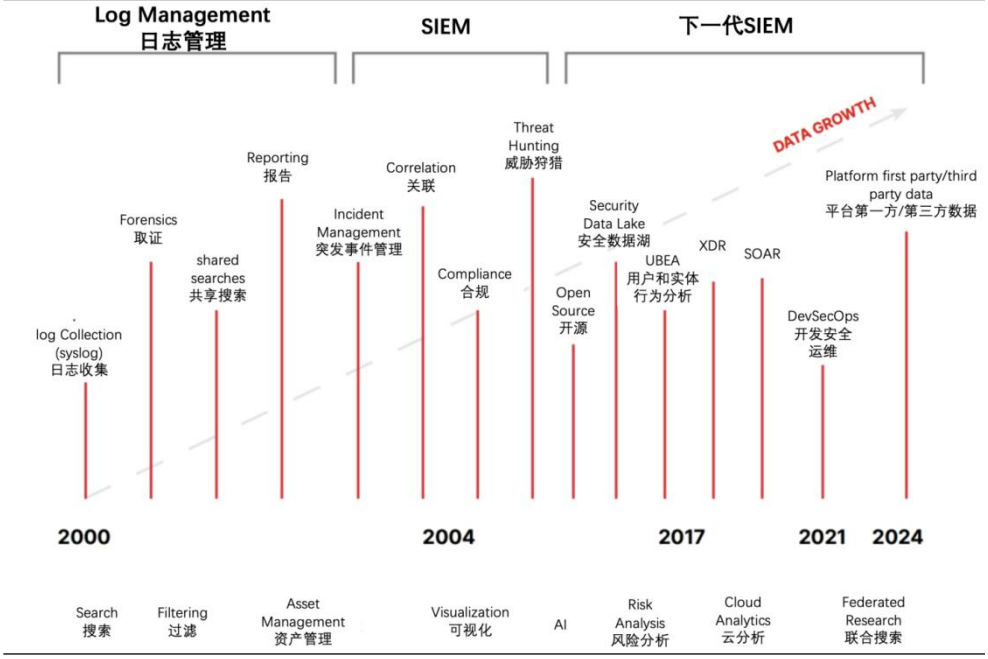
5. 下一代 SIEM：AI+自动化+高搜索性能实现差异化

随着企业组织迁移到云端并采用 SaaS 应用，企业安全团队面临着从复杂的云提供商和服务网络中收集日志（Log）的挑战。安全信息和事件管理（SIEM，Security Information and Event Management）为企业组织提供集中式平台，汇集和整合来自客户组织整个数字环境（包括本地和云环境）中多个工具的安全数据。SIEM 的核心功能是提供对组织安全态势的可见性，帮助客户公司满足安全合规要求。

- **日志管理**：传统 SIEM 主要为日志管理（Log Management）功能，主要专注于收集和索引组织网络中各种应用和系统的日志输出，受到垂直扩展性限制，不支持日益增长的数据量分析。
- **SIEM**：SIEM 采用云部署模式，集成了用户和实体行为分析（UEBA，User and Entity Behavior Analytics）、SOAR 以及威胁情报源等功能。这一阶段，SIEM 从单纯的数据存储库演变为主动的、以情报驱动的安全平台。
- **下一代 SIEM**：下一代 SIEM 具备事件分组和优先级排序、生成式 AI 以及全面的威胁检测、调查与响应（TDIR，Threat Detection, Investigation, and Response）能力，并集成在一个统一的 SOC 平台中。根据 CrowdStrike，相较于初期 SIEM，下一代 SIEM 能够摄取多样化的流式遥测数据（Streaming

telemetry，一种实时数据采集和传输技术），提供 PB 级扩展性、亚秒级延迟和超高的搜索性能，为安全团队提供潜在风险和漏洞的全面实时视图。

图 12、下一代 SIEM 发展历史



数据来源：公司下一代 SIEM 介绍书，兴业证券经济与金融研究院整理

Falcon 下一代 SIEM 平台包含安全监控（Security monitoring），威胁检测（Threat detection），威胁猎捕（Threat hunting），突发事件管理（Incident management），传统 SIEM 替代升级，合规性，日志管理（Log management），下一代 MDR 等技术组件，主要产品为 Falcon Fusion SOAR、Falcon Foundry、Falcon LogScale 和 Falcon Search Retention。

- **Falcon Fusion SOAR：通过集成的 SOAR 能力减少事件响应时间。**通过本地集成加速并自动化 SIEM 警报的调查和响应，大限度地降低威胁影响；针对特定威胁量身定制响应方案，简化事件管理；允许客户将 Falcon Fusion SOAR 与其现有的安全工具集成，形成统一的防御策略。
- **Falcon Foundry：提供低代码应用程序开发平台。**
  - **简化应用开发：**使用可视化构建器简化应用构建，帮助各个技能水平的开发者完成工作；
  - **结合 CrowdStrike 平台：**利用 Falcon 平台数据，结合专家见解，允许开发者基于 CrowdStrike 的数据和基础设施构建应用，并可以使用基于 HTTP 的应用程序编程接口（API，Application Programming Interface）

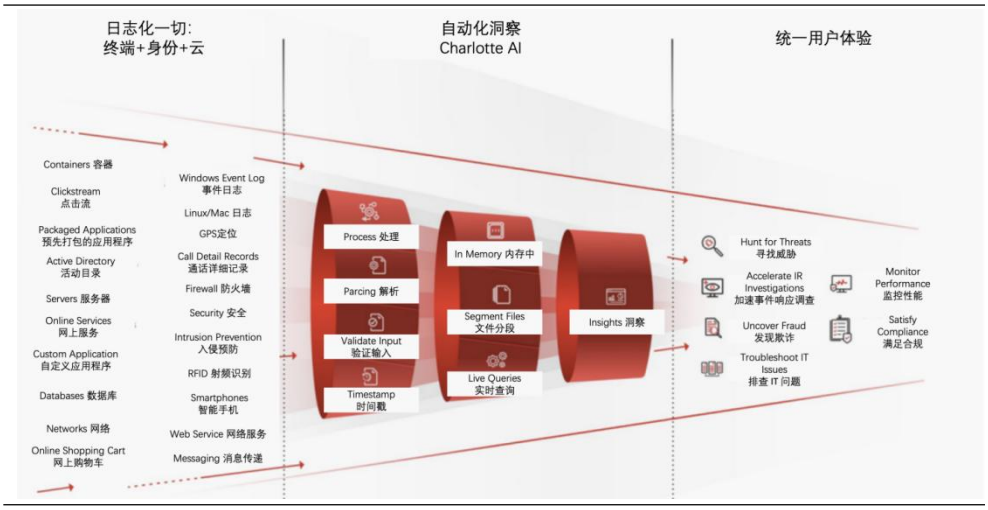
连接器集成第三方工具；通过 Falcon Fusion SOAR 自动化工作流程，并直观地可视化数据，帮助开发者识别模式和趋势；

- **简化管理控制**：单一平台简化应用管理，采用基于角色的访问控制（RBAC，Role-Based Access Control），防止未经授权的访问，确保安全合规性。

- **Falcon LogScale**：
  - **日志化数据**：无索引架构（Index-Free Architecture）使用户能够记录所有数据并保留多年；允许用户在不影响性能情况下收集更多数据用于调查（Investigation）、威胁狩猎（如容器数据、服务器数据、网络服务数据），实现每天超过 1PB 的数据摄取；
  - **数据搜索和分析**：结合 Charlotte AI，提升客户的搜索、狩猎和故障排除（Troubleshooting）能力；通过过滤（Filtering）、聚合（Aggregation）和正则表达式（Regex Support，允许用户在文本中进行搜索、替换或验证）支持深入挖掘以获取额外背景信息；支持自由文本搜索；
  - **实时仪表盘发现威胁**：使用户能够立即优先处理威胁、监控趋势和解决问题，并允许构建和分享自定义仪表盘；
  - **简化体验**：凭借直观的界面和易于学习的搜索语言，允许用户快速创建实时流式搜索、仪表盘和警报，极大简化用户体验；
  - **易于部署**：允许用户设置新的日志记录实例并立即开始摄取数据，并可以通过 LogScale Collector、CrowdStream 数据管道或 LogScale 市场应用程序引入数据，快速实现价值。

- **Falcon Search Retention**：
  - **加速威胁狩猎**：利用高速、无索引的架构和功能丰富的查询语言实时发现威胁，同时从 Falcon 平台的情报源中集成现实世界的威胁背景信息，利用 125 多个自动化工作流程，以快速和精准的方式追踪对手；
  - **统一数据查看**：全面覆盖端点、用户和云活动，通过全面的端点遥测简化分析，使客户快速获得调查和响应所需的洞察和归属细节；
  - **SOC 安全性合规性扩展**：凭借 PB 级别的数据存储，允许用户以具有成本效益的方式扩展安全运营，而不会影响性能。

图 13、Falcon 下一代 SIEM 工作流程示意图



数据来源：公司官网，兴业证券经济与金融研究院整理

6. 威胁情报&狩猎：提供业界唯一整合的“情报+狩猎”

CrowdStrike 的威胁情报与猎杀（Threat Intelligence & Hunting）板块包含 Adversary OverWatch、Adversary Intelligence、Counter Adversary Operations Elite 产品，提供业界唯一的统一威胁情报和猎捕解决方案。

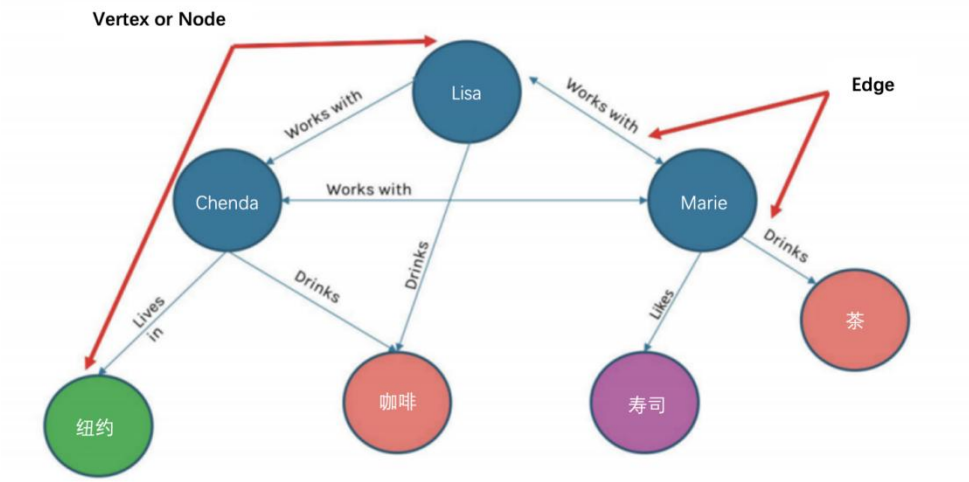
（二）底层架构优势：风险图谱为核心+统一云原生平台

1. 基础设施：风险图数据库协同攻击指标（Indicator of Attack）

自主设计风险图数据库。与其它网络安全供应商基于 AI&机器学习（ML，Machine Learning）（如 Microsoft）或者其它公司提供的商用数据库（如 Palo Alto Networks 和 Wiz（Alphabet））不同，CrowdStrike 的网络安全平台 Falcon 由公司自主设计的 CrowdStrike 风险图数据库（Threat Graph）驱动。

- **传统数据库**：（如关系数据库，Relational Database）将数据适配到称为模式（schemas）的预定义结构中，不符合预定义模式的新型攻击数据会显示丢失，造成安全分析盲点。
- **图数据库**：与传统数据库相反，图数据库将每个数据项作为独立对象（称为“Vertex”或者“Node”）存储，每个数据之间可以拥有多个关系（称为“Edge”）。图数据库将数据及其属性附加至图中，无需遵循预定义模式，因此**能够无限增长并接受新类型的数据。**

