2024 年 6 月 18 日

光大证券 EVERBRIGHT SECURITIES

行业研究

AI 驱动网络安全供需提升，架构迭代引领行业变革

——美股网络安全行业深度报告

要点

股价表现和估值：23 年美股主要网络安全公司的股价明显跑赢大盘，主要由估值抬升驱动，CrowdStrike、Palo Alto Networks、Zscaler 等公司股价表现强劲，截至 24M4 多数网络安全公司 PS 估值位于五年均值以下。

企业网络安全支出维持强劲。24 年全球信息安全支出有望同比增长 14.3%，增速较快的细分领域是云安全、数据隐私安全、基础设施保护。CIO 调查显示，24 年 80%企业提高网络安全投资，网络安全在 IT 预算中的占比逐年提升。

生成式 AI 使网络安全攻防升级。网络攻击的门槛降低，23 年网络攻击数量提升，社会工程攻击、Web 应用程序攻击在生成式 AI 的帮助下更加容易。但 AI 也加强了网络安全工具的监测和应对能力：1）AI/ML 技术强化威胁检测和安全保护能力；2）生成可视化安全日志；3）嵌入 AI 助手降低技术门槛。

网络安全产业链涵盖端点安全、网络监控、权限管理等环节。1）端点安全：包括威胁情报和识别、安全评估与风险管理、防御技术部署等；2）网络监控：包括云安全、安全信息和事件管理等；3）权限管理：包括身份和访问管理、数据隐私保护等；4）其他：包括应急响应和事故处理、安全培训、合规等。

端点安全：微软和 CrowdStrike 双寡头基本形成。端点安全旨在保护接入网络的设备，主要分为 EPP、EDR、XDR 三种类型。22 年全球端点安全市占率前二的微软、CrowdStrike 市场份额分别为 19%、15%，整体呈现供应商整合趋势，两家公司在第三方竞争格局和安全技术评估中整体领先其他公司。

云安全：云发展带来网络安全架构变革，竞争格局尚不稳定。云安全解决方案主要分为 CNAPP、CWPP、CSPM 等类型，Trend Micro、Palo Alto Networks 为龙头企业，相比端点安全市场更为分散，CrowdStrike 技术评估较为领先。

身份和访问管理/安全信息和事件管理：市场成熟，竞争格局稳定。身份和访问管理市场规模 24-32 年 CAGR 有望达到 13.2%，龙头为 Okta、微软；安全信息和事件管理市场规模 24-29 年 CAGR 有望达到 17.1%。

安全访问服务边缘（SASE）：高速发展的新兴网络安全架构。随着边缘计算、云服务和混合网络的兴起，SASE 架构可以解决传统架构的复杂性和延迟性问题。SASE 的核心技术包括边缘计算、零信任网络访问等。Netskope、Zscaler、Palo Alto Networks 是安全服务边缘（SSE）行业领导者。

投资建议：我们认为，随着企业数字化转型的不断推进，在云计算、物联网、AI 等产业趋势下，传统网络安全架构难以适应，新兴的网络安全架构蓬勃发展，有望持续引发行业竞争格局的变化，使更加有竞争力的供应商脱颖而出。在本轮生成式 AI 的浪潮下，网络安全面临广泛而深刻的变革，网络攻击门槛降低的同时，AI 技术提升了威胁检测能力，并提供自动化安全评估和漏洞修复等功能，大幅降低安全员的使用门槛。**首次覆盖给予美股网络安全行业“买入”评级，推荐微软、CrowdStrike，建议关注 Zscaler。**

风险提示：行业竞争加剧风险、AI 技术发展不及预期、行业政策风险。

重点公司盈利/营收预测和估值表

证券代码	公司名称	股价（美元）	估值方法	净利润/营收 23-26 年 CAGR	24 年 PE/PS	投资评级	评级变动
MSFT.O	微软	448.4	PE	15.8%	38	买入	维持
CRWD.O	CrowdStrike	390.4	PS	27.6%	24	增持	首次

资料来源：Wind，光大证券研究所预测，微软为净利润预测，CrowdStrike 为营收预测，股价时间 2024-06-17。微软的净利润 CAGR 为 FY23-FY26，CrowdStrike 的营收 CAGR 为 FY24-FY27。

美股网络安全

买入（首次）

作者

分析师：付天姿

执业证书编号：S0930517040002

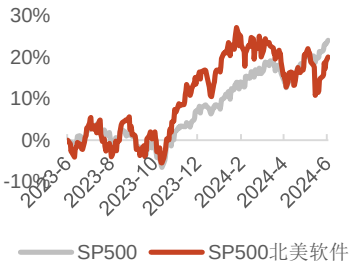
021-52523692

futz@ebscn.com

联系人：宾特丽亚

binteliya@ebscn.com

行业与标普 500 指数对比图



资料来源：彭博

相关研报

《24 年美股三大股指再创新高，业绩超预期和 AI 行情能否持续？——美股跟踪系列报告》（2024-06-15）

《CrowdStrike FY25Q1 业绩及指引超预期，AI 助力 SIEM 高速增长———美股互联网传媒行业跟踪报告（十三）》（2024-06-06）

《23 年牛市受“业绩+估值”双引擎驱动，24 年增长动力在哪里？——纳斯达克指数复盘及美股展望》（2024-03-02）

《梳理全球 AIGC 数据版权规范，哪些领域具备商业化潜力？——AI 产业前瞻系列报告（二）》（2023-12-25）

《美股 AIGC 应用端全产业链布局，商业化箭在弦上——AIGC 系列跟踪报告（二十八）》（2023-10-14）

《美股 AIGC 产业链及投资逻辑分析——AIGC 行业跟踪报告（五）》（2023-06-10）

投资聚焦

网络安全行业增速较快的细分领域是云安全、数据隐私和安全、基础设施保护。1）云安全：24 年全球云服务行业有望从周期底部复苏，提升云安全的需求。**2）数据隐私和数据安全：**随着生成式 AI 的快速发展，世界各国有望持续完善数据版权保护和个人隐私保护政策。**3）基础设施保护：**作为网络安全的核心，基础设施保护对于国家战略安全和私营部门信息安全都具有十分重要的意义。

生成式 AI 使网络安全攻防升级。生成式 AI 使网络攻击的门槛降低，全球网络攻击数量增多、效率提升。同时，生成式 AI 赋能网络安全解决方案，提升企业应对网络攻击的能力，主要手段包括：1）AI/ML 技术强化威胁检测和安全保护能力；2）生成可视化安全日志；3）嵌入 AI 助手降低技术门槛。

我们的创新之处

美股网络安全行业以 SaaS 服务为主，供应商数量多、各具特色，针对不同的细分领域提供差异化的服务。因此，我们在行业分析中加入了详细的公司横向对比，梳理网络安全产业链的各个环节，对于每个产业链环节的竞争格局进行深入分析，从产品阵营、技术评估、AI 集成等方面分析龙头企业的竞争优势。例如，我们深入研究了端点安全领域 15 家供应商，分析每家公司的差异化服务、技术优势、产品优势以及潜在的风险和挑战。

此外，我们将行业发展历程和产业内在规律结合起来，论证网络安全产业如何持续发展、不断焕发新的生命力。例如，端点安全从传统的本地部署转向云原生平台和 SaaS 服务，云服务、物联网的发展以及远程办公需求的提升，促使了云安全、安全访问服务边缘等全新安全架构的诞生。

股价上涨的催化因素

短期催化因素：1）全球大选：24 年全球许多国家进入大选年，网络攻击的频率和强度或将显著提升，涉及敏感信息企业的网络安全需求有望提高；**2）地缘政治冲突：**全球地缘政治冲突不断升级，涉及国防军工等重点行业的网络安全需求水涨船高；**3）政策变化：**23M10 CISA 宣布修订网络事件响应计划，更严格的安全政策会使相关企业受益，尤其是涉及应急响应和事故处理服务的公司。

长期催化因素：生成式 AI 的快速发展对数据治理和隐私保护提出了更高的要求，网络安全环境的变化有望催生网络安全架构的转型，形成行业市场规模的第二成长曲线，类似 SASE、零信任等网络安全新概念可能逐步涌现。

投资观点

我们认为，随着企业数字化转型的不断推进，在云计算、物联网、AI 等产业趋势下，传统网络安全架构难以适应，新兴的网络安全架构蓬勃发展，有望持续引发行业竞争格局的变化，使更加有竞争力的供应商脱颖而出。在本轮生成式 AI 的浪潮下，网络安全面临广泛而深刻的变革，网络攻击门槛降低的同时，AI 技术提升了威胁检测能力，并提供自动化安全评估和漏洞修复等功能，大幅降低安全员的使用门槛。**首次覆盖给予美股网络安全行业“买入”评级，推荐微软（MSFT.O）、CrowdStrike（CRWD.O），建议关注 Zscaler。**

目 录

图目录

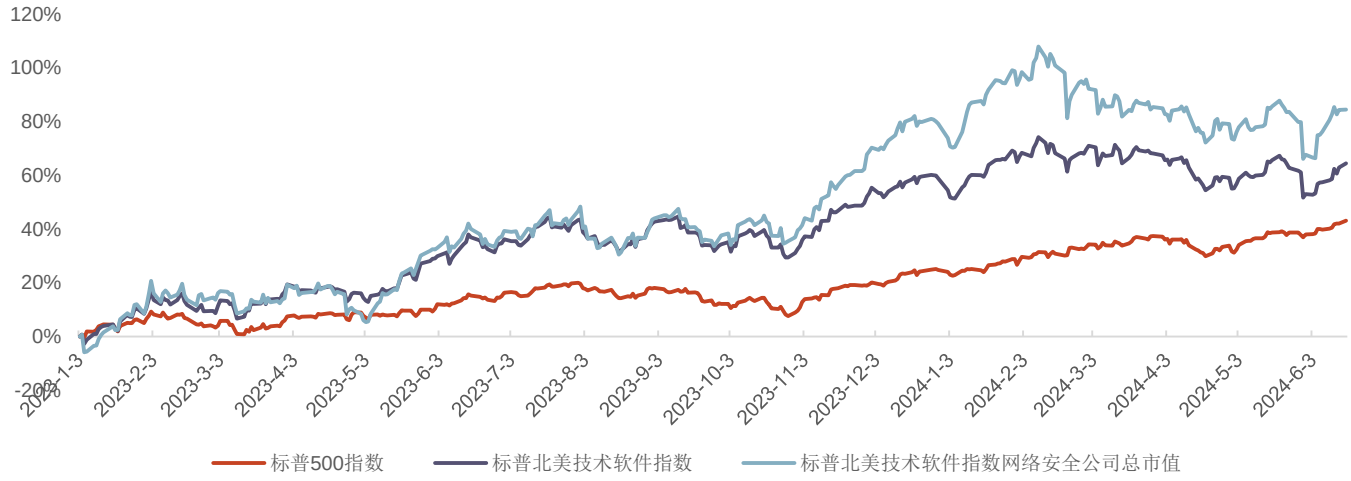
表目录

1、 美股网络安全公司 23 年股价表现强劲，主要受估值增长驱动

1.1 23 年美股网络安全公司股价明显跑赢大盘

2023 年美股软件公司中，网络安全公司市值涨幅居前。2023 年标普北美技术软件指数市值上涨 54.2%，大幅跑赢标普 500 指数，标普北美技术软件指数成分股中 15 家网络安全公司总市值涨幅为 77.0%。CrowdStrike、Palo Alto Networks、Zscaler、Varonis、SentinelOne 等网络安全公司股价涨幅均明显跑赢标普北美技术软件指数。

图 1：标普 500 指数、标普北美技术软件指数和其中的 15 家网络安全公司市值涨跌幅



资料来源：彭博，光大证券研究所整理，股价时间为 2023 年 1 月 3 日-2024 年 6 月 17 日，网络安全公司指标普北美技术软件指数成分股中网络安全公司，包括 Everbridge、Q2、CrowdStrike、Fortinet、Tenable、A10 Networks、Varonis、Gen Digital、Clear Secure、N-able、Palo Alto Networks、Rapid7、Zscaler、Qualys、SentinelOne

23 年多数网络安全公司股价集中在 23Q4 上涨。23Q1-23Q2 美股软件公司股价主要受生成式 AI 投资情绪提振，23Q3 因美债收益率上升、CPI 数据高于预期等利空因素影响而承压，23Q4 随着美债收益率下降、市场降息预期强化而上涨。**标普北美技术软件指数中：1）**CrowdStrike、Zscaler、Varonis、SentinelOne、Qualys 五家公司在 23Q4 期间股价涨幅相对其他季度更高，主要受到业绩强劲、降息预期强化等因素的影响；**2）**Palo Alto Networks、N-able、Tenable、Fortinet 四家公司在 23Q1 或 23Q2 期间股价涨幅相对其他季度更高，主要受到生成式 AI 投资热点的驱动。

24 年以来股价表现优异的公司与 23 年有一定的差异。标普北美技术软件指数成分股中，23 年股价涨幅跑赢标普北美技术软件指数的网络安全公司共有 8 家；24Q1 标普北美技术软件指数中股价涨幅前三的网络安全公司为 CrowdStrike、Zscaler、Palo Alto Networks，涨幅分别达到 53.1%、29.9%、24.4%，24Q2 以来（截至 6 月 17 日）CrowdStrike 股价小幅回调，Zscaler、Palo Alto Networks 股价继续强势上涨。标普北美技术软件指数以外的美股网络安全公司中，仅 CyberArk 在 23 年和 24 年以来均跑赢标普北美技术软件指数。主营业务为硬件响应和事故处理的 Everbridge 虽然在 23 年股价下跌，但 24 年至今股价强劲增长 52.7%，明显领先于其他网络安全公司。

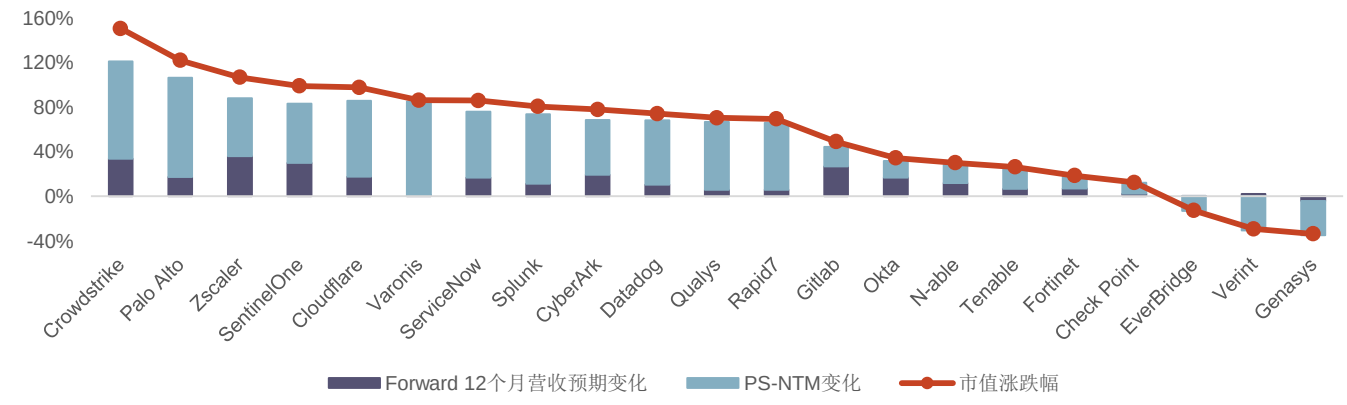
表 1：美股网络安全公司 2023 年和 2024 年至今股价涨跌幅表现

	2023 年	23Q1	23Q2	23Q3	23Q4	24Q1	24Q2 至今
标普 500 指数	24.7%	7.5%	7.9%	-3.8%	11.2%	10.8%	4.4%
标普北美技术软件指数	58.9%	19.4%	14.8%	-0.9%	17.6%	8.8%	-1.8%
CrowdStrike	147.2%	32.9%	7.6%	14.7%	50.6%	53.1%	-0.2%
Palo Alto Networks	113.0%	44.3%	30.1%	-7.9%	24.5%	24.4%	14.6%
Zscaler	101.1%	6.0%	29.6%	6.1%	37.7%	29.9%	22.2%
Varonis	88.4%	8.2%	4.9%	15.4%	49.2%	18.2%	-10.2%
SentinelOne	88.3%	12.3%	-8.3%	11.4%	62.7%	12.4%	-19.2%
Qualys	76.0%	16.6%	1.6%	18.8%	28.3%	5.6%	-0.9%
Rapid7	63.3%	31.3%	1.1%	1.3%	23.4%	6.0%	-6.6%
Q2	59.7%	-9.4%	28.0%	4.9%	35.1%	-1.1%	6.7%
N-able	28.5%	28.0%	9.2%	-10.5%	1.5%	6.2%	-11.6%
Tenable	21.5%	25.4%	-5.1%	4.9%	0.9%	-1.1%	10.1%
Fortinet	20.6%	37.0%	14.0%	-21.4%	-0.2%	-1.7%	14.4%
Gen Digital	8.3%	-20.2%	8.9%	-3.6%	31.0%	-10.8%	-25.3%
Everbridge	-15.2%	21.0%	-17.2%	-17.6%	7.9%	-9.3%	-4.0%
A10 Networks	-20.5%	-7.8%	-0.4%	5.7%	-13.8%	-13.0%	-18.3%
Clear Secure	-22.6%	-6.1%	-9.2%	-17.3%	19.2%	-9.9%	-19.9%
标普北美技术软件指数以外的网络安全公司							
Cloudflare	93.5%	43.3%	6.8%	-4.2%	33.2%	22.0%	-18.8%
CyberArk	73.4%	17.2%	8.9%	5.8%	33.1%	22.9%	-4.0%
Okta	30.2%	24.0%	-16.9%	17.7%	12.2%	20.3%	-13.2%
Check Point	20.5%	2.5%	-3.9%	5.5%	14.5%	7.7%	-4.0%
Verizon	0.9%	-1.5%	-3.6%	-11.5%	21.2%	9.7%	-5.2%

资料来源：Wind，光大证券研究所整理，24Q2 至今股价涨跌幅截至 2024-06-17

网络安全公司股价上涨主要由估值抬升驱动。23 年美股主要网络安全公司中，年底相较于年初 Forward 12 个月营收预期提升最明显的公司是 Zscaler、CrowdStrike 和 SentinelOne，分别为 36.1%、33.7%、30.1%，其余网络安全公司的 Forward 12 个月营收预期多数为正增长，仅 Genasys 下降 4.2%。整体来看，23 年美股网络安全公司的市值增长主要驱动力是估值的提升，Palo Alto、CrowdStrike、Varonis 的 23 年 PS-NTM 估值分别提升 89.0%、87.4%、84.2%。

