证券研究报告—深度报告

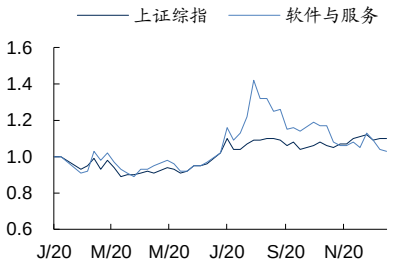
软件与服务

信息安全深度剖析 2

超配
（维持评级）

2021 年 01 月 04 日

一年该行业与上证综指走势比较



相关研究报告：

《计算机行业专题：从供需格局看银行 IT 高景气》 ——2020-12-15

《PDF 行业专题报告：PDF 群雄逐鹿：Adobe、金山、福昕各领风骚》 ——2020-09-18

《信息安全深度剖析 1：从奇安信看信息安全新玩法、新技术、新市场和新格局》 ——2020-07-09

《医疗信息化行业快评：上海市将互联网医疗纳入医保报销，互联网医疗再下一城》 ——2020-02-23

《医疗信息化行业快评："疫情+再融资"新规双推动医疗信息化蓬勃发展》 ——2020-02-17

证券分析师：熊莉
E-MAIL: xiongli1@guosen.com.cn
证券投资咨询执业资格证书编码：S0980519030002
证券分析师：库宏垚
电话：021-60875168
E-MAIL: kuhongyao@guosen.com.cn
证券投资咨询执业资格证书编码：S0980520010001

独立性声明：

作者保证报告所采用的数据均来自合规渠道，分析逻辑基于本人的职业理解，通过合理判断并得出结论，力求客观、公正，其结论不受其它任何第三方的授意、影响，特此声明

行业专题

海外网安巨头如何映射国内——Crowdstrike 终端云安全可复制

- **AI 和威胁情报助终端安全技术蝶变，全球市场格局已变**

传统终端安全以"杀毒软件"为代表，以特征库匹配为主要技术，主要解决已知问题。随着各类未知攻击的诞生，终端安全也引入 AI、威胁情报等新的技术应对。终端处，产品升级为下一代杀毒 NGAV、终端检测响应 EDR、云工作负载保护 CWPP；云端处，威胁情报成为新的"生产资料"，为终端乃至全部安全体系赋能。IDC 预计 2022 年终端安全市场将超过 92 亿美元，年复合增长率 8.6%。

- **Crowdstrike 实现基于云的终端安全颠覆，快速成长新王当立**

Crowdstrike 以威胁情报和终端安全起家，云端建设威胁图，Falcon 平台的动态威胁数据库；终端部署轻量级代理，类似终端处的"传感器"。通过终端代理，客户可以实现多种 SaaS 安全功能订阅。除了终端安全，公司还推出多种产品组合，基础版价格已由 6.99 提升至 8.99 美元/月。凭借产品在体验端、技术端、市场端的优势，公司迅速得到市场认可。近年来公司营收增速均保持 85%以上，预计 2020 年收入 8.55-8.6 亿美元，增速为 78%。同时，公司净留存率保持 120%以上，各项 SaaS 指标优异。当前市值达到 470 亿美金，对应今年 PS 在 50 倍以上。

- **市场、政策、技术推动国内终端安全市场重启，终端已成必争之地**

杀毒软件是国内消费者接触最早的终端安全产品，国内早期消费级市场由江民、瑞星、金山主导，随后 360 通过免费将时代终结。海外消费级终端安全市场依然存在，但国内外企业级均是最核心的市场。市场端，2017 年 wannacry 病毒带动了终端需求的催化，近期 Solarwinds 事件也验证了终端保护的重要性；政策端，等保 2.0 进一步强调了主机安全；技术端，除了终端自身技术进化之外，在态势感知为代表的体系化安全建设中，终端已经是必不可少的一环。国内终端安全有望快速增长。

- **投资建议：终端安全价值深远，关注关键卡位厂商**

终端安全具备五大价值：C 端触角的产品、持续收费的模式、威胁情报的"探针"、安全运维的衍生、万物即可终端的市场。重点关注关键技术和市场卡位厂商：奇安信、深信服、安恒信息、山石网科、360 等。

- **风险提示：**

疫情反复影响全社会 IT 支出；行业竞争加剧。

重点公司盈利预测及投资评级

公司代码	公司名称	投资评级	昨收盘（元）	总市值（亿元）	EPS 2020E	EPS 2021E	PE 2020E	PE 2021E
300454	深信服	买入	248.01	1014	2.23	3.06	111.22	81.05
688561	奇安信-U	买入	126.10	857	-0.18	0.21	-	600.48
688023	安恒信息	买入	260.10	193	1.78	2.49	146.12	104.46
688030	山石网科	买入	37.80	68	0.57	0.73	66.32	51.78

资料来源：Wind、国信证券经济研究所预测

投资摘要

关键结论与投资建议

终端安全价值重启，重点关注终端领域技术和市场具备卡位优势的厂商。传统以特征库匹配技术为代表的终端安全，已经进入以 AI 和威胁情报为基础的技术升级。以 Crowdstrike 为代表的终端厂商，验证了云化下技术和商业模式的双重变革。国内终端安全在市场、政策、技术的推动下，EDR 产品呈现较快增长，已经成为各厂商必争之地。终端安全具备 C 端触角的产品、持续收费的模式、威胁情报的“探针”、安全运维的衍生、万物即可终端的市场五大价值。重点关注关键技术和市场卡位厂商：奇安信、深信服、安恒信息、山石网科、360 等。

核心假设或逻辑

第一，AI 和威胁情报已经给终端安全带来新的技术蝶变，终端已经成为云网端安全一体化建设的必备。叠加勒索病毒泛滥催化市场需求，等保 2.0 政策推动，终端安全有望迎来高速发展期。

第二，以 Crowdstrike 为代表的终端安全厂商成为新王，无论是产品本身的技术优势，还是商业上各种订阅服务的组合，都验证了终端安全云化的优越性。

与市场预期不同之处

第一，市场认为企业级终端安全仅仅是信息安全领域一个小版块，当前市场不大，难有太大的成长空间。我们认为，终端价值深远，其具备 C 端触角、持续收费、威胁情报、运维衍生等多个优势；而且未来万物皆可为智能终端，市场空间理论没有边界。

第二，市场认为安全产品同质化竞争，难以形成海外厂商的竞争优势。我们认为，终端产品相比于其他安全产品，具备企业员工用户直观的体验。较差的产品将直接影响办公体验，必将被市场淘汰。国内头部厂商，在技术和市场上已经取得了优势。

股价变化的催化因素

第一，信息安全事件爆发。近期 Solarwinds 被攻击事件对美国造成了极严重的影响，恶意软件会将其自身植入受害者终端，进一步感染网络。该事件催化下，美股 APT 厂商 Fireeye 和终端安全 Crowdstrike 均股价大涨。安全事件的爆发，会倒逼全球加大信息安全投入。

第二，新兴安全领域的高增长。美国以云安全为代表的 Crowdstrike、Zscaler、OKTA 等厂商增速较高，市场也给予了较高的估值。国内安全厂商也在加大新兴领域安全的投入，例如终端安全、威胁情报、云安全资源池等，新兴安全收入占比的提升将提升公司整体估值。

核心假设或逻辑的主要风险

第一，疫情影响持续，全社会 IT 及安全开支缩减。

第二，全行业竞争加剧，各厂商陷入同质化价格战导致毛利率下降。

内容目录

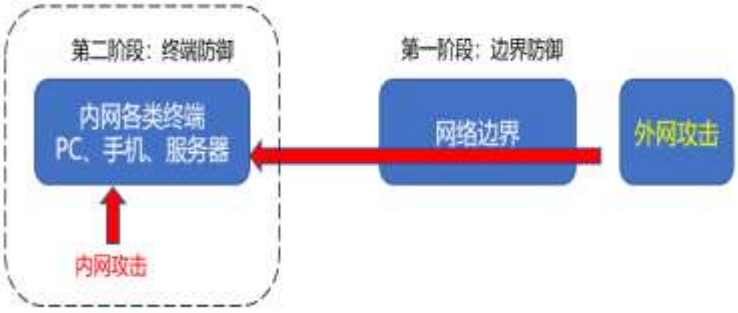
图表目录

终端安全技术蝶变，威胁情报成为安全新风口

终端安全面临下一代技术升级，AI 成为新驱动力

“杀毒软件”永不过时。安全的本质是攻防的较量，网络攻击有造成网络端崩溃的（如 DDoS 攻击），也有窃取机密数据或勒索的（如 WannaCry 病毒）。当边界防御被攻击突破后，终端自身的防御系统则成为关键，需要及时排查恶意软件。另一方面，内网本身存在攻击风险，如企业 PC 上插一个 U 盘，直接就从内部开始感染。尤其当前云化、移动化办公趋势明显，很多办公设备并不是永远处在被边界保护的环境中，疫情下广泛的远程办公，更是让办公终端处于“放任”状态。因此终端自身需要具备防御能力，安全产品依然刚需。

图 1：终端被攻击的形式



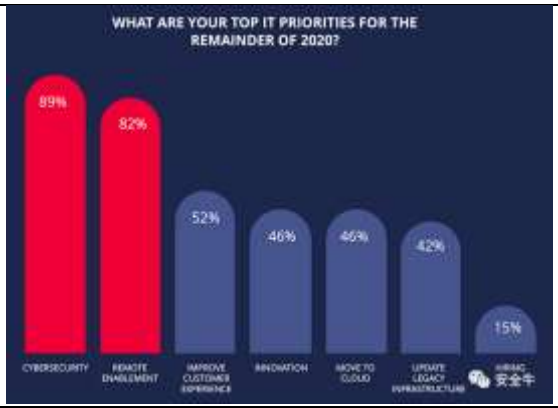
资料来源：国信证券经济研究所整理

IOT 终端急剧膨胀，后疫情时代，终端是安全投入的重点。物联网的快速发展必然会带来海量的 IOT 设备，当前除了移动化的办公设备外，服务器、打印机、销售站、可穿戴设备等均是潜在被攻击对象。即使企业上云后，云上的工作负载，如虚拟机和容器，也成为了新的终端需要被保护。后疫情时代，各办公终端、及网络场景，处于高度分散化状态，边界被打破带来了攻击面的扩大。因此根据日立发布的企业首席信息官（CIO）调查，2020 年下半年最高 IT 支出优先级是网络安全。疫情改变了大多数 CIO 的 IT 计划，现在有 89％的人表示他们专注于网络安全，而 82％的人则致力于远程支持；有一半的人表示要增加网络安全预算。具体方向来看，有 43％的 CIO 在身份和访问管理（IAM）上进行了投资，有 34%的 CIO 加强了终端安全的投资。这两项技术也非常匹配当下云场景办公需求，终端安全持续受益。

图 2：广泛的终端类型

资料来源：高盛，国信证券经济研究所整理

图 3：日立对疫情后 CIO 的 IT 支出调查



资料来源：安全牛，国信证券经济研究所整理

技术方面，终端安全正处于变革期，下一代杀毒和终端安全响应成为新方向。以国外 McAfee、国内 360 为代表的传统杀毒软件，主要通过升级静态病毒库来与恶意软件进行匹配。该方法在面对如“无文件攻击”时会失效。而以 APT 为代表的高级持续性攻击，隐秘性极强，迫使传统终端安全引入新的技术，如人工智能、大数据、行为分析等技术，产品形态有终端检测响应 EDR、威胁情报、沙箱技术等。

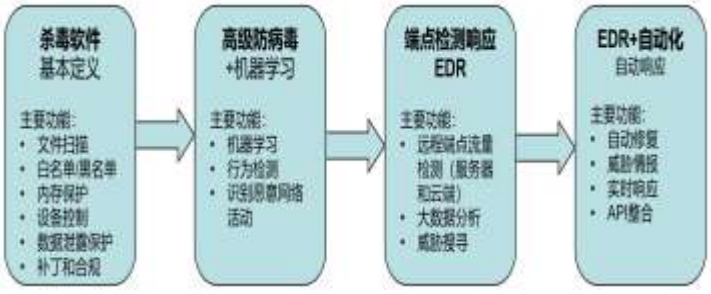
图 4：新型攻击持续推动终端防御体系进化

资料来源：国信证券经济研究所整理

下一代杀毒 NGAV（EPP）:。基于签名的防病毒产品，依然是当前的主流，但是攻击的复杂性提升，导致传统杀毒软件越来越力不从心。2019 年 Ponemon Institute 的一项调查发现，防病毒产品平均错过了 60％的攻击。因此也诞生出下一代杀毒软件 NGAV，通过引入机器学习、异常行为分析等技术，利用人工智能来识别和防止恶意行为。

终端安全响应（EDR）:。EDR 核心为记录，收集和存储来自端点设备活动的大量数据，从而使安全专业人员可以识别潜在威胁，调查和补救任何潜在攻击。重要的是，EDR 为安全团队提供了可视性，其中包含大量数据，可以对其进行分析以磨练恶意或异常行为，并检测端点保护技术遗漏的攻击。EDR 在 2016～2019 年连续进入 Gartner 的 10 大技术之列，成为当前终端领域最热门产品。

图 5：杀毒软件 EPP 技术升级至检测响应 EDR



资料来源：国信证券经济研究所整理

当前终端安全主要分两类：办公终端和云工作负载。假设极限办公 IT 场景只有办公终端和云（无论公有云，还是私有云）服务端，以 PC 为代表的终端安全主要以 EPP 和 EDR 产品为主；而以云为代表的服务终端，则是虚拟机、容器等工作负载，以 CWPP 产品为主。