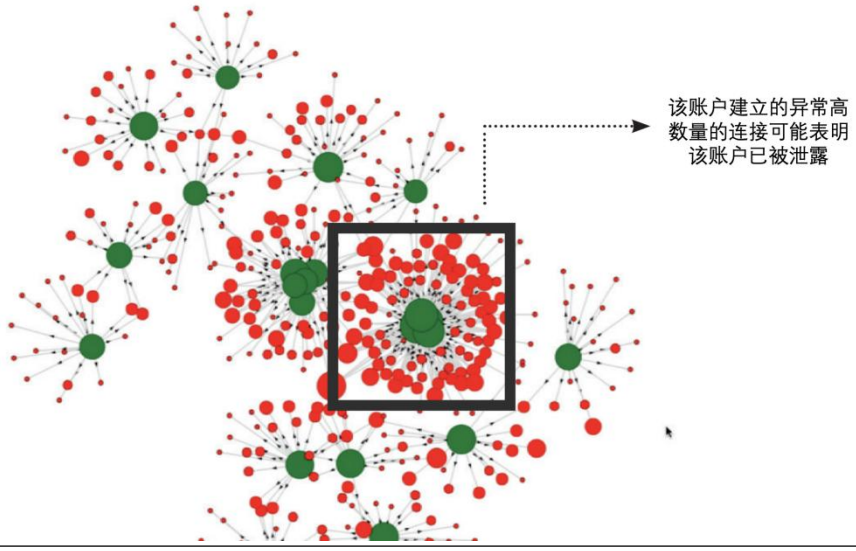
图 14、图数据库结构例子



数据来源：公司风险图数据库白皮书，兴业证券经济与金融研究院整理

- **风险图数据库**：公司层面上，CrowdStrike 风险图数据库允许数据写入数据库后立即进行自动化分析，**（1）提供即时数据访问能力（包括终端执行情况和威胁上下文信息），提升调查速度+允许深入分析。**同时，风险图数据库**（2）映射依赖关系（Dependency），以可视化方式呈现信息，实现安全问题的实时可见性和可视化。**得益于图数据库的强关联性和可扩展能力，Threat Graph 在核心功能、客户拥有成本、数据留存时间等方面存在竞争优势。

图 15、CrowdStrike 风险图数据库可视化信息呈现示意图



数据来源：公司风险图数据库白皮书，兴业证券经济与金融研究院整理

✧ **核心性能：**相较于 Palo Alto Networks 和 Wiz（Alphabet）使用 Amazon 的 Neptune 图数据库/SentinelOne 仅用于终端安全的数据库，CrowdStrike 使用公司自主研发的风险图数据库，具有更强的核心性能和集成性。根据公司博客，CrowdStrike 风险图谱支持每天分析和关联来自全球 176 个国家数百万个传感器收集的超过 340 亿个事件，功能覆盖全系列安全产品。

表 3、CrowdStrike Threat Graph 核心功能

功能	作用	CrowdStrike 风险图谱特殊性
数据捕捉（Capture）	收集和索引原始终端数据所需的硬件/软件	● 涵盖数万亿安全事件； ● 捕获并揭示数据元素之间的关系；
数据丰富（Enrich）	补充强化威胁情报、上下文和关联标记	● 将遥测数据与有关现实世界威胁的上下文信息相结合，帮助识别与已知威胁行为者相关的新活动
数据分析（Analyze）	寻找可疑和恶意活动	● 利用 AI 和行为深度分析识别新出现/异常威胁； ● 实时识别、警报、阻止威胁活动
搜索查询引擎（Search）	对存储数据的实时搜索能力	● 查询和搜索引擎确保无缝访问
数据存储（Store）	多重备份和容错机制+高性能的企业存储	● 与第三方和自定义安全解决方案紧密集成； ● 解锁安全编排、自动化和其他高级工作流； ● 定期提取增强的安全数据集，支持合规性、长期归档、与第三方分析引擎和数据湖的集成。
部署维护（Deploy & Maintain）	执行硬件和软件部署、集成维护和升级需要工作人员	● 无需本地基础设施的云交付； ● 解决方案可无缝扩展； ● 提供所有必要的存储和计算资源； ● 完整的丰富后数据集持续可用（包括临时、离线或已销毁的系统）

数据来源：公司风险图谱白皮书，兴业证券经济与金融研究院整理

表 4、SentinelOne、Palo Alto Networks、Wiz（Alphabet）和 CrowdStrike 图数据库核心功能对比

	SentinelOne	Palo Alto Networks	Wiz（Alphabet）	CrowdStrike
可扩展性	N/A	128TiB 存储扩展+15 个副本读取扩展	128TiB 存储扩展+15 个副本读取扩展	满足任何数据量的扩展需求
性能	N/A	每秒 >100,000 次查询	每秒 >100,000 次查询	每秒 >500,000 次事件写入
功能范围	终端安全	Prisma Cloud	云安全	Falcon 平台全系列安全产品

数据来源：各公司官网，兴业证券经济与金融研究院整理

协同攻击指标（IoA，Indicator of Attack）阻止数据泄露。不同于 Palo Alto Networks、Microsoft 和 Wiz（Alphabet）仅使用入侵指标（Indicator of Compromise，IoC），CrowdStrike 使用 IoA 作为威胁检测方式。传统的威胁检测 IoC 主要依赖

于签名（Signature，即与恶意软件相关的已知代码或行为模式），对于已知威胁有效，但在面对零日漏洞或新的攻击方法时则性能较差。IoA 则强调基于行为（Behavior）的检测，能够在可疑行为演变为全面入侵之前进行识别，提供实时响应，允许主动的威胁应对。此外，大多数基于签名的检测系统会将许多无害活动误判为攻击，而 IoA 因为更关注行为而非特定的威胁签名，误报率较低。CrowdStrike 风险图数据库**使得包括 IoA 等多种检测方法和算法能够同时运行于数据之上，并几乎即时生成结果**。

图 16、IoA 与 IoC 对比示意图

数据来源：公司 IoA 白皮书，兴业证券经济与金融研究院整理

表 5、SentinelOne、Palo Alto Networks、Wiz（Alphabet）和 CrowdStrike 指标使用对比

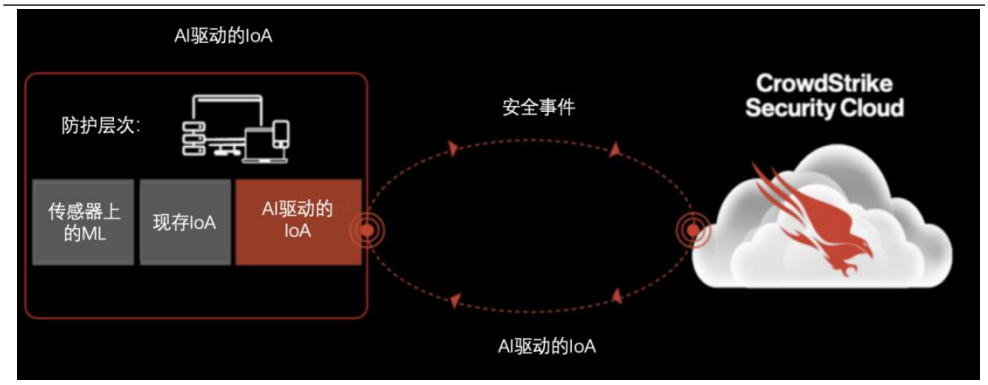
	SentinelOne	Palo Alto Networks	Microsoft	Wiz（Alphabet）	CrowdStrike
IoA	☑	缺乏	缺乏	缺乏	☑；发布行业首个 AI 驱动的 IoA（2022.08.10）
IoC	☑	☑（2024.11.18 发布）	☑	☑	☑

数据来源：各公司官网，兴业证券经济与金融研究院整理

推出 AI 驱动的 IoA（2022.08.10）进一步增强现有云安全防御功能。AI 生成的 IoA 使用基于云的机器学习和实时威胁情报，与现有传感器防御层异步运行，实时分析事件并向传感器发出动态 IoA。随后，传感器将 AI 生成的 IoA 与本地事件和文件数据关联，以评估恶意性。

- **提升速度**：通过预测不断变化的攻击手法，保持领先，并启用与现有防御层协作的主动本地防御。
- **驱动自动预防**：云原生的人工智能模型与 CrowdStrike Falcon 传感器共享实时 IoA，实时预防攻击。
- **减少误报，提高生产力**：AI 驱动的 IoA 综合 CrowdStrike 威胁猎捕团队的洞察，提供自动化的威胁猎捕专业知识。

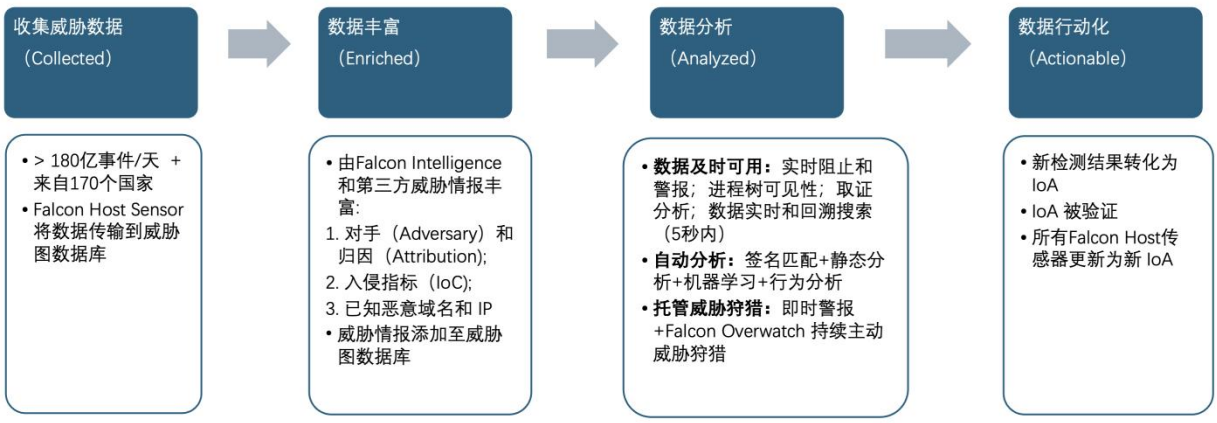
图 17、AI 驱动的 IoA 与现有 IoA 协同示意图



数据来源：公司 IoA 博客，兴业证券经济与金融研究院整理

风险图数据库+AI 驱动的 IoA 加快检测速度，提升分析覆盖率、可见性。与竞争对手分散点解决方案相比，CrowdStrike 利用风险图数据库整合数据捕获、增强、分析、查询、存储、部署维护功能，实现**在统一平台上自动关联数据**；同时，CrowdStrike 风险图数据库能够**存储检测和预防攻击所需的活动时间线，自动化事件分类和触发因素所需要的手动流程**，显著提升 CrowdStrike 威胁情报&狩猎及其它功能的检测、响应、调查速度。另外，CrowdStrike 风险图数据库**使用 AI 驱动的 IoA 而不是仅使用 IoC（如 Palo Alto Networks、微软和 Wiz（Alphabet））将威胁数据行动化**，实现差异化的数据泄露预防，展现为更高的保护度、检测率和分析覆盖率。根据 MITRE Engenuity ATT&CK 评估数据，CrowdStrike 的保护度（100%）、分析覆盖率（100%）和可见性（100%）相较于 SentinelOne、Palo Alto Networks、Wiz（Alphabet）和 Microsoft 均处于领先地位，能够覆盖更广泛的攻击技术并全面分析威胁；平均检测时间仅 4 分钟，显著优于竞争对手。

图 18、CrowdStrike 风险图数据库与 IoA 协同工作示意图



数据来源：公司官网，兴业证券经济与金融研究院整理

表 6、SentinelOne、Palo Alto Networks、Wiz（Alphabet）、Microsoft 和 CrowdStrike 核心性能对比

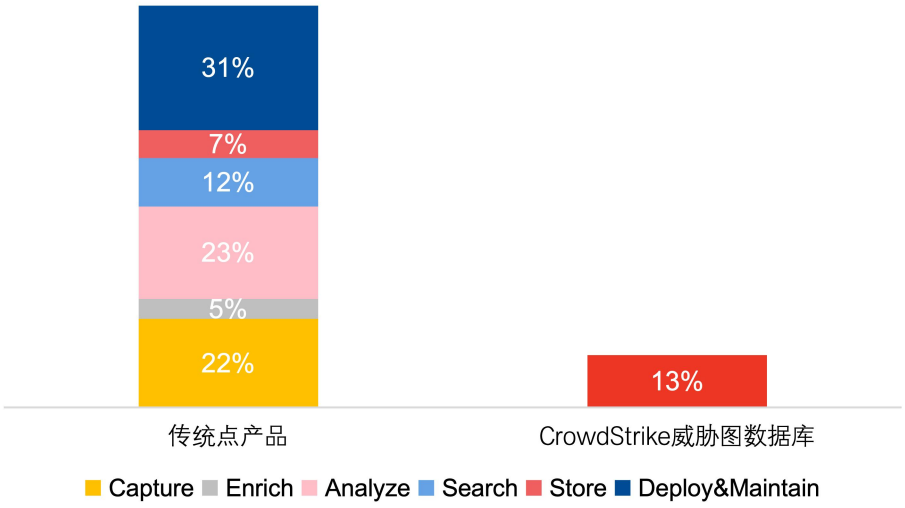
	SentinelOne	Palo Alto Networks	Wiz（Alphabet）	Microsoft	CrowdStrike
分析覆盖率	84%	**100%**	N/A	98%	**100%**
可见性	88%	**100%**	N/A	100%	**100%**
平均检测时间	47 分钟	6.6 分钟	7.6 分钟	N/A	**4 分钟**