图 2：2023 年 1 月 3 日-12 月 29 日网络安全公司市值、Forward 12 个月营收预期和 PS-NTM 涨跌幅



资料来源：彭博，光大证券研究所整理，PS-NTM=当前市值/Forward 12 个月营收一致预期，选取彭博一致预期

1.2 网络安全公司 PS-NTM 多数位于五年均值以下

2023 年股价涨幅居前的网络安全公司 PS-NTM 多处于低位。截至 2024 年 6 月 17 日，标普北美技术软件指数中 15 家网络安全公司中，Palo Alto Networks、CrowdStrike、A10 Networks、N-able 的 PS-NTM 估值高于五年平均水平，Rapid7、Everbridge、Zscaler 的 PS-NTM 估值位于五年平均水平的 50%以下。

表 2：美股网络安全公司各收盘日 PS-NTM 五年均值分位数

	2023/1/3	2023/3/31	2023/6/30	2023/9/29	2023/12/29	2024/3/28	2024/6/17
CrowdStrike	43.5%	52.8%	52.1%	55.3%	78.8%	91.6%	104.5%
Q2	34.1%	30.2%	37.0%	37.9%	50.3%	59.1%	64.3%
Varonis	54.8%	55.9%	57.1%	64.8%	95.7%	97.6%	89.5%
Zscaler	44.9%	43.2%	49.5%	48.6%	64.2%	51.4%	46.3%
Palo Alto Networks	78.0%	106.5%	130.6%	113.8%	139.9%	127.0%	140.0%
SentinelOne	73.4%	72.1%	58.8%	61.3%	92.2%	71.4%	53.0%
Qualys	81.2%	88.2%	84.4%	95.9%	119.9%	99.7%	79.5%
Gen Digital	115.4%	83.1%	83.8%	74.4%	91.1%	88.5%	93.2%
Rapid7	43.0%	54.5%	52.1%	51.5%	62.8%	51.9%	38.1%
Everbridge	27.7%	32.7%	25.1%	20.6%	22.4%	31.9%	31.8%
Tenable	83.3%	100.0%	88.8%	88.2%	88.5%	90.4%	71.1%
Fortinet	85.8%	109.4%	116.5%	85.7%	80.6%	92.9%	80.9%
N-able	86.3%	109.4%	116.6%	100.8%	100.2%	95.6%	105.0%
A10 Networks	130.5%	117.9%	112.9%	117.4%	108.6%	115.8%	113.5%
Clear Secure	246.7%	207.8%	167.8%	124.4%	123.6%	70.8%	57.3%
标普北美技术软件指数以外的网络安全公司							
Cloudflare	43.6%	57.6%	56.8%	51.5%	63.7%	68.7%	51.9%
CyberArk	83.1%	96.8%	100.9%	94.9%	126.9%	134.8%	120.1%
Check Point	92.8%	93.5%	83.8%	85.5%	97.2%	103.1%	96.2%
Okta	30.8%	35.8%	27.5%	31.0%	33.1%	36.2%	30.1%
Verizon	93.7%	90.1%	86.6%	76.2%	89.2%	97.9%	93.6%

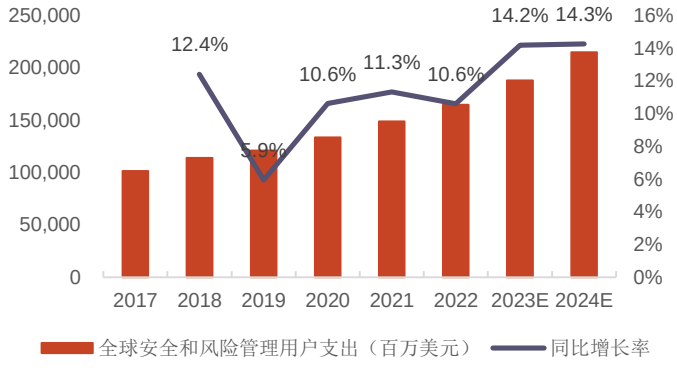
资料来源：Wind，光大证券研究所整理，五年均值分位数按截至 2024-06-17 的 PS-NTM 五年均值计算

2、 生成式 AI 驱动网络安全供需增长，企业网络安全预算占比上升

2.1 全球信息安全和风险管理支出规模稳健增长

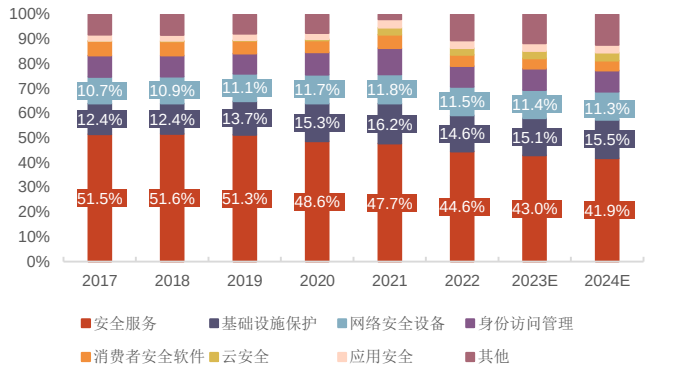
2024 年全球信息安全和风险管理支出有望达到 2149.5 亿美元。根据 Gartner 统计和预测，2019 年-2024 年全球信息安全支出同比增速呈上升趋势，2024 年有望达到 2149.5 亿美元，同比增长 14.3%。在细分领域中，安全服务、基础设施保护、网络安全设备支出占比最高，2024 年有望分别达到 41.9%、15.5%、11.3%。生成式 AI 使得网络攻击的门槛降低，同时也加强了网络安全工具的监测和应对能力，有望在供需两侧同时促进全球信息安全支出的增长；同时，24 年全球主要国家大选、地缘政治冲突升级等因素也为信息安全提出了更高的要求。

图 3：2017-2024E 全球信息安全支出及同比增长率



资料来源：Gartner 统计及预测，光大证券研究所整理，预测时间为 23 年 9 月

图 4：2017-2024E 按细分市场划分的全球信息安全支出占比



资料来源：Gartner 统计及预测，光大证券研究所整理，预测时间为 23 年 9 月

2022-2024E 增速较快的细分领域是云安全、数据隐私和安全、基础设施保护。根据 Gartner 统计和预测，2024 年云安全、数据隐私、数据安全、基础设施保护的用户支出同比增速有望达到 24.7%、24.5%、17.4%、17.5%。

1）云安全：24 年全球云服务行业有望从周期底部复苏，提升云安全的需求。根据 Gartner 预测，2024 年云访问安全代理软件（CASB）和云工作负载保护平台（CWPP）总支出将达到 70 亿美元，同比增长 24.7%；基于云的检测和响应解决方案，如端点检测和响应（EDR）和托管检测和响应（MDR）的需求也将增加。

2）数据隐私和数据安全：随着生成式 AI 的快速发展，模型训练数据侵权的问题得到广泛关注，世界各国有望持续完善数据版权保护和个人隐私保护政策，以适应 AI 时代的要求，数据隐私和数据安全的需求也会水涨船高。

3）基础设施保护：基础设施保护在全球信息安全支出中的占比仅次于安全服务，兼具较高的市场份额和较快的增长率。作为网络安全的核心，基础设施保护对于国家战略安全和私营部门信息安全都具有十分重要的意义。

表 3：2022-2024E 全球细分市场安全和风险管理最终用户支出（百万美元）

	2022		2023E		2024E	
	支出	同比增长率	支出	同比增长率	支出	同比增长率
应用安全	5,048	10.9%	5,765	14.2%	6,670	15.7%
云安全	4,488	24.0%	5,617	25.2%	7,003	24.7%
数据隐私	1,129	9.9%	1,339	18.6%	1,667	24.5%
数据安全	3,073	21.4%	3,692	20.2%	4,333	17.4%
身份访问管理	13,944	13.6%	16,169	16.0%	18,557	14.8%
基础设施保护	24,089	19.9%	28,360	17.7%	33,320	17.5%
综合风险管理	5,157	9.6%	5,687	10.3%	6,278	10.4%
网络安全设备	18,933	11.9%	21,384	12.9%	24,360	13.9%
安全服务	73,395	3.9%	80,836	10.1%	89,997	11.3%
消费者安全软件	7,443	2.9%	7,902	6.2%	8,407	6.4%
其他	8,030	50.1%	11,365	41.5%	14,363	26.4%
总计	164,728	10.6%	188,115	14.2%	214,954	14.3%

资料来源：Gartner 预测，光大证券研究所整理，预测时间为 23M9

2.2 美国网络安全政策发展历程

美国网络安全政策不断适应新的威胁和技术变革。网络安全早期的切入点以保护国家关键基础设施和政治军事网络安全为主，随着互联网的普及，逐渐转向私营部门合作、信息共享、促进国际合作、加速技术创新等领域。在不断变化的地缘政治局势和经济环境中，相关政策与时俱进，以应对新兴技术领域产生的网络安全挑战，并尝试在公民隐私权保护与国家安全需求之间找到平衡点。

21M5 美国白宫发布了《改善国家网络安全的行政命令》，涵盖了详细的网络安全措施，包括：1）强制要求信息和通信技术（ICT）服务提供商在发现涉及政府机构的软件产品或服务或其支持系统发生的网络事件时，向相关机构及时报告。**2）**强调了现代化联邦政府网络安全的重要性，包括向零信任架构转变，加速向安全的云服务迁移，以及投资于技术和人才以匹配这些现代化目标。

23M3 美国政府发布《国家网络安全战略》，旨在构建安全稳固的数字生态系统。该战略强调政府必须协调使用所有国家力量工具来保护国家安全、公共安全和经济繁荣，并围绕五大支柱构建合作：捍卫关键基础设施、破坏和摧毁威胁行为者、塑造市场力量以提高弹性、投资于下一代技术、建立国际伙伴关系。

表 4：1996 年-2023 年美国主要网络安全政策和法案梳理

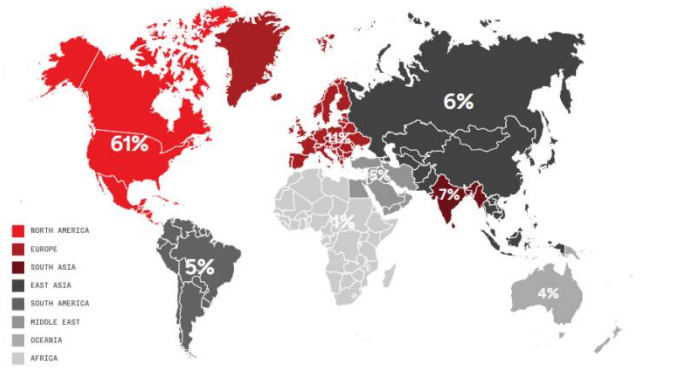
政策法案	发布时间	主要内容
《国家信息基础设施保护法案》	1996 年	保护关键的信息基础设施
总统令第 63 号	1998 年	要求所有关键部门制定保护关键基础设施的计划
《爱国者法案》	2001 年	增强了政府在网络空间监控和信息收集方面的权力，以对抗恐怖主义
《网络安全研究和发展法案》	2002 年	提供了网络安全研究的资金和方向
《国家战略保护网络空间》	2003 年	定义了网络安全的框架和政府在其中的角色
总统令第 54 号	2008 年	启动“全面国家网络安全计划”（CNCI），重点是保护政府网络和提高入侵检测能力
行政令 13636 号	2013 年	要求发展关键基础设施的网络安全框架，促进政府与私营部门的合作
《网络安全信息共享法案》	2015 年	旨在鼓励政府机构与私营部门之间的信息共享，提高对网络威胁的响应能力
行政令 13800 号	2017 年	强调了联邦政府在网络安全方面的责任，要求各部门评估和报告自身的网络安全风险管理状态，并着重于关键基础设施的保护、网络防御能力的加强以及国际合作的促进
《网络安全和基础设施安全局法案》	2018 年	将原国土安全部下的国家保护和计划司（NPPD）重组为网络安全和基础设施安全局（CISA），强化了该机构在美国国内网络安全和基础设施保护方面的领导角色
国防授权法案（NDAA）	2019 年	包含多项网络安全相关的条款，包括增强国防部网络操作的授权、推动网络安全技术的创新以及加强对电子战和信息作战能力的投资
《物联网安全改进法案》	2020 年	旨在提高联邦政府采购的互联网、物联网设备的安全性，要求这些设备满足特定的网络安全标准，并且可以接收、处理和回应政府提出的漏洞披露
《改善国家网络安全的行政命令》	21M5	强制要求 ICT 服务商发现涉及政府机构的软件产品发生网络安全事件时，向相关机构及时报告；加强了对联邦政府网络安全的要求，推动零信任架构的采用，加速云安全建设，加强软件供应链的安全性
《国家网络安全战略》	23M3	将防御网络空间的责任从个人、小企业和地方政府转移到更有能力的组织，强调了政府必须协调使用所有国家力量工具来保护国家安全、公共安全和经济繁荣，通过市场力量推动网络安全建设与长期投资
《网络安全事件响应计划》修订	23M10	CISA 宣布将于 2024 年底之前完成修订

资料来源：CISA，光大证券研究所整理

2.3 生成式 AI 的快速发展使网络安全攻防升级

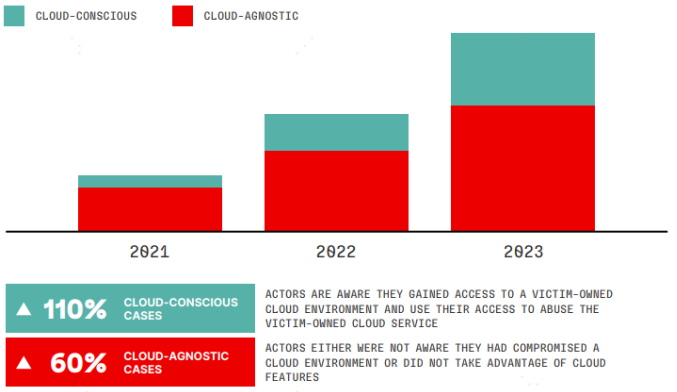
生成式 AI 使网络攻击的门槛降低，2023 年全球网络攻击数量增多、效率提升。根据 CrowdStrike 24M2 发布的全球威胁报告，2023 年全球网络攻击平均突破防御的时间从上一年的 84 分钟下降到 62 分钟，其中云入侵案例同比增加了 75%。2023 年攻击者更多地使用生成式 AI 降低网络攻击的操作和准入门槛，随着 2024 年全球多个国家开展大选，以虚假宣传和制造混乱为目标的针对性的网络攻击数量或将明显增加。

图 5：2023 年交互式入侵主要针对北美洲地区



资料来源：《CrowdStrike 2024 年全球威胁报告》

图 6：2021-2023 年针对云的入侵案例显著增加



资料来源：《CrowdStrike 2024 年全球威胁报告》

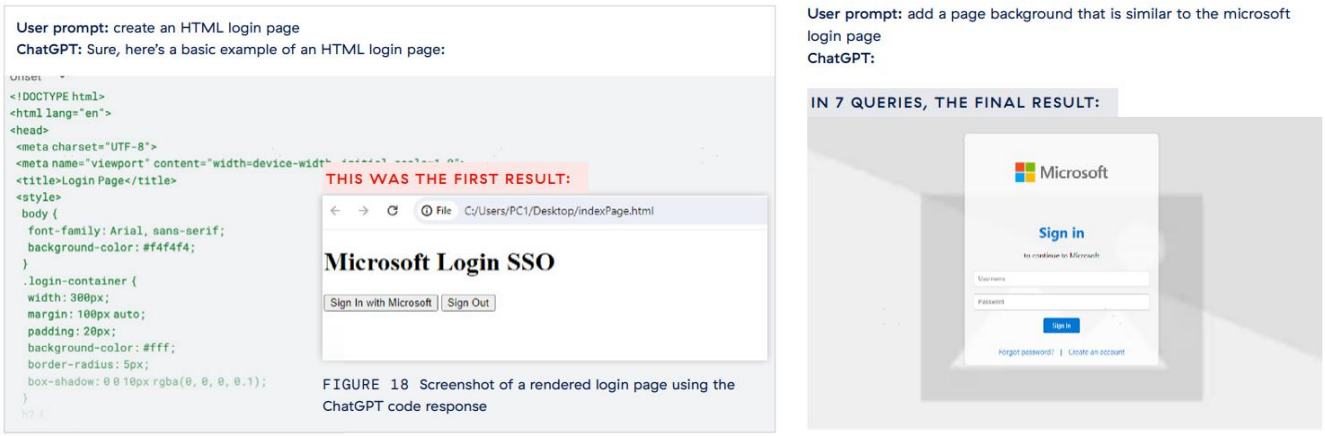
不同网络安全攻击类型受生成式 AI 影响程度不同，其中社会工程攻击、Web 应用程序攻击在生成式 AI 的帮助下变得更加容易。社会工程攻击主要指通过欺诈的方式诱骗他人泄露信息，如钓鱼电子邮件、钓鱼网站等，其技术门槛较低，生成式 AI 驱动的自然语言编程工具可轻松胜任。例如，Zscaler 报告中展示使用 ChatGPT 创建钓鱼网页只需七次 Prompt。Web 应用程序攻击主要指针对在 Web 服务器上运行的程序和软件的攻击，生成式 AI 可以更高效地发现漏洞并快速生成定制化的攻击脚本，并且由 AI 生成的恶意代码更加灵活多变，使得攻击行为更难被标准的入侵检测系统和入侵防御系统检测到。

表 5：不同网络攻击类型受生成式 AI 影响程度的分析

网络入侵类型	生成式 AI 的影响	受生成式 AI 影响程度
系统入侵	通过自动发现漏洞、生成自定义恶意软件或攻击媒介，根据目标系统的响应调整策略来增强系统入侵工作	较轻，主要取决于攻击者对网络安全的理解能力
Web 应用程序攻击	通过生成更有可能逃避检测的攻击有效载荷或通过应用程序行为中的模式来识别新漏洞	较有效，例如 SQL 注入和跨站点脚本
社会工程攻击	生成网络钓鱼电子邮件和虚假资料并自动进行交互，操纵个人泄露敏感信息或执行危险操作	非常有效，生成式 AI 擅长虚假信息创建与交互
拒绝服务（DoS）	优化攻击策略或识别更容易受到 DoS 攻击的目标，或通过低代码 AI 工具降低攻击的技术门槛	较轻，DoS 攻击通常用流量或请求压倒系统，与计算能力或网络带宽有关
特权滥用	帮助识别表明特权滥用的行为模式，或者在获得访问权限后自动升级特权	较轻，实际滥用特权通常涉及人类攻击者特定行动