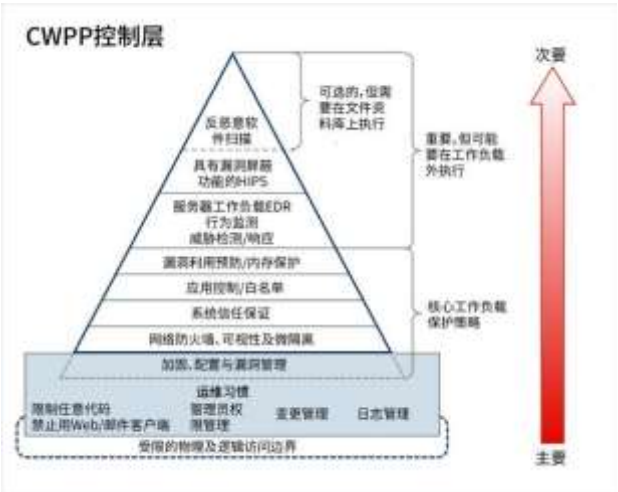
EPP（终端保护平台，以杀毒软件为主）和 EDR 的组合成为终端安全的良药。EDR 与 EPP 有一部分的价值重叠，EPP 专注预防，EDR 能够描述整个攻击过程，实现高级威胁的检测与响应，二者共同部署是最好的组合。EDR 在 2016～2019 年连续进入 Gartner 的 10 大技术之列，并且认为 EPP 与 EDR 技术融合将成为总体趋势，这也带动 EPP 技术向 AI 发展的重大转变。

图 6：EPP 和 EDR 的异同

资料来源：FreeBuf、国信证券经济研究所整理

云上的工作负载将成为新的终端安全场景。云工作保护平台（Cloud Workload Protection Platform，简称 CWPP），与以解决 PC 和服务器终端安全的 EPP、EDR 不同，CWPP 主要解决混合的数据中心架构中，物理机、虚拟机、容器和无服务器工作负载的安全问题，为他们提供统一的可视化和控制力。根据 Gartner 的定义，CWPP 侧重数据和流量的问题，包括了 WAF、Firewall 和 IPS 等，并且越是靠近基座的功能越重要，越是靠近塔尖的功能越次要。CWPP 部署在操作系统层，采用服务端 agent+远程控制台的部署模式，agent 支持云、物理、混合环境部署。随着云承载 IT 工作的范围越来越广，云工作负载已经成为新的场景，CWPP 有望与传统 EPP 一样，成为新的终端安全必备。根据 Gartner 指引，2019 年市场达到 12.44 亿美元，同比增长 20.5%。

图 7：云工作保护平台（CWPP）主要能力



资料来源：青藤云安全、国信证券经济研究所整理

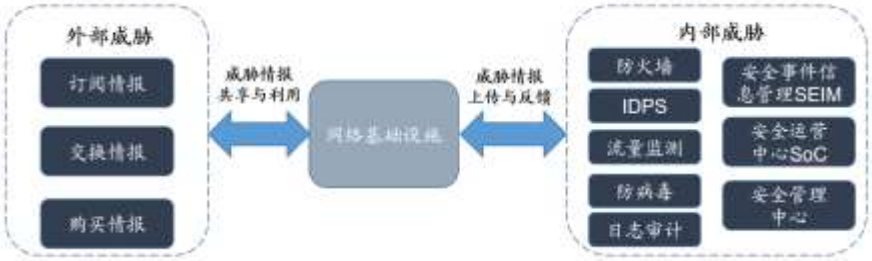
威胁情报为云端赋能打下基础，成为安全行业新“生产资料”

威胁情报弥补攻防两端信息不对称，已经成为安全必需品。当前新一代攻击者常常发起高级持续性攻击（APT）。APT 是精心策划下对特定组织的攻击，其攻击隐秘性极强，通常以盗取数据为目标，并不对系统造成伤害，被攻击者可能自始至终无法察觉。例如近期美国 Solarwinds 事件就是典型的 APT 攻击。过去基于恶意程序签名的技术，以防火墙、IPS、杀毒软件为代表的老三件产品无法解决此类问题，因为这是未知领域的攻击。而通过威胁情报的大量“内外援”

信息，新方法尽可能消除信息不对称。

威胁情报并非简单的“数据”和“信息”汇总。威胁情报更多是一种“知识”的概念，基于自身 IT 和信息资产面临的潜在威胁和攻击事件，形成上下文、机制、标示、含义和能够执行的建议等，能够为响应和处理提供决策的“知识”。威胁情报可以来自外部，如互联网公开情报源：各类安全事件、预警信息、监控数据分析、IP 地址信誉等，也有情报交换、商业情报公司订阅等；也可以来自企业内部，企业自身网络基础设施产生的威胁数据，如通过提炼 SEIM 系统数据、异常流量、漏洞信息、日志信息等形成威胁情报。威胁情报常见部署状态为云端和本地的共享，一方面借力云端的情报助力，一方面本地形成内生性的场景，情报的“消费”和“生产”进行循环。通过共享，威胁情报可以在全行业发挥作用。

图 8：威胁情报系统框架



资料来源：CIO 时代、国信证券经济研究所整理

威胁情报内涵广阔，价值巨大。根据 David J. Bianco 在《The Pyramid of Pain》一文中提出的威胁情报相关指标，当“己方”掌握这些“知识”后，可以让攻击者感受相应困难的“痛苦”。威胁情报中价值最低的是 Hash 值、IP 地址和域名，其次是网络/主机特征、攻击工具特征，对攻击者影响最大的是 TTP(战术、技术和行为模式)类型的威胁情报。威胁情报的内涵早已超过传统的基于特征的病毒库，成为防护策略定制的新“生产资料”。

图 9：威胁情报各级别的价值

资料来源：FreeBuf、国信证券经济研究所整理

威胁情报赋能同样提升终端能力。在终端安全领域，基于各个端点广泛的检测、攻防、行为等数据，后台对各信息进行聚和、关联分析。形成威胁情报后，进而指导终端做出响应。终端安全领域，传统以特征库升级为主，威胁情报技术已产生了深刻的变革。除此之外，威胁情报还能用在传统产品上，如防火墙、

IDPS 等，形成实时的最新策略。同时，威胁情报还可以应用到业务安全中，如防欺诈；网络资产管理也可应用。随着威胁情报逐步普及，市场持续扩大，IDC 预计 2021 年市场规模达到 22 亿美金。

图 10：威胁情报对终端赋能

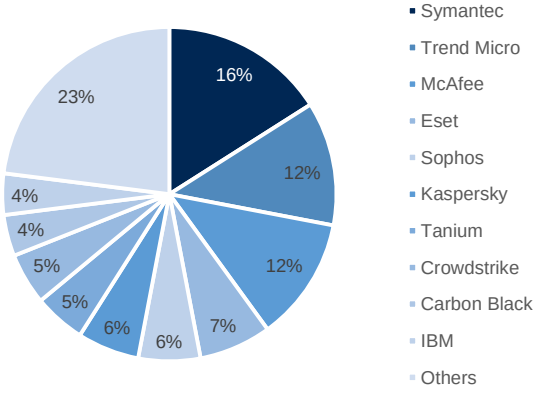
资料来源：火绒安全、国信证券经济研究所整理

终端安全领域格局已变——传统没落，新王当立

终端安全市场持续增长。根据《IDC 全球企业级终端安全预测，2018-2022》数据，2017 年全球企业级终端安全市场规模达到 61.46 亿美元，2022 年将超过 92 亿美元，年复合增长率 8.6%。其中传统 EPP 产品增速已经放缓，而 EDR 产品成为重要增长动力。

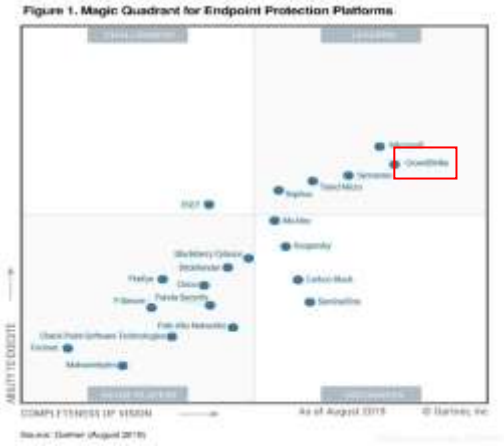
终端领域著名玩家众多，但行业领导者已经更替。无论是企业级终端市场，还是消费级终端市场，最耳熟能详的是 McAfee（迈克菲）、Symantec（赛门铁克-诺顿）、Kaspersky（卡巴斯基）等传统杀毒软件厂商，多数消费者在购置 PC 时也使用他们的预装安全产品。在企业级终端市场，传统厂商市场份额较高，Symantec、Trend Micro（趋势科技）、McAfee 占据了 40%的市场份额。然而根据 Gartner 最新的终端安全魔力象限，新兴终端安全厂商 Crowdstrike 已经跃升为行业领导者。Crowdstrike 在技术和市场上均表现优异，虽然当前市场份额仍较小，但是超高速增长下，公司持续侵蚀传统厂商的份额。公司基于云原生的 SaaS 方案，已经开始颠覆行业格局。

图 11：终端安全全球市场份额



资料来源：Gartner，国信证券经济研究所整理

图 12：终端安全魔力象限



资料来源：Gartner，国信证券经济研究所整理

防火墙龙头也纷纷加大终端布局，但思路仍以边界为主。传统防火墙类厂商将内网按照边界圈起来保护，但随着移动办公、云和多种 IOT 终端的兴起，边界正被不断打破。边界外的终端设备对整个网络造成风险，因此防火墙厂商均加入了终端安全模块。边界安全厂商的优势在于基于自身防火墙平台，打造云网端一体的防护。因此，防火墙龙头通过收购，纷纷加大了终端布局；但是基于防火墙厂商的发展路径，终端更多是整体解决方案的补充。目前在终端领域，海外边界安全厂商仍处于追赶者角色。

Fortinet 在 2019 年 10 月收购终端安全公司 enSilo，增强了公司安全平台的终端解决能力。enSilo 在被收购之前就已经是 Fortinet Security Fabric 的合作伙伴，并已完成与 FortiGate NGFW，FortiSandbox 沙盒方案，FortiSIEM 和 FortiClient Fabric Agent 的联动。

Palo Alto Networks 在 2014 年 3 月以 2 亿美元收购一家安全初创公司 Cyvera，其旗舰产品为 TRAPS。 TRAPS 对未修复的漏洞、无文件攻击、应用漏洞利用均有较好的效果，但是缺乏事后补救工具和响应机制，仍需要其他产品配合。Palo Alto 始终认为防护才是最重要的，检测和响应永远只能是其次；这个理念和近两年企业安全的主流价值观存在一些冲突。公司以网络端为核心，NGFW 边界平台提供强大支撑， TRAPS 成为与防火墙联动的模块，是整体方案的有益补充。

图 13：Palo Alto 对终端安全的布局

资料来源：Palo Alto Networks，国信证券经济研究所整理

终端安全领域赛道拥挤，Crowdstrike 通过新技术突围。目前终端安全玩家主要分为三类：传统杀毒厂商、网络安全厂商（收购）、新兴终端厂商。纵观终端安全发展历史，传统杀毒软件厂商众多，且依然占据较大市场。然而终端领域已经不再是基于特征库签名的 McAfee 和 Symantec 主导的时代，新兴厂商基于白名单、AI 等技术已经得到市场认可。相比于其他新兴终端厂商，Crowdstrike 基于云端平台，通过威胁情报、大数据、AI 等新技术成为行业领导者，市场上的高速增长，也确认了公司成为终端安全的新王。

表 1：终端安全厂商分类

竞争对手	代表厂商	技术特点
传统杀毒厂商	McAfee、Symantec	传统的基于特名的防病毒技术，与已知病毒库的匹配
网络安全厂商	Palo Alto、Fireeye	以边界安全为核心，通过收购或自研，补充终端安全能力
新兴终端安全厂商	Cylance、Carbon Black	基于纯恶意软件或应用程序白名单技术的端点产品

资料来源：国信证券经济研究所整理

终端安全的云化：从 Crowdstrike 看云端颠覆

基于云的终端安全，Crowdstrike 带来技术和商业模式双重变革

终端领域的 SaaS，Crowdstrike 新架构重塑终端安全。Crowdstrike 成立于 2011 年，由两位传统杀毒软件 McAfee 的高管创立。公司以威胁情报起家，开启 EDR 产品的黄金赛道，不断推出新产品实现交叉销售。公司曾因索尼影业遭黑客入侵事件，“特朗普通俄门”事件而名声大噪。相比于传统杀毒厂商基于特征签名只能解决已知威胁，公司创建了一个云安全平台 Falcon，基于大数据和 AI 的主动防御平台，以 SaaS 的模式提供多种安全服务，包括端点安全、安全与 IT 运营、威胁情报，能够解决未知威胁。终端安全基于各种海量设备布置（PC、服务器、移动、IOT、虚拟机云工作负载等），SaaS 模式让各端点更简单的部署、扩展和管理，迅速得到市场的欢迎。

表 2：公司发展历程

时间	大事件
2011 年 11 月	Crowdstrike 成立
2012 年 7 月	推出威胁情报产品
2013 年 6 月	推出单一解决方案 EDR
2013 年 8 月	推出威胁搜索云模块（threat hunting）
2017 年 2 月	推出 IT 卫生云模块（IT hygiene），开启多产品市场策略
2017 年 2 月	推出下一代防病毒云模块（NGAV）
2017 年 7 月	推出恶意软件搜索云模块（Malware search）
2017 年 11 月	推出沙箱和漏洞管理云模块（Sandbox and vulnerability management）
2018 年 4 月	推出端点保护即服务（Falcon Complete）云模块
2018 年 8 月	推出设备控制（device control）云模块
2019 年 2 月	推出首个基于开放云的用于端点安全的应用程序平台，以及业界首个受信任的第三方应用生态系统（Crowdstrike Store）
2019 年 3 月	推出首个针对移动设备的企业 EDR 解决方案
2020 年 10 月	Falcon 平台已发展到 16 个云模块，覆盖企业工作负载安全，安全和漏洞管理，托管安全服务，IT 运营管理和威胁情报服务

