

AI浪潮下的网络安全产业变革

深度报告

分析师：方闻千 SAC S0910523070001
2023年12月17日

华金证券客户中的专业投资者参考

更多免费行业报告

并购家

www.ipoipo.cn

并购家 免费行业报告网

IPOIPO.CN 每日更新 不用注册会员 无广告 永久免费

AI将带来网络安全在攻防两端的重要变革：

- 1) 攻击视角（提升需求）：1、安全赋能攻击——AI/大模型能够显著降低安全攻击门槛，加剧安全威胁，进而提升行业需求；2、大模型自身风险——数据安全相关需求受到AI/大模型的直接拉动。
- 2) 防御视角（改造产品）：AI/大模型带来安全产品形态的变化，从能力提升（从一线运营到安全专家）和效率提升（响应处置时间从天/小时到秒）两大维度，带来了竞争格局改善的可能性。

海外AI2.0+安全已经实现初步商业化落地，并且对头部安全厂商公司报表已产生实质性影响。得益于AI+安全新逻辑驱动，Panw和Crwd为代表的的海安厂商年初至今涨幅达100%以上，目前主流AI2.0产品形态可分为两大类：

- 1) 安全Copilot产品：代表为Microsoft Security Copilot和Crowdstrike Charlotte AI，目前大部分生成式AI产品聚焦在这个方向，主要功能包括安全监控、威胁检测、资产风险、创建报告等，能够辅助安全管理人员提升安全运营的自动化水平。安全Copilot产品目前已有多个标杆产品且进入商业化早期，Crowdstrike认为未来5年生成式AI产品的潜在市场规模将达到70亿美金，不亚于目前的核心产品线。随着AI赋能安全运营效率提升和规模效应的体现，Crowdstrike也上调了盈利模型的预期，将OPM从22%上修到28-32%
- 2) AI驱动的安全平台：代表为Palo Alto Networks推出的基于AI驱动的新产品XSIAM（扩展安全智能和自动化管理）。XSIAM是一个云交付的集成SOC平台，将EDR、XDR、SOAR、ASM、UEBA、TIP和SIEM等多个产品和功能整合到一个集成平台中，底层完全由AI驱动。目前XSIAM商业化取得极大成功，此前第一年的收入目标为1亿美元，而实际第一年XSIAM收入已达2亿美元，远远超出了此前设立的目标，最新财季XSIAM的pipeline已经达到10亿美元体量，有望成为公司增长最快且体量最大的产品线。

AI+安全的未来产业格局思考：1) AI驱动下，安全平台的能力边界向外进一步延伸，能够对不同安全域实现全方位纳管，形成整体防御合力；2) 安全大数据是核心壁垒，AI提升了安全产品的海量数据分析、理解、自动化处理和生成的能力，头部厂商的优势非常明显，格局上强者恒强，头部的份额持续提升。

哪些公司能够受益：1) 拥有核心产品且产品联动做得比较好，具备比较强安全平台能力的厂商直接受益；2) 有比较广泛的客户触手，构建安全数据壁垒；3) 产品创新和执行力强，能够率先推动相关技术的商业化。

国内AI+安全目前正处于产品测试与市场推广的初期。包括深信服、奇安信、安恒等十余家头部厂商已发布AI+安全产品，预计明年起AI+安全产品将全面铺开。在大模型落地方式上，目前国内外安全市场存在明显差异。海外市场云化部署占主导。海外客户对安全SaaS接受度较高，包括CrowdStrike、Panw等头部安全厂商均采用云优先的战略来推AI，头部安全厂商能够基于安全大数据去迭代优化安全能力。国内市场以私有化本地化部署为主，同时考虑算力成本以及大模型本地实施需求，以及国内政府、金融等头部客户对数据安全要求较高，训练/推理一体机的模式有望成为主流。

投资逻辑：今年以来，由于网络安全的后周期性和政策空窗期承压，行业整体景气度处于低位。随着预算修复和竞争企稳，行业长期成长逻辑不变，且明年AI新品放量值得期待。**重点推荐：**启明星辰、安恒信息、深信服；**关注标的：**奇安信、天融信、绿盟科技、360、美亚柏科、中新赛克、电科网安、亚信安全、迪普科技。

风险提示：数据安全风险；技术发展风险；贸易摩擦加剧风险；道德和伦理风险。

攻击视角（提升需求）：1、AI赋能安全攻击——AI/大模型能够显著降低安全攻击门槛，加剧安全威胁，进而提升行业需求；2、大模型自身风险——数据安全相关需求受到AI/大模型的直接拉动。

防御视角（改造产品）：AI/大模型带来安全产品形态的变化，从能力提升（从一线运营到安全专家）和效率提升（响应处置时间从天/小时到秒）两大维度，带来了竞争格局改善的可能性。