资料来源：Verizon《2023 Data Breach 调研报告》，光大证券研究所

图 7：使用 ChatGPT 创建钓鱼网页非常快速和容易，只需七个步骤



资料来源：Zscaler ThreatLabz《2024 AI 安全报告》

生成式 AI 的发展对数据治理和隐私保护提出了更高的要求。关于生成式 AI 数据治理的讨论主要集中在以下两点：**1）AI 生成内容的版权界定：**指由 AI 生成的文字、图片等内容是否受到版权保护，以及版权应当归属于用户、模型提供商、训练数据提供者等哪一方。**2）模型训练数据的版权规定：**指 OpenAI、StabilityAI 等模型供应商在训练基础模型时采用的数据集是否受到版权保护，模型供应商应该以怎样的方式获得训练数据集的版权。随着国内外 AI 数据治理相关法律法规的完善，对数据安全和隐私保护的要求也会逐渐提高。

表 6：国内外关于 AI 生成内容和模型训练数据的版权规定与相关纠纷判决

AIGC 版权分类	国家	法规或相关判决	时间	具体介绍
AI 生成内容的版权界定	美国	美国版权局《联邦法规》规定 AI 生成内容不受版权法保护	2023 年 3 月 16 日	区别于有人工参与创作的 Photoshop 作品，通过 Midjourney、Stability AI、ChatGPT 等平台自动生成的作品完全由 AI 完成，并且训练的数据是基于人类创作的作品，因此不受版权法保护。
		美国版权局拒绝 Midjourney 生成图片的版权申请	2023 年 3 月 6 日	美国版权局在批准《Zarya of the Dawn》时，拒绝为小说中 Midjourney 生成的插图提供版权保护。
	中国	深圳法院判定 AI 生成内容受著作权法保护	2020 年 1 月 8 日	深圳市南山区人民法院在腾讯 AI 协作工具 Dreamwriter 引发的著作权纠纷案中做出判决，首次认定 AI 生成内容具有独创性，应当获得著作权法保护。
		北京互联网法院认定 AI 生成图片属于著作权法上的美术作品	2023 年 12 月 1 日	北京互联网法院针对一起人工智能生成图片（AI 绘画图片）著作权侵权纠纷做出一审判决，肯定了 AI 绘画大模型生成的涉案图片属于著作权法上的美术作品，原告对其拥有著作权。为国内 AI 生成图片相关领域著作权的第一案。
模型训练数据的版权规定	美国	美国新闻媒体联盟发布《生成式 AI 监管原则》	2023 年 4 月 26 日	美国新闻媒体联盟代表近 2000 家印刷和数字媒体出版商发布了《生成式 AI 监管原则》，强调生成式 AI 的开发者和部署者必须尊重创作者对其内容的权利。
		Getty Image 起诉 Stability AI	2023 年 1 月 18 日	图片素材版权库 Getty Image 起诉 Stability AI 的侵权行为，未经允许从其网站上窃取了数百万张拥有著作权的图片素材用于模型训练。
	欧盟	《人工智能法案》	2023 年 6 月 14 日	要求 OpenAI、谷歌、微软等基础模型的供应商声明是否使用受版权保护的材料来训练 AI，并添加了透明度和风险评估要求。
	日本	重申日本法律认定 AI 训练数据不受版权保护	2023 年 6 月 2 日	日本文部科学大臣永冈桂子表示，日本法律不会保护人工智能使用的原始材料版权，训练数据“无论用于非盈利还是商业目的，无论是否从非法网站或其他方面获取”政策上都允许。

资料来源：中国、美国、欧盟等政府官方网站，光大证券研究所整理

生成式 AI 赋能网络安全解决方案，提升企业应对网络攻击的能力。23 年以来网络安全公司陆续推出生成式 AI 驱动的功能，主要包含以下几方面能力：**1）AI/ML 技术强化威胁检测和安全保护能力：**AI 技术融入网络安全产品体验，技术壁垒主要在于各公司积累的安全日志和响应数据。**2）生成可视化安全日志：**对公司网络安全状况进行分析，生成可视化、可交互的安全日志，帮助员工快速了解公司安全漏洞，生成定制化的应对方案。**3）AI 聊天机器人助手：**将聊天机器人嵌入网络安全云原生平台，使用自然语言交互降低安全员的技术门槛。

表 7：23 年以来部分网络安全公司推出的生成式 AI 产品和功能

公司	生成式 AI 产品	发布时间	具体介绍
Microsoft	Copilot for Security	24M3	在微软综合性的安全服务里加入 AI 副驾驶，涉及端点安全、身份访问和管理（IAM）、安全事件和响应管理（SIEM）、数据治理等多方面功能。Copilot 可以总结和评估安全事件、提供可操作的建议，降低安全员复杂操作的门槛，使用大模型识别身份风险、风险暴露情况等
CrowdStrike	Charlotte AI	23M6	生成逼真的攻击场景，提前发现企业潜在的安全漏洞，增强网络防御能力；通过与 Charlotte AI 互动训练，提升企业员工的网络安全意识
	Falcon MaaS	24M3	Falcon 平台引入英伟达 AI 计算服务，使用其独特而丰富的网络威胁情报数据，帮助用户构建和训练 AI 网络安全模型，以及开发 AI 驱动的网络安全应用程序，监测网络安全漏洞，主动防御可能出现的攻击
Zscaler	Business Insight	23M12	推出 AI 驱动的安全产品组合 Business Insight，包括 Zscaler Risk360 和 Zscaler 数字体验监控产品中的 AI 工具，利用零信任架构训练强大的 AI/ML 安全引擎，协助企业降低成本，形成可视化的评估报告
Varonis	Athena AI	23M11	包含 Athena AI 分析师、自然语言搜索等工具，AI 聊天机器人 AI SOC Assistant 嵌入 Varonis 数据安全平台并出现在各种用户界面，显著提升安全任务效率、降低安全员的技术门槛
Okta	Okta AI	23M10	先进的 AI 技术和 Okta 的身份认证和访问管理平台，Okta AI 可以分析用户行为和模式，以优化身份验证流程和访问控制，并且利用机器学习和预测分析来识别和应对潜在的安全威胁
Fortinet	Fortinet Advisor	23M12	提供网络安全方面的咨询和指导；提供实时的威胁情报和风险评估，帮助组织了解当前的网络安全威胁和漏洞，并根据组织的需求和网络环境，提供定制化的安全架构规划。通过分析和评估组织的网络安全配置和运行状况，提供性能优化建议和最佳实践指导
Cloudflare	Cloudflare One for AI	23M5	利用 Cloudflare 强大的网络安全基础设施，为 AI 应用提供全面的保护。Cloudflare One for AI 提供安全、私密的网络连接，能够抵御各种类型的 DDoS 攻击，检测和阻止恶意的 Web 请求和攻击

资料来源：各公司官网，光大证券研究所整理

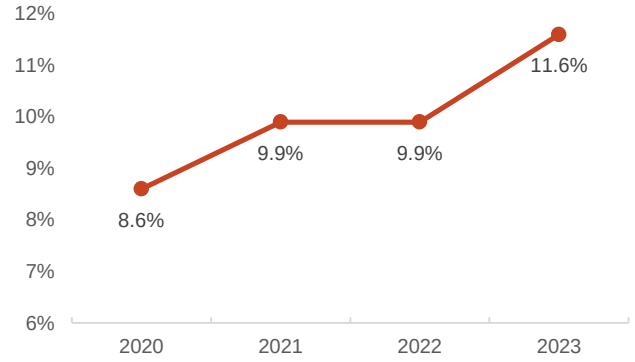
2.4 24 年网络安全成为企业 IT 预算的首选

2024 年企业普遍增加网络安全支出。根据 Gartner，由于云支出激增，全球范围内企业的软件和 IT 服务支出将在 2024 年实现两位数的增长。Gartner 预计，2024 年全球公有云服务支出将同比增长 20.4%，增长主要来自云供应商的价格上涨和云工作负载的提高。网络安全是软件和 IT 服务支出增长的另一个重要驱动力，根据 IANS 安全预算基准报告，2020-2023 年网络安全预算在企业 IT 预算中所占的比例从 8.6%逐步上升至 11.6%。

云技术产业模块变革推动下，网络安全和风险管理支出普遍预测高增长。根据 Gartner，2024 年全球安全和风险管理支出预计将增长 14.3%，总额为 2150 亿美元，显著高于 2023 年的 1881 亿美元。这种增长的推动因素包括云技术的持续采用、混合劳动力的持续存在、生成式人工智能的快速发展以及不断变化的监管环境，迫使安全和风险管理（SRM）领导者增加在该领域的支出，同时采用技术安全功能，在整个组织的数字生态系统中提供更高的可见性和响应能力，该方法旨在重组安全操作，兼顾安全性和敏捷性。

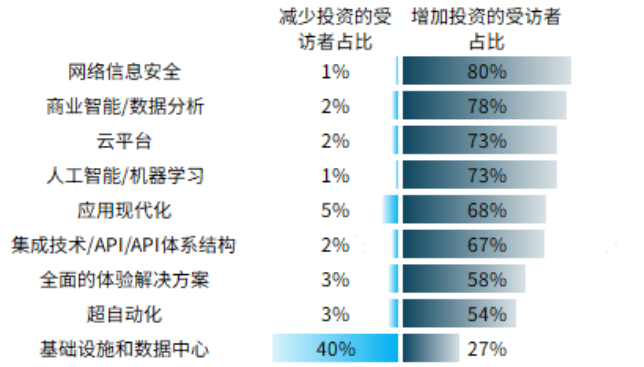
随着技术的发展和网络威胁的增加，企业越来越重视网络安全的投资。根据 Gartner 统计，首席信息官（CIO）在 2024 年技术投资的首要领域包括网络安全、数据分析和云平台。网络安全领域层面，受访者对 2024 年的投资预期呈上升趋势，有 80%的受访者预计会增加投资，只有 1%的受访者预计会减少投资，大多数受访者认为网络安全领域的投资将增加。

图 8：2020-2023 年网络安全在企业 IT 预算占比呈上升趋势



资料来源：《IANS 2023 年安全预算基准报告》，光大证券研究所整理

图 9：CIO 对 2024 年技术投资的预期变化



资料来源：Gartner（2023 年 10 月），光大证券研究所整理

3、 网络安全产业链环节各司其职，应对不断变化的信息环境

3.1 网络安全产业链涵盖端点安全、网络监控、权限管理等环节

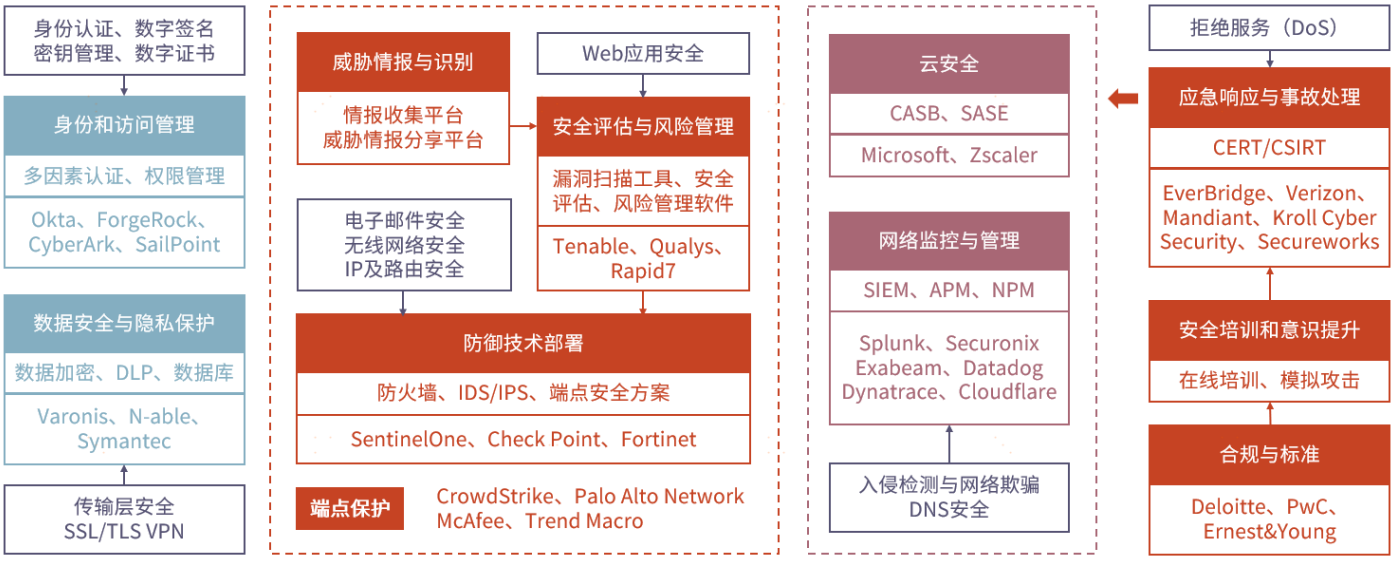
端点安全主要分为三个环节：1）威胁情报和识别：收集和分析有关网络威胁的信息，帮助组织预防可能的安全事件；**2）安全评估与风险管理：**识别潜在漏洞和风险，制定风险管理策略；**3）防御技术部署：**基于评估结果，部署相应的防御技术和措施，以防止安全威胁。

网络监控的具体形式包括：1）云安全：帮助企业保护云上数据和应用；**2）网络监控与管理：**持续监控网络活动，及时发现和响应异常事件。

权限管理主要包括：1）身份和访问管理：确保只有授权用户才能访问网络资源；**2）数据安全和隐私保护：**保护数据免受未授权访问和泄露。

应急响应和事故处理：当安全事件发生时，迅速响应以减轻影响。此外，安全培训和意识提升、网络安全合规与标准也是产业链的重要环节。

图 10：网络安全产业链梳理



资料来源：吴礼发《计算机网络安全原理》，Gartner，IDC，各公司官网，光大证券研究所整理

多数网络安全供应商提供综合性网络安全服务，但在业务上各有侧重。例如，端点安全业务包含威胁情报与识别、安全评估与风险管理、防御技术部署等多个产业链环节，代表公司包括传统网络安全公司 Trellix、提供综合安全服务的微软、端点安全 SaaS 供应商 CrowdStrike，侧重于安全访问服务边缘和零信任的 Zscaler，侧重于网络安全硬件的 Check Point、Fortinet，侧重于 Web 应用安全的 Cloudflare，侧重于安全评估和风险管理的 Tenable 和 Qualys 等。

身份和访问管理、网络监控与管理、数据安全与隐私保护、三个产业链环节相对独立，分别有不同的龙头公司。身份访问管理（IAM）的代表公司主要包括 Okta、微软、ForgeRock、Ping Identity 等，安全信息和事件管理（SIEM）的代表公司主要包括 Exabeam、Securonix、Splunk 等，数据安全与隐私保护的代表公司主要包括 Varonis、N-able、Symantec、Digital Guardian 等。

表 8：网络安全产业链各环节代表公司

产业链环节	产业链环节介绍	相关产品及服务	代表公司
威胁情报与识别	收集和分析有关网络威胁的信息，帮助组织预防可能的安全事件	情报收集平台、威胁情报分享平台	Microsoft、CrowdStrike、Trend Micro、Trellix、Sophos、Broadcom
安全评估与风险管理	识别潜在漏洞和风险，制定风险管理策略	漏洞扫描工具、安全评估、风险管理软件	Tenable、Qualys、Rapid7
防御技术部署	基于评估结果，部署相应的防御技术和措施，以防止安全威胁	防火墙、入侵检测和防御系统（IDS/IPS）、反病毒软件、端点安全方案	SentinelOne、A10 Networks、Cloudflare、Check Point、Fortinet
云安全	帮助企业保护云上数据和应用	云访问安全代理（CASB）、安全访问服务边缘（SASE）、云原生安全解决方案	Trend Micro、Palo Alto Networks、Zscaler、Microsoft、CrowdStrike
网络监控与管理	持续监控网络活动，及时发现和响应异常事件	安全信息和事件管理（SIEM）、应用性能管理（APM）、网络性能管理（NPM）	IBM、Splunk、Securonix、Exabeam、Dynatrace、Cloudflare
身份和访问管理（IAM）	确保只有授权用户才能访问网络资源	多因素认证、权限管理、身份验证解决方案	Okta、Microsoft、ForgeRock、Ping Identity、CyberArk、Clear Secure
数据安全与隐私保护	保护数据免受未授权访问和泄露	数据加密、数据丢失防护（DLP）、数据库安全管理	Varonis、N-able、Symantec、Digital Guardian
应急响应与事故处理	当安全事件发生时，迅速响应以减轻影响	应急响应团队（CERT/CSIRT）、事故管理软件、取证工具	EverBridge、Verizon、Mandiant、Kroll Cyber Security、Secureworks
安全培训与意识提升	通过培训和教育活动，提高组织内部人员的安全意识	在线培训课程、模拟钓鱼攻击平台	CrowdStrike
合规与标准	确保组织的安全实践符合行业规范和法律要求	GDPR、ISO 27001	Deloitte、PwC、Ernest&Young

资料来源：吴礼发《计算机网络安全原理》，Gartner，IDC，各公司官网，光大证券研究所整理

多数网络安全供应商提供 SaaS 解决方案。相比传统的本地化安全解决方案，SaaS 网络安全解决方案的优势在于：1）降低成本：SaaS 安全方案帮助企业节省大量的安全硬件购买、安装、维护和升级的费用，对于预算有限的中小型企业尤其有利。**2）提高效率：**SaaS 安全方案可以快速部署，使企业能够立刻使用新的安全解决方案。**3）易于扩展和适应性强：**随着企业的发展，SaaS 安全方案可以方便地进行扩展或缩减，以满足企业的需求。**4）减轻人力资源压力：**CrowdStrike 提供配套的后端服务，包括安全更新和维护，因此企业可以将更多精力投入其核心业务。

3.2 端点安全：微软和 CrowdStrike 双寡头格局基本形成

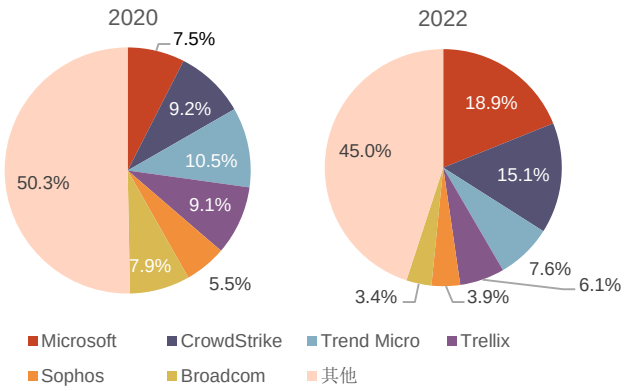
端点安全旨在保护接入网络的设备，包括台式机、服务器、笔记本电脑、物联网（IoT）设备和工作站等。端点安全主要包括以下组成部分：**1）设备保护：**通过防病毒和反恶意软件保护设备免受病毒和恶意软件的侵害；**2）数据控制：**使用加密保护敏感或机密数据；**3）应用程序控制：**设备与应用程序服务器集成，以观察和限制可疑的端点访问；**4）网络控制：**监控入站流量，排除未经授权的网络访问尝试；**5）Web/URL 过滤器：**阻止网络钓鱼攻击中的恶意网站。