资料来源：Crowdstrike 官网、国信证券经济研究所整理

公司核心技术是基于云端的威胁图平台，以及基于海量终端的轻量级代理。

威胁图（Threat Graph）：Falcon 平台的动态威胁数据库。威胁图基于云原生架构，汇聚海量终端的数据，同时利用自有的和第三方的威胁情报，通过 AI 和模式匹配技术来寻找恶意活动，包括攻击能力，动机，归因和威胁指标。威胁图每周实时处理，关联和分析全球客户中超过 4 万亿个与端点相关的事件，使每分钟的攻击决策指标达到 1.34 亿，并为数十亿字节的历史数据编制索引以进行探索和搜索。各端点独立的事件看似没有直接关系，但是通过 AI 的分析，可以挖掘未知威胁。威胁图可以为客户提供实时和历史的可见性，深入了解端点处发生的事件。

轻量级代理（Lightweight Agent）：Falcon 平台对于每个终端放置的“传感器”。代理设计轻巧，消耗 CPU 少于 1%，且无需重启部署，以静默的方式自动执行，每个传感器每天传输约 5-8 MB，对用户终端没有干扰。该传感器主要是捕获和记录终端数据，上传给 Falcon 平台，并保护终端安全；且保留了端点上必需的本地检测和预防功能，在离线情况下也能工作。轻量代理实现了数据众包的模式，每个端点均贡献自身的威胁数据，形成广泛的网络效应。该传感器以机器学习的方式工作，同时还能兼容本地的第三方杀毒软件。

图 14：Crowdstrike 产品架构和模块组成

资料来源：Crowdstrike 官网、国信证券经济研究所整理

产品模块持续迭代，跨入 IT 运维领域。威胁情报当前已经成为网络安全建设必不可少的“生产资料”，Crowdstrike 也是以威胁情报起家，通过将威胁情报赋能，不断推出新的产品，例如终端安全领域的 EDR 引领行业变革。公司从 2017 年 2 月开始，开始由单一产品向多模块发展，实现交叉销售和多模块集成订阅。凭借公司掌握的海量终端，公司进一步衍生至 IT 运营业务，现在已经覆盖端点安全、IT 运营、托管服务、威胁情报、云安全。2020 年 9 月公司以 9120 万美元收购 Preempt Security，加强零信任的能力，进军身份保护领域。同时，公司 2020 年推出 PaaS 安全平台 CrowdStrike Store，支持第三方安全应用，打造 SaaS + PaaS 的完整安全生态。公司模块数快速增加，已由 2020 年初的 11 个模块，发展至当前的 16 模块，多个模块预计在 2021 年推出。

表 3：Crowdstrike 主要产品

分类	具体产品	主要功能
云安全	Cloud security posture management	用于风险可视化和评估，事件响应，合规性监视和 DevOps 集成，可自动跨云基础架构识别和补救风险，包括 IaaS、PaaS、SaaS
	Cloud discovery	对整个云基础架构的可见性，持续监视错误配置，确保安全策略和合规性执行
	Cloud runtime Protection	针对云工作负载和容器的 EDR，以及受管理的威胁搜寻，实现运行时保护
安全与 IT 运营	Falcon Forensic	网络取证服务，处理安全事件并进行取证分析，用以调查网络违规情况
	Falcon Discover—IT Hygiene	可以识别客户网络中的恶意系统和应用程序，并监视客户环境中任何位置的特权用户帐户的使用
	Falcon Spotlight — Vulnerability Management	实时识别客户端点中存在的漏洞，不依赖于耗时较长的漏洞扫描系统，利用已有代理收集的数据
托管服务	Falcon OverWatch—Threat Hunting	威胁搜寻解决方案，由安全专家精英组成，主动为客户识别威胁
	Falcon Complete — Turnkey Security Solution	为客户提供全面的监视，管理，响应和补救解决方案
端点安全	Falcon Prevent—NGAV	下一代防病毒功能，具备针对未知恶意软件的机器学习功能，替换旧版的防病毒产品
	Falcon Insight—EDR	端点检测和响应 EDR，记录并自动分析端点上的活动，以提供深入的可见性，进行主动的威胁搜寻和取证分析
	Falcon Device Control	为管理员提供了 USB 外围设备的高度可见性和精细控制
	Falcon Firewall Management	提供对主机操作系统固有的防火墙功能的集中管理，使客户可以创建，实施和维护主机防火墙策略
身份保护	Preempt Security	提供现代化的零信任安全体系结构和威胁防护，Preempt Security 于 2020 年 9 月被公司收购
威胁情报	Falcon X—Threat Intelligence	提供对威胁的自动分析，以洞悉攻击的功能，动机和归因。
	Falcon Search Engine — Malware Search	搜索引擎使客户能够实时搜索 Falcon 平台中收集的约 800 TB 恶意软件，可以进行快速分析，领先攻击对手
	Falcon Sandbox—Malware Analysis	允许客户通过在虚拟机中安全引爆未知文件来分析恶意行为
	Falcon X Recon — Situational Awareness	从各类深度网络数据源收集数据，实现态势感知
应用商店	CS Store	基于 Crowdstrike 云原生平台，提供受信任的伙伴的安全应用

资料来源：Crowdstrike 官网、国信证券经济研究所整理

模块增加，带来产品组合价格提升空间。终端领域成为 Crowdstrike 掘金的第一蓝

海，公司按照部署端点数量和时间进行订阅收费，提供专业版、企业版、高级版多种产品组合。随着产品模块供给端的增加，以及组合灵活性的提升，产品价格也有所提升。专业版以 NGAV 为核心，价格由 6.99 提升至 8.99 美元/月；企业版以 NGAV 和 EDR 为核心，价格由 14.99 提升至 15.99 美元/月；高级版以 NGAV、EDR、IT Hygiene 为核心，价格由 17.99 提升至 18.99 美元/月。公司产品没有本地版本，自始至终坚持订阅模式，占营收比达到 91%。

图 15：Crowdstrike 产品和价格

资料来源：Crowdstrike 官网，国信证券经济研究所整理

海量终端下，Crowdstrike 开启七大增长战略。海外来看，终端领域一直有传统杀毒软件厂商占据。Crowdstrike 是基于云模式的 SaaS 终端安全产品，其成长逻辑优于传统设备厂商，大量客户可以实现快速海量终端部署，且云端助力比本地产品具备更好的效果。基于公司 Falcon 平台技术的领先性，公司具备替代老一代产品的能力。同时，不断丰富的产品模块供给，也提供了多种交叉销售的市场机会。而海量的移动、物联网终端也是公司新的增长点；同时还有机会切入 IT 运维等非安全领域。在政府客户和全球市场，公司也持续投资布局深入。

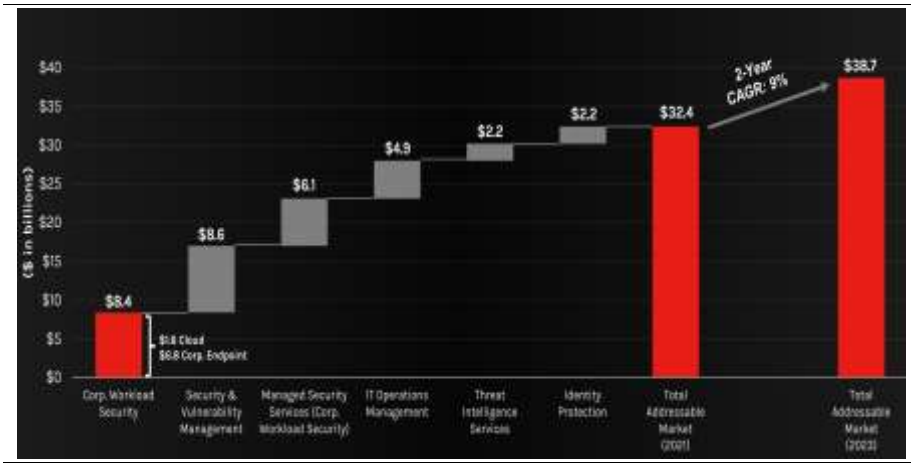
表 4：Crowdstrike 成长战略

成长战略	具体方法
替换其他终端产品	基于旧版产品技术局限性，Falcon 平台能够实现对传统产品的替换。公司客户数年增速在 100%以上
扩大现有客户销售	对于已经部署轻量级代理的客户，非常容易添加其他云模块，公司不断提供新产品，实现交叉销售
进入新市场	凭借 Falcon 平台和海量终端数据，可以扩展到移动、物联网终端领域，或切入安全以外的业务，如 IT 运维管理、性能监测等
扩展新客户	从最初的大企业客户为主，拓展至中小企业。面向 IT 能力较差的中小企业推出 Falcon Complete 整体解决方案，拓展客户群
扩展 Falcon 生态系统	CrowdStrike Store 是云原生 PaaS 平台，公司继续在 CrowdStrike 商店中进行投资。公司与 Dell 达成战略合作关系，加强与第三方生态合作
扩大与美国联邦政府的关系	投资收购联邦政府的市场客户，进入相关部门产品列表，公司的平台已部署在 AWS GovCloud 中
扩大国际市场	全球投资扩大国际业务范围，包括增加欧洲，中东，亚太地区和日本的员工人数，并建立海外数据中心

资料来源：Crowdstrike 年报，国信证券经济研究所整理

业务边界扩大，Crowdstrike 覆盖市场空间持续增长。公司以威胁情报起家后，凭借 Falcon 平台云原生的架构，不断赋能和挖掘新的功能模块。Falcon 也成为公司的孵化器，不断推出新产品，进入终端、漏洞管理、托管服务、以及 IT 运维管理类非安全领域。根据 IDC 和公司测算，公司目前产品覆盖的市场 2021 年达到 324 亿美元，在 9%的复合增速下，2023 年有望达到 387 亿美元。

图 16：Crowdstrike 各产品市场空间



资料来源：Crowdstrike 官网，国信证券经济研究所整理

具体来看，公司各细分产品和对应市场均有一定规模，其中终端和漏洞管理较大。相对于 300 亿美元以上的市场空间，公司上一财年收入仅为 4.81 亿美元，成长空间广阔。尤其云端结合有望成为普遍的 IT 架构，随着海量移动、IOT 等终端快速增长，公司成长边界仍会持续突破。

表 5：公司各细分产品和市场

细分市场	公司产品	市场规模
端点安全	2013 年推出 EDR；2017 年推出 NGAV，还包括 Firewall Management、CWPP、Horizon	预计该市场在 2021 年达到 84 亿美元，包括 16 亿美元的云工作负载和 68 亿美元的企业终端。市场复合增速为 8%
漏洞管理	2017 年推出 Falcon Spotlight，进入漏洞管理市场，当前还有产品 Forensic	预计 2021 年全球该市场将达到 86 亿美元，市场复合增速为 11%
托管安全服务	2018 年推出 Falcon Complete，进入托管安全服务市场，当前还有产品 OverWatch	预计全球该市场在 2019 年将达到 248 亿美元，公司有机会的市场在 2019 年大约为 44 亿美元，到 2021 年将达到 61 亿美元，市场复合增速为 9%
IT 服务管理软件	2017 年推出 Falcon Discover，进入 IT 资产管理（非安全市场），当前还有 Discover for Cloud and Containers	预计计全球该市场将在 2021 年达到 49 亿美元，市场复合增速为 9%
威胁情报	2012 年推出 Falcon X，公司以威胁情报起家，现在产品还有 Search、Sandbox、Falcon X Recon	预计全球该市场将在 2021 年达到 22 亿美元，市场复合增速为 11%
身份保护	2020 年收购 Preempt Security	预计 21 年市场规模达到 22 亿美金

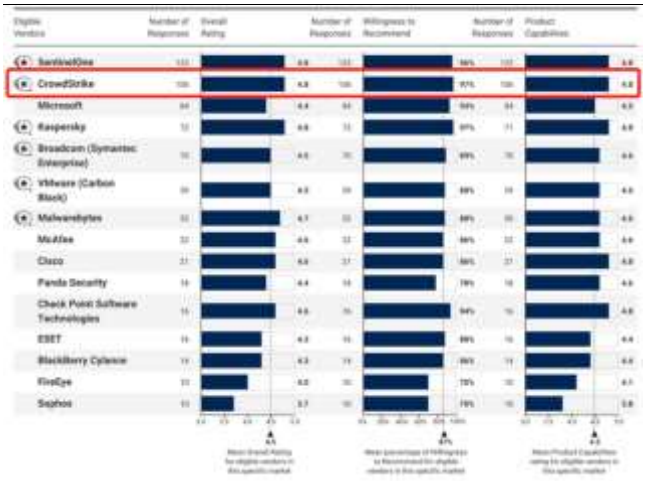
资料来源：IDC、Crowdstrike 预测，国信证券经济研究所整理

云和 AI 下的正循环，Crowdstrike 竞争优势强大

体验端：终端安全产品具备 C 端触角，云端 SaaS 用户体验成为关键因素之一。PC 上的安全软件是企业和消费者用户最常接触到的安全产品，传统模式下本地安装，配合实时更新的病毒库，整体产品较为臃肿，对本地 CPU 及内存消耗较大，因此常会造成“卡顿”现象。因此与网络端安全产品不同，终端安全软件用户体验极其重要，Crowdstrike 基于云原生的 SaaS 优势明显，公司可以在 24 小时内将 Falcon 平台部署到全球超过 10 万个端点，通过单一的轻量级代理，可以实施激活其他云模块。公司的轻量级代理设计轻巧，不用重启部署，也没有操作也没；且消