数据来源：各公司官网，兴业证券经济与金融研究院整理

注：分析覆盖率和可见性为 2023 自然年 MITRE Engenuity ATT&CK 企业版第五轮评估数据，检测时间为 CrowdStrike 公司官网数据

客户拥有成本低：相较于传统的点产品解决方案，CrowdStrike 风险图谱整合数据捕获、增强、分析、查询、存储、部署维护功能，TCO 仅为传统点产品解决方案的 13%，大幅降低客户拥有成本。

图 19、CrowdStrike 风险图谱功能集成带来 TCO 下降



数据来源：公司风险图数据库白皮书，兴业证券经济与金融研究院整理

数据留存时间长：与行业平均相比，CrowdStrike 风险图数据库检测摘要数据留存时间达 1 年（vs 行业平均 30 天），检测详情留存时间 90 天（vs30 天），强化后的传感器数据留存时间 7-90 天，并且提供无限期的传感器数据归档留存，确保用户始终掌握有效理解当前威胁所需的知识。

表 7、CrowdStrike 风险图谱数据留存时间

数据类型	描述	行业平均	CrowdStrike
检测摘要	按需访问与网络安全平台生成的所有威胁相关的元数据	30 天	1 年
检测详情	按需访问网络安全平台检测到的所有威胁的完整取证细节	30 天	90 天
增强补充后的传感器数据	按需访问超过 400 种事件类型的完整历史记录，用于追溯检测、威胁狩猎和调查	无功能	7-90 天
增强补充后的传感器数据归档	提供用于本地数据仓库或数据湖的离线增强传感器数据副本，并与从其他系统收集的日志进行关联	长短不均	无限期访问

数据来源：公司风险图谱白皮书，兴业证券经济与金融研究院整理

2. 代理架构：单一轻量级代理+单一控制台

单一代理+控制台简化操作。CrowdStrike 平台提供单一代理（Agent）和单一控制台（Console），整合包括云安全、终端、身份保护、下一代 SIEM 等全平台解决方案，简化部署操作。

表 8、SentinelOne、Palo Alto Networks、Wiz（Alphabet）和 CrowdStrike 代理对比

	SentinelOne	Palo Alto Networks	Microsoft	Wiz（Alphabet）	CrowdStrike
代理数量	3+代理	3 代理	3+代理	**单一代理**	**单一代理**
控制台数量	**单一控制台**	3+控制台	3+控制台	3+控制台	**单一控制台**
代理功能	**支持完整平台功能**	**支持完整平台功能**	**支持完整平台功能**	仅提供可视性	**支持完整平台功能**

数据来源：各公司官网，兴业证券经济与金融研究院整理

云原生轻量级代理实现快速部署+低系统延迟。CrowdStrike 的代理由云资源管理，而不是占用本地数据中心的资源，因此 CrowdStrike 代理在运行时不会显著影响客户组织终端性能。根据 Clearnetwork 官网数据，CrowdStrike 代理仅需要 20.15 MB 的磁盘空间、25.36 MB 的内存使用量，以及多 3.03% 的 CPU 使用率；根据 CrowdStrike 2017 年公司博客披露，Falcon 代理仅占用 10MB 的内存、15MB 的磁盘空间，并且 CPU 使用率通常低于 1%，均显著低于 SentinelOne、Palo Alto Networks 和 Microsoft 等竞争对手。

表 9、SentinelOne、Palo Alto Networks、Microsoft 和 CrowdStrike 代理对客户系统占用对比

	SentinelOne	PANW Cortex XDR 代理	Microsoft Defender	CrowdStrike
磁盘空间	200MB	10GB	> 1GB	20.15MB
内存使用	20MB	4GB，推荐 8GB	约 100MB	25.36MB
CPU 使用率	0%-4%	N/A	5%-10%，缓解威胁或扫描时可能达到 20%-30%	低于 1%，多 3.03%

数据来源：各公司官网，Clearnetwork 官网，兴业证券经济与金融研究院整理

3. 产品形式：云原生平台提供全面的安全事件防护

与 Microsoft 等竞争对手相比，CrowdStrike 将终端安全、云安全、身份保护、SIEM、威胁情报、数据保护、暴露管理等所有点产品集成于云原生 Falcon 平台，降低单一点产品带来的不一致性和数据泄露风险。

表 10、CrowdStrike 竞争对手细分领域覆盖对比

终端安全	云安全	身份保护	SIEM	威胁情报	数据保护	暴露管理
Kaspersky	Wiz（Alphabet）	Microsoft	Splunk	Recorded Future	DIGITAL GUARDIAN	Qualys
Microsoft	Aqua	SentinelOne	Elastic	ZEROFOX	RAPID7	Tenable
SOPHOS	Palo Alto Networks Prisma Cloud	SILVERFORT	Sumo Logic	Digital Shadows	Trellix	Censys
Palo Alto Networks	Lacework	Semperis	Securonix	INTEL471	McAfee	AXONIUS
Trellix	Orca		logRhythm		Symantec	CyCognito
McAfee			Arcsight		Broadcom	RAPID7
Cybereason			Radar			
SentinelOne			Exabeam			
Trend			Palo Alto Networks			
Symantec						
Broadcom						

数据来源：公司官网，兴业证券经济与金融研究院整理

表 11、CrowdStrike 平台产品与微软点产品情况

细分领域	技术模块	微软产品	CrowdStrike 产品
终端安全	原生扩展检测与响应（XDR，Extended Detection and Response） EDR 下一代防病毒 设备管理 防火墙管理 数据丰富、收集、关联（data collection, enrichment, and correlation） MDR	Microsoft Defender	Falcon 平台
云安全	安全态势管理 云合规性 云工作负载保护 漏洞管理 基础设施即代码扫描 CIEM 威胁狩猎与情报 容器安全 软件物料清单（SBOM）	Microsoft Entra Microsoft Defender Microsoft Salus	
SIEM	SIEM 安全监控（Security monitoring） 威胁检测（Threat detection） 突发事件管理（Incident management） SOAR 日志管理（Log management）	Microsoft Sentinel	
身份保护	零信任 Secure Web Gateway (SWG) 身份安全态势管理（ISPM，Identity Security Posture Management） 身份威胁检测与响应（ITDR，Identity Threat Detection and Response） 持续访问评估配置文件（CAEP，Continuous Access Evaluation Profile） 用户和实体行为分析（User and Entity Behavior Analytics） 非人类身份（Non-Human Identities）保护和可视化	Microsoft Entra 仅提供 assessment 功能 Microsoft Defender Microsoft Entra Microsoft Sentinel Microsoft Entra	与 Cloudflare 合作
暴露管理	网络攻击资产管理（CAASM，Cyber Attack Asset Security Management） 风险优先级排序（Risk Prioritization） 外部攻击面管理(EASM，External Attack Surface Management) 扩展物联网（xIoT） 基于风险的漏洞管理(RBVM，Risk-Based Vulnerability Management) 网络漏洞评估(NVA，Network Vulnerability Assessment) 攻击路径分析(APA，Attack Path Analysis) 浏览器扩展评估（Browser Extension Assessment） 漏洞情报（Vulnerability Intelligence） 安全配置评估(SCA，Security Configuration Assessment) 文件完整性管理（FileVantage）	Microsoft Defender - Microsoft Defender - -	Falcon 平台
威胁情报识别与猎杀	威胁猎捕（Threat Hunting） 对手档案（Adversary Profiling） 数字风险保护（Digital Risk Protection） 恶意软件分析（Malware Analysis） 威胁情报报告（Intelligence Report） 情报自动化与协调（Intelligence Automation&Orchestration） 攻击面管理（Attack Surface Management） CDR	Microsoft Defender - Microsoft Defender - -	
数据保护	DLP SOAR	Microsoft Purview Microsoft Sentinel	

数据来源：公司官网，兴业证券经济与金融研究院整理

vs Microsoft Defender：根据第三方测试结果，在终端安全和 XDR 方面，CrowdStrike Falcon 平台提供较微软更强的安全有效性、运营效率、总拥有成本和易用性，同时避免 Microsoft Defender 补丁漏洞带来的潜在风险。

表 12、CrowdStrike 平台产品与 Microsoft Defender 性能对比

	Microsoft Defender	CrowdStrike
安全有效性	无法检测无文件恶意软件（截止 2023 自然年，超过 70%的攻击使用无文件恶意软件）； 允许恶意软件完全执行后才采取行动，导致用户登录凭证泄露	100%检测
运营效率	需补丁维护（2022 自然年，微软发布超 900 个补丁，其中 20%是关键补丁，30 个针对零日漏洞）	避免补丁干扰
总拥有成本	基础设施投资频繁	基础设施投资较少
易用性	需分配 4 个全职员工	需分配半个全职员工

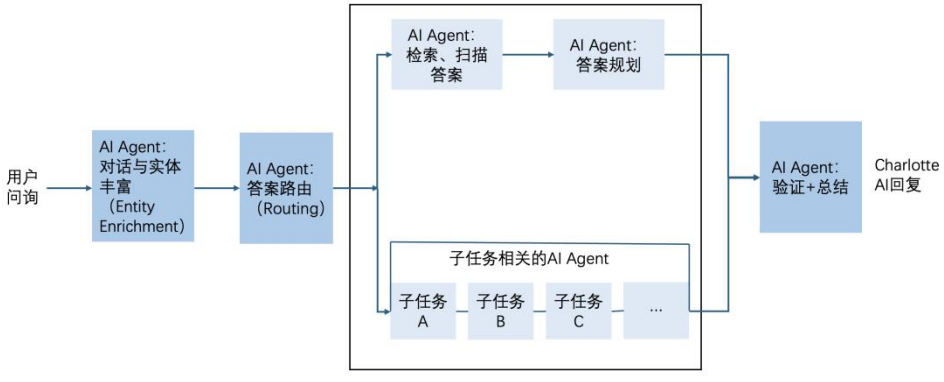
数据来源：CrowdStrike 公司博客，兴业证券经济与金融研究院整理

（三）适应 AI 时代：AI 驱动平台+防护 AI 安全

1. AI 产品： Charlotte AI 提升效率

Charlotte AI 加速网络安全和 IT 运营效率，简化操作难度。Charlotte AI 拥有多层 AI 架构（Multi-AI Architecture），提供差异化的通俗语言查询功能。相较于依赖一个 LLM 完成任务的单体（Monolithic）AI 产品（如 ChatGPT），多层 AI 架构代理能够将客户问题分解为离散的子任务，使客户组织能够分配不同的 LLM（甚至其他类型的模型，如小型语言模型）来完成不同的任务，更好适应网络安全领域的动态挑战。同时，多层 AI 架构代理使系统能够控制因任何模型性能变化（无论是无意的变化还是针对单个模型的定向攻击）而产生的连锁反应。

图 20、Charlotte AI 多层 AI 架构工作流程示意图



数据来源：公司 Charlotte AI 白皮书，兴业证券经济与金融研究院整理

Charlotte AI 主要用例包括：

- **提升速度**：与 Falcon Insight XDR、Falcon Intelligence 和 Falcon Exposure Management 等产品集成，优化结果的速度和准确性。
- **简化流程**：提取关于 230 多种对手的通俗语言见解，允许用户跳过繁琐的脚本编写、报告总结和告警分类周期，提升安全团队产出。
- **加速部署**：加速用户对 Falcon 平台的熟练掌握，通过定制和共享查询集合优化团队工作常见流程。
- **强化搜索**：Charlotte AI 配备专门的“图书管理员（Librarian）”代理，遵循检索增强生成（RAG，Retrieval Augmented Generation）模式搜索，使用指定的知识库（如特定的 Falcon 模块）回答问题，确保 LLM 的输出基于 Falcon 平台实际数据，提高搜索准确性。
- **隔离 LLM 风险**：Charlotte AI 的架构在 LLM 和终用户之间实施防护措施和控制机制，使系统能够验证 LLM 的输出并确保其可追溯性。

2. AI 安全：AI-SPM 和 AI 红队丰富现有产品，收购 Adaptive Shield 补充云安全功能

2.1 AI-SPM：推出 AI 安全态势管理（AI-SPM，AI Security Posture Management）(2024.09.18)保护 AI 和 LLM 安全。 根据公司披露，2023 自然年云利用案例增长 110%，身份攻击不断上升，其中 75%的初始访问攻击无恶意软件。为支持安全的云环境和 AI 创新，AI-SPM 监控在云中部署的 AI 服务和大型语言模型(LLMs)，检测配置错误，识别并解决漏洞。