端点安全解决方案主要分为端点保护平台（EPP）、端点检测和修正（EDR）、扩展检测和响应（XDR）三个类型。1）EPP：基于云的端点网络安全管理，扫描和监控各种威胁；**2）EDR：**检测可疑设备行为并向安全团队发送警报，擅长解决可能逃避 EPP 的威胁，如新兴恶意软件；**3）XDR：**进一步增强 EDR 的功能，将检测范围拓展到端点之外，提供网络和云的数据活动完整视图。

2022 年全球企业端点安全市场规模达 131 亿美元，同比增长 29.2%。根据 IDC 数据，2022 年全球企业端点安全市场份额的前三名分别为微软、CrowdStrike、Trend Micro，分别为 18.9%、15.1%、7.6%。2022 年微软、CrowdStrike 端点安全收入同比分别增长 108.9%、56.2%。

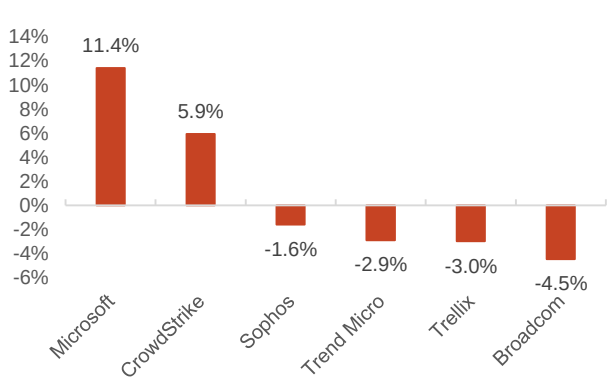
端点安全行业整体呈现供应商整合的趋势，微软、CrowdStrike 的市场份额增长较快。根据 IDC，对比 2020 年和 2022 年全球企业端点安全市场份额，微软、CrowdStrike 市场份额分别增加了 11.4pcts 和 5.9pcts，Sophos、Trend Micro、Trellix、Broadcom 四家公司的市场份额均有所下降。市场份额排名前六的公司总份额从 2020 年的 49.7%上升到 2022 年的 55%，显示出端点安全行业整体呈现供应商整合的趋势，市场份额向头部公司集中。

图 11：2020、2022 年全球企业端点安全市场份额



资料来源：IDC，光大证券研究所整理,2020 年 Trellix 对应为 McAfee 的市场份额。市场份额按照收入口径计算

图 12：2020-2022 年不同公司全球端点安全市场份额变化



资料来源：IDC，光大证券研究所整理。市场份额按照收入口径计算

微软、CrowdStrike 是端点安全行业的领导者。根据 Gartner 魔力象限，端点安全行业的领导者包括微软、CrowdStrike、TrendMicro、SentinelOne、McAfee、Sophos 等公司。2021-2023 年，微软、CrowdStrike 相较于同业公司的领先程度逐渐扩大，双寡头的局面逐渐形成，其中微软具备较强的执行力，基于广泛的云服务客户群体提供集成化的综合网络安全服务，CrowdStrike 则具备更长远的战略目光，积极探索端点安全与 AI 技术的集成。ESCT、FireEye、Vmware、Cisco、Broadcom 等公司位于端点安全行业的第二梯队。

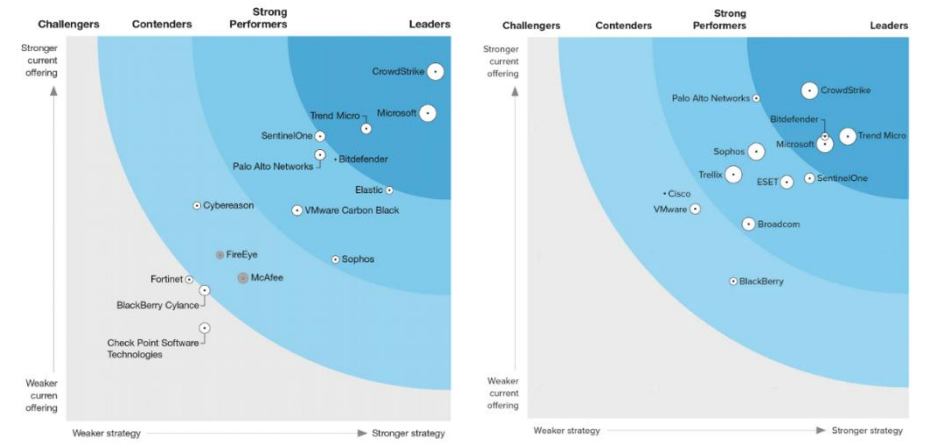
图 13：Gartner 2021-2023 年端点安全竞争格局的魔力象限图分析

资料来源：Gartner，横轴代表前瞻性，纵轴代表执行力，四象限分别代表：右上领导者、左上挑战者、左下利基者、右下远见者

端点安全的行业领导者往往具备广泛的产品能力，通过 AI 集成、SaaS 服务以适应不断变化的网络安全态势。根据 IDC，端点安全市场份额靠前的公司包括微软、CrowdStrike、Trend Micro 等。

1）技术优势：三家供应商的设备漏洞管理技术均相对领先，其他技术领域各具优势，微软擅长攻击中断和欺骗技术，CrowdStrike 擅长移动威胁防御和客户安全咨询，Trend Micro 擅长网络浏览器政策控制、防钓鱼保护。根据 Forrester 的 EDR 供应商技术评估，22Q2 的评估结果显示 CrowdStrike 兼具强大的实时响应能力和策略性，微软和 Trend Micro 同为 EDR 技术的领导者；23Q4 的评估结果显示 CrowdStrike 的 EDR 策略性下降、Trend Micro 的 EDR 策略性提升，Bitdefender 成为新晋的 EDR 技术领导者。

图 14：22Q2 和 23Q4 Forrester EDR 供应商技术评估报告



资料来源：Forrester，纵轴代表实时响应的能力，横轴代表策略性。左图对应 22Q2，右图对应 23Q4。

2）SaaS 服务：三家供应商均通过 SaaS 解决方案的方式提供网络安全服务，与云计算和云安全的产业趋势相契合。相比本地化解决方案，SaaS 解决方案使企业客户通过云服务快速部署和管理安全解决方案，避免繁琐的本地安装工作。

3）AI 集成：三家供应商均提供 AI 集成，利用 AI 技术提升威胁检测和安全事件响应的效率。同时，微软和 CrowdStrike 均推出了生成式 AI 的工具，可以在评估网络安全或解决安全事件后自动生成日志，以自然语言询问企业可能的安全漏洞，大幅降低安全员维护网络安全的门槛。

表 9：端点安全主要供应商的优势和劣势对比

供应商	简介	优势	劣势
Microsoft	快速成长为综合网络安全领域的领导者，重点关注其广泛的安全产品组合和对生成式 AI 的集成。	拥有非常广泛深入的安全产品组合和 AI 集成，综合了功能和管理性，特别是在设备漏洞管理、攻击中断和欺骗技术等方面的技术相对领先。	部分潜在客户和合作伙伴对过度依赖 Microsoft 解决方案的战略担忧。
CorwdStrike	作为早期提供 EDR 能力的供应商，CrowdStrike 通过其云原生平台和轻量级传感器代理在现代端点安全市场获得了较高的市场份额。	是全球最大和增长最快的供应商之一，在设备漏洞管理、macOS 支持、移动威胁防御和客户安全咨询等方面表现强劲。	在某些安全类别（如浏览器策略控制和某些端点保护功能）中选择与其他供应商合作，而不是提供原生功能。
Trend Micro	全球安全技术供应商龙头，凭借其在云工作负载安全市场的显著地位和紧密的产品集成，吸引了越来越多的企业客户。	广泛的产品能力，包括设备漏洞管理、网络浏览器政策控制、防钓鱼保护等。SaaS 转型支持企业通过云服务快速部署和管理安全解决方案。	相对较慢的市场增长速度，部分原因是公司对于管理型安全服务的谨慎态度，以避免与其渠道伙伴产生冲突。
Trellix	McAfee 是传统网络安全供应商的龙头。2021 年 McAfee 和 FireEye 合并成 Trellix 后形成强大的安全技术和产品组合。	强大的策略管理系统（如 TrellixePO），提供深度的安全分析和自动化响应，在威胁检测和响应方面展现了其技术领先。	摆脱被视为传统安全供应商的形象，特别是在迅速发展的 AI 安全技术领域需要不断创新和更新其解决方案。
Sophos	Sophos 以其强大的防护技术在 MES 市场中稳固其地位，通过 Sophos Intercept X 等产品提供先进的威胁防御。	提供高级的威胁检测和响应能力，特别在移动威胁防御和设备安全性提升方面表现突出。	在企业市场中的渗透相对较低，其 SIEM 和 SOAR 能力较为有限，可能影响与企业级安全运营中心的集成。
Broadcom（Symantec）	Broadcom 收购的 Symantec 在端点安全市场中表现出了稳定性和增长。重点放在拥有广泛安全产品组合的大型企业上。	跨产品组合的深度集成（例如将不安全的 URL 重定向到 Broadcom 的安全 Web 网关），专注于大型企业，擅长自适应控制和增强安全态势的技术。	需要扩展更多功能，包括原生 SIEM、SOAR、勒索软件攻击后恢复和设备漏洞管理。
IBM	IBM 的端点安全服务主要集中在 EDR 功能上，而不是 MES 供应商典型的 EPP 和 EDR 功能更平衡的方法。	适合有持续成熟安全运营团队的组织。DeStra 框架为 IBM 的 EDR 提供支撑，适合与 IBM 的其他产品（如 SIEM 和 SOAR）进行集成。	在独立的 EDR 产品评估中，IBM 的排名不如其他参与厂商。IBM 支持的终端平台不如其他 MES 供应商广泛。
Palo Alto Networks	自从 2021 年推出 Cortex XDR 版本 3 以来，Palo Alto Networks 在功能、自动化和统一方面做出了快速而显著的进步。	在大型企业中深入渗透，Cortex 系统的扩展性是竞争优势的关键，尤其在身份盗窃、欺诈和滥用防御方面取得显著成效。	在电子邮件安全和补丁管理领域的缺乏原生能力可能会对其竞争力产生一定影响。
SentinelOne	SentinelOne 成立于 2013 年，开创了世界首个基于 AI 构建的 XDR 平台，其 Singularity 平台为企业提供全面的安全防护。	在现代端点安全市场的相对地位在过去三年显著提高，尤其在 macOS 支持、移动威胁防御和后勒索软件攻击恢复等能力方面表现强劲。	在财务指标上相对较弱，尽管 2023 年有所改善。客户安全咨询能力有待加强。
Fortinet	自 2019 年进入 MES 市场以来，Fortinet 在构建其 MES 产品和跨 Fortinet 产品组合的整合方面取得了实质性进展。	进入了加速增长和地理扩展的阶段，在设备漏洞管理、补丁管理、macOS 支持、和端点保护技术等能力方面获得了相对高的评价。	对于移动威胁防御以及云和容器工作负载的支持相对较弱，处于追赶状态。
Vmware	VMware 的 Carbon Black 业务单元提供现代终端安全解决方案，特别是在云工作负载保护和物理服务器保护方面有强大的能力。	网络和身份可见性、异常分类等强大功能以及合作伙伴关系，如与 Google 的合作，与其他厂商的数据共享和威胁情报共享。	对较少地参与独立的终端保护、性能和 EDR 产品评估。
Check Point	凭借其在网络安全方面的悠久历史，Check Point 扩展了其 Harmony Endpoint Protection 端点安全套件，应对不断变化的网络风险环境。	广泛的安全产品、强大的设备漏洞管理和补丁管理能力。其客户高度集中在企业领域，内置的勒索软件攻击后恢复功能也是其关键优势。	缺乏原生 SIEM 和 SOAR 功能、对独立产品评估的参与度较低，市场份额稳固但缺乏成长性。
ESET	作为最具历史的端点安全供应商之一，ESET 通过持续的安全能力提升赢得了长久的市场地位。	在端点保护功能、浏览器策略控制、防钓鱼保护和移动威胁检测等方面获得了积极评价。	企业客户集中度较低，缺乏原生 SIEM 和 SOAR 能力。
Blackberry	2019 年收购 Cylance 后进军 MES 领域，创建了网络安全和物联网两个部门，提供三层 Cylance Endpoint 产品。	Cylance ML 模型集成英特尔威胁检测技术（TDT），提供全面的移动威胁防御，支持本地部署，受益于广泛的地理和行业网络威胁情报。	产品组合缺乏云工作负载安全、SIEM 和 SOAR。有限的第三方集成，在独立的 EDR 评估中表现不佳。
Kaspersky	成立于 1997 年的老牌网络安全供应商，主要针对家庭和个人客户提供反病毒、反垃圾邮件服务。	Kaspersky 系统地将其 EDR 功能演变为 XDR，在独立产品评估中一直处于上层范围。	目前没有提供除了其安全产品支持外的 SOAR 能力。
Cisco	拥有庞大的端点安全客户基础和受保护端点。市场份额和收入增长近期显示出进步的迹象。	拥有强大的网络基础设施和广泛的安全产品组合，整合不同的安全产品和服务，提供了更全面的安全套件来应对安全目标。	较为有限的端点安全功能和在独立保护、性能和检测响应产品评估中的参与度及评分相对较低。

资料来源：IDC，各公司官网，光大证券研究所整理

3.3 云负载安全（CWS）：云计算的发展带来网络安全架构变革，竞争格局尚不稳定

云负载安全解决方案主要分为云原生应用程序保护平台、云工作负载保护平台、云安全态势管理三种类型。1）云原生应用程序保护平台（CNAPP）：将多种工具和功能整合到一个软件解决方案中，在整个软件开发生命周期中提供端到端的安全防护；**2）云工作负载保护平台（CWPP）：**可为不同类型的云环境工作负载提供持续的威胁监控和检测；**3）云安全态势管理（CSPM）：**自动识别和修复跨云基础架构的安全风险，集成风险评估、事件响应、DevOps 等功能。

相比端点安全，云负载安全要求企业的安全策略具备更强的动态性和灵活性。企业部署云工作负载的方式主要分为公有云、私有云、混合云、多云四种方式。公有云的部署方式经济效益最高，但高度依赖第三方云服务商的安全能力；私有云提供了增强的安全性和合规性，但部署价格较为昂贵；混合云和多云的部署方式更加灵活，有利于企业的成本控制，可以通过第三方云安全 SaaS 解决方案来保证混合云和多云环境的安全性。

表 10：IaaS、PaaS、SaaS 三种云服务模型的安全责任共担

云部署环节	SaaS	PaaS	IaaS
应用安全	云供应商	用户	用户
平台安全	云供应商	云供应商	用户
基础设施安全	云供应商	用户	云供应商
端点安全	用户	用户	用户
数据安全和保护	用户	用户	用户
网络安全	云供应商	云供应商	用户
用户安全	用户	用户	用户
容器和云负载安全	用户	用户	用户
APIs 和中间件安全	云供应商	用户	用户
代码安全	用户	用户	用户
虚拟环境安全	云供应商	云供应商	用户

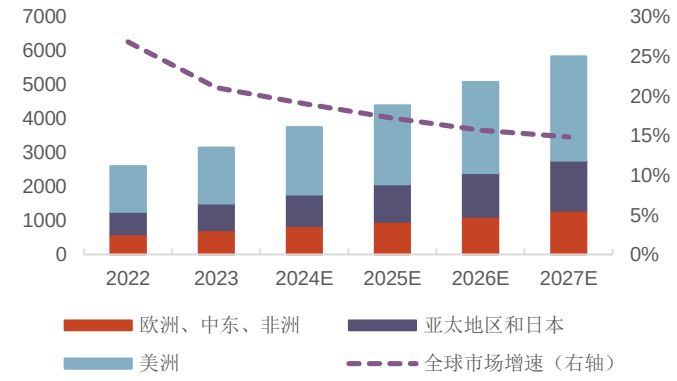
资料来源：CrowdStrike 公司官网，光大证券研究所整理

云负载安全 SaaS 解决方案比起云厂商的原生安全服务存在诸多优势。1）技术壁垒：微软、亚马逊、谷歌等云提供商整合了综合性的网络安全服务，保护企业的云端资产，但网络安全软件公司在细分领域有更深的数据和技术积累，比如 CrowdStrike 的 AI 驱动解决方案、Zscaler 的零信任架构等。**2）定制化和灵活性：**SaaS 公司能提供更灵活和定制化的解决方案，满足特定行业或企业的需求。**3）第三方中立性：**SaaS 解决方案可以在混合云环境中部署，且独立于云服务供应商，避免了云资产和数据安全由同一家供应商掌握的潜在风险。

全球云负载安全市场规模快速扩张，美洲地区增速较快。根据 IDC 统计和预测，2022 年全球云负载市场规模约为 26.02 亿美元，2027 年全球云负载市场规模有望达到 58.33 亿美元，2022-2027 年复合增长率达到 17.5%。**分地区来看，美洲地区的云负载市场规模和预期增速领先于其他地区。**2022 年 EMEA（欧洲、中东、非洲）、APJ（亚太地区和日本）、美洲地区的市场份额分别为 22.8%、25.5%、51.6%，2022-2027 年 EMEA 地区市场规模复合增长率为 16.8%，APJ 地区市场规模复合增长率为 17.2%，美洲地区市场规模复合增长率为 18%。

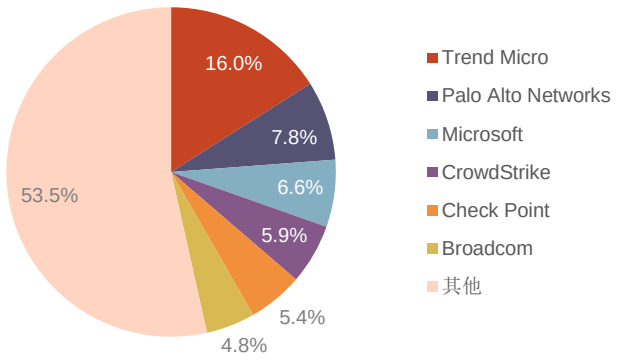
Trend Micro、Palo Alto Networks 等公司为全球云负载安全市场的龙头企业。根据 IDC 统计，2022 年全球云负载安全市场份额前六名为 Trend Micro、Palo Alto Networks、微软、CrowdStrike、Check Point 和 Broadcom，市场份额分别为 16.0%、7.8%、6.6%、5.9%、5.4%、4.8%。相比端点安全，云负载安全的市场份额更为分散，市占率前六名的公司占据了 46.5%的市场份额。