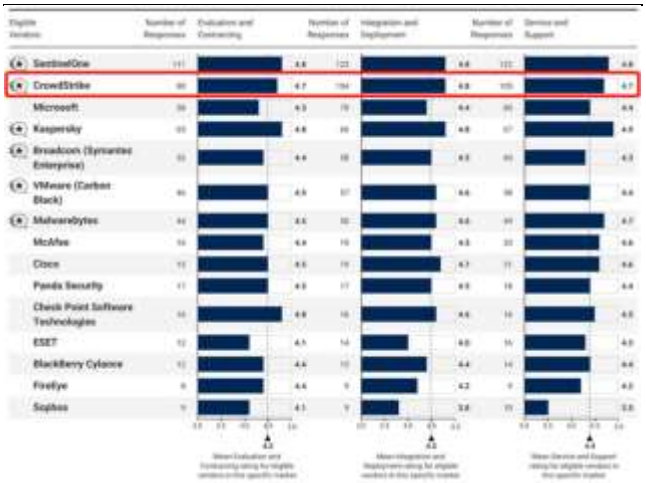
耗 CPU 不超过 2%，每天仅需上传 5-8M 数据。经过 AI 的训练，即使离线状态也能正常工作。根据 Gartner Peer Insights “客户之声”的调查统计，Crowdstrike 在整体评价、推荐意愿、产品力、评估签约、集成部署、服务支持等多个方面位居前二，其良好的用户体验获得客户的广泛认可。

图 17：客户对各厂商 EDR 产品评价（1/2）



资料来源：Gartner Peer Insights 2020，国信证券经济研究所整理

图 18：客户对各厂商 EDR 产品评价（2/2）



资料来源：Gartner Peer Insights 2020，国信证券经济研究所整理

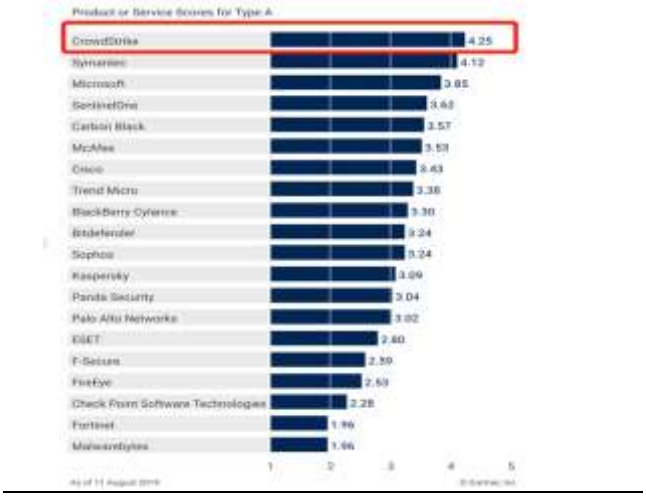
技术端：众包效应显著，基于 AI 的分析形成正反馈。凭借 Crowdstrike 在广泛客户终端的部署，数据汇聚到 Falcon 平台，可以进行充分的训练，实现产品更高的检测率和更低的误报率，进而吸引更多客户，其数据贡献也会更多。新一代终端安全厂商均是以 AI 为核心技术，公司 Falcon 已经早在 2016 年就被认证为传统杀毒软件的替代品。公司在 AV-Comparatives、SE Labs、VirusTotal 等多个第三方测评中均名列前茅，基于云的 AI 技术让公司与传统厂商在性能和检测率上拉开差距。

图 19：Crowdstrike 核心技术的网络效应

资料来源：国信证券经济研究所整理

市场端：Crowdstrike 技术能力同样深受市场认可。公司已经是 EPP 魔力象限的领导者。除此之外，根据 Gartner 终端保护平台（EPP）2019 关键能力报告，在 A 类客户中（具备“前瞻性”的小型组织，将技术建设视为竞争力，愿意在新技术上进行投入），公司关键功能排名第一。在 B 类客户（最大的组织，受到预算和人员限制，等待新技术成为主流之后再考虑实施）、C 类客户（中型组织，预算更为严格，看重产品稳定性和运营成本），公司也保持了前三名的排名。同样，在 Forrester Wave 2020 年终端保护平台矩阵中，对各厂商当前产品力、战略演进、市场地位做了 14 项评分，其中有 10 项 Crowdstrike 获得第一。

图 20：Gartner 端点保护平台关键能力排名



资料来源：Gartner 2019，国信证券经济研究所整理

图 21：Forrester Wave 端点保护平台矩阵

资料来源：Forrester Wave 2020Q1，国信证券经济研究所整理

当前 Crowdstrike 主要竞争者有传统杀毒厂商 McAfee 和 Symantec，新兴终端安全厂商 Carbon Black 和 SentinelOne，分别和对手一一对比。

Crowdstrike VS McAfee。McAfee 在消费者领域的用户体验较差，臃肿的本地部署和高 CPU 消耗让用户难以接受。公司在 EDR 等新技术领域投入滞后数年，基于签名的技术已经落后于新兴的基于 AI 的检测。虽然 McAfee 近年来持续加强 AI、威胁情报、云安全的投入，但当前 Crowdstrike 基于云的更轻巧的方案和更有效的全新产品更能满足客户需求，公司难以阻挡被 Crowdstrike 抢夺市场份额。

McAfee 是杀毒软件鼻祖，在市场份额和知名度上依然占据领先，目前在消费者领域，McAfee 保护了 6 亿台设备，但其近 10 年发展波折较大。2010 年英特尔以 76.8 亿美元收购了 McAfee，希望将网络安全功能整合到芯片中，以更深层次侦测网络威胁。但英特尔对 McAfee 的业务整合并不顺利，2016 年又将其出售。2020 年 10 月，McAfee 成功二次上市，市值约 70 亿美元左右。2019 年 McAfee 实现收入 26.35 亿美元，同比增长 9.38%；其中消费者 C 端实现收入 13.03 亿美元（+12%），企业 B 端实现收入 13.32 亿美元（+7%）。

表 6：Crowdstrike 和 McAfee 产品对比

功能	Crowdstrike	McAfee
检测	基于机器学习，防御已知和未知威胁	基于签名，专注于已知威胁
交付	云原生架构。易于设置，维护和可扩展性	本地部署，需要额外的硬件成本和维护负担。
安装时间	5 分钟。静默部署，无需重启	多日。终端必须重启，以进行安装和更新
传感器	1 个传感器。轻巧设计实现所有功能，本地 CPU 使用率低于 2%	多个传感器。包括预防、检测、响应等，扫描时 cpu 使用率大于 30%
基于行为的保护	基于事件的检测。包括可疑事件，零日攻击	基于签名规则
端点检测响应（EDR）	高级 EDR。自动警报和主动搜寻	基本 EDR。基本的记录和响应功能，支持有限的威胁搜寻用例

资料来源：Crowdstrike 官网，国信证券经济研究所整理

Crowdstrike VS Symantec。Symantec 各产品较为分散，如 EDR 和威胁情报等均需要单独产品，多种部署方式也容易造成版本混乱。Crowdstrike 云端部署更为简洁，集成性更高。Symantec 于 2016 年底也发布了 Symantec Endpoint Protection 14 解决方案，基于终端和云端的人工智能技术，但是市场认为该产品与真正的下一代产品性能和体验上仍有差距。

Symantec 目前占据终端安全市场最大的市场份额，2019 年公司将企业安全业务

以 107 亿美元出售给博通，数月后，博通又将 Symantec 卖给了爱尔兰的埃森哲，埃森哲主要从事企业咨询、信息安全咨询和运营等业务。Symantec 的消费者业务更名为 NortonLifeLock，由其收购的著名杀毒软件 Norton 和身份保护 LifeLock 组成，继续保持上市公司地位，目前市值约 120 亿美元左右。NortonLifeLock 在上一财年收入 24.9 亿美元，同比增长 1.38%。

表 7：Crowdstrike 和 Symantec 产品对比

功能	Crowdstrike	赛门铁克
交付	一个云原生平台和一个轻量级代理	具有本地、云、混合的多个平台和代理
检测	基于机器学习，行为分析和威胁情报，无需特征签名	仍然依赖特征签名和扫描
攻击可视化	全面了解所有攻击细节	关于威胁的上下文信息有限，更多可见性需要 EDR 产品配合
响应	实时响应，建立安全的远程连接快速调查和修复	仅限于策略更新的规则，远程响应需要 EDR 产品
威胁情报	自动集成威胁情报和恶意软件分析	需要 Symantec EDR 和威胁情报两个产品

资料来源: Crowdstrike 官网，国信证券经济研究所整理

Crowdstrike VS Carbon Black。Carbon Black 主打基于大数据分析的云交付安全平台，技术创新性与 Crowdstrike 相似。Carbon Black EDR 产品较强，但威胁情报相对单薄，且其最初的“白名单机制”有效但难以扩展。Crowdstrike 在威胁情报和服务上更为完善，且第三方测评认可度更高。

Carbon Black 成立于 2002 年，在 2014 年之前采用 Bit9 名称。公司同样聚焦下一代终端安全，其“白名单机制”技术与当时的终端产品思路完全不同。2013 年公司遭受黑客攻击，暴露终端检测和响应方面的缺陷，随即收购 Carbon Black，并 2016 年正式改名。Carbon Black 于 2018 年上市，2019 年被虚拟化巨头 VMware 以 21 亿美元收购。对于云里的“终端”——云工作负载，VMware 需要加强虚拟机、容器等新终端的安全。Carbon Black 2018 年收入达到 2.1 亿美元，同比增长 30%，收入体量已经被同期 Crowdstrike 超过，且 Crowdstrike 增速显著更高。

表 8：Crowdstrike 和 Carbon Black 产品对比

功能	Crowdstrike	Carbon Black
检测	基于机器学习，行为分析和威胁情报，无需特征签名	包含基于签名的杀毒引擎
维护	无需重启，直接更新	传感器和关键服务器更新可能需要重启
交付	基于云原生，适用所有工作负载。可以跨 Windows，Linux 和 macOS 服务器和端点部署	本地版本和云版本不一致，支持 macOS、Linux 发行版
行业认可	被行业分析师和独立测试组织评为领导者	没有一致参与独立的公开测试（如 SE 实验室和 AV Comparatives）
威胁情报	自动添加威胁情报，包括参与者归因，沙箱分析以及针对威胁和所有已知变体的恶意软件	威胁情报仅限于信誉和监视列表的指标
搜寻威胁	专家团队 24/7 主动针对威胁活动进行狩猎，调查并提供建议	对威胁进行分类和验证，而非主动搜寻

资料来源:

Crowdstrike VS SentinelOne。SentinelOne 同样强调 AI 技术的应用，在 EPP 上具备优势，但是 EDR 仍在完善中，且威胁情报功能不全面。SentinelOne 会在设备本地进行大量运算，因此 CPU 消耗高。Crowdstrike 在云端体验更好，且产品完整性和成熟度更高。

SentinelOne 成立于 2013 年，以 AI 技术前瞻性地预判出终端安全，而非出问题后再解决。公司强项在 EPP，自信可打败任何勒索软件，推出“网络威胁担保”服务：如果客户感染了勒索软件，最高可获 100 万美元损害赔偿。2020 年 2 月，公司完成 2 亿美金融资，估值已超过 11 亿美金。SentinelOne 表示，目前 3500 多家客户中包括数百家全球 2000 强企业，并且在过去 12 个月中收入实现增长 104％。

表 9：Crowdstrike 和 SentinelOne 产品对比

功能	Crowdstrike	SentinelOne
EDR	充分可见。连续和全面捕获原始事件信息，提供所需的上下文	部分可见性。仅专注于流程、文件、网络和用户事件
部署方式	数分钟内部署完成，无需重启	必须重启安装
搜寻威胁	专家团队 24/7 主动针对威胁活动进行狩猎，调查并提供建议	对检测的威胁进行警报、监视、分类和调查，而非主动搜寻
威胁情报	自动添加威胁情报，包括参与者归因，沙箱分析以及针对威胁和所有已知变体的恶意软件	仅限于文件哈希信誉值
托管服务	专家团队管理端点安全的所有方面，从部署，配置，维护和监视到警报处理，事件响应和补救。	对检测到的威胁（而不是完整的端到端托管服务）执行警报监视，分类和调查

资料来源：Crowdstrike 官网，国信证券经济研究所整理

技术和服务优势让 Crowdstrike 脱颖而出。公司产品优势主要在体验、技术、市场方面，总结来说，主要是云原生、AI、单一代理；威胁情报、7*24 小时服务、整体解决方案。公司对传统（McAfee 为代表）和同样新兴（Carbon Black 为代表）的终端安全厂商均形成压制。尤其传统竞争对手被资本裹挟较多，增速放缓，也显示其无法及时跟进最新的技术转型。而同样新兴的厂商也成为巨头布局的补充，VMware 收购 Carbon Black，重心在云工作负载的终端。同样，与 Crowdstrike 颇有渊源的 Cylance 也被黑莓收购，重心在 QNX 部门，车联网的新终端。当前终端市场预计持续增长，Crowdstrike 在技术和市场上均成为领导者，成长势如破竹。

表 10：Crowdstrike 主要优势

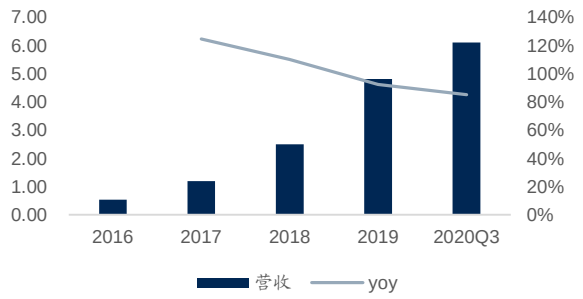
两大优势	主要亮点	核心价值
技术	云原生	简化部署，降低运营成本
	人工智能驱动	基于大数据和 AI 分析，提高即时可见性
	单一代理	一个代理解决所有问题，实现最大效率
服务	一流的威胁情报	威胁情报反应攻击全貌，实现主动安全
	7*24 小时威胁搜寻	主动搜索威胁，7*24 小时服务团队
	全面管理的服务	提供整体解决方案，团队专家进行配置和运行，同时支持远程修复