- **记录 AI 使用**：识别发现客户组织在混合云环境中使用的所有 AI 依赖项（即构建和运行 AI 应用程序时所需的各种组件、库、框架和服务），包括那些隐藏在容器（Containers）和镜像（Images）中的依赖项，确保所有 AI 相关的工具和服务都被记录和管理。
- **清点（Inventory）AI 应用和模型**：扫描客户组织的云基础设施、容器和镜像，以查找 AI 服务、应用和模型。
- **优先处理并保护 AI 漏洞（Vulnerability）**：允许客户查看哪些 AI 应用和模型引用了具有可利用和可访问的关键漏洞的库和包。
- **保护 AI 工作负载**：监控 AI 模型和容器的运行时行为，主动阻止潜在的安全漏洞。
- **发现 AI 配置错误（Misconfiguration）**：提供 AI 配置错误可视化功能。

图 21、CrowdStrike AI-SPM 界面

数据来源：公司官网，兴业证券经济与金融研究院整理

2.2 AI 红队：推出 AI 红队服务（AI Red Team）（2024.11.07）以加强对 AI 基础设施的保护。随着企业组织加速采用 AI，针对 AI 应用程序及其底层数据的威胁日益增长，如模型篡改、数据污染、敏感数据暴露等，AI 系统（包括 LLMs）的破坏可能导致机密性泄露、模型有效性降低，以及对抗性操控的易受攻击性。为防御 AI 系统安全风险，AI 红队主要功能包括：

- **AI 应用的渗透测试**：深入评估 LLM 应用程序，针对开放网络应用安全项目(OWASP，Open Web Application Security Project) 的十大漏洞进行测试，在对手发起攻击之前揭示漏洞并识别安全配置错误。
- **对手模拟演练**：模拟针对用户独特 AI 环境的现实攻击，根据用户的具体用例和 AI 实施量身定制场景。
- **红队/蓝队演练**：通过 CrowdStrike 红队模拟现实攻击，蓝队负责检测和响应，结合 Charlotte AI 提高检测能力，增强用户的团队识别和缓解不断演变威胁的能力。

2.3 Adaptive Shield：收购 SaaS 安全态势管理（SSPM，SaaS Security Posture Management）龙头 Adaptive Shield（2024.11.06），阻止针对 AI SaaS 的攻击，其突出优势在于：

- **创新性**：根据 Frost & Sullivan 2024 年 SaaS 安全态势管理报告，Adaptive Shield 创新性地将 SSPM 与身份威胁检测和响应（ITDR，Identity Threat Detection and Response）相结合，是行业唯一拥有全面的设备到 SaaS 保护功能的供应商。其中，Adaptive Shield 的 SSPM 具有大量开箱即用集成功能，提供行业广泛的集成支持。
- **增长性**：预计 2024 自然年 Adaptive Shield 收入同比增长高达 101.7%，在全球拥有超过 300 个活跃的商业伙伴，增长势头强劲。
- 通过持续监控生成式 AI SaaS 应用，Adaptive Shield 使 CrowdStrike 用户组织能够通过检测配置变化、控制 AI 设置防止数据泄露、识别未授权 AI 应用并根据其风险评估撤销访问等方式，执行一致的安全标准，确保 AI 集成的应用程序与安全政策保持一致，保护敏感数据。

三、商业模式：订阅为主，客户为导向的销售模式驱动增长

（一）订阅收费：弹性组合满足不同安全需求

Falcon Go：涵盖客户支持服务、移动设备保护、设备控制、下一代防病毒等模块。

Falcon Pro：涵盖客户支持服务、防火墙管理、设备控制、下一代防病毒等模块，同时客户可按需添加移动设备保护模块。

Falcon Enterprise：在 Falcon Pro 基础上添加 XDR 和威胁情报及狩猎模块。

Falcon Complete：以定制化方案呈现，基础服务包括 IT 环境卫生、XDR、威胁情报和狩猎和下一代防病毒，同时客户可按需添加 Express Support、移动设备保护和身份保护模块。

表 13、CrowdStrike 产品定价情况

	Falcon Go	Falcon Pro	Falcon Enterprise	Falcon Complete
定价	59.99 美元/设备	99.99 美元/设备	184.99 美元/设备	定制价格
Express Support（客户支持服务）	☑	☑	☑	可额外付费购买
Falcon for Mobile（移动设备保护）	☑	可额外付费购买	可额外付费购买	可额外付费购买
Falcon Indentity Protection（身份保护）				可额外付费购买
Falcon Discover（IT 环境卫生）				☑
Falcon Insight XDR			☑	☑
Falcon Adversary Overwatch（威胁情报及狩猎）			☑	☑
Falcon Firewall Management（客户防火墙管理）		☑	☑	
Falcon Device Control（设备控制）	☑	☑	☑	可额外付费购买
Falcon Prevent（下一代防病毒）	☑	☑	☑	☑

数据来源：公司官网，兴业证券经济与金融研究院整理

（二）Land-and-Expand 策略推动多模块采用

CrowdStrike 采用“Land-and-Expand”销售模式，提供模块化平台，使客户可以从基本的云安全需求开始部署 CrowdStrike 平台，随后按需无缝添加更多保护模块，允许客户兼顾预算和网络安全需求。

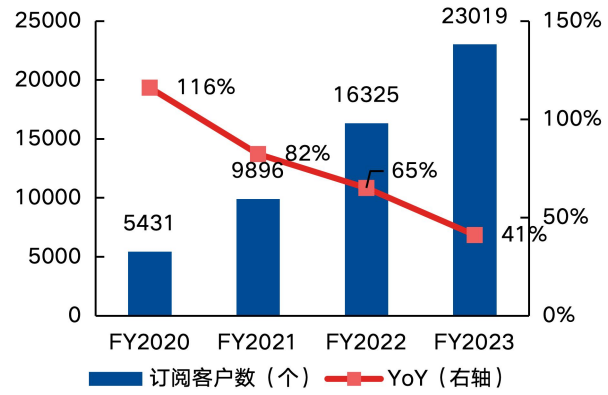
1. 订阅客户数：快速增长

截至 2023 年 1 月 31 日，CrowdStrike 总订阅客户数达 23019 位，同比增长 41%。

2. 模块采用：客户采用积极，多模块订阅趋势显著

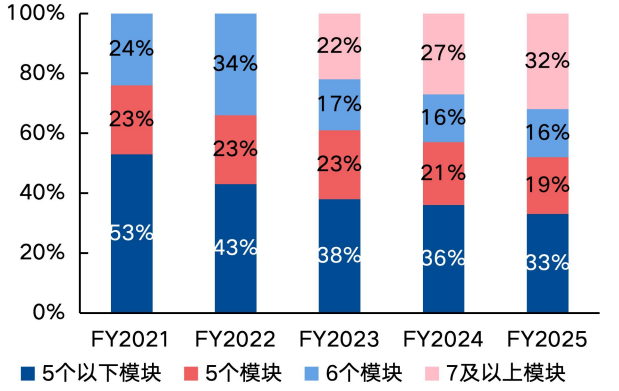
截至 2025 年 1 月 31 日，购买 5 个模块及以上的客户占比达 67%，同比增长 3pcts，较 2021 财年 47%的水平大幅提升 20pcts。其中，购买 6 个模块及以上的客户占比达 48%，同比增长 5pcts；购买 7 个模块及以上的客户占比达 32%，同比增长 5pcts。

图 22、CrowdStrike FY2020-2023 订阅客户数



数据来源：公司季度报，兴业证券经济与金融研究院整理
注：FY2025 期间为 2024.2.1-2025.1.31

图 23、CrowdStrike FY2021-2025 模块采用情况



数据来源：公司季度报，兴业证券经济与金融研究院整理
注：FY2025 期间为 2024.2.1-2025.1.31

（三）维系渠道合作伙伴生态系统，增强客户采用

启动合作渠道，持续推广云安全解决方案。为扩展解决方案的业务、技术合作，帮助客户降低总体拥有成本（TCO）、整合点产品并保持全面保护，CrowdStrike 启动的关键渠道计划包括加速合作伙伴计划（Accelerate Partner Program）、Falcon Complete for Service Providers、扩展其生态系统的 CrowdStrike MarketPlace，以及激励合作伙伴参与的 CrowdCredit 奖励计划。

1. Accelerate Partner Program（2023.09.18）：提升合作伙伴盈利能力

- **教育与娱乐结合**：推出 CrowdClass，允许客户随时随地按需观看 10 分钟内短视频分享 CrowdStrike 的专业知识。
- **需求生成和销售工具**：新基础设施和运营增强使合作伙伴更快速地创造需求、登记注册销售机会、开展基于价值的销售活动；推出 CrowdStrike 的自助营销活动平台 The Grid，提供着陆页、电子邮件和社交媒体帖子，帮助合作伙伴在 CrowdStrike Falcon 平台上加速交易。
- **加速提升奖励**：推出支付奖励工具 CrowdCard，使个人销售和解决方案工程专业人员可以在品牌的 CrowdStrike 借记卡上获得现金返还奖励，激励新的客户交易以及在战略解决方案领域的扩展；提供有吸引力的利润率、折扣层级和后端返利。

2. Falcon Complete for Service Providers：在 MDR&身份威胁保护层面推动与服务提供商的合作

CrowdStrike 在提供全面的 MDR 及 AI 驱动的威胁情报和狩猎服务的同时配置 Falcon Complete 分析师远程访问受影响的系统，精准移除威胁，并将系统恢复到可操作状态。此外，CrowdStrike 允许服务提供商随时通过 Falcon 消息中心、电子邮件或 API 与 Falcon Complete 团队进行沟通，提升客户安全能力和运营稳定性。

表 14、Falcon Complete for Service Providers MDR 职责分工

职责	CrowdStrike	CrowdStrike 合作伙伴
客户入驻与规划		
入驻客户		☑
管理客户关系		☑
安装传感器		☑
移除冲突服务		☑
创建和设置客户 ID	☑	☑
创建和更新政策	☑	
启动 Falcon Complete 监控	☑	
监控与修复		
响应 Falcon Complete 升级和通信		☑
提供所需报告		☑
进行传感器故障排除		☑
管理额外的 Falcon 模块（注：不由 Falcon Complete 管理）		☑
与终客户沟通		☑
响应 Falcon OverWatch 警报	☑	
响应 Falcon 平台检测	☑	
管理白名单	☑	

数据来源：公司 Falcon Complete for Service Providers Data Sheet，兴业证券经济与金融研究院整理

表 15、Falcon Complete for Service Providers 身份威胁保护职责分工

职责	CrowdStrike	CrowdStrike 合作伙伴
客户入驻与规划		
创建和应用高级威胁情报（ATI，Advanced Threat Intelligence）政策		☑
配置多重身份验证（MFA，Multi-Factor Authentication）连接器和身份即服务（IDaaS，Identity as a Service）连接器		☑
实施、调整和配置政策规则		☑
监控与修复		
对支持的基于身份的检测进行初步分类	☑	
响应支持的基于身份的检测	☑	
根据 Falcon Complete 的定义采取对策	☑	
根据升级/修复工单采取建议的恢复措施		☑

数据来源：公司 Falcon Complete for Service Providers Data Sheet，兴业证券经济与金融研究院整理

3. CrowdStrike MarketPlace：协助客户优化网络安全投资

CrowdStrike Marketplace 为全球客户提供访问 CrowdStrike 技术和服务合作伙伴生态系统的方式，以识别和实施适合其业务的解决方案。这有助于客户通过充分利用 CrowdStrike 生态系统、无缝集成新技术、减少复杂性和改善安全结果，以增强其网络安全堆栈。

- **技术合作伙伴**：截至 2024 年 10 月 3 日，Marketplace 的列表产品数量已超过 260 个，来自 140 家领先技术合作伙伴，如亚马逊网络服务（AWS）、Cloudflare、Cohesity、NVIDIA、Rubrik 和 Zscaler。
- **解决方案合作伙伴**：CDW、GuidePoint Security、Optiv 和世界技术公司（WWT）等关键解决方案提供商也加入了 Marketplace 私人报价计划，使上市合作伙伴和选定的经销商能够为共同客户创建定制的安全解决方案。

4. CrowdCredit：折扣计划激励合作与购买

- **产品购买**：在 CrowdStrike Marketplace 购买符合条件的产品，提供高达总费用 5% 的折扣。
- **产品续订**：在 Marketplace 购买的符合条件的产品，提供高达续订期内总费用 3% 的折扣。
- **余额处理**：未使用的 CrowdCredits 折扣余额将在订单完成后根据相关条款结转到未来的订单中。