图 15：2022-2027E 各地区云负载安全市场规模（百万美元）



资料来源：IDC 预测，光大证券研究所整理

图 16：2022 年全球云负载安全市场份额



资料来源：IDC，光大证券研究所整理

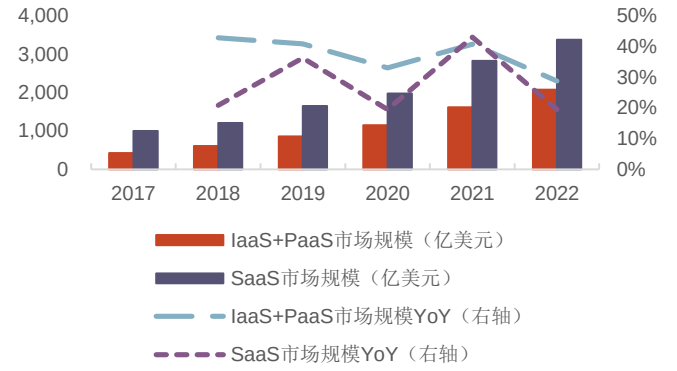
Palo Alto Networks、CrowdStrike 的云负载安全技术评估结果超越 Trend Micro 成为行业的领导者。由于全球公有云市场的快速发展，云负载安全的技术竞争格局尚不稳定。根据 Forrester 的 EDR 供应商技术评估，19Q4 的评估结果显示 Trend Micro 兼具强大的实时响应能力和策略性，McAfee 和 Bitdefender 同为 EDR 技术的领导者；24Q1 的评估结果显示 Trend Micro 难以维持行业领先的技术水平，而 Palo Alto Networks、CrowdStrike 成为新晋的 EDR 技术领导者，其中 Palo Alto Networks 具备更强的实时响应能力，CrowdStrike 具备更强的策略性。

图 17：19Q4、24Q1 Forrester 云负载安全供应商技术评估报告

资料来源：Forrester，纵轴代表实时响应的能力，横轴代表策略性。左图对应 19Q4,右图对应 24Q1。

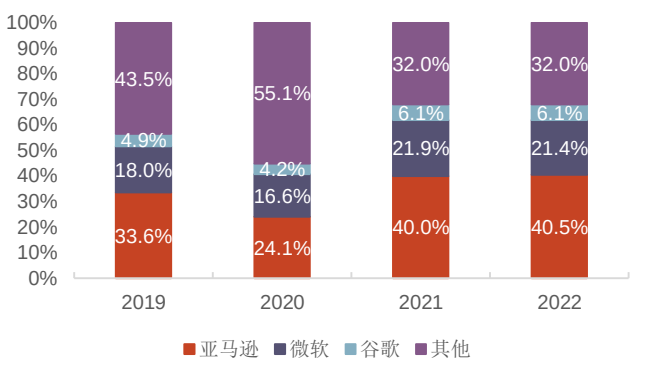
云负载安全的市场份额提高受益于全球公有云 IaaS+PaaS 市场规模的快速增长。2017-2022 年，全球公有云 IaaS+PaaS 市场收入维持 30%以上的增速；SaaS 市场收入 2022 年同比增长 19.5%。2022 年全球公有云 IaaS+PaaS+SaaS 市场收入为 5458 亿美元，同比增长 22.9%。**1）**随着全球化的拓展和跨地区合作的扩张，企业上云需求不断扩大。**2）**云服务所具有的节约运营成本、灵活的团队合作和简化工作流程的能力得到了更多企业的认可。2022 年大型企业贡献了超 50%的全球公有云市场份额。**3）**疫情带来企业对远程办公的广泛需求，经济的不确定性促使云服务提供商提升产品竞争力。

图 18：2017-2022 年全球公有云市场收入



资料来源：IDC，光大证券研究所整理

图 19：2019-2022 年全球公有云 IaaS+PaaS 市场份额



资料来源：IDC，光大证券研究所整理。市场份额按照收入口径计算

与传统的本地架构相比，公有云带来了更多网络安全挑战。云安全策略在许多方面与端点安全策略存在差别：**1）数据泄露：**在云中的发生方式与本地攻击不同，不依赖恶意软件，而是利用错误配置、访问不足、凭据被盗和其他漏洞。**2）混合云导致的可见性降低和管理分散：**在混合云和多云环境中的工作负载往往导致分散的控制和管理，从而在产生端点、工作负载、流量等环节产生监控盲点，留下安全漏洞；**3）配置错误：**在数据和资产向云端迁移的过程中，应用程序容易受到错误配置的影响，造成账户权限过于宽松、日志记录不足等安全漏洞。

表 11：企业在云环境中面临的安全挑战

挑战	具体介绍
数据泄露	数据泄露在云中的发生方式与本地攻击不同，与恶意软件不太相关。相反，攻击者会利用错误配置、访问不足、凭据被盗和其他漏洞。
可见性	为了满足不同的业务和运营需求，超过 80% 的组织使用多个云提供商，如果管理不当，可能会导致整个云环境缺乏可见性。这导致了分散的控制和管理，端点、工作负载和流量没有得到适当监控，留下的安全漏洞经常被攻击者利用。
动态工作负载	应用由许多工作负载（虚拟机、容器、Kubernetes、微服务、无服务器函数、数据库等）。如果不能正确保护工作负载中的每个环节，就会使应用程序和组织更容易受到攻击，延迟应用程序开发，影响生产和性能，阻碍业务发展。
配置错误	快速迁移会使应用程序容易受到错误配置的影响，这是云环境中的头号漏洞。错误配置会导致帐户权限过于宽松、日志记录不足以及其他安全漏洞，使组织面临数据泄露和内部威胁，以及利用漏洞访问公司的数据和网络的攻击者。
访问控制	使用多云环境的组织往往依赖于其云提供商的默认访问控制，这在多云或混合云环境中可能会成为一个问题。内部威胁可以利用特权访问、对攻击地点的了解以及隐藏其踪迹的能力造成很大的损害。
安全合规和审计	云合规性和治理以及行业、国际、地方法规非常复杂，云合规性存在于多个级别，并非同一方控制，使云合规性更具挑战性。

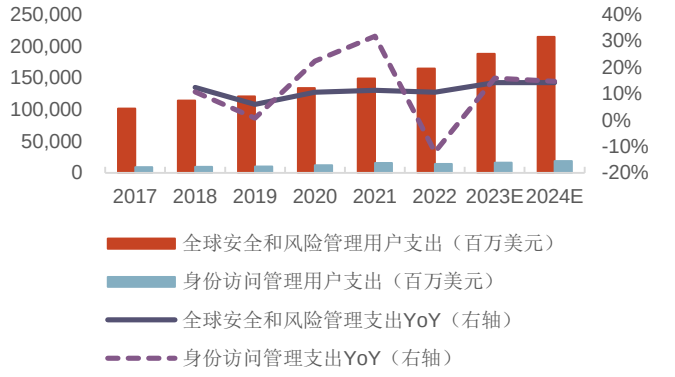
资料来源：CrowdStrike 公司官网，光大证券研究所整理

3.4 身份和访问管理（IAM）、安全信息和事件管理（SIEM）：市场相对成熟，竞争格局较为稳定

身份和访问管理（IAM）是网络安全的关键环节，确保得到授权的用户在正确的时间和地点访问特定资源。IAM 通常提供以下核心功能：**1）标识管理：**创建、储存和管理标识信息；**2）用户身份验证：**确认用户、计算机或软件组件身份，可为单个用户添加多重身份验证（MFA）或添加单一登录（SSO）身份验证；**3）用户授权和访问控制：**定义用户角色和权限，指定哪些用户有权访问哪些资源。

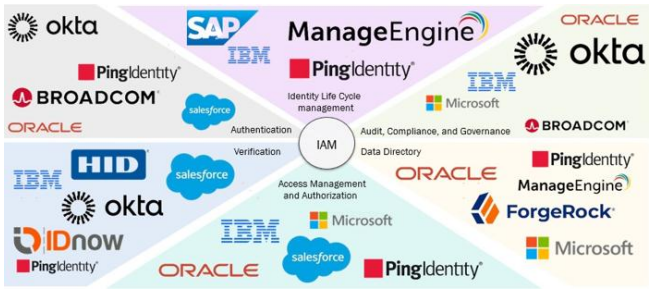
预计 2024-2032 年全球身份和访问管理市场规模将以 13.2%的复合增速增长。根据 Gartner，2023 年全球身份和访问管理市场规模约为 162 亿美元，预计 2032 年市场规模将增长至 493 亿美元，2024-2032 年复合增长率约为 13.2%。

图 20：2017-2024E 全球身份访问管理用户支出



资料来源：Gartner 预测，光大证券研究所整理

图 21：全球身份和访问管理各细分领域代表公司



资料来源：Markets and Markets

Okta、微软是身份和访问管理行业的领导者。根据 Gartner 魔力象限，身份和访问管理行业的领导者包括 Okta、微软、Ping Identity、ForgeRock 等公司，其中 Okta 具备较强的执行力，具备成熟的产品服务和稳定的客户群，微软则具备长远的战略目光，积极探索身份访问管理与 AI 等前沿技术结合。CyberArk、IBM、Micro Focus 等公司位于第二梯队。

图 22：Gartner 2021-2023 年身份和访问管理行业竞争格局的魔力象限图分析

资料来源：Gartner，横轴代表前瞻性，纵轴代表执行力，四象限分别代表：右上领导者、左上挑战者、左下利基者、右下远见者

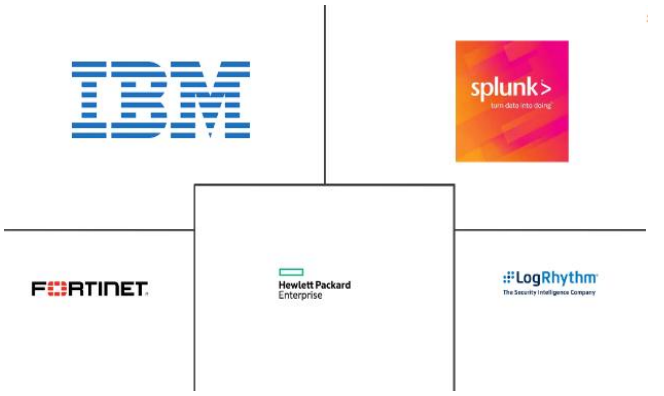
安全信息和事件管理（SIEM）是网络安全的重要组成部分，它通过提供实时分析来帮助企业检测潜在的安全威胁。SIEM 提供以下核心功能：**1）日志管理：**收集、存储和分析日志数据；**2）事件检测：**识别和通知潜在的安全事件；**3）事件响应：**对检测到的事件进行响应和调查。

预计 2024-2029 年全球安全信息和事件管理市场规模将以 17.11%的复合增速增长。根据 Mordor intelligence，2024 年全球安全信息和事件管理市场规模预计为 71.8 亿美元，预计 2029 年市场份额将增长至 158.2 亿美元，2024-2029 年复合增长率约为 17.11%。其中北美占据最大规模市场，而亚太市场规模增速最快。

图 23：2024-2029 年 SIEM 市场规模预测

资料来源：Mordor intelligence

图 24：SIEM 领域主要代表公司



资料来源：Mordor intelligence

Exabeam、Securonix、IBM 和 Splunk 是 2020-2022 的行业领导者。根据 Gartner 魔力象限，SIEM 行业的领导者包括 Exabeam、Securonix、IBM、Splunk 等公司，其中 Exabeam 具备较强的执行力，具备成熟的产品服务和稳定的客户群，IBM 则具备长远的战略目光，积极探索 SIEM 与 AI 等前沿技术结合。其他一些公司如 McAfee、Rapid7 等位于第二梯队。

图 25：Gartner 2020-2022 年安全信息和事件管理行业竞争格局的魔力象限图分析

资料来源：Gartner，横轴代表前瞻性，纵轴代表执行力，四象限分别代表：右上领导者、左上挑战者、左下利基者、右下远见者

3.5 安全访问服务边缘（SASE）：高速发展的新兴网络安全架构，相比传统架构更适应新需求

安全访问服务边缘（SASE）是云服务、边缘计算、混合网络等新趋势下的全新网络安全架构。SASE 可以为企业提供全网流量的可见性，包括本地、云、移动端访问应用和互联网的流量，并提供一系列丰富的网络安全功能。SASE 的概念最早在 2019 年由 Gartner 提出，Gartner 认为随着边缘计算、云服务和混合网络的兴起，传统网络安全架构已无法适用，常产生延迟、联网盲点、管理开销过大等问题，而 SASE 架构可以解决传统架构的复杂性和延迟性等问题。

表 12：SASE 模型的六个基本要素

基本要素	具体介绍
软件定义广域网（SD-WAN）	SD-WAN 是一种叠加架构，通过选择流向互联网、云应用程序和数据中心的流量的最佳路由来降低复杂性并优化用户体验，帮助企业快速部署新的应用和服务，以及跨距离管理策略。
安全 Web 网关（SWG）	SWG 可防止不安全的网络流量进入企业的内部网络，保护用户免受恶意 Web 流量、攻击网站、病毒、恶意软件和其他网络威胁的访问和感染。
云访问安全代理（CASB）	CASB 通过确保安全使用云应用和服务来防止数据泄露、恶意软件感染、法规不合规和缺乏可见性，保护托管在公有云、私有云或 SaaS 的云应用。
防火墙即服务（FWaaS）	FWaaS 将物理防火墙设备替换为云防火墙，提供高级防火墙功能和访问控制功能，例如 URL 过滤、高级威胁防御、入侵防御系统（IPS）和 DNS 安全。
零信任网络访问（ZTNA）	ZTNA 解决方案使远程用户能够安全地访问内部应用程序。使用零信任模型时从不假定信任，根据精细策略授予最低特权访问权限，为远程用户提供安全连接，无需将应用程序暴露在互联网上。
集中管理	通过从单个控制台管理上述所有内容，可以消除更改控制、补丁管理、协调中断窗口和策略管理方面的许多挑战，同时在整个组织中提供一致的策略。

资料来源：Zscaler 公司官网，光大证券研究所整理

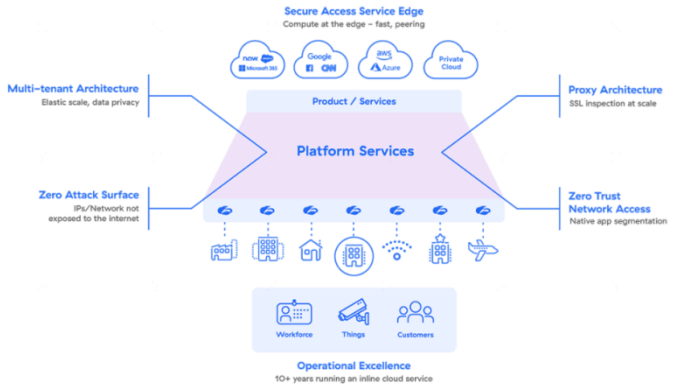
SASE 的核心技术包括边缘计算、零信任等。根据 CSA2022 年发布的《SASE 安全访问服务边缘白皮书》，SASE 有四个核心技术：边缘计算、零信任网络访问、网络即服务、安全即服务。

1）边缘计算：SASE 的低延迟特性要求处理节点尽量靠近企业和用户，因此与边缘计算密不可分。边缘计算为云计算能力下沉的一种新型计算模式，在更靠近数据源所在的本地计算，尽量不将数据回传到云端，以降低延迟、减轻云端压力。

2）零信任网络访问（ZTNA）：传统网络安全模型假设组织网络内所有事物都应受到信任，而 ZTNA 认为不能信任出入网络的任何内容，一旦进入网络，用户就可以自由地横向移动、访问和泄露权限之外的数据。ZTNA 环境下，企业应用程序在公网上不可见，通过信任代理建立企业应用程序和用户之间的链接，根据身份、属性和环境动态授予访问权限。

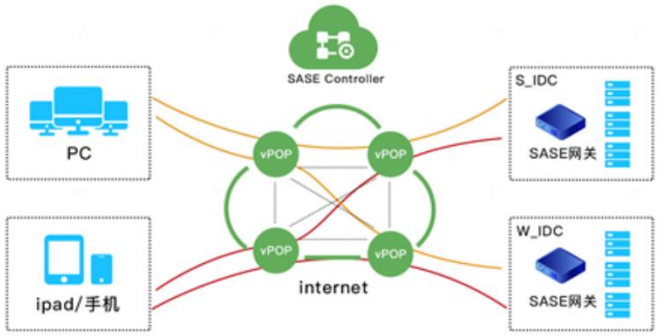
3）网络即服务、安全即服务：网络即服务指基于网络技术，实现用户终端、分支机构、企业总部、数据中心间的数据互通和网络管理能力，安全即服务指采用云原生架构快速部署安全功能，更灵活地进行扩容和迭代更新。SASE 的架构需要将网络即服务和安全即服务结合起来。

图 26：SASE 架构示意图



资料来源：Zscaler 公司官网

图 27：SASE Controller 基于零信任理念管理各终端访问权限

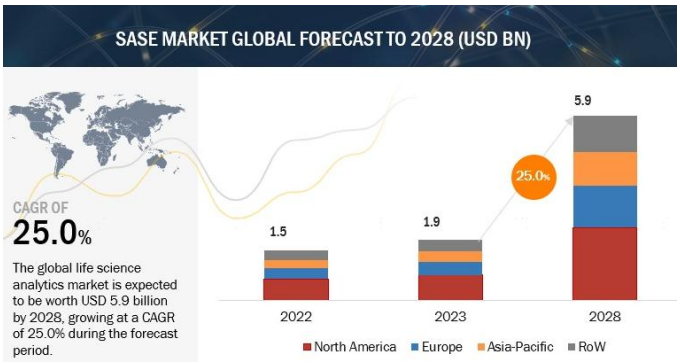


资料来源：CSA《SASE 安全访问服务边缘白皮书》

全球 SASE 市场规模有望快速增长。作为更加契合企业数字化转型需求的新型网络安全框架，SASE 市场具备较大的增长潜力。根据 Gartner 预测，到 2024 年全球至少 40%的企业将转变战略，尝试采用 SASE 架构，而 2018 年底仅有 1%的企业尝试 SASE 架构。根据 Markets and Markets 测算和预测，2023 年全球 SASE 市场规模约为 19 亿美元，2028 年市场规模有望达到 59 亿美元，23-28 年以 25%的复合增长率快速扩大市场规模。

Netskope、Zscaler、Palo Alto Networks 是安全服务边缘（SSE）行业领导者。安全服务边缘（SSE）是安全访问服务边缘（SASE）的一部分，专注于保护对云服务、私有应用程序和 Web 访问的解决方案。根据 Gartner 魔力象限，24M2 SSE 行业的领导者包括 Netskope、Zscaler、Palo Alto Networks，同时具备强大的执行力和长远的战略目光。