资料来源：Crowdstrike 官网、国信证券经济研究所整理

新终端龙头快速增长，SaaS 各项指标表现优异

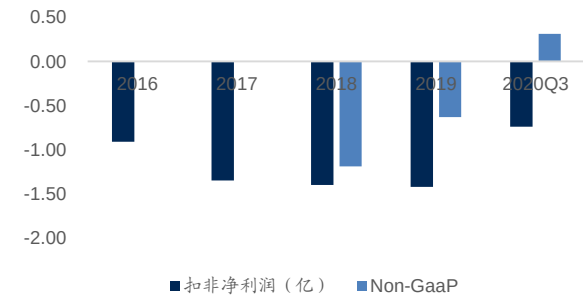
营收快速增长，持续超预期。Crowdstrike 近年来营收增速均保持 85%以上，2019 年（2020 年 1 月 31 日年报，近似 2019 年全年业绩）公司实现收入 4.81 亿美元，同比增长 92.7%；2020 年前三季度，公司实现收入 6.1 亿美元，同比增长 85%。单 Q3 收入 2.32 亿美元，再次超出二季度指引的 2.11-2.15 亿美元。公司也再次上调全年收入指引，预计 21 财年（近似于 2020 年）收入 8.55-8.6 亿美元，增速为 78%。公司表观利润依然为负，但公司已经连续 3 个季度实现 Non-GaaP 盈利，2020Q3 实现盈利 0.32 亿元，预计全年 Non-GaaP 也实现盈利。

图 22：Crowdstrike 收入增长（亿美元）



资料来源：Crowdstrike 公告，国信证券经济研究所整理

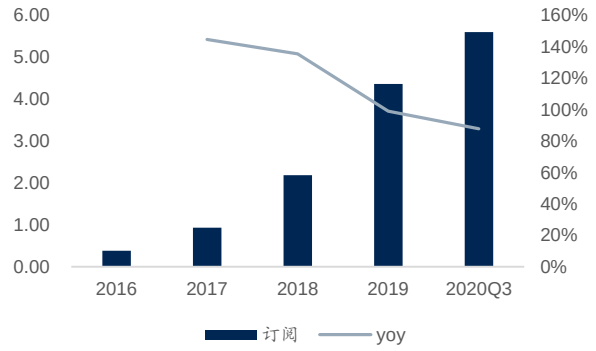
图 23：Crowdstrike 利润表现（亿美元）



资料来源：Crowdstrike 公告，国信证券经济研究所整理

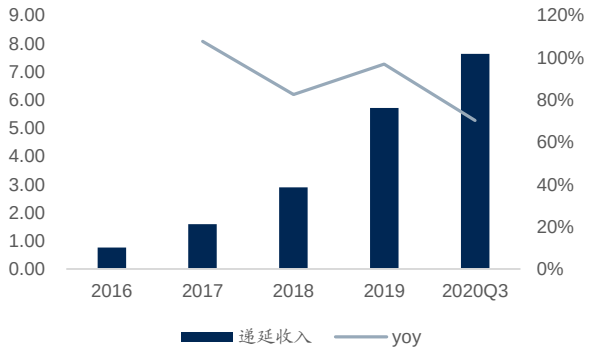
订阅模式为主体，递延收入健康增长。公司以 SaaS 模式提供终端安全服务，订阅收入占比达到 90%以上。2019 年订阅收入为 4.36 亿，同比增长 99%，20Q3 增速达到了 88%。随着订阅产品的增加，毛利率由 16 年的 36%，提升至当前的 77%。服务业务 2019 年收入为 0.45 亿，同比增长 50%，20Q3 增速达到 56%。得益于订阅业务的快速增长，公司 2019 年递延收入达到 5.71 亿美元，同比增长 97%；2020Q3 达到 7.63 亿美元，同比增长 70%。

图 24：Crowdstrike 订阅收入（亿美元）



资料来源：Crowdstrike 公告，国信证券经济研究所整理

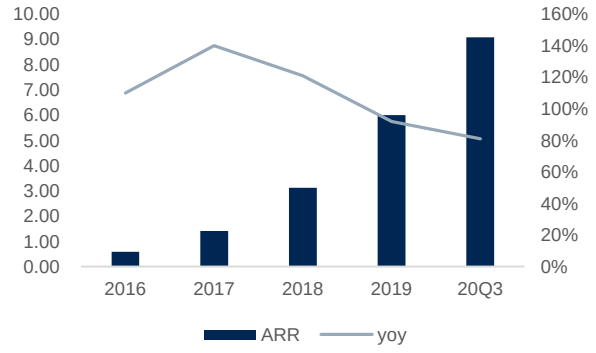
图 25：Crowdstrike 递延收入（亿美元）



资料来源：Crowdstrike 公告，国信证券经济研究所整理

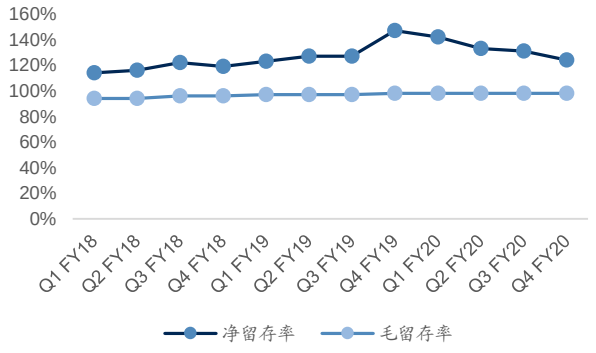
ARR 持续高增长，净留存率保持 120%以上。Crowdstrike 年度经常性收入 ARR 保持高速增长，20Q3 达到 9.07 亿美元，同比增长 81%；其中有 1.17 亿美元是本季度新增 ARR。公司 ARR 净留存率近年来保持 120%以上，FY21 Q1-Q3 虽没有具体披露，但也在 120%以上，主要是因为现有客户内部端点的扩展，以及新增的云模块订阅。公司 ARR 毛留存率也保持在 98%的高水平。

图 26：Crowdstrike ARR（亿美元）



资料来源：Crowdstrike 公告，国信证券经济研究所整理

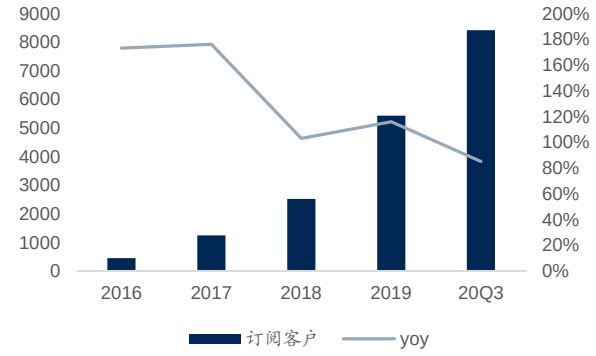
图 27：Crowdstrike 基于美元的 ARR 留存率



资料来源：Crowdstrike 公告，国信证券经济研究所整理

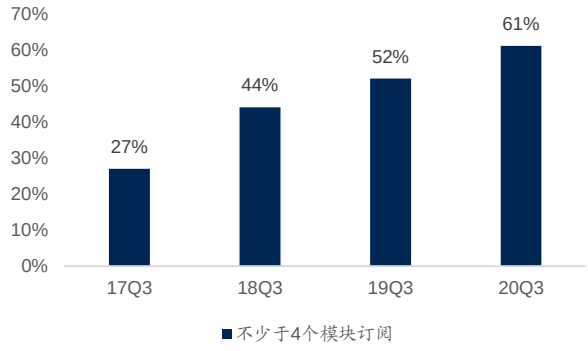
客户数保持高增长，多产品扩张路线推进顺利。2020Q3 公司订阅客户数达到 8416 家，同比增长 85%，本季度新增 1186 名客户，仍保持较高增长。同时，订阅不少于 4 个模块的客户持续增加，占比达到 61%；订阅不少于 5 个模块的客户占比也达到 44%，订阅不少于 6 个模块的客户占比达到 22%。公司不断加大产品布局，新产品认可度逐步提升。

图 28：Crowdstrike 客户数



资料来源：Crowdstrike 公告，国信证券经济研究所整理

图 29：Crowdstrike 订阅不少于 4 个模块的客户比例



资料来源：Crowdstrike 公告，国信证券经济研究所整理

核心 SaaS 指标亮眼。2019 年公司新增客户 2915 家，销售费用增速低于客户增速，公司 CAC 进一步下降，2020Q3 整体有所回升。ARR 增速也低于客户数量增长，新客户一般开始的订阅较少，因此 MRR 有所下降。随着客户后续订阅模块增加，预期 MRR 有望回升。公司当前季度客户毛留存率为 98%（月度水平更高），按照当前假设，2019 年公司 LTV/CAC 超过 5 倍，20Q3 也有 4.6 倍。

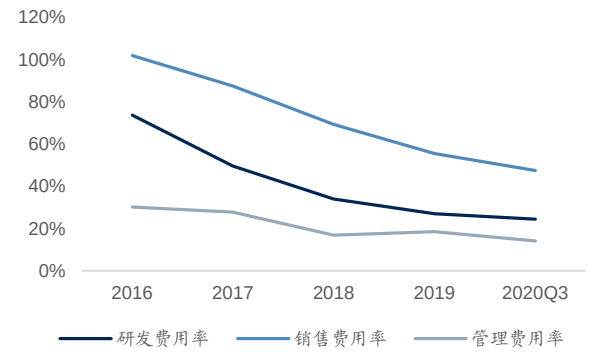
表 11：Crowdstrike CAC 和 LTV 计算

	2016	2017	2018	2019	2020Q3
销售费用（百万）	53.75	104.28	172.68	266.6	288.87
订阅客户	450	1242	2516	5431	8416
新增客户		792	1274	2915	2985
CAC（万）		13.17	13.55	9.15	9.68
ARR（百万）	58.76	141.31	312.66	600.46	907.4
MRR（万）		0.95	1.04	0.92	0.90
客户留存率		98%	98%	98%	98%
LTV		47.41	51.78	46.07	44.92
LTV/CAC		3.60	3.82	5.04	4.64

资料来源：Crowdstrike 公告，国信证券经济研究所整理

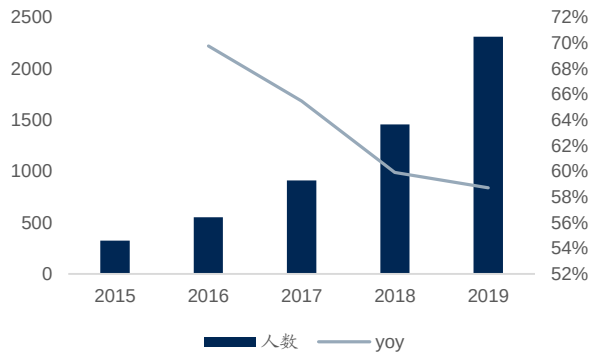
费用率持续下降，人员保持高增长。受益于 SaaS 模式的规模效应，公司各项费用率水平持续下降。2019 年公司研发费用率下降为 27.0%；销售费用率下降为 55.5%；管理费用率为 18.5%，比 2018 年略有上升；2020Q3 也进一步下降。公司员工数量也保持较快增长，公司 2019 年人员达到 2309 人，同比增长 58.7%。其中研发人员增速较为稳定，销售和管理人员增速较快。

图 30：Crowdstrike 费用率水平



资料来源：Crowdstrike 公告，国信证券经济研究所整理

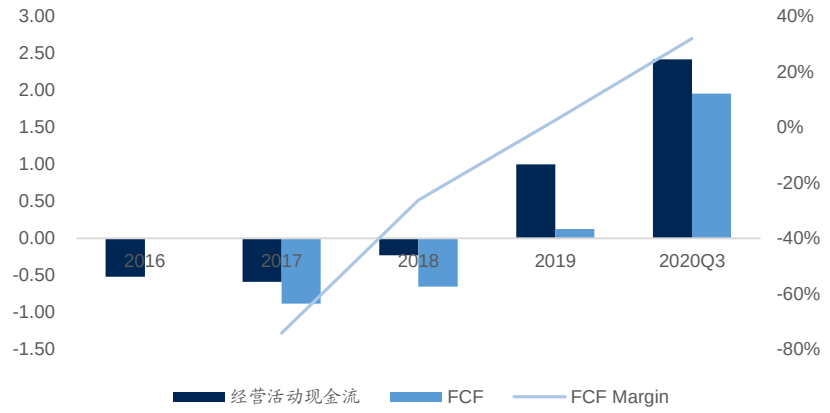
图 31：Crowdstrike 员工数量



资料来源：Crowdstrike 公告，国信证券经济研究所整理

现金流逐步好转。公司经营活动现金流和自由现金流均在 2019 年转正，经营活动现金流达到 1 亿美元，FCF 达到 0.12 亿美元。2020Q3 二者均有明显提升，FCF 达到 1.95 亿美元，且公司已经连续 5 个季度实现正的自由现金流。FCF Margin 也提升至 32%。