（四）客户支持模型提高留存率，进一步扩大全面平台采用

CrowdStrike 提供 Standard、Express、Essential 和 Elite 客户服务，持续提供实时、定制化安全问题解决方案。截至 2025 年 1 月 31 日，CrowdStrike 毛客户留存率超过 97%，净留存率达 112%。

- **Elite 支持**：为大型企业或复杂环境设计，提供具备客户所处行业特定知识的技术账户经理（TAM，Technology Account Manager）的访问。
- **Essential 支持**：适用于中型企业或复杂环境，帮助客户团队利用 CrowdStrike 生态系统。
- **Express 支持**：适用于小型到中型企业 IT 环境，提供部署和运营问题迅速解决方案。

- **Standard 支持：**与所有 Falcon 订阅捆绑提供的免费基本支持服务。

表 16、CrowdStrike 客户支持服务

支持服务	Standard	Express	Essential	Elite
		技术支持		
支持界面（知识库、案例提交）	☑	☑	☑	☑
24/7/365 电话支持	仅 P1 关键问题	☑	☑	☑
实时聊天（工作时间）		☑	☑	☑
案例优先级		中等	高	高
关键突发事件管理				☑
		技术账户管理		
TAM 分配		与其它客户共享 TAM	产品专家	产品和行业专家
健康检查		每季度	每季度	每月
季度报告		☑	☑	☑（每年多现场 2 次）
产品启用网络研讨会		网络研讨会	TAM 主办	指导性工坊
主动案例管理			☑	☑
针对相关产品更新或问题的主动参与			☑	☑
定期运营评审			☑	☑
成功规划服务				☑
关于客户战略计划的合作伙伴关系				☑
发布审查				☑
全球覆盖的额外 TAM				☑（额外收费）
		支持响应时间		
普通技术问题	1 个工作日	4 小时内	4 小时内	4 小时内
P1 关键问题	-	1 小时内	1 小时内	1 小时内

数据来源：公司官网，兴业证券经济与金融研究院整理

（五）加强与云厂商集成，提高客户渗透率

1. AWS: CrowdStrike CNAPP 产品维护 AWS 云安全

Falcon 云安全产品提供部署时安全保护、Amazon 资源保护、云可见性三个方面的解决方案。根据公司季度报，截至 2025 年 1 月 31 日，CrowdStrike 成为首个在 AWS Marketplace 年销售额超过 10 亿美元的云原生网络安全独立软件供应商（ISV），并被评为 2024 年 AWS 全球安全合作伙伴。

表 17、AWS 与 Falcon 云安全主要集成功能

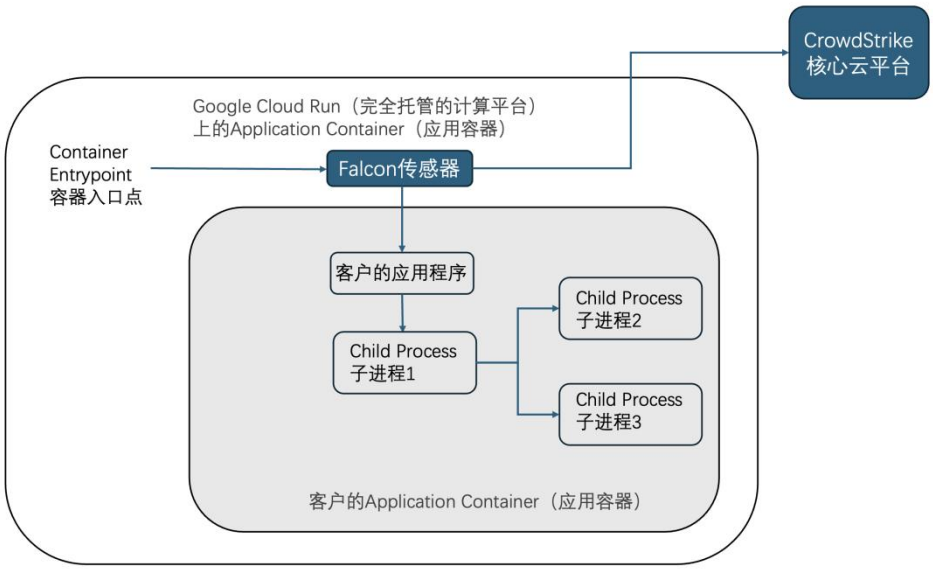
板块	用例	CrowdStrike 集成功能描述
安全部署	云迁移	● 帮助客户组织安全迁移到云环境
	事件驱动的自动化	● Falcon Cloud Security 组件在 AWS 客户配置新的 AWS 资源时自动部署，以确保全天候的全面覆盖
	多账户支持	● 与 AWS Organizations 和 Control Tower 集成，提供集中资产可见性和在所需分段环境中的 Falcon Cloud Security 部署
保护 AWS 资源	集成保护	● 与 AWS 计算服务（如 EC2、Graviton 实例、ECS、EKS、Fargate、ROSA、Workspaces 和 Outposts）无缝集成，提供运行时保护； ● 对 ECR 容器镜像、Lambda 函数和基础设施即代码模板进行预运行时漏洞和错误配置扫描，使组织能够在云端安全高效地创新
	安全工具整合	● 提供完整的 CNAPP 解决方案，将多个安全工具整合到一个平台中
	混合身份支持	● Falcon 身份保护提供对应用程序、资源和身份存储（包括 Microsoft Active Directory、Azure Entra ID、Okta 和 PingFed）的统一可见性和控制； ● 使组织能够在云和传统系统之间实施一致的风险策略； ● 仅存储相关的身份验证日志，优化日志存储成本
全面的云可见性	全面的资产可见性	● 提供所有 AWS 资产的概述，识别漏洞、配置错误、过度权限或未经授权访问的实例
	增强应用安全性	● 提供对应用层的可见性，保护在 AWS 上运行的应用程序

数据来源：AWS 官网，兴业证券经济与金融研究院整理

2. GCP：借助 CrowdStrike on Google Cloud，阻止安全漏洞

在 Google Cloud 的基础架构和主权云功能上（如完全托管的计算平台 Google Cloud Run），客户保持对数据的完全控制权。与 Google Cloud 的集成中，GCP 的 Container Entrypoint（容器入口点）确保 Google Cloud 容器能够正确加载并运行 CrowdStrike 的安全组件。在 Google Cloud 的应用容器上完成部署后，CrowdStrike Falcon 传感器会监控客户应用容器内的活动，并将数据发送到 CrowdStrike 云进行分析，确保客户应用程序的安全性。

图 24、CrowdStrike 与 Google Cloud 协同示意图



数据来源：谷歌官网，兴业证券经济与金融研究院整理

CrowdStrike 保护客户向谷歌云迁移的全流程。云迁移保护流程主要包括评估和动员（Assess & Mobilize）、提升和转移迁移（Lift-and-shift migration）、应用程序现代化（Application Modernization）、云原生服务采用（Cloud-Native Services Adoption）四个阶段。

表 18、CrowdStrike 保护谷歌云迁移概述

云迁移阶段	概述	客户组织面临的挑战	CrowdStrike 解决方案
评估和动员（Assess & Mobilize）	客户组织收集清单并优先考虑其 IT 组合，以决定何时迁移哪些部分； 停用或归档不需要的基础设施	技术债务（Technical Debt）容易暴露漏洞	● Falcon 传感器提供关于客户组织安全态势的透明度和可审计的证据
提升和转移迁（Lift-and-shift migration）	客户组织将虚拟机从本地环境迁移到云端	迁移过程中及之后的无缝安全	● 部署 Falcon 平台获得虚拟机资产全面可见性+端到端保护 ● Falcon 云资产清单显示客户组织迁移管道以及有关服务错误配置的报告
应用程序现代化（Application Modernization）	迁移应用程序并修改其架构，以利用云原生功能提高敏捷性、性能和可扩展性	容器需要管理+保护	● Falcon 云安全生成、摄取、分析和关联云资源和传统数据中心资产的遥测数据 ● Falcon 镜像（image）扫描功能在批准容器镜像部署前检查易受攻击的包、暴露的密钥和错误配置
云原生服务采（Cloud-Native Services Adoption）	采用谷歌领先的 Kubernetes 和容器领域云原生服务	保持深层次的可见性和自动化的安全态势	● Falcon 注册表扫描检查自镜像构建以来可能发现的新漏洞 ● Falcon 云安全在预生产测试环境中检测安全错误配置+提供修复指导

数据来源：公司谷歌云迁移 eBook，兴业证券经济与金融研究院整理

3. Microsoft：协同部署安全产品+兼容内核模式

3.5.3.1 与 Microsoft Defender 协同部署。

对于依赖 Microsoft Defender 的客户，管理复杂的政策、签名更新和多个控制台的复杂性导致了可能被对手利用的保护缺口。2024 年 5 月 7 日，CrowdStrike 宣布推出 CrowdStrike Falcon® for Defender，提高运行 Microsoft Defender 的端点的安全态势。

- **对漏掉攻击的可见性**：CrowdStrike 经过验证的 AI 驱动检测，结合行业领先的威胁情报，识别 Microsoft Defender 漏掉的威胁。
- **Falcon OverWatch 24x7 威胁狩猎**：OverWatch 将人类专业知识与技术相结合，检测和追踪逃避 Microsoft Defender 的异常活动。
- **精准响应**：直接从 Falcon 平台消灭复杂威胁。

3.5.3.2 深化与 Microsoft EntraID 集成。

2024 年 11 月，CrowdStrike 推出针对 Microsoft Entra ID 的实时保护，根据用户的风险状况动态控制其对资源的访问权限，使 CrowdStrike Falcon 身份保护可以与 Entra ID 身份验证流程并行工作。

- **实时威胁防护**：通过与 Entra ID 认证流程内联，Falcon 身份保护在基于身份的攻击开始之前就阻止它们。
- **动态访问决策**：Falcon 平台基于动态风险上下文和 Falcon 零信任评估分数，实现准确、实时的访问决策，确保只有受信任的用户能够访问。
- **混合基于风险的条件访问**：由于此集成基于 OpenID Connect 标准，Falcon 身份保护现在可以在 Active Directory（传统的本地身份管理系统）和 Entra ID 两个系统中同时实施安全策略。未来，CrowdStrike 可以扩展到其他提供云原生身份管理服务的厂商，以阻止未经授权的访问或根据威胁级别注入多因子认证（MFA，Multi Factor Authentication）。

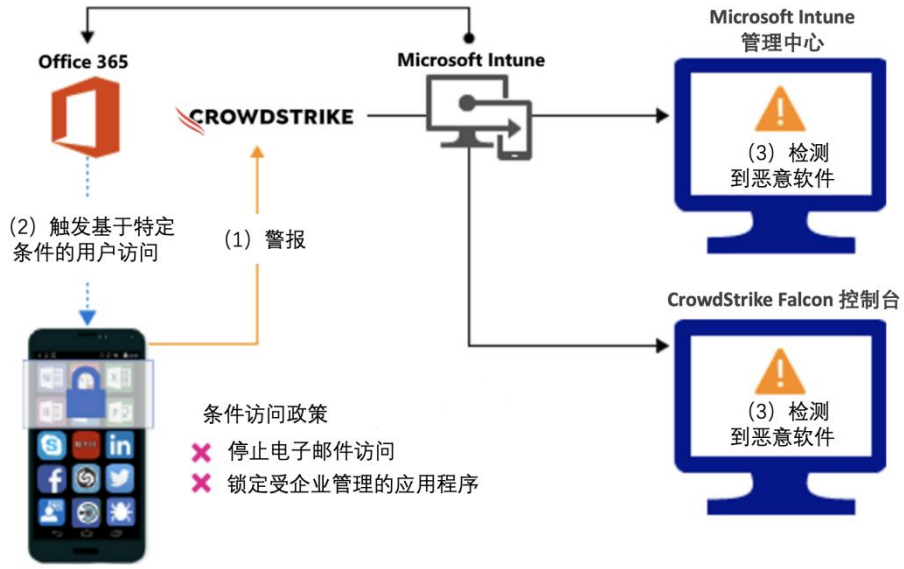
图 25、CrowdStrike 与 Microsoft Entra ID 协同示意图

数据来源：公司投资者 PPT，兴业证券经济与金融研究院整理

3.5.3.3 Falcon for Mobile 与 Microsoft Intune 合作。

通过 Intune 和 CrowdStrike Falcon for Mobile 的集成，企业可以根据设备的风险动态控制对公司资源的访问，确保在检测到威胁时及时用户阻止访问公司资源。此外，用户还会从安装在设备上的 CrowdStrike Falcon 应用程序中收到指导，以解决问题并重新获得对公司资源的访问权限，用例涵盖检测到恶意软件/网络威胁时阻止访问等。