图 28：2022-2028E 全球 SASE 市场规模预测



资料来源：Markets and Markets

图 29：Gartner 24M2 SSE 行业竞争格局的魔力象限图分析

资料来源：Gartner，横轴代表前瞻性，纵轴代表执行力，四象限分别代表：右上领导者、左上挑战者、左下利基者、右下远见者

4、 投资建议

我们认为，随着企业数字化转型的不断推进，在云计算、物联网、AI 等产业趋势下，传统网络安全架构难以适应，新兴的网络安全架构蓬勃发展，有望持续引发行业竞争格局的变化，使更加有竞争力的供应商脱颖而出。在本轮生成式 AI 的浪潮下，网络安全面临广泛而深刻的变革，网络攻击门槛降低的同时，AI 技术提升了威胁检测能力，并提供自动化安全评估和漏洞修复等功能，大幅降低安全员的使用门槛。**看好 AI 赋能网络安全行业，首次覆盖给予网络安全行业“买入”评级，推荐微软（MSFT.O）、CrowdStrike（CRWD.O），建议关注 Zscaler。**

4.1 微软：受益于供应商整合趋势，基于 Azure 云平台提供全面的网络安全支持

微软网络安全业务的竞争优势在于多样化的综合性解决方案，以及与微软产品生态的深度集成。22 年微软网络安全业务收入超过 200 亿美元。截至 23Q4，微软网络安全业务已拥有超过 100 万用户，其中 70 万用户使用四款以上的安全产品。微软所提供的综合性解决方案满足了企业在大部分场景下的安全需求，集成在 Windows 操作系统、Azure 云平台和 Microsoft 365 企业服务等微软产品生态中。同时，微软生态的广泛用户基础和海量的安全数据为微软提供丰富的反馈，进一步提升 AI 威胁检测、分析和响应的能力。

微软主要网络安全产品包括：1）Microsoft Defender：提供端点保护和综合性的云安全解决方案，抵御终端、应用程序、云工作负载的网络威胁；**2）Microsoft Entra：**提供身份和访问管理服务，包括权限管理、身份验证、网络访问审查等功能；**3）Microsoft Sentinel：**提供安全信息和事件管理服务，以及安全业务流程、自动化和响应解决方案；**4）Microsoft Purview：**提供数据治理和合规性服务，包括数据分类、数据丢失防护等功能；**5）Microsoft Priva：**提供隐私管理服务，包括隐私风险管理、数据访问和控制等功能；**6）Microsoft Intune：**提供企业移动端管理和统一端点管理服务，帮助企业管理移动设备安全。

表 13：微软主要网络安全产品介绍及各细分领域主要竞争对手

产品名称	分类	具体介绍	主要竞争对手
Microsoft Defender	端点保护（EEP） 综合云安全服务	综合性威胁防护解决方案，提供对终端、应用程序、云工作负载的保护，通过自动化安全管理和实时威胁检测抵御网络威胁	CrowdStrike
Microsoft Entra	身份和访问管理（IAM）	提供权限管理、身份验证、网络访问审查等具体功能，帮助企业管理用户和设备访问权限，保护敏感信息和资源	Okta、Ping Identity
Microsoft Sentinel	安全信息和事件管理（SIEM）安全自动化响应（SOAR）	安全业务流程、自动化和响应解决方案，提供智能的安全分析和威胁检测，帮助企业快速识别、调查和响应网络安全威胁	IBM、Splunk
Microsoft Purview	数据治理和合规性	数据治理和合规性服务，帮助企业管理数据，确保遵守全球数据保护法规，功能包括数据分类、数据丢失防护（DLP）等	Informatica、Varonis
Microsoft Priva	隐私管理	帮助企业更好地管理个人信息的使用与共享，以符合全球隐私法规，功能包括隐私风险管理、数据访问和控制等	OneTrust、TrustArc
Microsoft Intune	企业移动端管理（EMM） 统一端点管理（UEM）	基于云的终端管理安全服务，帮助企业管理移动设备和移动应用程序，确保企业数据的安全	Vmware、Sophos

资料来源：微软官网，光大证券研究所整理

Copilot for Security 将微软的综合网络安全服务和先进的大模型结合，协助企业应对安全威胁和评估风险。微软于 2024 年 4 月 1 日推出 Copilot for Security，采用按需付费的灵活定价模式，使企业客户可以根据自身需求和预算控制使用量和成本，AI 副驾驶助手将可触达微软丰富而全面的网络安全功能，通过更加灵活的方式应对网络威胁，快速评估风险暴露。

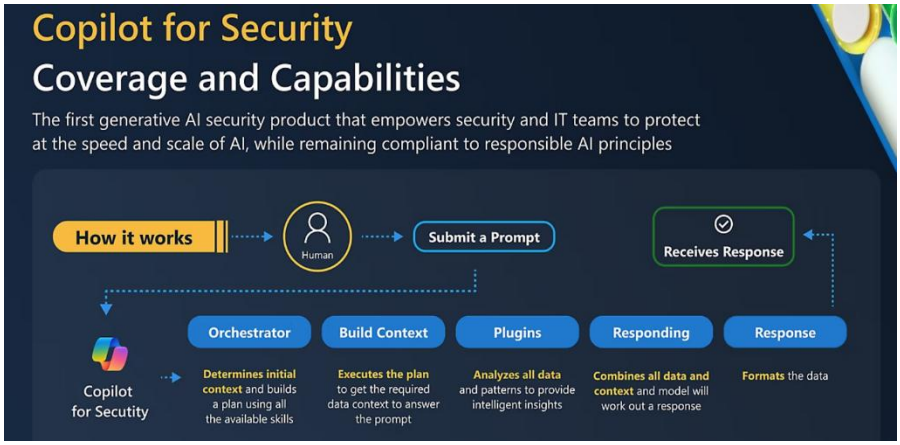
表 14：Copilot for Security 在微软安全产品中提供的具体功能

微软安全产品	Copilot for Security 的具体功能
Microsoft Defender	1）Copilot 可以总结事件，评估其影响，提供可操作的建议，并生成一份响应报告。 2）提升安全员技能，使员工能够完成威胁猎取、恶意软件逆向工程等复杂任务。 3）以自然语言询问安全威胁和风险暴露情况，提前预防和迅速响应。
Microsoft Entra	1）使用自然语言快速调查身份风险。 2）查找访问策略中的漏洞，快速找到问题的根源。 3）大幅简化登录日志分析等复杂手动的操作。
Microsoft Sentinel	1）评估新威胁及风险暴露情况，提供 AI 驱动见解和响应方案。 2）为安全员提供事件摘要、事件影响的评估、操作建议等。 3）降低高级安全运营功能的操作门槛，例如将自然语言分析恶意脚本。
Microsoft Purview	1）快速深入了解相关的合规监管要求。 2）快速总结和长内容的警报，以数据安全和合规政策的视角进行审查。 3）通过自然语言搜索降低操作门槛，无需使用特定的查询语言。
Microsoft Intune	1）提供 AI 驱动见解和响应方案。 2）预先设置针对性策略，通过假设分析、AI 指导以及对设备、用户和应用状态的深入理解解决终端问题。

资料来源：微软公司官网，光大证券研究所整理

Copilot for Security 的使用流程为：1）用户向 Copilot for Security 提交自然语言指示，确定初始提示词，利用可用工具制定计划。**2）**执行计划以获取网络安全相关数据，通过插件进行数据分析，提供智能见解。**3）**结合所有数据和分析，由大模型解析出响应手段。

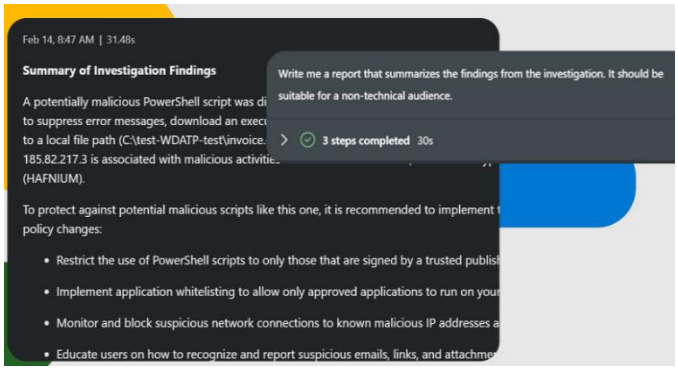
图 30：Copilot for Security 使用流程



资料来源：微软官方博客

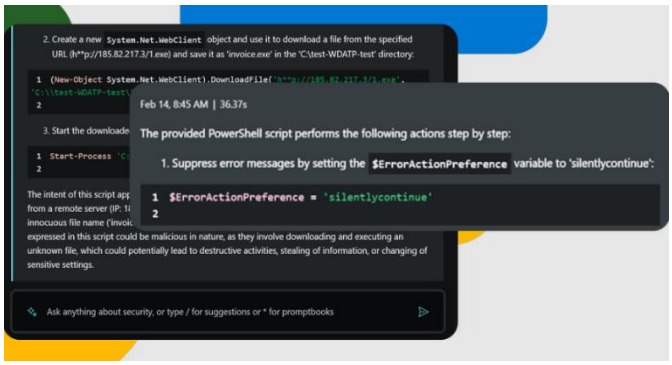
Copilot for Security 用户使用反馈较为积极。根据微软官方调研，安全工作的新手在使用 Copilot for Security 时任务准确率提高了 35%，工作效率提高了 26%；经验丰富的安全专业人员使用 Copilot 时任务准确率提高了 7%，工作速度提高了 22%，97%的人表示希望下次执行相同的任务时使用 Copilot。

图 31：Copilot for Security 总结长文本安全报告



资料来源：微软官方博客

图 32：Copilot for Security 使用自然语言进行复杂操作



资料来源：微软官方博客

投资建议：微软提供综合的网络安全服务，涵盖端点安全、云安全、IAM、SIEM 等多个产业链环节，拥有深厚的技术壁垒和丰富的安全响应数据。Gartner、Forrester 等第三方机构评估结果显示，微软在端点安全、云安全、IAM 等领域均处于行业领导者的位置。同时，作为云供应商的微软在 MaaS 服务领域具备一定的技术壁垒和先发优势，Azure AI 已成为微软云服务收入增速的重要驱动力，微软的云安全业务也将受益于 AI+云服务的蓬勃发展。

我们维持 24-26 财年收入预测 2484.7/2878.6/3246.9 亿美元，维持 24-26 财年净利润预测 871.9/985.4/1124.1 亿美元，维持“买入”评级。

表 15：微软盈利预测与估值简表

指标	FY2022	FY2023	FY2024E	FY2025E	FY2026E
营业收入（亿美元）	1,982.7	2,119.2	2,484.7	2,878.6	3,246.9
营业收入同比增速	18.0%	6.9%	17.2%	15.9%	12.8%
净利润（亿美元）	727.4	723.6	871.9	985.4	1,124.1
净利润同比增速	18.7%	-0.5%	20.5%	13.0%	14.1%
EPS（美元）	9.70	9.72	11.73	13.26	15.13
P/E	46	46	38	34	30

资料来源：彭博，光大证券研究所预测，股价时间 2024-06-17，微软财年为上一年度 7 月 1 日至本年度 6 月 30 日

风险提示：网络安全负面事件风险、网络安全行业竞争加剧风险、AI 技术发展不及预期、与 OpenAI 绑定过深的风险。

4.2 CrowdStrike：基于云原生平台的端点安全领导者

4.2.1 公司基于云原生平台提供网络安全 SaaS 服务

CrowdStrike 成立于 2011 年，顺应云时代网络安全新需求，逐渐发展为涵盖端点安全、IT 运维、威胁检测、应急响应等丰富云功能的网络安全 SaaS 服务公司。公司构建了 CrowdStrike Falcon 平台作为网络安全问题的多租户、云原生、智能的安全解决方案，检测威胁并阻止入侵；Falcon 平台能够保护在笔记本电脑、台式机、服务器、虚拟机和物联网设备等终端上运行的工作负载，包括本地、虚拟化和云环境。平台目前提供 27 个云模块，采用 SaaS 模式，涵盖多个大型安全市场，包括企业终端安全、安全和 IT 运维、托管安全服务、可观测性、云安全、身份保护、威胁情报、数据保护和网络安全生成 AI 等细分领域。

表 16：CrowdStrike 公司发展历程与大事件梳理

时间	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	推出下一代防病毒云模块（NGAV）
2017 年 2 月	推出 IT 卫生云模块（IThygiene）,开启多产品市场策略
2017 年 7 月	推出恶意软件搜索云模块（Malware search）
2017 年 11 月	建立基金会
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
2019 年 6 月	纳斯达克交易所上市
2019 年 11 月	推出防火墙管理模块
2020 年 2 月	推出云工作负载保护模块、端点恢复服务
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
2022 年 8 月	Falcon 平台已发展到 27 个云模块,包括企业终端安全、安全和 IT 运营、托管安全服务、可观测性、云安全、身份保护、威胁情报、数据保护和网络安全生成 AI

资料来源：CrowdStrike 公司官网，光大证券研究所整理

CrowdStrike 的主营业务基于 SaaS 的网络安全解决方案，改变传统的本地化安全解决方案，围绕云原生平台 Falcon 提供丰富的网络安全服务。

1）云安全：包括 Falcon Cloud、Falcon Horizon、Bionic 产品，提供漏洞保护、威胁检测等功能。

2）端点安全和 XDR：包括 Falcon Prevent、Falcon Insight XDR 等，提供防病毒功能、跨域强测、物联网、OT、医疗设备等的保护。

3）风险暴露管理：包括 Falcon Discover、Falcon Spotlight、Falcon Surface 等，实时识别客户端点中存在的漏洞，发现和映射所有面向互联网的资产。

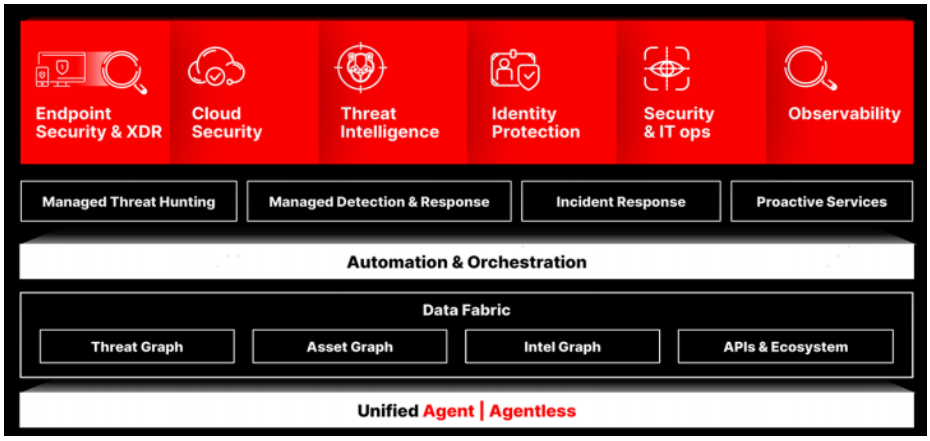
4）威胁情报和分析：包括 Falcon Intelligence、Falcon Sandbox 等，将威胁情报集成到端点保护中，并对检测到的威胁进行自动分析。

5）身份保护：包括 Falcon Identity Threat Protection、身份威胁检测等，可以分辨和预防基于身份的攻击和异常。

6）IT 运维管理：包括 Falcon for IT、Falcon Foundry 等，将安全和 IT 运营与融合进统一平台，降低用户创建定制化网络安全应用程序的门槛。

7）生成式 AI：Charlotte AI 拥有自然语言处理的能力，帮助安全分析师做出更快、更准确的决策。

图 33：CrowdStrike Falcon 平台细分功能



资料来源：CrowdStrike 公司官网

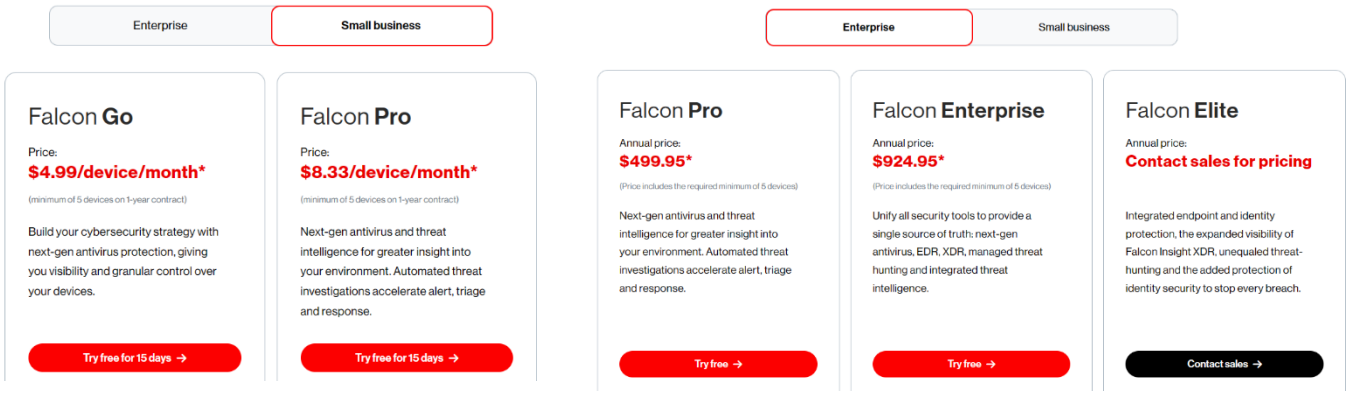
表 17：CrowdStrike Falcon 平台的细分功能和具体产品服务

类别	产品	描述
云安全	Falcon 云负载保护	在运行时为工作负载和容器事件以及实例元数据提供全面的漏洞保护
	Falcon Horizon	为多云环境提供统一的可见性、威胁检测以及持续监控和合规性
	Bionic	通过收购应用安全态势管理（ASPM）的先驱 Bionic，扩展云原生应用程序保护方面的能力
端点安全和 XDR	Falcon Prevent	为客户提供下一代防病毒功能，提供全面的保护
	Falcon Insight XDR	以行业领先的 EDR 为核心，通过一个统一的、以威胁为中心的事件工作台，综合跨域遥测
	Falcon Insight XDR for IoT	对整个企业的物联网、OT、医疗设备、工业物联网和连接设备进行保护、检测和响应
	Falcon 设备控制	为管理员提供了对 USB 外围设备的高度可见性和精细控制
	Falcon 防火墙管理	提供对主机操作系统原生防火墙功能的集中管理
	Falcon Data Protection	通过跟踪内容的自动策略实施来阻止对手和恶意内部人员窃取敏感信息
风险暴露管理	Falcon Exposure Management	整合来自 Falcon Discover、Falcon Spotlight 和 Falcon Surface 的安全功能和 IT 数据集
	Falcon Discover	可识别托管、非托管和恶意系统以及应用程序及其在客户网络中的使用情况
	Falcon Spotlight	实时识别客户端点中存在的漏洞
	Falcon Surface	允许客户发现和映射所有面向互联网的资产
	Falcon Forensics	基于 CrowdStrike 多年的事件响应经验和取证调查服务，简化了时间点和历史取证分类数据的收集
	Falcon FileVantage	通过构建其他代理通常提供的服务来降低合规性的复杂性
托管服务	Falcon Complete	为我们的客户提供全面的监控、管理、响应和修复解决方案
反对手行动	Falcon OverWatch	是一种威胁搜寻解决方案，由一支由专门的安全专家组成的精英团队组成
Falcon Intelligence	Falcon Intelligence	将威胁情报集成到端点保护中，并对检测到的威胁进行自动分析
	Falcon 搜索引擎	使客户能够实时搜索在我们的 Falcon 平台中收集的恶意软件
	Falcon Sandbox	允许客户通过在虚拟机中安全地引爆未知文件来分析它们是否存在恶意行为
	Falcon Intelligence Recon	使客户能够识别和减轻清晰、深层和暗网隐藏区域的数字风险
身份保护	Falcon Identity Threat Protection	使用身份、行为和风险分析，通过实时威胁防御和 IT 策略实施来阻止基于身份的攻击
	Falcon 身份威胁检测	提供基于身份的攻击和异常的可见性，将实时流量与行为基线和规则进行比较
SIEM 和日志管理	Falcon LogScaleSIEM	完整的 SOC 平台，旨在通过 AI 原生检测、调查和响应来阻止违规行为
IT 自动化	Falcon for IT	将安全和 IT 运营与单一代理和统一平台融合在一起
生成式 AI	Charlotte AI	AI 对话助手，通过自然语言处理帮助安全分析师用简单、通俗易懂的问题做出更快、更准确的决策
应用开发	Falcon Foundry	无代码应用程序开发平台，允许客户快速创建自己的应用程序，以解决自定义安全和 IT 用例