图 32：Crowdstrike 现金流表现（亿美元）



资料来源：Crowdstrike 公告，国信证券经济研究所整理

Crowdstrike 成为市值最高的网络安全公司。凭借先进的云原生架构，以及超高速的增长，公司成为网络安全领域的超新星，市值达到 450 亿美元，是当前市值最高的网络安全公司。公司当前仍在高投入高增长过程中，利润体量较小。参考 PS 估值，对于 20 年公司约 8.6 亿美元的收入指引，当前 PS 达到了 52 倍。在众多 SaaS 公司中，估值也是处于较高的一类。公司开辟了终端安全 SaaS 模式，不断的网络攻击，以及海量的终端市场，均是公司持续增长的动力，市场也给予了极高的期待。

图 33：Crowdstrike 估值水平（PS TTM）

资料来源：Wind，国信证券经济研究所整理

国内终端安全需求重启，新领域成必争之地

国内终端安全发展史：杀毒软件时代被免费终结

江民、瑞星、金山主导杀毒软件的黄金时代。早期盗版系统和软件广为流传，网络病毒和木马泛滥，最臭名昭著的是“熊猫烧香”病毒，它将 PC 系统里的多种文件锁定成熊猫图表，中毒企业和政府机构已经超过千家，迅速传播造成极为恶劣的影

响。同时，在 PC 产业发展初期，电脑相对来说仍是“奢侈品”，因此杀毒软件成为终端安全的刚需品。国内第一代杀软厂商以江民、瑞星、金山为代表，以光盘出售产品，且当时 100-200 元的价格并不便宜，却受到了市场的广泛追捧，掘到了市场第一桶金。

首先是江民，发布国内第一款杀毒软件，1996-1998 年快速发展，KV300 曾占据市场 80%的份额；公司为了反盗版，在产品中加入了“逻辑炸弹”，也一度遭到市场巨大谴责。然后是瑞星，通过 OEM 的方式，与各个 PC 厂商合作，迅速扩大市场份额，桌面小狮子形象深入人心；在 CIH 病毒肆虐时，公司做到第一个清除病毒，也一战成名；鼎盛时期，公司一年杀毒软件能卖 7 亿元。最后是金山，金山毒霸以低价的市场策略起步，很快市场份额升至第二，仅次于瑞星；后期更是率先宣布“软件免费、服务有偿”，通过升级病毒库收取月费和年费。因此，在 2000 年左右，光盘杀软时代形成了江民、瑞星、金山三足鼎立的态势。

图 34：瑞星杀毒软件以光盘形式出售

资料来源：虎嗅，国信证券经济研究所整理

图 35：熊猫烧香病毒

资料来源：中关村在线，国信证券经济研究所整理

360 以免费杀毒最终接管消费者的 PC 桌面。互联网与 PC 的普及，也将杀毒软件带入网络时代，同时也吸引了 McAfee、Norton 等海外厂商的进入，面对新型的攻击，技术上也有进步，但商业模式变化并不大，部分厂商开始向企业级市场切入，比如瑞星。2005 年，360 免费杀毒横空出世，激进的产品策略以及强烈的广告宣传下，尤其是消费者的 PC 迅速被 360 占领。而 360 以此为入口，通过游戏、广告等互联网打法迅速变现，成为互联网安全龙头。随后，桌面杀毒软件也进化成更互联网化的“安全管家”版本，提供多种非“杀毒”类的功能，承载了用户 PC 管理和运维的工作。时至今日，360 在 PC 安全产品的市场渗透率为 97.84%，持续排名市场第一；同时，360 凭借云端的“安全大脑”，进一步开拓政企市场。

表 12：杀毒软件时代发展历程

发展阶段	光盘杀软	网络杀软	免费查杀	安全管家
时间节点	90 年代至 2002 年	2002 至 2007 年	2008 至 2012 年	2012 至今
时代特征	单机杀毒 技术决定市场份额	联网杀毒 国内外差距较大	免费杀毒 免费是平台建立手段	安全管家 互联网巨头间拼抢
主要威胁	早期病毒	病毒变种增多 传播性增强	木马泛滥 用户隐私泄露 兴起黑色产业链	木马 垃圾信息
杀毒方法	研发杀毒引擎	启发式扫描 白名单	云查杀	安全管家维护
商业模式	贩卖光盘 OEM	网络营销 拓展企业级市场	免费查杀崛起	倒贴钱模式
盈利障碍	盗版产品泛滥	国外软件进入中国	面对免费措手不及	--
主流厂商	江民、金山、瑞星	除国内主流厂商外，卡巴斯基、迈克菲、小红伞等被熟知	360	360、腾讯、金山 反病毒引擎：火绒 物联网：青莲云

资料来源：中关村在线，国信证券经济研究所整理

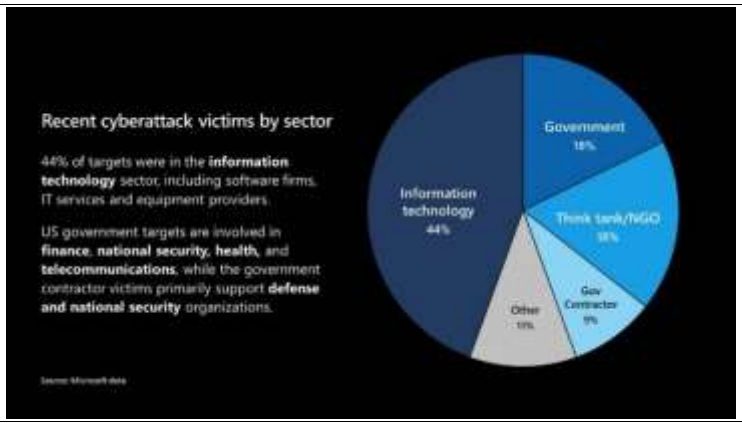
Windows 进一步内嵌杀毒软件，也挤压了第三方杀毒软件的市场空间。微软早年通过收购也形成了自己的终端安全能力，并于 2005 年就推出了测试版，2009 年微软正式推出免费独立杀毒软件 Microsoft Security Essentials（MSE），但 2013 年 MSE 在 AV-TEST 的测试中成绩极差，因此也一直没有成为市场的选择。桌面上运行的安全软件，需要和操纵系统进行适配，同时对 PC 性能产生一定影响。因此，基于 Windows 系统天然的优势，微软 Microsoft Defender 持续进步，已经连续两次在 AV-TEST 中排名第一。AV-TEST 是位于德国的独立组织，评估基于 Windows 系统的杀毒产品；在 2020 年 8 月发布的“家庭用户最佳防病毒软件”报告中，Windows Defender 在三个关键类别（性能，保护和可用性）上获得了满分，与多家知名杀毒厂商并列第一。随着 Microsoft Defender 在 Windows 最新操作系统的原生集成普及，以及消费者对于杀毒产品的淡化，消费领域的第三方杀毒软件市场进一步被挤压。

图 36：Microsoft Defender 测评第一

资料来源：AV-TEST，国信证券经济研究所整理

免费让终端安全被市场忽视，但攻击并未减少，而是转向企业级。早期的病毒制作都有“炫技”的成分，如“熊猫烧香”会直观的将用户 PC 破坏的面目全非。对于黑客组织而言，隐秘的在“地下”盗取数据而不暴露是更有利的，而且企业级客户的价值显然更大。因此近年来在消费者领域，大规模安全事件在逐步减少，但网络安全风险却没有丝毫下降，政企市场仍面临严峻风险：如 2017 年“永恒之蓝”，以及最近的 Solarwinds 事件。根据微软的调查，44%的攻击是面向 IT 基础设施单位，政府、金融领域也是被攻击的常客。从国外市场来看，消费级安全市场仍有传统杀毒厂商主导，企业级终端安全市场成为发展方向。

图 37：美国常被网络攻击的行业



资料来源：微软，国信证券经济研究所整理

市场、政策、技术推动企业级终端安全市场重生，成为安全必争之地

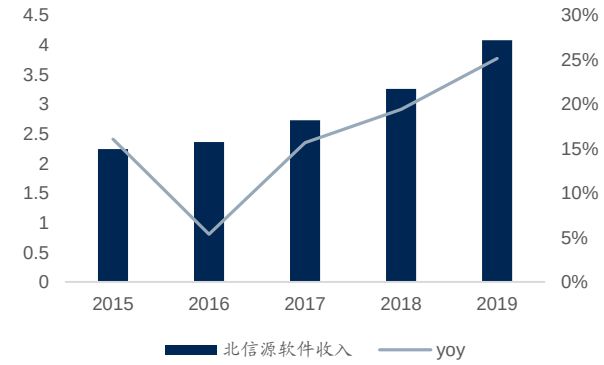
终端安全是长期被忽视的优质企业安全赛道。以杀毒软件为代表的终端安全，是消费者最常接触的产品，但是国内消费级市场已经被免费策略归零，互联网厂商仅仅把安全作为获取消费者的入口。随着近年来勒索病毒肆虐，企业级终端安全市场逐渐升温，且有望演化出新的商业模式。目前Gartner将终端安全市场分为三类产品：其中针对 PC 及其他移动设备的终端安全包括 EPP（包括防病毒、个人防火墙、端口及设备控制等功能）和 EDR（和 EPP 相互融合、但目前仍为独立市场），而 CWPP 主要包含指针对物理机器、虚拟机、容器和无服务器工作负载的安全产品。另一方面，根据赛迪的分类，除了终端防病毒（EPP）和终端检测响应（EDR），终端安全领域还包括主机监控、终端管理等产品，帮助企业统一管理和审计数量庞大的终端设备，也是企业级终端市场常见产品。

图 38：终端安全细分

资料来源：赛迪顾问，国信证券经济研究所整理

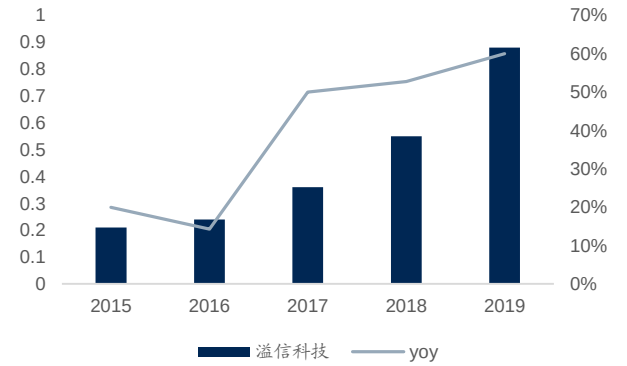
勒索病毒持续肆虐，近年来终端安全行业增速向上。北信源是终端安全领域最早上市的公司，终端安全产品线全面，主打终端安全管理，也有防病毒类产品，主要面向政企市场。溢信科技也是以终端安全业务为核心，主要包括主机监控审计、终端检测响应、终端安全管理，当前已经终止了上市。虽然公司收入规模仍较小，但也服务了 2 万家企业，超过 500 万台终端。2017 年由于“永恒之蓝”wannacry 勒索病毒爆发，全球 IT 产业均遭受重创。受到事件催化，政企对终端安全投入增加，两家偏终端管理类的安全厂商从 17 年开始增速显著向上。2016 年全球 RSAC 大会中，下一代终端安全成为热点，端点技术正经历由防病毒到威胁检测和响应的复兴，而 EDR 类产品也从 17 年开始进入国内市场范畴。国内终端安全市场也吸引了更多玩家，行业整体开始加速。

图 39：北信源软件收入（亿元）



资料来源：公司公告，国信证券经济研究所整理

图 40：溢信科技收入（亿元）



资料来源：公司公告，国信证券经济研究所整理

市场、政府、技术三方面原因推动企业级终端安全市场重塑：

政策方面，等保 2.0 带来市场对“主机安全”重新关注，涉及操作系统和数据库多个控制点。同时，等保 2.0 相比 1.0 在二级和三级系统测评中，更加注重了“处置安全事件”和“监测攻击行为”，而这正是以 EDR 为代表的新一代终端安全的价值点。**市场方面，勒索病毒泛滥带来企业级内生需求。**根据腾讯安全 2018 年的《医疗行业勒索病毒专题报告》，在全国三甲医院中，有 247 家医院检测出勒索病毒。其中以广东、湖北、江苏检出的勒索病毒最多。根据最新腾讯安全威胁情报大数据，传统企业、教育、医疗、政府机构遭受攻击依然最为严重。

图 41：等保对主机安全的要求

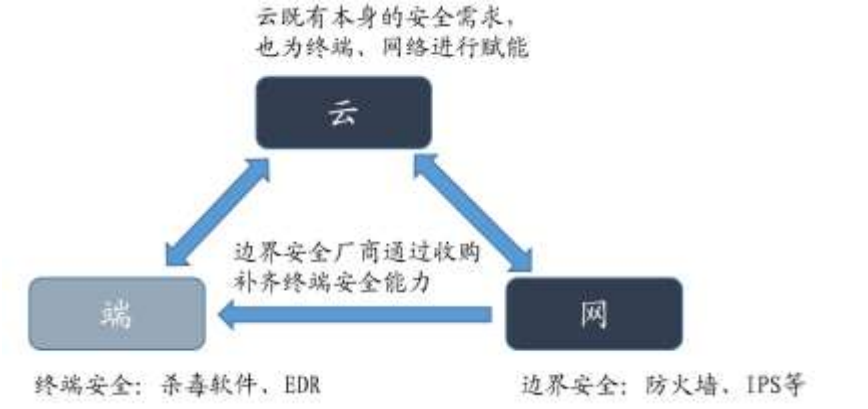
资料来源：等保 2.0、国信证券经济研究所整理

图 42：2018 年医疗行业勒索病毒情况

资料来源：腾讯安全、国信证券经济研究所整理

技术方面，终端已成为安全体系的必选项。上文分析了终端安全向 AI、大数据、威胁情报等技术的发展，EDR 产品的推出也带动了终端市场的革新。但从整个安全体系建设来说，终端已由可有可无变成不可或缺，尤其是在建立全网态势感知的层面，需要云、网、端的联动。终端仍是被攻击和入侵的主要对象，也成为了云端威胁情报获取的天然“探针”。而国内多数企业安全公司是从网络端起家，一开始并没有终端安全能力。近年来，通过自研和并购，传统网络安全厂商也逐步补齐终端产品线。因此在政策推动和市场需求下，随着技术升级带来的更替市场，终端安全市场呈现快速发展。