图 26、CrowdStrike 与 Microsoft Intune 协同示意图



数据来源：微软官网，兴业证券经济与金融研究院整理

3.5.3.4 CrowdStrike Falcon 传感器兼容 Windows 内核操作系统。

- **初始架构：提供支持微软内核模式（Kernel Access）的安全产品。**在 Windows Vista 之前，绝大多数安全产品都由多个复杂的内核驱动程序组成，缺乏文档化和公开的供应商级能力来提供端点保护产品所需的安全保障。在 Windows Vista 及后来的 Windows 7 中，微软引入替代技术和内核模式代码签名（KMCS，Kernel Mode Code Signing，要求只有经过数字签名的驱动程序和内核模式代码才能被加载到 Windows 内核中），以保证内核代码的完整性，显著减少不稳定性、安全性和兼容性问题，为所有安全供应商现在遵循的标准化和统一编程模型奠定了基础。2011 年成立时，CrowdStrike 选择仅支持 Windows 7 及未来版本，并与微软的内核系统完全兼容。
- **后续集成：CrowdStrike 持续与微软安全功能更新保持协同。**随着微软继续构建用于用户模式防篡改、可见性和安全操作执行的新技术，Falcon 传感器迅速采用微软内核系统新功能，并与相应的新机制兼容。

表 19、微软内核系统和 CrowdStrike 后续集成情况

微软版本	微软内核系统功能更新	CrowdStrike 集成	CrowdStrike 与微软集成优势
-	内核模式驱动程序（kernel-mode driver）	Falcon 在早期配置和启用微软内核模式驱动程序	Falcon 能够在操作系统启动的早期阶段监控系统执行，检测意外行为，提前启动设备控制等服务； 预防早期的恶意组件篡改系统
Windows 8.1	首次引入受保护进程轻量级（PPL，Protected Process Lightweight）功能	CrowdStrike 迅速采取微软 PPL 架构	防止具有较高许可/访问权限的用户干扰安全产品的正常运作，或篡改用户模式组件以获取系统状态信息的各种信息源
Windows 10	AppContainer 技术（安全沙箱机制）	CrowdStrike 是第一个利用 AppContainer 技术创建 PPL 的第三方安全产品	消除在 Falcon 沙箱中拥有完整系统权限的需要
Windows 10	引入安全事件跟踪（ETW，Event Tracing for Windows）机制	Falcon 传感器的架构迅速支持微软安全 ETW 机制	进一步改善用户模式安全组件的态势
Windows 10	引入反恶意软件扫描接口（AMSI，Antimalware Scan Interface）	Falcon 传感器大量使用微软 AMSI 接口	消除进行复杂脚本、文档和宏解析的需要
-	Windows 硬件质量实验室（WHQL，Windows Hardware Quality Labs）认证	CrowdStrike 驱动程序被认证为 WHQL 驱动程序	允许客户利用 Windows Defender 应用程序控制（WDAC）来加强系统； 如 Falcon 传感器检测到其运行的操作系统内核版本未经 CrowdStrike 全面测试，将会自动禁用部分功能，以确保稳定性并避免崩溃
-	内存完整性（Memory Integrity）功能	所有 Falcon 驱动程序代码都与微软内存完整性兼容	确保内核内存页在通过代码完整性检查后才可执行，并且可执行页永远不会可写

数据来源：各公司官网，兴业证券经济与金融研究院整理

四、未来发展情况：产品+销售创新扩大 TAM

（一）产品创新：锚定增长领域，创新持续加速

1. 内部创新节奏：模块功能整合+加速 AI 创新

2012-2016 年，公司主要在 Falcon 平台上实现了威胁情报和狩猎、EDR 和下一代防病毒的整合。2017-2019 年，公司加快创新速度，陆续推出暴露管理、设备管理、MDR 和防火墙管理领域的服务，扩展 TAM。自 2020 年始，公司逐步实现关键模块的功能整合，同时引入 AI 驱动发展。云安全领域，公司先后加入 CWPP、CSPM、DSPM 等技术组件，推出行业完整的 CNAPP；SIEM 领域，公司先后推出 Fusion SOAR、Falcon LogScale 和 Falcon Foundry 等产品；身份保护领域，公司于 2022 整合将 Falcon 身份威胁保护模块与 Falcon Complete 托管服务结合，推出 Managed Identity Threat Protection。

图 27、2012-2024 年 CrowdStrike 产品发布情况

数据来源：公司官网，兴业证券经济与金融研究院整理
注：图中年度数据以自然年为统一标准

2. 对外收购：开辟新业务+完善云安全生态系统覆盖

自 2020 年始，CrowdStrike 开始收购 Freempt Security、Flow Security、Adaptive Shield 等企业，在零信任、数据安全等领域开辟业务，同时利用被收购企业的技术推出 DSPM、SaaS 安全态势管理等模块，完善云安全生态系统覆盖。

表 20、CrowdStrike 收购企业情况

时间	收购企业	扩展方向
2020 年	Freempt Security	零信任安全能力
2021 年	Humio	无索引 XDR 数据平台
2021 年	Secure Circle	零信任数据保护
2022 年	Reposify	外部攻击面风险
2023 年	Boinic	代码到运行时云安全
2024 年	Flow Security	数据安全态势管理（DSPM）
2024 年	Adaptive Shield	SaaS 安全

数据来源：公司官网，兴业证券经济与金融研究院整理
注：图中年度数据以自然年为统一标准

3. 扩大操作系统支持，推动平台整合

自成立以来，公司持续支持微软操作系统，包括 Windows 7 及未来版本。除此之外，公司 Falcon 平台支持 Mac、Linux、ChromeOS、iOS 和安卓等操作系统。2024 年，公司持续扩大操作系统支持，宣布更新对 Windows XP、Windows Server 2003、Windows Vista、Windows Server 2008、销售点（POS）终端 Windows Embedded POS Ready、Windows 8 和物联网的支持。

（二）销售创新：Falcon Flex +客户承诺套餐策略稳定提升 TCV

1. Falcon Flex 许可模型：以客户为导向的灵活销售促进平台采用。

2023 年 9 月 19 日，CrowdStrike 引入 Falcon Flex 订阅方案，允许企业根据自身需求和优先级灵活地选择和部署模块，快速实现安全防护价值。此外，Falcon Flex 方案提供低总支出承诺，允许客户在控制成本同时满足安全需求。2025 财年第三季度，Falcon Flex 带来的账户总交易价值（TAV）达 13 亿美元，环比增长 86%，实现强劲反弹；第四季度 Falcon Flex TAV 超 25 亿美元，同比增长超 10 倍。

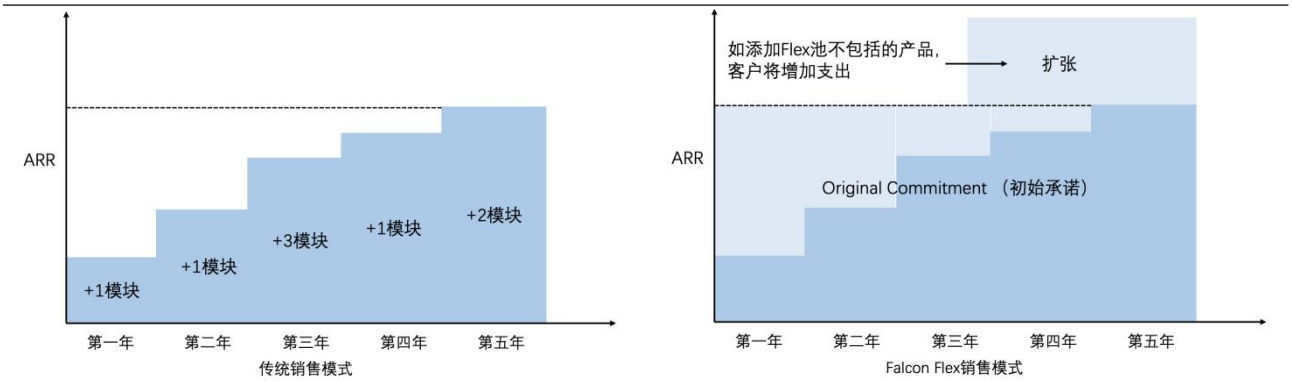
传统模式：

- **采用策略**：企业通常采取模块化的采用策略，每个模块独立部署，在已部署模块基础上逐步添加模块。
- **订阅周期**：通常需要较长部署的时间和多个销售周期。

Falcon Flex：

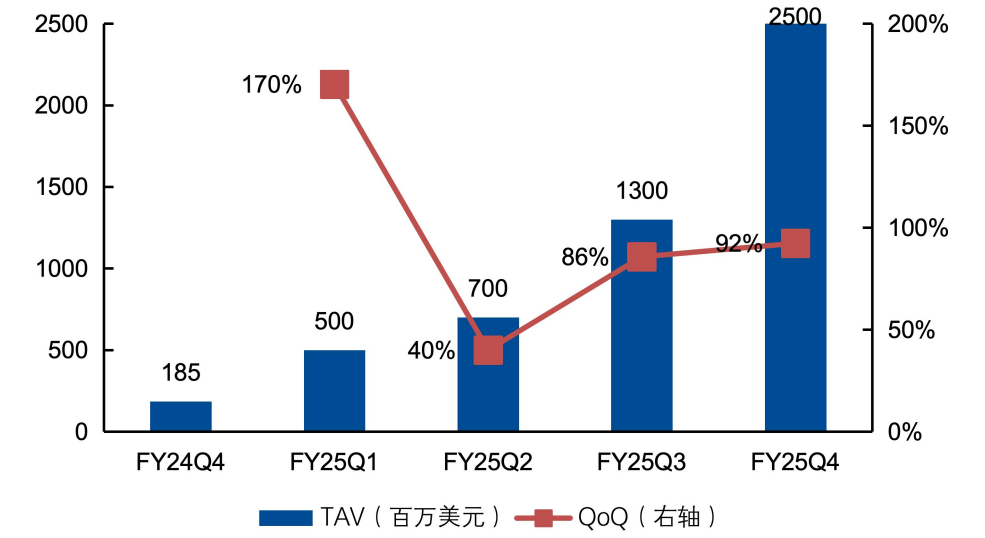
- **采用策略**：许可规模取决于企业平台需求；允许客户每年切换调整已采用的模块，并可选择在许可期内公司新推出的模块。
- **订阅周期**：允许 1-5 年的灵活订阅周期；通过单一轻量级代理和控制台交付，消除额外配置、部署或切换成本的需求。

图 28、CrowdStrike 销售模式与传统模式对比



数据来源：公司投资者 PPT，兴业证券经济与金融研究院整理

图 29、Falcon Flex 许可模型 TAV



数据来源：公司 2024 年投资者 PPT，公司季度报，兴业证券经济与金融研究院整理
注：图中季度均为财年季度（FY2025 期间为 2024.2.1-2025.1.31）

2. 客户承诺套餐（Customer Commitment Package）：应对 719 事件+提升增长潜力

2025 财年第三季度（起止日期：2024 年 8 月 1 日-2024 年 10 月 31 日，即 719 事件后的第一个季度），CrowdStrike 在 Falcon Flex 中推出客户承诺套餐，包括折扣、模块添加、专业服务的灵活付款条款以及延长客户订阅的期限等客户购买刺激。预计 CrowdStrike 客户承诺套餐总金额为 6000 万美元，将持续提高客户留存率，进一步推动 Falcon 的使用和平台价值的实现。

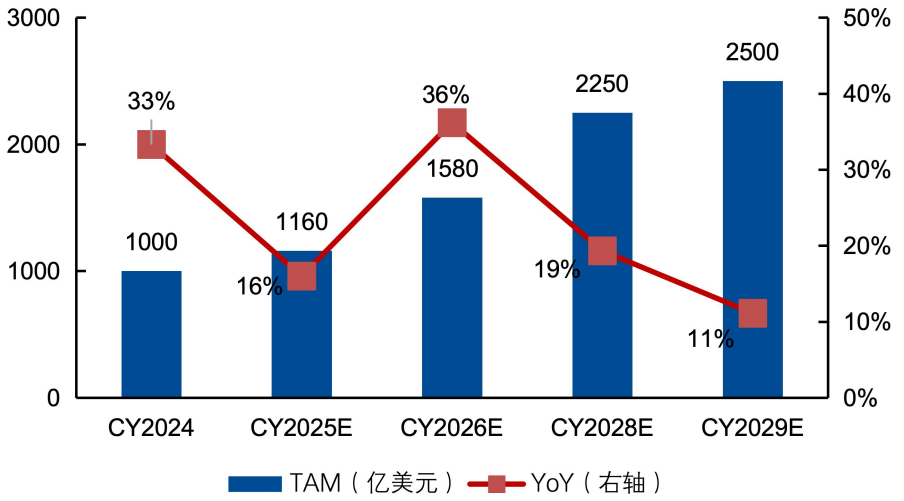
图 30、CrowdStrike 客户承诺套餐图例

数据来源：公司投资者 PPT，兴业证券经济与金融研究院整理

（三）TAM 持续提升，原生 AI 安全平台增长潜力巨大

CY2024 公司 TAM 达到 1000 亿美元，同比增长 33%。CrowdStrike 预计 CY2029 公司 TAM 将达 2500 亿美元，较 CY2024 年增长 250%。