资料来源：CrowdStrike 官网，光大证券研究所整理

CrowdStirke 针对不同企业规模和细分功能，提供五种订阅方案。1）针对小型企业，CrowdStrike 提供 4.99 美元/设备/月的 Falcon Go 和 8.33 美元/设备/月的 Falcon Pro，按设备数量进行收费。2）针对大型企业，CrowdStrike 提供年费 499.95 美元的 Falcon Pro 和 924.95 美元的 Falcon Enterprise，当公司设备量超过 9 台时采购年费企业版更为优惠。

图 34：CrowdStrike Falcon 平台定价方案



资料来源：CrowdStrike 官网，光大证券研究所整理

表 18：CrowdStrike Falcon 平台各付费层提供的功能

产品	小型企业	大型企业	相比上一付费层新增功能
Falcon Go	$4.99/设备/月		**防病毒：**保护设备免受恶意软件、勒索软件的威胁。 **设备控制：**提供对 USB 设备的可见性和精确控制。 **快速支持：**可协助中小型企业解决安装和运营问题。
Falcon Pro	$8.33/设备/月	$499.95/年（≥5 台设备）	**集成威胁情报：**丰富平台检测到的事件和事故。 **防火墙管理：**简化主机防火墙管理。 **CrowdStrike Marketplace：**访问应用程序和集成，管理风险并构建网络安全生态系统。
Falcon Enterprise		$924.95/年（≥5 台设备）	**终点检测响应：**提供持续、全面的端点可见性，自动检测恶意活动并智能确定优先级。 **威胁搜寻：**在平台内不断寻找复杂入侵的微弱迹象。
Falcon Elite		非固定价格	**IT Hygiene：**实时识别环境中任何位置的未经授权的帐户、设备、IoT/OT 系统和应用程序，加快修复速度，改善整体安全状况。 **身份认证保护：**通过结合高级 AI、行为分析和灵活的策略引擎的强大功能来实施基于风险的条件访问，实现超准确的威胁检测和基于身份的攻击的实时防御。
Falcon MDR		非固定价格	24 小时专业咨询，跨端点、身份、云工作负载和 XDR 连接提供托管的威胁检测和响应。

资料来源：CrowdStrike 公司官网，光大证券研究所整理

4.2.2 Charlotte AI 协助发现潜在安全漏洞，应对 AI 时代网络安全新需求

生成式 AI 工具 Charlotte AI 通过模拟复杂的攻击场景发现企业潜在的安全漏洞，提升员工的安全意识。23 年 5 月 CrowdStrike 发布生成式 AI 功能 Charlotte AI，旨在降低 Falcon 平台的技术门槛，提高安全分析师的工作效率。CrowdStrike 收集了全球大量的安全事件和来自用户、设备、云工作负载的威胁情报，以及特有的人工反馈情报，构成 Charlotte AI 的核心竞争力。**Charlotte AI 的主要功能包括：1）**通过生成逼真的攻击场景，帮助企业在实际受到攻击之前发现潜在的安全漏洞；**2）**模拟复杂的网络攻击手段，帮助企业提前准备应对策略，从而增强其网络防御能力；**3）**通过与 Charlotte AI 的互动训练，提高企业员工的网络安全意识，这在防范依赖于人为因素的攻击手段时尤为重要。

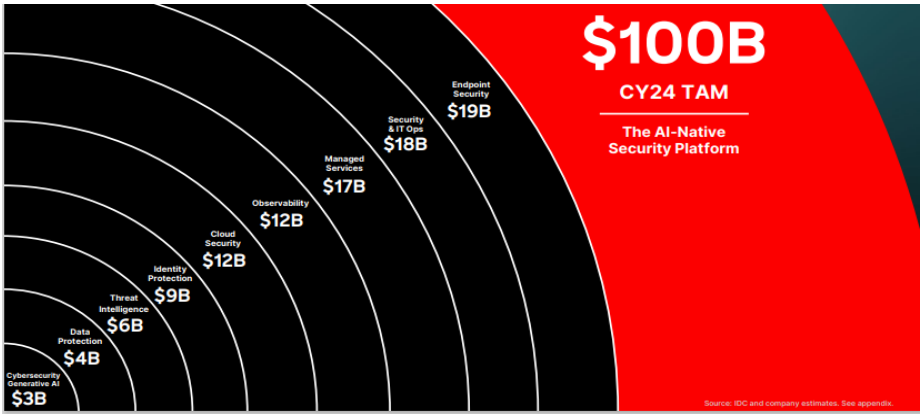
表 19：Charlotte AI 与 Falcon 平台的集成联动优势

优势	具体介绍
XDR 平台强化	CrowdStrike 的 XDR 平台通过集成生成式 AI 功能，利用其高保真数据优势，能够为整个 Falcon 平台提供更为强大的安全防护，使得安全检测和响应更加迅速和精准，从而提高了整体网络安全水平。
威胁检测能力提升	AI 技术的引入，尤其是机器学习和行为分析的结合，使得 CrowdStrike 在检测未知威胁方面的能力得到了显著提升。这一点对于传统的 EDR、防火墙、APT 等产品来说是一个重大的进步，因为它超越了传统病毒引擎的局限性。
自动化智能运维	Charlotte AI 的引入还意味着 CrowdStrike 在自动化智能运维方面迈出了重要一步。这种基于 AI 的运维模型类产品旨在实现智能化的自动化操作，减少人工干预，提高效率和准确性。
应对 AI 网络攻击	随着人工智能网络攻击的激增，通过 Charlotte AI 等技术的应用不仅体现在对传统攻击手段的防御上，更在于对新兴 AI 驱动的攻击手段的有效应对。
提升员工安全意识	通过与 Charlotte AI 的互动训练，企业员工的网络安全意识可以得到提高，这在防范社会工程学等依赖于人为因素的攻击手段时尤为重要。
适应性强	Charlotte AI 可以根据网络环境的变化自动调整防御策略，使得 CrowdStrike 的安全解决方案具有很高的适应性。

资料来源：CrowdStrike 公司官网，光大证券研究所整理

除 Charlotte AI 外，Falcon Data Protection 等新产品也为客户提供 AI 技术帮助。当敏感数据被复制、粘贴或上传到基于网络的商业 GenAI 工具时，可以立即阻止数据泄漏；CrowdStrike 通过 Falcon for IT 结合安全与信息技术释放生成性人工智能的变革力量，为现代网络安全的未来保驾护航。

图 35：24 年 AI 原生安全平台和细分领域的 TAM



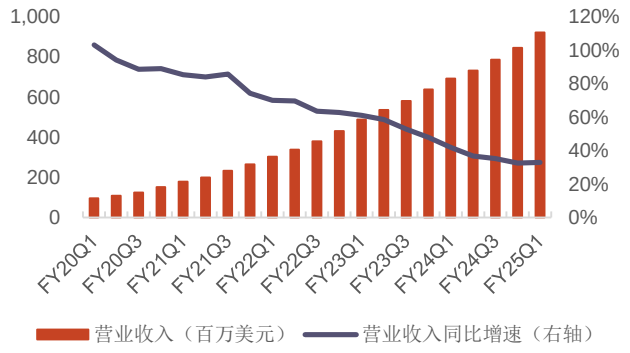
资料来源：CrowdStrike 官网

24 年以来美国企业更加重视 AI 大规模普及背后的数据治理、网络安全等问题，CrowdStrike 作为领先的 AI 驱动云原生平台，丰富的平台安全数据构成其重要的竞争壁垒。24M3 CrowdStrike 宣布与英伟达合作，在 Falcon 平台提供英伟达 AI 计算服务。客户可以使用该服务创建定制化 AI 模型，更加契合 AI 时代数据安全和网络安全的要求。Falcon 平台使用其独特而丰富的网络威胁情报数据，帮助用户构建和训练 AI 网络安全模型，以及开发 AI 驱动的网络安全应用程序，监测网络安全漏洞，主动防御可能出现的攻击。

4.2.3 财务分析：营收维持高增速，营业利润率转正

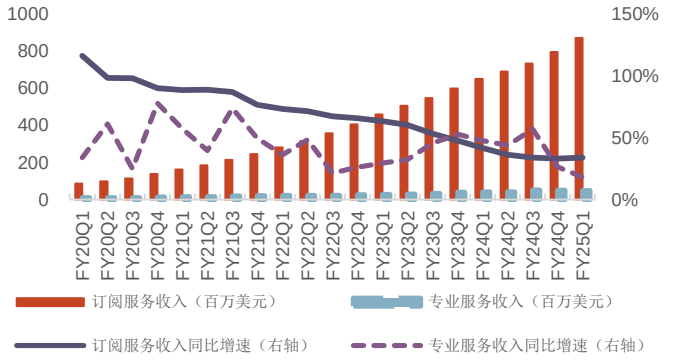
CrowdStrike 收入以订阅服务为主，近五年公司营收稳步增长。CrowdStrike 财年为上一年度 2 月 1 日至本年度 1 月 31 日。FY25Q1 公司实现营业收入 9.2 亿美元（高于 Refinitiv 一致预期 1.8%），同比增长 33%，FY20Q1-FY25Q1 营收同比增速从 103%平稳放缓至 33%。FY25Q1 公司订阅服务收入 8.7 亿美元，占公司营业收入的 95%，专业服务收入占比较低。

图 36：FY20Q1- FY 25Q1 CrowdStrike 营业收入与同比增速



资料来源：CrowdStrike 公司公告，光大证券研究所整理

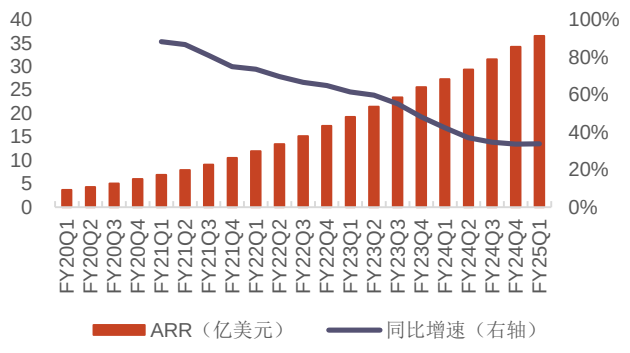
图 37：FY 20Q1- FY 25Q1 CrowdStrike 分部门收入与同比增速



资料来源：CrowdStrike 公司公告，光大证券研究所整理

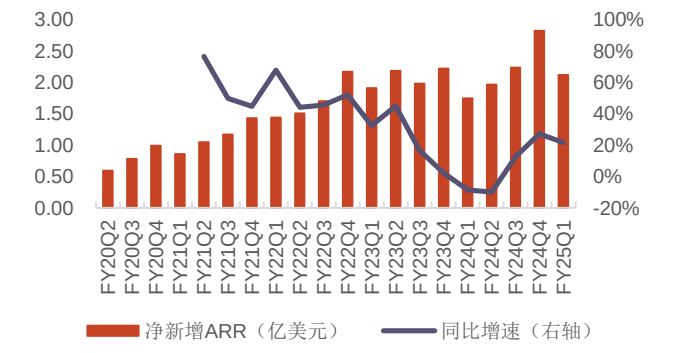
作为衡量收入成长性和稳定性的重要指标，CrowdStrike 的 ARR 和净新增 ARR 保持稳健增长。FY21Q1-FY25Q1，公司 ARR 同比增速从 88.2%逐步放缓至 33.7%，同期的 ARR 同比增速与营业收入增速基本持平。从净新增 ARR 来看，FY23Q2-FY24Q2 的净新增 ARR 同比增速呈放缓趋势，对应 22 年和 23H1 美国宏观经济预期不振、企业削减 IT 支出的背景。FY24Q3-FY24Q4 公司的净新增 ARR 同比增速大幅回暖至 27.2%，反映出企业网络安全需求的复苏。

图 38：FY 20Q1- FY 25Q1 CrowdStrike ARR 与同比增速



资料来源：CrowdStrike 公司公告，光大证券研究所整理

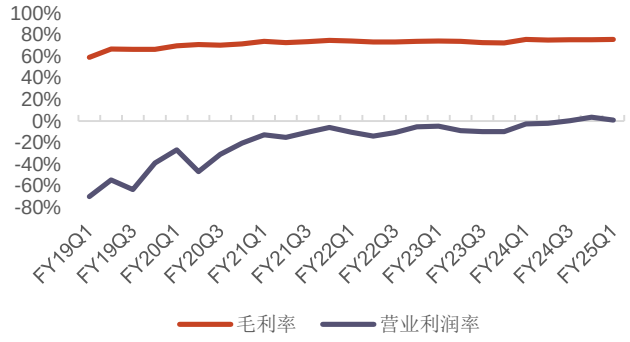
图 39：FY 20Q2- FY 25Q1 CrowdStrike 净新增 ARR



资料来源：CrowdStrike 公司公告，光大证券研究所整理

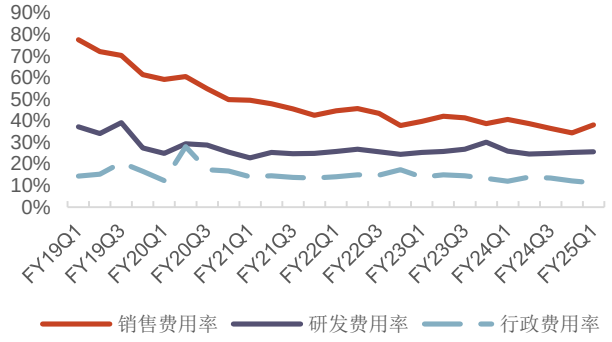
净利润大幅超预期，营业利润率转正。FY25Q1 公司实现归母净利润 4626 万美元。FY24Q1-FY24Q4 公司毛利率稳定在 75%左右，营业利润率 FY24Q3 首次实现转正，销售费用率从 F19Q1 的 77.4%大幅下降到 FY25Q1 的 38.0%，研发费用率、行政费用率也呈下降趋势。

图 40：FY 19Q1- FY 25Q1 CrowdStrike 毛利率与营业利润率



资料来源：CrowdStrike 公司公告，光大证券研究所整理

图 41：FY 19Q1- FY 25Q1 CrowdStrike 费用率



资料来源：CrowdStrike 公司公告，光大证券研究所整理

4.2.4 盈利预测与估值评级

收入拆分关键假设：CrowdStrike 的营业收入以订阅收入为主，22-24 财年订阅收入占公司营收比例分别为 93.7%、94.2%、93.9%，专业服务收入占公司营收比例分别为 6.3%、5.8%、6.1%。

1）净新增 ARR、订阅收入关键假设：作为衡量 SaaS 公司收入稳定性的重要先验指标，公司的净新增 ARR 在 21-24 财年分别同比增长 60.7%、51.1%、22.1%、6.0%。24 财年净新增 ARR 增速明显放缓，主要系 23H1 美国宏观经济逆风，企业普遍削减 IT 支出，使网络安全公司获得新客户更具挑战性，FY24Q1、FY24Q2 公司净新增 ARR 同比分别下降 8.6%和 10.0%，但 FY24Q3、FY24Q4 公司净新增 ARR 同比增速回暖至 12.6%、27.2%。考虑到生成式 AI 的快速发展使网络安全攻防升级，25 财年全球企业客户 IT 支出调研显示网络安全需求强劲增长，我们假设 25-27 财年净新增 ARR 分别同比增加 18%、16%、15%。

21-24 财年公司净新增 ARR 和订阅收入净增长的比例分别为 1.22、1.23、1.10、1.16，考虑到随着公司客户群逐渐稳定，净新增 ARR 转化为订阅收入的比例总体呈下降趋势，我们假设 25-27 财年净新增 ARR/订阅收入净增长的比例分别为 1.16、1.14、1.13。综上，25-27 财年公司订阅收入同比增速分别为 31.1%、28.1%、25.4%。

2）专业服务收入关键假设：21-24 财年公司专业服务收入同比增速分别为 54.7%、31.9%、40.8%、42.8%。随着公司订阅用户数的增加和产品矩阵的逐渐成熟，公司专业服务收入有望得到持续提振，使专业服务收入增速高于订阅收入。但考虑到专业服务收入基数逐渐扩大，我们假设 25-27 财年公司专业服务收入同比增速呈逐年下降趋势，分别为 20%、17%、16%。