图 43：终端安全成为安全体系不可或缺的组成



资料来源：国信证券经济研究所整理

看好终端安全云转型，推荐关键卡位厂商

终端领域的价值深远，国内有望复制 Crowdstrike

价值一：具备 C 端触角，强调产品体验和技术水平，优秀产品易脱颖而出。与部署在企业网络机房的防火墙类产品不同，终端安全产品直接部署在办公 PC、服务器、移动设备上，办公场景下的 C 端员工具有直观体验。如果产品做的过于臃肿，影响正常办公体验（如卡顿、打扰较多等），且误报较多，市场用脚投票自然会将其淘汰。因此 Crowdstrike 的轻量化、高检测率才迅速得到市场认可。从美国各类高增长的 SaaS 应用来看，均是具备办公 C 端场景下的软件工具。国内同样场景下的软件工具较少，但安全领域里，终端是难得具备该类属性的赛道。

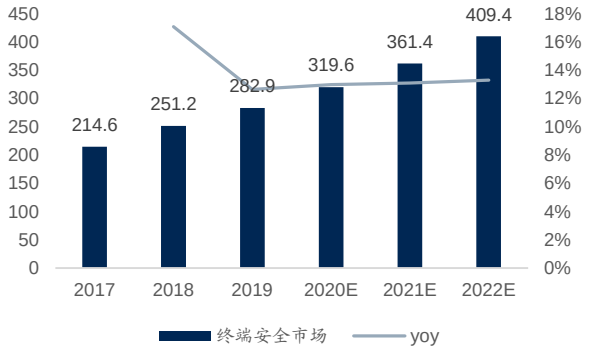
价值二：标准化的快捷部署，持续收费模式，长期净利率较高。相比与其他应用工具软件，面临大客户时难免会有定制化成分。而安全领域产品迭代与各类网络、威胁、检测等技术本身有关，并不需要为特定客户做定制。终端产品持续向轻巧、零打扰方向演进，更多功能可以放在云端，与各类系统适配也会越来越简易，部署也更加方便，如 Crowdstrike 可以一天部署上万台终端。另一方面，不管是本地部署，还是云端，特征库、威胁情报、AI 大数据等资源需要持续的服务，因此好产品会产生较高的付费粘性和持续性，成为订阅式收费模式。因此终端安全长期净利率水平较高，参考溢信科技来看，其净利率持续提升至 50%以上。

价值三：终端云转型，同时成为威胁情报生产的“探针”，反哺安全能力提升。安全以保护终端设备为目标，因此云转型中，终端仍需要“代理”来时刻感知本地的异常流量和行为。终端“代理”足够轻巧有效，才能通过对云端各类安全能力的订阅，实现终端的及时保护和响应。Crowdstrike 的轻量级代理就实现了这样的价值。另一方面，对于云工作负载的保护（CWPP），云转型也是终端安全发展的必然。终端也成为了威胁情报获取的重要来源之一，各个终端将数据反馈到云端后，进而形成了广泛的网络效应，AI 和大数据支撑下，不断提升可输出的安全能力。终端已经成为安全体系化建设不可或缺的一环。

价值四：复制消费版“杀毒软件”到“安全管家”逻辑，终端安全的衍生空间大。消费者领域，安全管家产品也成为桌面主流，其提供的功能除了安全之外，还有多种非安全类的 PC 管理工具，例如清理垃圾文件、优化加速、wifi 热点等。在企业级终端安全市场，该产品发展路径依然可以复制，例如 Crowdstrike 除了安全类订阅，也切入终端运维等非安全领域。因此，厂商在占据客户海量终端后，也有机会提供其他工具类产品，终端安全领域衍生性强。

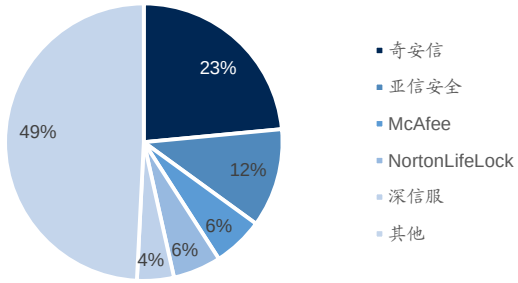
价值五：未来终端市场广阔，国产替代持续。根据 IDC 数据，当前我国终端安全市场仅为 20 亿人民币左右，规模仍非常小。预计到达 2022 年国内终端安全市场将达到 4.09 亿美元，复合增速为 13.8%。目前国内终端安全市场主要聚焦在政府国企等合规性要求较高的场景，广泛的企业级市场仍待挖掘。另一方面，万物皆可为智能终端，优越的技术和商业模式，可以不断催生新的市场。例如 VMware 收购 Carbon Black，加强虚拟机、容器等云工作负载业务，布局“云终端”安全；黑莓收购 Cylance，与车联网业务协同，布局“车终端”安全。因此未来终端安全市场潜力巨大，Crowdstrike 产品可触达市场空间已经超过 300 亿美金。国内安全厂商近年来纷纷布局终端领域，也是嗅到了市场机遇。奇安信以 23%的市占率占据第一，其次是亚信安全。随着国产替代的持续推进，McAfee 和 Norton 也会陆续被国产厂商取代。

图 44：国内终端安全市场规模（百万美元）



资料来源：IDC 中国 IT 安全市场预测、国信证券经济研究所整理

图 45：终端安全市场份额



资料来源：IDC 2019、国信证券经济研究所整理

重点关注终端卡位厂商。美国信息化发展成熟，客户侧 IT 基础较强，更偏好选择产品和技术最好的厂商，因此细分领域安全厂商众多，Crowdstrike 在终端安全领域风头正盛。相比而言，国内客户侧技术薄弱，更偏向解决方案的整体选择，因此国内厂商常常走产品线扩张的“大而全”路线。国内终端安全领域，可以分为三类：第一类以奇安信、360、亚信（未上市）为代表，具备终端安全基因的厂商；第二类是以深信服、安恒、山石为代表，快速跟进终端领域；第三类以火绒、微步在线为代表，新兴技术领域创新厂商，同样值得关注。

奇安信——企业级终端安全龙头，云网端布局最全面

奇安信终端产品线全面，本地部署同样可享受云端能力。终端安全是奇安信区别与其他信息安全厂商的重要产品，也是奇安信真正做到“云网端”安全一体化的关键一环。“天擎”是一整套面向终端安全的产品集合和方案，主要有防病毒、终端安全管控、终端准入、终端审计、外设管控、EDR 等功能，相比传统杀毒软件具备更丰富的一体化终端管控能力。Crowdstrike 基于纯公有云部署，但是对于国内政府、金融、医疗等行业私有化部署的环境，奇安信可以在本地部署总部数据平台，将丰富的云端威胁情报、大数据通过单向导入的方式实现供给。

图 46：奇安信终端安全管理系统（天擎）

资料来源：奇安信官网、国信证券经济研究所整理

图 47：奇安信终端安全部署方式

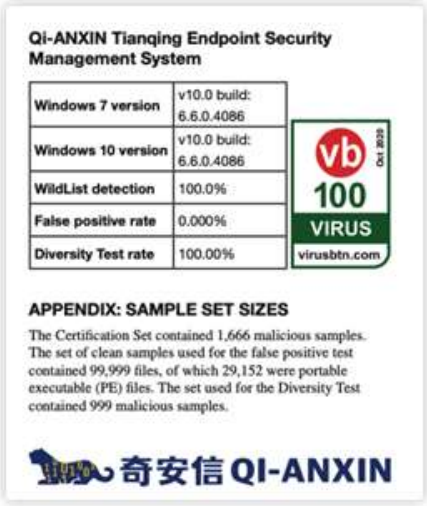
资料来源：奇安信官网、国信证券经济研究所整理

奇安信终端安全技术已经自主。早期奇安信和 360 在终端产品上有合作，但在双方《终止协议》之后，奇安信于 2019 年 7 月推出了自主研发的终端安全产品，对曾经 360 的技术进行了替换：如自主研发了“基于权限的行为管理引擎-天狗”；自主研发 QOWL、QDE 杀毒引擎；自主研发功能驱动；自主研发的云端支持平台。奇安信预计在 2020 年第四季度停止批量销售存量的老版一体化终端管理（天擎）

产品，逐步替换成新版的奇安信产品。

产品能力得到市场广泛认可。奇安信“新版天擎”在 2020 年 4 月首次参加国际杀毒软件评测机构 Virus Bulletin 最新的 VB100 测评，以零误报、100%多样化样本检出率通过 VB100 测试，标志着奇安信正式加入全球顶级反病毒厂商俱乐部。根据 IDC 最新的《中国终端安全检测与响应市场 2020》评估，根据策略（未来能力规划，包括增长、创新、交付、资金等）和能力（包括客户满意度、客服交付、平台适配、功能特性）等多个关键指标进行打分，奇安信 EDR 获得策略和市场份额双第一，位居领导者象限。

图 48：奇安信 Virus Bulletin 测评结果



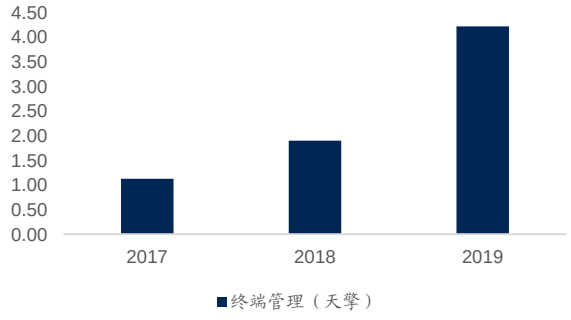
资料来源：奇安信官网、国信证券经济研究所整理

图 49：中国终端安全检测与响应市场矩阵

资料来源：IDC 2020、国信证券经济研究所整理

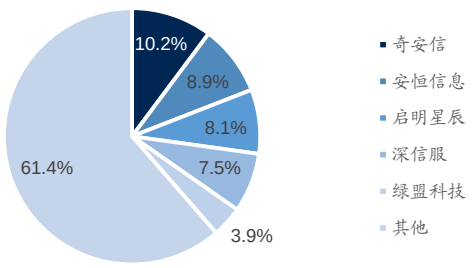
奇安信终端覆盖已超过 5000 万，威胁情报同样第一。奇安信终端安全迅速增长，2019 年收入达到 4.22 亿元，同比增长 122%；市场份额进一步扩大，达到 23.5%。目前奇安信天擎已广泛部署国内超 5 万家政企客户，管理和保护着超 5000 万台终端的安全。在为终端赋能的威胁情报领域，根据 IDC 2020 上半年报告，奇安信以 10.2%的市场份额排名第一。根据 Gartner 统计，2019 年使用商业威胁情报的组织比例接近 10%，预计 2022 年提升至 20%。奇安信率先提出“情报内生”理念，建立基于企业自身和行业情报生产和消费能力。2020 上半年，公司还发布了“TI INSIDE 计划”，加强情报领域生态合作。目前，奇安信威胁情报中心已累计首发 9 个国内外 APT 组织，监测到的针对国内发动 APT 攻击的黑客组织达到 44 个。

图 50：奇安信终端安全（天擎）收入（亿元）



资料来源：公司公告，国信证券经济研究所整理

图 51：2020 上半年安全分析和威胁情报市场份额



资料来源：IDC 2020，国信证券经济研究所整理

深信服——迅速迭代，终端安全进入市场前五

深信服 EDR 迭代迅速，表现已获得业内认可。深信服于 2018 年推出 EDR，目前已经迭代到 3.0 版本，完成三大国内主流操作系统银河麒麟、中标麒麟、深度操作系统的兼容认证，2019 年市场份额达到第五。深信服推出的 EDR 采用独创的 SAVE 安全智能检测引擎，无特征检测技术，形成 AI 智能、信誉库、基因特征、行为分析等多梯度、全方面检测分析，响应速度更快速，资源占用更低消耗。以勒索病毒 GlobeImposter 家族最新变种为例，在对相关样本没有做任何分析的情况下，通过深信服 EDR，可以对其进行 100%的准确检测和查杀。深信服 EDR 在测试机构 AV-TEST 最新的性能测试中，以仅影响系统或软件运行速度 7.83%的测评成绩获得满分 6 分，实现对正常办公业务“零干扰”。产品获得微软 WHQL 认证，并成为微软官方 Windows10/8/8.1 的推荐杀毒软件。