图 31、CrowdStrike 2024-2029 年 TAM 预测



数据来源：公司投资者 PPT，公司季度报，兴业证券经济与金融研究院整理
注：图中年度均为自然年

云安全板块：云安全板块 TAM 预计在 CY2025 年达到 170 亿美元，同比增长 42%，在 CY2028 年达到 310 亿美元，较 2025 年增长 82%。在 2031 财年前，预计云安全板块的 ARR 将达 25-30 亿美元。

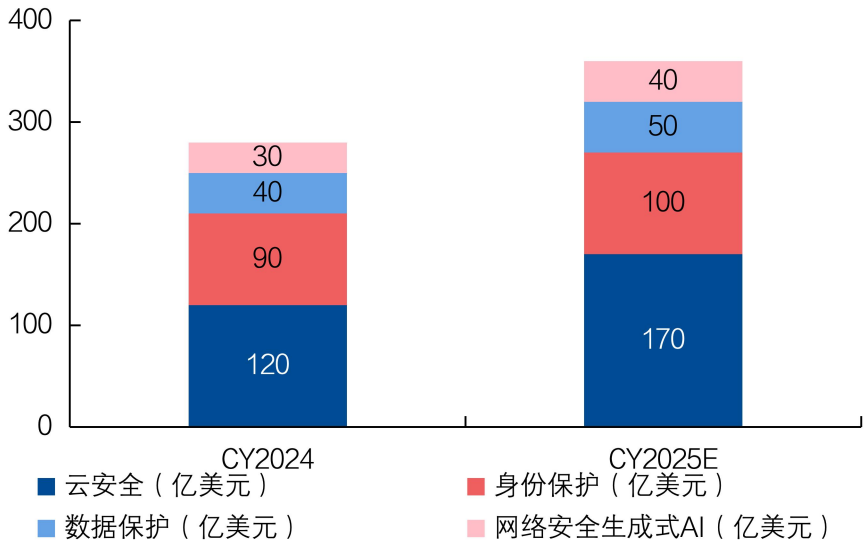
身份保护板块：身份保护板块 TAM 预计在 CY2025 年达到 100 亿美元，同比增长 11%。在 CY2028 年达到 170 亿美元，较 2025 年增长 70%。在 2031 财年前，预计身份保护板块的 ARR 将达 10-15 亿美元。

下一代 SIEM 板块：下一代 SIEM 板块 TAM 预计在 CY2028 年达到 160 亿美元。在 2031 财年前，预计下一代 SIEM 板块的 ARR 将达 15-20 亿美元。

数据保护板块：2024 自然年，企业寻求减少数据安全供应商，替换传统数据丢失防护（DLP，Data Loss Prevention）系统，对统一的安全与 IT 管理平台需求日益增长。数据保护板块 TAM 预计在 CY2025 年达到 50 亿美元，同比增长 25%，CY2029 年达到 90 亿美元，较 2025 年增长 80%。

生成式 AI 板块：针对 AI 的数据泄露、数据盗窃和对手间谍活动日益增加，CrowdStrike 推出创新性 AI 功能（如解析器、调查员、警报分类），保护企业云基础设施中的 AI 安全。得益于此，CrowdStrike 网络安全生成式 AI 板块 TAM 预计在 CY2025 年达到 40 亿美元，同比增长 33%，CY2029 年达到 60 亿美元，较 2025 年增长 50%。

图 32、CrowdStrike 2024-2029 年细分 TAM



数据来源：公司投资者 PPT，公司季度报，兴业证券经济与金融研究院整理
注：图中年度均为自然年

五、盈利预测与估值

预测逻辑为：

1）收入：公司收入由订阅收入和专业服务收入构成。根据公司业绩会和投资者日 PPT 公开表述，719 事件将对公司 FY2026 年第一季度造成约 7300 万美元的支出，但自 FY2026 年下半年始，历史高客户留存率和续约率将恢复并维持高位，与云安全、身份保护、下一代 SIEM 等未来发展机遇共同推动预计净新增 ARR 加速增长。假设 FY2026-2028 年公司基于美元的净留存率分别为 112%/115%/114%，净新增 ARR 年增长率为 8%/42%/15%，则 FY2026-2028 年公司期末 ARR 为 5,115/6,357/7,785 百万美元，公司订阅收入为 4,558.53/5,580.27/6,891.57 百万美元；假设 FY2026-2028 年专业服务收入同比

增长 13%/27%/25，则 FY2026-2028 年公司专业服务收入 216.40/275.46/344.33 百万美元，总收入为 4,774.93/5,855.73/7,235.90 百万美元。

2）毛利：假设公司 FY2026-2028 年毛利率为 78%/79%/79%，则分别实现毛利润 3,742.47/4,619.71/5,737.70 百万美元。

3）营业费用：假设公司 FY2026-2028 年营销费用率为 33%/31%/30%，研发费用率为 19%/19%/18%，管理费用率为 6%/6%/5%，则分别实现营销费用 1,562.05/1,843.22/2,138.14 百万美元，研发费用 912.38/1,094.86/1,280.98 百万美元，管理费用 293.24/296.88/329.54 百万美元。

4）Non-GAAP 净利润：预计公司 FY2026-2028 年 Non-GAAP 净利润为 906.27/1,275.05/1,822.74 百万美元，Non-GAAP 净利率为 19%/22%/25%。

表 21、CrowdStrike FY2026-2028 年盈利预测

会计年度	FY2025A	FY2026E	FY2027E	FY2028E
营业收入(百万美元)	3,954	4,775	5,856	7,236
增长率	29%	21%	23%	24%
毛利润(百万美元)	3,089	3,742	4,620	5,738
毛利率	78%	79%	79%	79%
营销费用	1,264	1,562	1,843	2,138
研发费用	732	912	1,095	1,281
管理费用	256	293	297	330
Non-GAAP 净利润	988	906	1,275	1,823
Non-GAAP 净利率	25.0%	19.0%	21.8%	25.2%
摊薄每股收益(元)	**4.05**	**3.61**	**4.99**	**6.96**

数据来源：公司季度报，兴业证券经济与金融研究院整理
注：FY2025 期间为 2024.2.1-2025.1.31

投资建议：

719 事件的负面影响我们预计将逐季消散，我们看好公司差异化产品质量、创新集成能力及灵活销售体系在网络安全行业新趋势中的长期价值，当前市值对应 FY2026/27/28 年 P/S 值分别为 19.6/16.0/12.9。首次覆盖，给予“增持”评级。

表 22、网络安全行业企业 P/S 估值（截至 2025 年 4 月 9 日）

证券代码	证券简称	股价（当地货币）	总市值（亿美元）	月涨跌	2025 年年初至今涨跌幅	营收同比增速预期				调整后净利润同比增速预期				PS			
						24A/E	25A/E	26E	27E	24A/E	25A/E	26E	27E	24A/E	25A/E	26E	27E
PANW-US	Palo alto networks	173.0	1145.6	1.0%	(5%)	16%	14%	15%	15%	35%	17%	16%	19%	14.3	12.5	10.9	9.5
CRWD-US	Crowdstrike	378.0	937.0	4.3%	10%	29%	21%	22%	24%	31%	(11%)	35%	39%	23.7	19.6	16.1	13.0
FTNT-US	Fortinet	99.9	768.4	3.4%	6%	12%	13%	12%	13%	43%	5%	13%	15%	12.9	11.4	10.1	8.9
DDOG-US	Datadog	97.4	335.9	(3.6%)	(32%)	26%	19%	20%	23%	41%	(2%)	25%	31%	12.5	10.5	8.7	7.1
NET-US	Cloudflare	112.6	388.4	(2.7%)	5%	29%	26%	27%	29%	59%	8%	31%	44%	23.3	18.5	14.6	11.3
ZS-US	Zscaler	202.1	312.7	0.5%	12%	34%	22%	20%	20%	83%	(1%)	20%	24%	14.4	11.8	9.8	8.2
OKTA-US	Okta	101.7	176.6	(2.8%)	29%	15%	10%	10%	13%	78%	17%	13%	3%	6.8	6.2	5.6	5.0

数据来源：factset，兴业证券经济与金融研究院整理

注：图中年度数据以自然年为统一标准；证券代码为 factset 代码

附表

资产负债表

单位：百万美元

会计年度	FY2025	FY2026E	FY2027E	FY2028E
流动资产	**6,113**	**7,761**	**10,301**	**13,472**
现金及现金等价物	4,323	5,588	7,691	10,327
短期投资性证券	0	0	0	0
应收账款	1,129	1,345	1,648	2,027
其它流动资产	661	829	962	1,117
非流动资产	**2,588**	**2,687**	**2,924**	**3,205**
资产与设备	789	776	904	1,073
使用权资产	43	43	43	43
商誉	913	913	913	913
其他非流动资产	844	956	1,064	1,177
资产总计	**8,702**	**10,448**	**13,225**	**16,677**
流动负债	**3,461**	**4,029**	**4,993**	**6,029**
应付账款	131	120	34	39
递延收入	2,733	3,367	4,078	4,909
应计费用及其他负债	597	541	881	1,080
非流动负债	**1,922**	**1,975**	**2,261**	**2,567**
长期递延收入	996	1,122	1,359	1,636
长期租赁负债	31	31	31	31
长期负债	744	744	744	744
其他非流动负债	151	77	126	155
负债合计	**5,383**	**6,003**	**7,253**	**8,595**
额外实收资本	4,367	5,322	6,200	7,286
累计亏损	-1,078	-1,146	-773	-64
非控股权益	39	39	39	39
其他综合收益	-9	229	505	820
总权益	**3,319**	**4,444**	**5,972**	**8,081**
负债及权益合计	**8,702**	**10,448**	**13,225**	**16,677**

现金流量表

单位：百万美元

会计年度	FY2025	FY2026E	FY2027E	FY2028E
经营活动产生现金流量	1,414	1,247	2,206	2,777
投资活动产生现金流量	-537	-221	-378	-456
融资活动产生现金流量	107	238	276	316
汇率变动影响	-5	0	0	0
现金净变动	948	1,264	2,103	2,636
现金的期初余额	3,375	4,323	5,588	7,691
现金的期末余额	4,323	5,588	7,691	10,327

利润表

单位：百万美元

会计年度	FY2025	FY2026E	FY2027E	FY2028E
营业收入	**3,954**	**4,775**	**5,856**	**7,236**
营业成本	865	1,032	1,236	1,498
毛利	**3,089**	**3,742**	**4,620**	**5,738**
经营费用	2,251	2,768	3,235	3,749
研发费用	732	912	1,095	1,281
营销费用	1,264	1,562	1,843	2,138
管理费用	256	293	297	330
经营利润	**838**	**975**	**1,385**	**1,989**
利息及其它收入	195	213	285	387
利息费用	-24	-24	-24	-24
税前收入	**1,009**	**1,164**	**1,645**	**2,352**
所得税	21	257	370	529
Non-GAAP 净利润	988	906	1,275	1,823
稀释 EPS(美元)	**4.05**	**3.61**	**4.99**	**6.96**

主要财务比率

会计年度	FY2025	FY2026E	FY2027E	FY2028E
成长性				
营业收入增长率	29.4%	20.8%	22.6%	23.6%
毛利润增长率	29.7%	21.2%	23.4%	24.2%
经营利润增长率	28.3%	16.4%	42.1%	43.6%
盈利能力(%)				
毛利率	78.1%	78.4%	78.9%	79.3%
经营利润率	21.2%	20.4%	23.6%	27.5%
ROE	34.9%	23.3%	24.5%	25.9%
ROA	11.3%	8.7%	9.6%	10.9%
偿债能力				
资产负债率	61.9%	57.5%	54.8%	51.5%
流动比率	1.77	1.93	2.06	2.23
每股资料(美元)				
稀释 EPS（美元）	4.05	3.61	4.99	6.96
每股净资产	13.62	17.68	23.36	30.87
每股经营现金流	5.93	1.57	1.31	1.28
估值比率(倍)				
Diluted-PE	93.2	104.8	75.8	54.3
PB	27.7	21.4	16.2	12.2