综上，我们预测公司 25-27 财年营业收入分别为 39.86、50.80、63.47 亿美元，同比分别增长 30.4%、27.5%、24.9%。

表 20：CrowdStrike 分部门营收及指标预测表（单位：百万美元）

	FY23	FY24	FY25E	FY26E	FY27E
营业收入	2,241.2	3,055.6	3,985.5	5,079.9	6,347.3
订阅收入	2,111.7	2,870.6	3,763.5	4,820.1	6,046.0
净新增 ARR	830.0	880.0	1,038.4	1,204.5	1,385.2
净新增 ARR 同比增速	22.1%	6.0%	18.0%	16.0%	15.0%
净新增 ARR/订阅收入净增长	1.10	1.16	1.16	1.14	1.13
专业服务收入	129.6	185.0	222.0	259.7	301.3
营业收入增速	54.4%	36.3%	30.4%	27.5%	24.9%
订阅收入增速	55.3%	35.9%	31.1%	28.1%	25.4%
专业服务收入增速	40.8%	42.8%	20.0%	17.0%	16.0%

资料来源：CrowdStrike 公司公告，光大证券研究所预测

毛利率关键假设：1）订阅服务毛利率：21-24 财年公司订阅服务毛利率分别为 77.0%、76.3%、75.8%、78.0%，呈先降后升的趋势。考虑到 SaaS 产品的收入成本主要由服务器和基础设施的建设和维护升级成本构成，随着时间的推移边际成本逐渐降低，我们假设 25-27 财年订阅服务毛利率呈上升趋势，分别为 78.5%、78.8%、80.0%。**2）专业服务毛利率：**21-24 财年公司专业服务毛利率分别为 36.5%、33.4%、30.9%、32.4%，呈先降后升的趋势。考虑到专业服务通常为非标准化服务，22-24 财年毛利率相对稳定，我们取 22-24 财年的平均值 32.2%作为 25-27 财年专业服务毛利率的预测值。

费用率关键假设：1）销售费用率：21-24 财年公司销售费用率分别为 45.9%、42.5%、40.4%、37.3%，呈下降趋势。考虑到 SaaS 公司前期需要投入较高的销售费用以累积客户，形成用户粘性后即可持续贡献收入，我们预测 25-27 财年公司销售费用率维持下降趋势，分别为 35%、34.5%、33%；**2）行政费用率：**21-24 财年公司行政费用率分别为 13.9%、15.4%、14.2%、12.9%，我们假设 25-27 财年行政费用率维持 12%的水平。**3）研发费用率：**21-24 财年公司研发费用率分别为 42.5%、14.8%、27.1%、25.2%，23-24 财年研发费用率回升主要系公司持续探索 AI 与网络安全产品的结合形式。随着公司产品技术逐渐成熟，我们假设 25-27 财年公司研发费用率呈下降趋势，分别为 24.5%、24.0%、23.8%。

综上，我们预测公司 25-27 财年归母净利润分别为 2.01、3.33、5.85 亿美元，同比分别增长 125.0%、65.5%、75.8%。

表 21：CrowdStrike 分部门毛利率与费用率预测表

	FY23	FY24	FY25E	FY26E	FY27E
毛利率	73.2%	75.3%	75.9%	76.4%	77.7%
订阅服务毛利率	75.8%	78.0%	78.5%	78.8%	80.0%
专业服务毛利率	30.9%	32.4%	32.2%	32.2%	32.2%
销售费用率	40.4%	37.3%	35.0%	34.5%	33.0%
行政费用率	14.2%	12.9%	12.0%	12.0%	12.0%
研发费用率	27.1%	25.2%	24.5%	24.0%	23.8%
归母净利润（百万美元）	-183.2	89.3	201.0	332.6	584.6
同比增长率	-	-	125.0%	65.5%	75.8%

资料来源：CrowdStrike 公司公告，光大证券研究所预测

相对估值：由于 SaaS 公司具备前期销售成本高、后期盈利能力可观的特点，网络安全领域的多家 SaaS 公司收入增长强劲，具备持续的成长能力，我们采用 PSG 估值法，选取主营业务同为端点安全的 SaaS 公司 Palo Alto Networks、Fortinet、Check Point 作为可比公司。可比公司在网络安全相关技术评估中均位于行业前列，拥有丰富的产品阵营和一定的技术壁垒，商业模式稳定，下一财年 PSG 估值位于 0.7-1.2 之间，平均值为 0.9。CrowdStrike 现价对应 25 财年 PSG 约为 0.9 倍，与可比公司 PSG 平均值大致持平。

表 22：CrowdStrike 相对估值表

证券代码	公司名称	总市值（百万美元）	营收（百万美元）				23-26 年 CAGR	1FY 估值	
			当前财年	1FY（E）	2FY（E）	3FY（E）		PS	PSG
PANW.O	Palo Alto Networks	102,745	6,893	8,000	9,129	10,660	15.6%	12.8	0.8
FTNT.O	Fortinet	46,432	5,305	5,800	6,547	7,500	12.2%	8.0	0.7
CHKP.O	CheckPoint	18,308	2,415	2,559	2,698	2,863	5.8%	7.2	1.2
	平均值							9.3	0.9
CRWD.O	CrowdStrike	93,800	3,056	3,986	5,080	6,347	27.6%	23.5	0.9

资料来源：可比公司营收为 Refinitiv 一致预期，CrowdStrike 营收为光大证券研究所预测，股价时间 2024-6-17。1FY、2FY 和 3FY 对应下一财年，下两财年和下三财年

盈利预测、估值与评级：我们预测公司 25-27 财年营业收入 39.9/50.8/63.5 亿美元，归母净利润 2.01/3.33/5.85 亿美元，现价对应 PS 24x/19x/15x。公司连续三年位列端点安全行业的领导者地位，在技术评估中领先，拥有一定的技术壁垒和丰富的产品阵营。考虑到公司营收维持高增长，云原生安全平台与生成式 AI 产品无缝集成，顺应 AI 时代网络安全新需求，首次覆盖给予“增持”评级。

风险提示：行业竞争加剧风险、AI 技术发展不及预期、行业政策风险。

表 23：CrowdStrike 盈利预测与估值简表

指标	FY2023	FY2024	FY2025E	FY2026E	FY2027E
营业收入（百万美元）	2,241	3,056	3,986	5,080	6,347
营业收入增长率	54.4%	36.3%	30.4%	27.5%	24.9%
归母净利润（百万美元）	-183	89	201	333	585
归母净利润增长率	-	-	125.0%	65.5%	75.8%
EPS（美元）	-0.79	0.37	0.83	1.38	2.42
P/S	42	31	24	19	15

资料来源：Wind，光大证券研究所预测，股价截至 2024-06-17

4.3 Zscaler：安全访问服务边缘（SASE）和零信任（ZTNA）领域的领导者

Zscaler 被视为云安全领域的技术先行者，代表着网络安全架构设计的根本转变。Zscaler 成立于 2007 年，当时正值云应用和移动性的早期阶段，公司预测随着云技术的迅速采用和员工流动性的增加，传统的外围安全方法将无法为用户和数据提供足够的保护，用户体验将越来越差，因此创立了完全云原生的安全架构。在后续发展过程中，Zscaler 在其安全架构中引入安全访问服务边缘（SASE）和零信任网络访问（ZTNA），如今均成为网络安全领域的重要趋势。

Zscaler 的安全访问服务边缘（SASE）解决方案凭借其领先的云安全技术和广泛的全球云服务节点网络赢得了市场的广泛认可。SASE 代表了一种创新的网络安全模型，结合了广域网技术和云原生安全服务，旨在为企业提供更灵活、更安全的远程访问解决方案。Zscaler SASE 通过安全网关、云防火墙、数据保

护、威胁防护等一系列安全服务，为企业提供全方位的网络安全保障。此外，Zscaler 的服务还能与企业现有的 IT 架构无缝集成，支持快速部署和简化管理。

Zscaler 的零信任网络访问（ZTNA）业务是其网络安全解决方案的核心。ZTNA 严格管理企业资源的身份认证和访问，提供最小化的动态访问权限，在远程办公、物联网等领域有广泛的应用。**Zscaler 的 ZTNA 业务主要优势包括：1）云原生架构：**ZTNA 解决方案完全基于云，提供可扩展且灵活的安全访问控制，支持企业的远程工作和数字化转型需求。**2）简化的用户体验：**消除传统 VPN 所需的复杂配置和维护，优化用户体验。**3）细颗粒度的访问控制：**确保只有合适的用户能够访问特定的企业资源，进一步加强了安全性。**4）集成和兼容性：**与企业现有的 IT 和安全架构无缝集成，支持多种云平台和应用，简化了部署和管理过程。

表 24：Zscaler 以零信任为核心的 SASE 解决方案概述及竞争优势

解决方案	简述	竞争优势
安全网络访问（ZIA）	以业界最完整的云原生安全服务边缘（SSE）平台，提供一流的安全、高速互联网和 SaaS 访问功能。 将安全、快速的网络和 SaaS 访问定义为业界最全面的云原生零信任平台的一部分。	1）多平台：支持 windows、MacOS、Linux、Android、iPhone 等多个平台。2）技术优势：Zscaler 先进的防护引擎搭配多元的威胁情报与原生的 SSL 扫描技术，可以快速的辨识威胁。3）简化管理：不需要任何硬件设备，云端策略实时布署不需要定时更新。4）云端应用支持：协助企业保护云端 SaaS 应用（CASB）。
安全私人访问（ZPA）	基于 ZTNA 架构，ZPA 让应用程序不会暴露在互联网上，未经授权的用户无法访问应用程序。无须传统 VPN 的远程应用程序访问，不需要进入公司网络，就可以访问公司在公、私有云的应用服务。	1）应用服务保护：可以将应用程序隐藏起来，内部用户无法知道主机的真正位置，看不到就无法攻击。2）微通道区隔：每个通过授权的用户与应用服务的连接都是单一微通道，增强安全性能。3）远程办公：不管用户位于世界的哪个位置，都可以透过云端执行服务政策的设定，快速的反应企业需求。
数字体验（ZDX）	基于云端的多租户监控平台，可用于探测、基准测试及测量组织内每位用户的数字体验。对指定的 SaaS 应用程序或互联网服务（如 OneDrive、Gmail 等）进行综合式探测。	1）快速解决性能问题：确保无缝的用户体验，并让用户更快地恢复工作。 2）确保应用程序效能：监控应用程序，确保用户体验不间断的服务。 3）获取全面的网络信息：利用所需的网络可见性支持在办公室和远程工作的用户。 4）获取详细的设备信息：获取每台设备的详细信息，了解组织中装置和软件的广度。
云安全态势管理（CSPM）	是云端资料安全的关键组成部分，可以搜索云端环境，提醒工作人员注意云端服务中的合规风险和配置的安全弱点，自动修复云端应用程序错误配置。	围绕零信任架构开发，是全球唯一以欺骗为基础的威胁侦测解决方案。使用先进的诱饵和圈套来侦测并破坏一贯绕过传统防御的高度复杂威胁，包括组织型的勒索软件操作者、供应链攻击和 APTs。

资料来源：Zscaler 公司官网，光大证券研究所整理

相比传统的端点安全解决方案，Zscaler 的 SASE 解决方案更专注于网络访问安全，适合依赖云服务和数据传输的企业。我们选取 CrowdStrike 作为端点安全的代表公司，横向对比 CrowdStrike 和 Zscaler 各有优势：**1）优势业务和适用公司：**CrowdStrike 更适合采用多云和混合云架构的企业，以及在大量分散设备中储存敏感信息的企业，如政府机构、金融机构、律师事务所等；Zscaler 更强调云安全和访问安全，更依赖云服务、通过互联网传输远程工作的企业，如互联网公司、私营企业等。**2）部署方法：**CrowdStrike 通过云原生平台 Falcon 提供终端保护，而 Zscaler 通过将流量重定向到其云平台提供网络层面的保护。

风险提示：行业竞争加剧风险、AI 技术发展不及预期、行业政策风险。

表 25：CrowdStrike 和 Zscaler 的网络安全横向对比

	CrowdStrike	Zscaler
公司类型	端点安全	云安全和网络安全
业务简介	专注于端点保护，提供先进的防病毒、威胁情报以及端点检测和响应等高级功能	专注于互联网访问安全，提供 Web 过滤、数据丢失防护、云应用程序可见性控制等功能
优势业务	1）覆盖多种操作系统和设备，适用于混合云；2）在处理复杂网络攻击和高级持续性威胁（APT）方面具有显著优势	1）零信任网络访问（ZTNA） 2）云访问安全代理（CASB）
适用的企业	在大量分散终端设备中储存敏感信息，日常运营中面临 APT 的企业，如政府机构、金融机构、法律事务所等	依赖云服务、通过网络传输进行远程工作的企业，如互联网公司、私营企业等
部署方法	通过云原生平台 Falcon 提供终端保护，无需部署客户端即可在所有端点访问，无需手动更新传统安全软件或硬件	通过将流量重定向到其云平台，提供网络层面的保护，支持零信任网络访问和 IT 架构的灵活集成
威胁监测方法	利用 AI 和 ML 算法，通过分析端点行为来检测和预防复杂的威胁	采用多层方法进行威胁检测，将基于签名的检测、沙盒和异常检测相结合
网络基础设施	基于云原生平台，无需基础设施，在不影响端点性能的情况下实时分析威胁	使用全球数据中心网络来重定向和检查互联网流量，可能会带来延迟和潜在的性能问题
集成能力	适用于几乎所有操作系统和平台，提供开放 API 支持，可集成多种领域的第三方工具	与 AWS、Azure 等云服务提供商集成，通过与 Okta 等身份提供商集成提供零信任能力

资料来源：各公司官网，光大证券研究所整理

5、 风险提示

行业竞争加剧风险：网络安全部分细分领域出现供应商整合的趋势，市场份额或将向技术领先的供应商集中；

AI 技术发展不及预期：网络安全估值提升的逻辑部分来自生成式 AI 的发展，使网络安全供需两端同时受到催化，但 AI 技术发展可能不及预期；

行业政策风险：网络安全需求部分依赖于政策的严格程度，当前生成式 AI 正处于发展前期，相关数据安全和隐私保护政策仍存在较多不确定性。

行业及公司评级体系

	评级	说明
行业及公司评级	买入	未来 6-12 个月的投资收益率领先市场基准指数 15%以上
	增持	未来 6-12 个月的投资收益率领先市场基准指数 5%至 15%；
	中性	未来 6-12 个月的投资收益率与市场基准指数的变动幅度相差-5%至 5%；
	减持	未来 6-12 个月的投资收益率落后市场基准指数 5%至 15%；
	卖出	未来 6-12 个月的投资收益率落后市场基准指数 15%以上；
	无评级	因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，致使无法给出明确的投资评级。
基准指数说明：		A 股市场基准为沪深 300 指数；香港市场基准为恒生指数；美国市场基准为纳斯达克综合指数或标普 500 指数。

分析、估值方法的局限性说明

本报告所包含的分析基于各种假设，不同假设可能导致分析结果出现重大不同。本报告采用的各种估值方法及模型均有其局限性，估值结果不保证所涉及证券能够在该价格交易。

分析师声明

本报告署名分析师具有中国证券业协会授予的证券投资咨询执业资格并注册为证券分析师，以勤勉的职业态度、专业审慎的研究方法，使用合法合规的信息，独立、客观地出具本报告，并对本报告的内容和观点负责。负责准备以及撰写本报告的所有研究人员在此保证，本研究报告中任何关于发行商或证券所发表的观点均如实反映研究人员的个人观点。研究人员获取报酬的评判因素包括研究的质量和准确性、客户反馈、竞争性因素以及光大证券股份有限公司的整体收益。所有研究人员保证他们报酬的任何一部分不曾与，不与，也将不会与本报告中具体的推荐意见或观点有直接或间接的联系。

法律主体声明

本报告由光大证券股份有限公司制作，光大证券股份有限公司具有中国证监会许可的证券投资咨询业务资格，负责本报告在中华人民共和国境内（仅为本报告目的，不包括港澳台）的分销。本报告署名分析师所持中国证券业协会授予的证券投资咨询执业资格编号已披露在报告首页。

中国光大证券国际有限公司和 Everbright Securities(UK) Company Limited 是光大证券股份有限公司的关联机构。

特别声明

光大证券股份有限公司（以下简称“本公司”）成立于 1996 年，是中国证监会批准的首批三家创新试点证券公司之一，也是世界 500 强企业——中国光大集团股份公司的核心金融服务平台之一。根据中国证监会核发的经营证券期货业务许可，本公司的经营范围包括证券投资咨询业务。

本公司经营范围：证券经纪；证券投资咨询；与证券交易、证券投资活动有关的财务顾问；证券承销与保荐；证券自营；为期货公司提供中间介绍业务；证券投资基金代销；融资融券业务；中国证监会批准的其他业务。此外，本公司还通过全资或控股子公司开展资产管理、直接投资、期货、基金管理以及香港证券业务。

本报告由光大证券股份有限公司研究所（以下简称“光大证券研究所”）编写，以合法获得的我们相信为可靠、准确、完整的信息为基础，但不保证我们所获得的原始信息以及报告所载信息之准确性和完整性。光大证券研究所可能将不时补充、修订或更新有关信息，但不保证及时发布该等更新。

本报告中的资料、意见、预测均反映报告初次发布时光大证券研究所的判断，可能需随时进行调整且不予通知。在任何情况下，本报告中的信息或所表述的意见并不构成对任何人的投资建议。客户应自主作出投资决策并自行承担投资风险。本报告中的信息或所表述的意见并未考虑到个别投资者的具体投资目的、财务状况以及特定需求。投资者应当充分考虑自身特定状况，并完整理解和使用本报告内容，不应视本报告为做出投资决策的唯一因素。对依据或者使用本报告所造成的一切后果，本公司及作者均不承担任何法律责任。

不同时期，本公司可能会撰写并发布与本报告所载信息、建议及预测不一致的报告。本公司的销售人员、交易人员和其他专业人员可能会向客户提供与本报告中观点不同的口头或书面评论或交易策略。本公司的资产管理子公司、自营部门以及其他投资业务板块可能会独立做出与本报告的意见或建议不相一致的投资决策。本公司提醒投资者注意并理解投资证券及投资产品存在的风险，在做出投资决策前，建议投资者务必向专业人士咨询并谨慎抉择。

在法律允许的情况下，本公司及其附属机构可能持有报告中提及的公司所发行证券的头寸并进行交易，也可能为这些公司提供或正在争取提供投资银行、财务顾问或金融产品等相关服务。投资者应当充分考虑本公司及本公司附属机构就报告内容可能存在的利益冲突，勿将本报告作为投资决策的唯一信赖依据。

光大证券研究所

上海
静安区新闸路 1508 号
静安国际广场 3 楼

北京
西城区武定侯街 2 号
泰康国际大厦 7 层

深圳
福田区深南大道 6011 号
NEO 绿景纪元大厦 A 座 17 楼

光大证券股份有限公司关联机构

香港
中国光大证券国际有限公司
香港铜锣湾希慎道 33 号利园一期 28 楼

英国
Everbright Securities(UK) Company Limited
6th Floor, 9 Appold Street, London, United Kingdom, EC2A 2AP