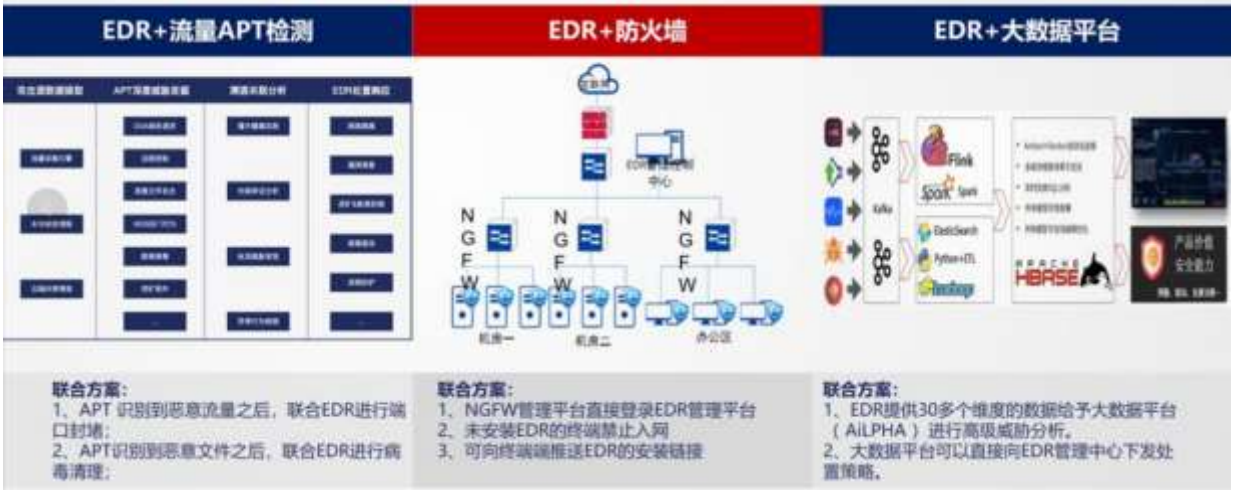
图 52：深信服 EDR 产品技术领先

资料来源：深信服官网，国信证券经济研究所整理

安恒信息——终端是态势感知的必要环节

安恒 EDR 是态势感知等多种安全能力的必要补充。安恒以应用和数据安全起家，态势感知成为公司整体安全能力输出的代表。安恒 EDR 是客户海量端点的触角，可以与 APT 流量检测类产品联合，联合 EDR 进行端口封堵、病毒清理；可以与防火墙产品联合，对终端进行统一的管控；可以与与大数据平台联合，进行高级威胁分析和统一策略下发。

图 53：安恒 EDR 与各类安全能力形成闭环



资料来源：安恒信息官网，国信证券经济研究所整理

360——再次迈向政企市场，推出政企终端安全产品

360 以安全大脑为核心，持续加大政企安全投入。360 在剥离奇安信后，仍持续加大政企安全市场的布局。2018 年 360 发布安全大脑，开始为各地政府建设安全运营中心，连续中标各地大单。

表 13：360 政企安全中标大单

时间	项目	金额
2019 年 6 月	重庆市合川区 360 网络安全协同创新产业园一期	2.4 亿
2019 年 10 月	天津市应急管理局应急管理信息化（一期）项目	1.18 亿
2019 年 12 月	天津市高新区网络安全协同创新产业基地项目	2.51 亿
2020 年 5 月	青岛网络安全产业基地相关项目	2.5 亿
2020 年 7 月	天津省级工业互联网安全态势感知平台项目	3400 万
2020 年 10 月	鹤壁网络安全协同创新产业基地项目	1.1 亿
2020 年 10 月	苏州网络安全协同创新暨安全大脑项目	2.6 亿
2020 年 10 月	长沙市“数字法治，智慧司法”信息化项目	4181 万

资料来源：360 官网，国信证券经济研究所整理

终端安全积累深厚，云端大脑持续赋能。360 以免费杀软起家，在消费级市场依然占据极高的市场份额，因此也积累了广泛的安全大数据。2020 年 10 月，360 也推出了 360 终端安全管理系统、360 终端安全管理系统(信创版)、360 安全卫士团队版、360 企业安全浏览器等终端产品，进一步开拓政企市场。同时，360 云端安全大脑也具有海量的威胁情报优势。

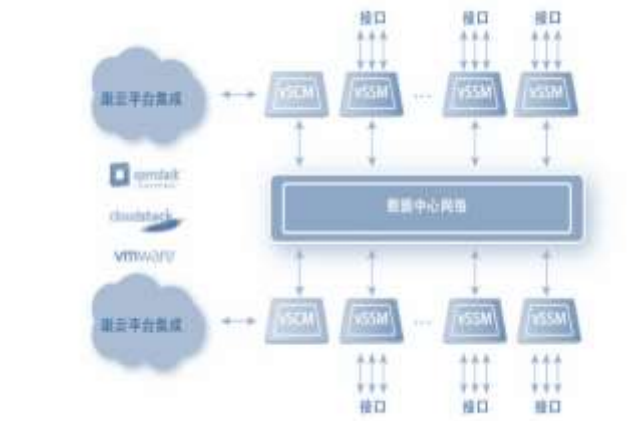
图 54：360 终端安全管理系统

资料来源：360 官网，国信证券经济研究所整理

山石网科——基于云工作负载，云格唯一入选 Gartner CWPP 目录

山石 CWPP 产品国内领先，360 入股有望加强终端能力。山石早在 2015 年就推出了“云格”，主要面向云计算工作负载的保护产品。云格可以视为每台虚拟机的贴身保镖，通过虚机微隔离实现虚拟机之间实时流量和应用的可视，完成“东西流量”的保护。在 Gartner 发布的《2020 年 CWPP 市场指南》中，山石云格（CloudHive）成功入选指南中“基于身份的隔离、可视和控制能力”分类，成为中国首家获得指南推荐的微隔离与可视化云安全产品全球供应商。“云工作负载”也是新的终端类型，云计算下该市场成为各家终端安全厂商相继布局的热点。另一方面，山石也推出了云鉴主机安全管理系统 EDR 产品。近期 360 通过鸿腾智能不断增持山石股份，目前已经接近 10%。双方存在多方面合作潜力，360 的终端产品和山石的边界产品有望形成良好的互补。

图 55：山石云格架构



资料来源：天极网，国信证券经济研究所整理

图 56：山石云格入选 Gartner CWPP 全球市场指南


Market Guide for Cloud Workload Protection Platforms Published 14 April 2020
Table 3: Identity-Based Segmentation, Visibility and Control Capabilities
Gartner

ColorTokens	Xshield
Edgewise	Zero Trust Auto-Segmentation for Hybrid Cloud
Guardicore	Centra
Hillstone Networks	CloudHive
Illumio	Adaptive Security Platform (ASP)
Palo Alto Networks (acquired Aporeto)	Prisma Cloud
TrueFort	TrueFort
Shield X (container-based)	Shield X Elastic Security Platform

资料来源：Gartner 2020，国信证券经济研究所整理

亚信安全——收购趋势科技中国区业务，终端安全不容小觑

亚信收购趋势中国区业务，增强终端实力。亚信科技是老牌电信运营商服务企业，2015 年收购趋势科技在中国的全部业务，包括核心技术及知识产权 100 多项，同时建立独立安全技术公司—亚信安全。趋势科技是一家跨国安全公司，常年处于 Gartner 终端安全领导者象限，在国内也有广泛的客户基础。因此，亚信安全相对于其他安全厂商，在终端领域具备基因优势。目前公司国内终端安全市场份额第二，处于行业领导象限。2020 年公司推出“大终端一体化解决方案”，包含高级威胁终端检测及响应系统 EDR、 终端安全防病毒网络版 OfficeScan、 文档保护、 虚拟补丁 VP 以及 终端安全管理五大模块。亚信 OfficeScan 在 IDC 上连续三年国内排名前三，为超过 1 亿终端提供服务，市场认可度远高于行业平均水平。

图 57：亚信终端安全全景图

资料来源：亚信安全官网，国信证券经济研究所整理

火绒安全——终端安全新玩家，反病毒引擎被多家厂商 OEM

终端安全新星，火绒已被行业广泛集成。火绒成立于 2011 年 9 月，创业团队多数来自老牌杀毒厂商瑞星。通过多年技术和产品打磨，火绒打造了拥有自主知识产权的新一代反病毒引擎，具备“通用脱壳”、“动态行为查杀”等技术。2012 年公司

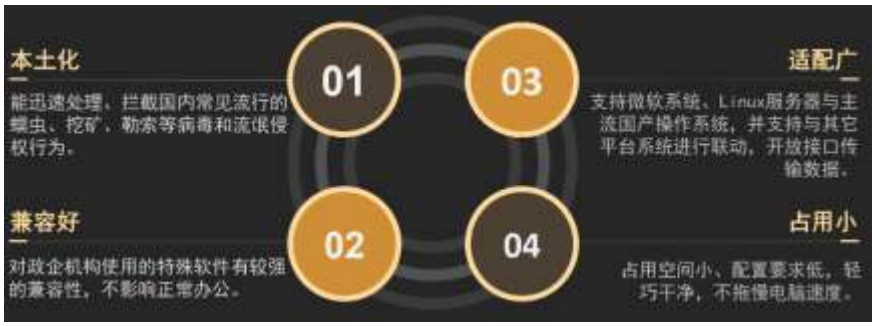
推出免费个人产品，凭借“专业、干净、轻巧”的特点收获了良好的用户口碑。早期，公司以流量变现和 OEM 引擎为主要商业模式，其中奇安信、天融信、迪普科技、联想等多家厂商均是公司客户。2018 年，为了进一步提升用户体验，公司关停流量业务，同年推出企业版，正式进入 B 端市场，仅两年就有上万家企业用户参与试用购买。

图 58：火绒发展历程

资料来源：火绒安全，国信证券经济研究所整理

以“情报驱动安全”为理念，技术和产品独具优势。火绒以反病毒引擎起家，相比与杀毒软件本身，反病毒引擎技术更加底层。公司新一代的反病毒引擎是通过行为特征来精准判别各种电脑病毒和威胁代码，这与过去通过其他特征来判断截然不同。火绒还是国内唯一的“通用脱壳”反病毒引擎，无需“云查杀”和“白名单”，本地引擎部署，但是产品轻巧、性能强悍。例如，根据公司披露的案例，某药企客户电脑老旧，内存仅 512M，普通杀软安装后导致系统缓慢，无法正常办公。火绒企业版大小仅为 47M，日常使用不占大量 CPU，得到客户认可。火绒产品具备本土化、适配广、兼容好、占用小等优势，同时具备完整的 EDR 运营体系。火绒以全面、真实、及时的互联网威胁情报为基础，来驱动技术研发和产品开发，并建立相应的安全服务运营体系。

图 59：火绒产品优势



资料来源：火绒安全，国信证券经济研究所整理

火绒已获天融信投资，未来发展可期。火绒于 2017 年获国内防火墙龙头天融信 1500 万人民币 Pre-A 轮投资，并签署战略合作。火绒可以帮助天融信打造终端产品，同时携手扩张企业级终端市场。根据亿欧网报道，火绒企业版不做定制，按照用户的规模、电脑终端数量收费，一台电脑三年 150 块钱，并且坚决不打折，该

产品营收在2018年12月单月就已突破100万元，2019年每月营收保持稳定增长。火绒的销售方式主要是通过线上推广和合作伙伴渠道推广，2019 年火绒安全个人版服务用户超 600 万，企业版则创下日同时在线企业数量超 2000 家的记录，包括拼多多、京东金融等互联网巨头也是火绒客户。

微步在线——威胁情报初长成，SaaS 化安全服务快速增长

微步在线是独立威胁情报公司，营收保持高速增长。威胁情报已经成为终端，乃至各类安全产品新的“生产资料”，是体系化安全能力的重要支撑。微步在线成立于 2015 年，以威胁情报起家，已经获得北极光、高瓴资本等多次融资。2020 年 9 月，公司完成 3 亿元人民币 D 轮融资，由中金资本、中信证券、云晖资本等多家国资背景投资机构联合投资。公司为客户提供威胁情报数据分析，是标准的 SaaS 模式。根据 36 氪报道 2020 年 12 月份报道，公司过去几年营收均保持着 150%以上的增速，预计 2020 年营收过亿。公司有约 80%的收入都来自订阅制，用户粘性较高，续约率达到 95%左右。当前微步的客户包括国家电网、中石油、工商银行、小米、格力、京东、中信集团等来自能源、金融、智能制造、互联网等行业的 300+家大型企业客户。

公司连续三次入选 Gartner《全球威胁情报市场指南》。微步在线被列入商业化威胁情报服务推荐名单，是中国乃至亚太地区唯一入围供应商，与 FireEye、Google(VirusTotal)、CrowdStrike 等二十多家顶级的国际厂商同台。威胁情报为现有安全产品赋能，如 SIEM、防火墙、IDS/IPS、EDR 等，将成为行业必然趋势。

图 60：威胁情报对各类产品赋能

资料来源：微步在线官网，国信证券经济研究所整理

风险提示

疫情影响持续，全社会 IT 及安全开支缩减。

全行业竞争加剧，各厂商陷入同质化价格战导致毛利率下降。

国信证券投资评级

类别	级别	定义
股票投资评级	买入	预计 6 个月内，股价表现优于市场指数 20%以上
	增持	预计 6 个月内，股价表现优于市场指数 10%-20%之间
	中性	预计 6 个月内，股价表现介于市场指数 ±10%之间
	卖出	预计 6 个月内，股价表现弱于市场指数 10%以上
行业投资评级	超配	预计 6 个月内，行业指数表现优于市场指数 10%以上
	中性	预计 6 个月内，行业指数表现介于市场指数 ±10%之间
	低配	预计 6 个月内，行业指数表现弱于市场指数 10%以上

分析师承诺

作者保证报告所采用的数据均来自合规渠道，分析逻辑基于本人的职业理解，通过合理判断并得出结论，力求客观、公正，结论不受任何第三方的授意、影响，特此声明。

风险提示

证券投资咨询业务的说明

本公司具备中国证监会核准的证券投资咨询业务资格。证券投资咨询业务是指取得监管部门颁发的相关资格的机构及其咨询人员为证券投资者或客户提供证券投资的相关信息、分析、预测或建议，并直接或间接收取服务费用的活动。

证券研究报告是证券投资咨询业务的一种基本形式，指证券公司、证券投资咨询机构对证券及证券相关产品的价值、市场走势或者相关影响因素进行分析，形成证券估值、投资评级等投资分析意见，制作证券研究报告，并向客户发布的行为。

国信证券经济研究所

深圳
深圳市罗湖区红岭中路 1012 号国信证券大厦 18 层
邮编：518001　总机：0755-82130833

上海
上海浦东民生路 1199 弄证大五道口广场 1 号楼 12 楼
邮编：200135

北京
北京西城区金融大街兴盛街 6 号国信证券 9 层
邮编：100032