数据来源：公司季度报、兴业证券经济与金融研究院

注：每股收益均按照新股本摊薄计算；FY2025 期间为 2024.2.1-2025.1.31

分析师声明

本人具有中国证券业协会授予的证券投资咨询执业资格并登记为证券分析师，以勤勉的职业态度，独立、客观地出具本报告。本报告清晰准确地反映了本人的研究观点。本人不曾因，不因，也将不会因本报告中的具体推荐意见或观点而直接或间接收到任何形式的补偿。

投资评级说明

投资建议的评级标准	类别	评级	说明
报告中投资建议所涉及的评级分为股票评级和行业评级（另有说明的除外）。评级标准为报告发布日后的 12 个月内公司股价（或行业指数）相对同期相关证券市场代表性指数的涨跌幅。其中：沪深两市以沪深 300 指数为基准；北交所市场以北证 50 指数为基准；新三板市场以三板成指为基准；香港市场以恒生指数为基准；美国市场以标普 500 或纳斯达克综合指数为基准。	股票评级	买入	相对同期相关证券市场代表性指数涨幅大于 15%
		增持	相对同期相关证券市场代表性指数涨幅在 5%～15%之间
		中性	相对同期相关证券市场代表性指数涨幅在-5%～5%之间
		减持	相对同期相关证券市场代表性指数涨幅小于-5%
		无评级	由于我们无法获取必要的资料，或者公司面临无法预见结果的重大不确定性事件，或者其他原因，致使我们无法给出明确的投资评级
	行业评级	推荐	相对表现优于同期相关证券市场代表性指数
		中性	相对表现与同期相关证券市场代表性指数持平
		回避	相对表现弱于同期相关证券市场代表性指数

信息披露

本公司在知晓的范围内履行信息披露义务。客户可登录 www.xyzq.com.cn 内幕交易防控栏内查询静默期安排和关联公司持股情况。

有关财务权益及商务关系的披露

兴证国际证券有限公司及/或其有关联公司在过去十二个月内与 XIANGYU INVESTMENT (BVI) CO., LTD.、佛山市高明建设投资集团有限公司、淮安开发控股有限公司、都江堰市城乡建设集团有限公司、保定国家高新技术产业开发区发展有限公司、河南航空港投资集团有限公司、河南省中豫融资担保有限公司、济源济康科技有限公司、泉州市南翼投资集团有限公司、兰溪市国有资本运营有限公司、兰溪市交通建设投资集团有限公司、青岛市即墨区城市开发投资有限公司、枣庄市基础设施投资发展集团有限公司、株洲市城市建设发展集团有限公司、嵊州市交通投资发展集团有限公司、嵊州市投资控股有限公司、福建石狮国有资本运营集团有限责任公司、湖南金霞发展集团有限公司、长沙金霞新城城市发展有限公司、福建红树林投资集团有限公司、漳州市龙海区国有资产投资经营有限公司、浙江长兴金融控股集团有限公司、滨江国投有限公司、GF Financial Holdings BVI Ltd.、广发证券、广发证券、泰州港城投资集团有限公司、湖州吴兴国有资本投资发展有限公司、湖州吴兴经开建设投资发展集团有限公司、申万宏源(国际)集团有限公司、申万宏源证券有限公司、扬州经济技术开发区开发(集团)有限公司、郑州建中建设开发(集团)有限责任公司、淄博市城市资产运营集团有限公司、青岛北岸控股集团有限责任公司、青岛动车小镇投资集团有限公司、青岛胶州城市发展投资有限公司、景德镇市城市发展集团有限责任公司、成都东方广益投资有限公司、青岛蓝谷投资发展集团有限公司、滕州信华投资集团有限公司、重庆市合川城市建设投资(集团)有限公司、淄博市淄川区财金控股有限公司、晋江市路桥建设开发有限公司、北京银行、湘潭振湘国有资产经营投资有限公司、湖北省联合发展投资集团有限公司、萍乡市城市建设投资集团有限公司、江西省信用融资担保集团股份有限公司、岳阳市城市建设投资集团有限公司、沂盛（维尔京）国际有限公司、山东沂蒙产业集团有限公司、嵊州市城市建设投资发展集团有限公司、丽水经济技术开发区实业发展集团有限公司、印象大红袍股份有限公司、兖矿集团（开曼群岛）有限公司、山东能源集团有限公司、科学城(广州)融资租赁有限公司、科学城(广州)投资集团有限公司、南阳城投控股有限公司、淮安市投资控股集团有限公司、淮北市建设投资有限责任公司、稠州国际投资有限公司、江门高新技术工业园有限公司、义乌市国有资本运营有限公司、安徽海螺材料科技股份有限公司、安徽海螺水泥股份有限公司、脑动极光医疗科技有限公司、天长市农业发展有限公司、四川省金玉融资担保有限公司、徽商银行股份有限公司、湖北省融资担保集团有限责任公司、抚州市数字经济投资集团有限公司、重庆兴农融资担保集团有限公司、重庆丰都文化旅游集团有限公司、盐城高新区投资集团有限公司、杭州富阳交通发展投资集团有限公司、浙江德盛（BVI）有限公司、成都市羊安新城开发建设有限公司、三水国际发展有限公司、江苏姜堰经开集团有限公司、唐山国控集团有限公司、曹妃甸国控投资集团有限公司、贵溪市发展投资集团有限公司、青岛市即墨区城市旅游开发投资有限公司、湖州市城市投资发展集团有限公司、安徽西湖投资控股集团有限公司、淮北市建投控股集团有限公司、衢州市衢通发展集团有限公司、山东泉汇产业发展有限公司、成都武侯产业发展投资管理集团有限公司、宁国市宁阳控股集团有限公司、温州市鹿城区国有控股集团有限公司、邹城市城资控股集团有限公司、山东明水国开发展集团有限公司、Mixin International Trading Co., Limited、河南中豫信用增进有限公司、南阳交通控股集团有限公司、宜昌高新投资开发有限公司、中原资产管理有限公司、中原大禹国际（BVI）有限公司、威海市环通产业投资集团有限公司、成都交通投资集团有限公司、滨州市滨城区经济开发投资有限公司、福清市国有资产营运投资集团有限公司、湖州莫干山高新集团有限公司、湖州莫干山国有资本控股集团有限公司、郑州市金水控股集团有限公司、郑州地铁集团有限公司、漳州圆山发展有限公司、漳州高鑫发展有限公司、靖江港口集团有限公司、娄底市城市发展控股集团有限公司、怀远县新型城镇化建设有限公司、徽商银行、JUNFENG INTERNATIONAL CO., LTD、烟台国丰投资控股集团有限公司、济南高新控股集团有限公司、洛阳国晟投资控股集团有限公司、漳州台商投资区资产运营集团有限公司、浙江省新昌县投资发展集团有限公司、浦江县国有资本投资集团有限公司、平度市城市开发集团有限公司、万晟国际（维尔京）有限公司、新沂市交通文旅集团有限公司、XD 民生银行、常德财鑫融资担保有限公司、湖南瑞鑫产业运营管理有限公司、赣州城市投资控股集团有限责任公司、湖北省融资担保集团有限责任公司、黄石产投控股集团有限公司、赤壁城市发展集团有限公司、江苏中扬清洁能源发展有限公司、重庆三峡融资担保集团股份有限公司、江苏银行、无锡恒廷实业有限公司、四海国际投资有限公司、福建省晋江市建设投资控股集团有限公司、济南章丘控股集团有限公司、湖南省汨罗江控股集团有限公司、湖南省融资担保集团有限公司、China Cinda 2020 I Management Ltd、中国信达(香港)控股有限公司、重庆兴农融资担保集团有限公司、资阳发展投资集团有限公司、荆州市城市发展控股集团有限公司、南京银行、淄博市城市资产运营集团有限公司、上饶创新发展产业投资集团有限公司、宜宾市新兴产业投资集团有限公司、Zhongyuan Zhicheng Co., Ltd.、中原豫资投资控股集团有限公司、南昌金开集团有限公司、九江银行、无锡市交通产业集团有限公司、保定市国控集团有限责任公司、海翼（香港）有限公司、济南市中财金投资集团有限公司、政金金融国际(BVI)有限公司、重庆新双圈城市建设开发有限公司、Shenghai Investment Co.,Limited、Coastal Emerald Limited、山东高速集团、青岛军民融合发展集团有限公司、泰兴市港口集团

有限公司、潍坊市城区西部投资发展集团有限公司有投资银行业务关系。

使用本研究报告的风险提示以及法律声明

兴业证券股份有限公司经中国证券监督管理委员会批准，已具备证券投资咨询业务资格。

，本公司不会因接收人收到本报告而视其为客户。本报告中的信息、意见等均仅供客户参考，不构成所述证券买卖的出价或征价邀请或要约，投资者自主作出投资决策并自行承担投资风险，任何形式的分享证券投资收益或者分担证券投资损失的书面或口头承诺均为无效，任何有关本报告的摘要或节选都不代表本报告正式完整的观点，一切须以本公司向客户发布的本报告完整版本为准。该等信息、意见并未考虑到获取本报告人员的具体投资目的、财务状况以及特定需求，在任何时候均不构成对任何人的个人推荐。客户应当对本报告中的信息和意见进行独立评估，并应同时考量各自的投资目的、财务状况和特定需求，必要时就法律、商业、财务、税收等方面咨询专家的意见。对依据或者使用本报告所造成的一切后果，本公司及/或其关联人员均不承担任何法律责任。

本报告所载资料的来源被认为是可靠的，但本公司不保证其准确性或完整性，也不保证所包含的信息和建议不会发生任何变更。本公司并不对使用本报告所包含的材料产生的任何直接或间接损失或与此相关的其他任何损失承担任何责任。

本报告所载的资料、意见及推测仅反映本公司于发布本报告当日的判断，本报告所指的证券或投资标的的价格、价值及投资收入可升可跌，过往表现不应作为日后的表现依据；在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的报告；本公司不保证本报告所含信息保持在最新状态。同时，本公司对本报告所含信息可在不发出通知的情形下做出修改，投资者应当自行关注相应的更新或修改。

除非另行说明，本报告中所引用的关于业绩的数据代表过往表现。过往的业绩表现亦不应作为日后回报的预示。我们不承诺也不保证，任何所预示的回报会得以实现。分析中所做的回报预测可能是基于相应的假设。任何假设的变化可能会显著地影响所预测的回报。

本公司的销售人员、交易人员以及其他专业人士可能会依据不同假设和标准、采用不同的分析方法而口头或书面发表与本报告意见及建议不一致的市场评论和/或交易观点。本公司没有将此意见及建议向报告所有接收者进行更新的义务。本公司的资产管理部门、自营部门以及其他投资业务部门可能独立做出与本报告中的意见或建议不一致的投资决策。

本报告并非针对或意图发送予或为任何就发送、发布、可得到或使用此报告而使兴业证券股份有限公司及其关联子公司等违反当地的法律或法规或可致使兴业证券股份有限公司受制于相关法律或法规的任何地区、国家或其他管辖区域的公民或居民，包括但不限于美国及美国公民（1934 年美国《证券交易所》第 15a-6 条例定义为本「主要美国机构投资者」除外）。

本报告由受香港证监会监察的兴证国际证券有限公司(香港证监会中央编号：AYE823)于香港提供。香港的投资者若有任何关于本报告的问题请直接联系兴证国际证券有限公司的销售交易代表。本报告作者所持香港证监会牌照的牌照编号已披露在报告首页的作者姓名旁。

本报告的版权归本公司所有。本公司对本报告保留一切权利。除非另有书面显示，否则本报告中的所有材料的版权均属本公司。未经本公司事先书面授权，本报告的任何部分均不得以任何方式制作任何形式的拷贝、复印件或复制品，或再次分发给任何其他人，或以任何侵犯本公司版权的其他方式使用。未经授权的转载，本公司不承担任何转载责任。

特别声明

在法律许可的情况下，兴业证券股份有限公司可能会持有本报告中提及公司所发行的证券头寸并进行交易，也可能为这些公司提供或争取提供投资银行业务服务。因此，投资者应当考虑到兴业证券股份有限公司及/或其相关人员可能存在影响本报告观点客观性的潜在利益冲突。投资者请勿将本报告视为投资或其他决定的唯一信赖依据。

兴业证券研究

上 海	北 京
地址：上海浦东新区长柳路 36 号兴业证券大厦 15 层	地址：北京市朝阳区建国门大街甲 6 号世界财富大厦 32 层 01-08 单元
邮编：200135	邮编：100020
邮箱：research@xyzq.com.cn	邮箱：research@xyzq.com.cn
深 圳	**香 港（兴证国际）**
地址：深圳市福田区皇岗路 5001 号深业上城 T2 座 52 楼	地址：香港德辅道中 199 号无限极广场 32 楼全层
邮编：518035	邮编：518035
邮箱：research@xyzq.com.cn	邮箱：ir@xyzq.com.hk