图表：AI+网络安全整体逻辑框架

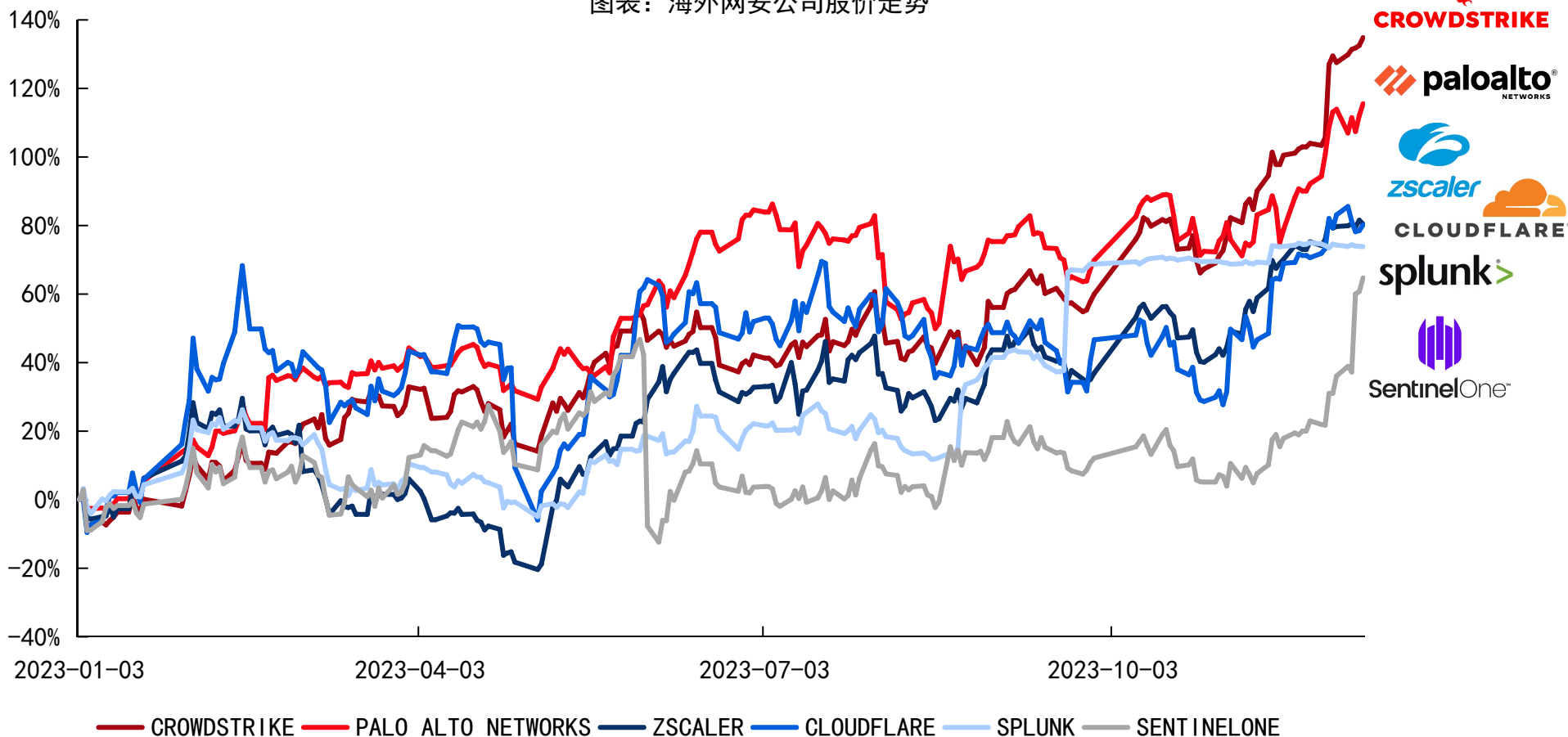


美股安全公司股价整体走势强劲

今年以来海外安全公司整体走势强劲，Panw和Crwd为代表的厂商年初至今涨幅达100%以上，主要原因在于：

- 1) 海外科技股整体Beta，叠加估值修复；
- 2) 安全公司今年业绩表现亮眼，财报表现超预期，同时云转型快速推进；
- 3) AI+安全新逻辑驱动，Gen AI对头部安全厂商公司报表已经产生实质性影响。

图表：海外网安公司股价走势



01

AI+安全驱动需求侧：AI加剧安全威胁

02

AI+安全变革产品侧：安全运营自动化

03

AI+安全的长期思考：竞争格局改变

04

国内AI+安全现状：明年产品有望放量

05

投资策略

AI赋能安全攻击加剧整体安全威胁

大模型/生成式AI对于网络安全行业的影响与其他行业有所不同，AI不仅仅是对于安全产品形态本身带来改变（防御视角），而且能够通过大幅降低了安全攻击的门槛，进而带来行业总需求的提升（攻击视角）。

AI将带来安全攻击的新变化：社会工程攻击、漏洞与攻击面发现、恶意代码生成等。

AI/自动化攻击工具今年下半年进入规模化和产业化阶段。比如FraudGPT在暗网市场和Telegram平台进行售卖：

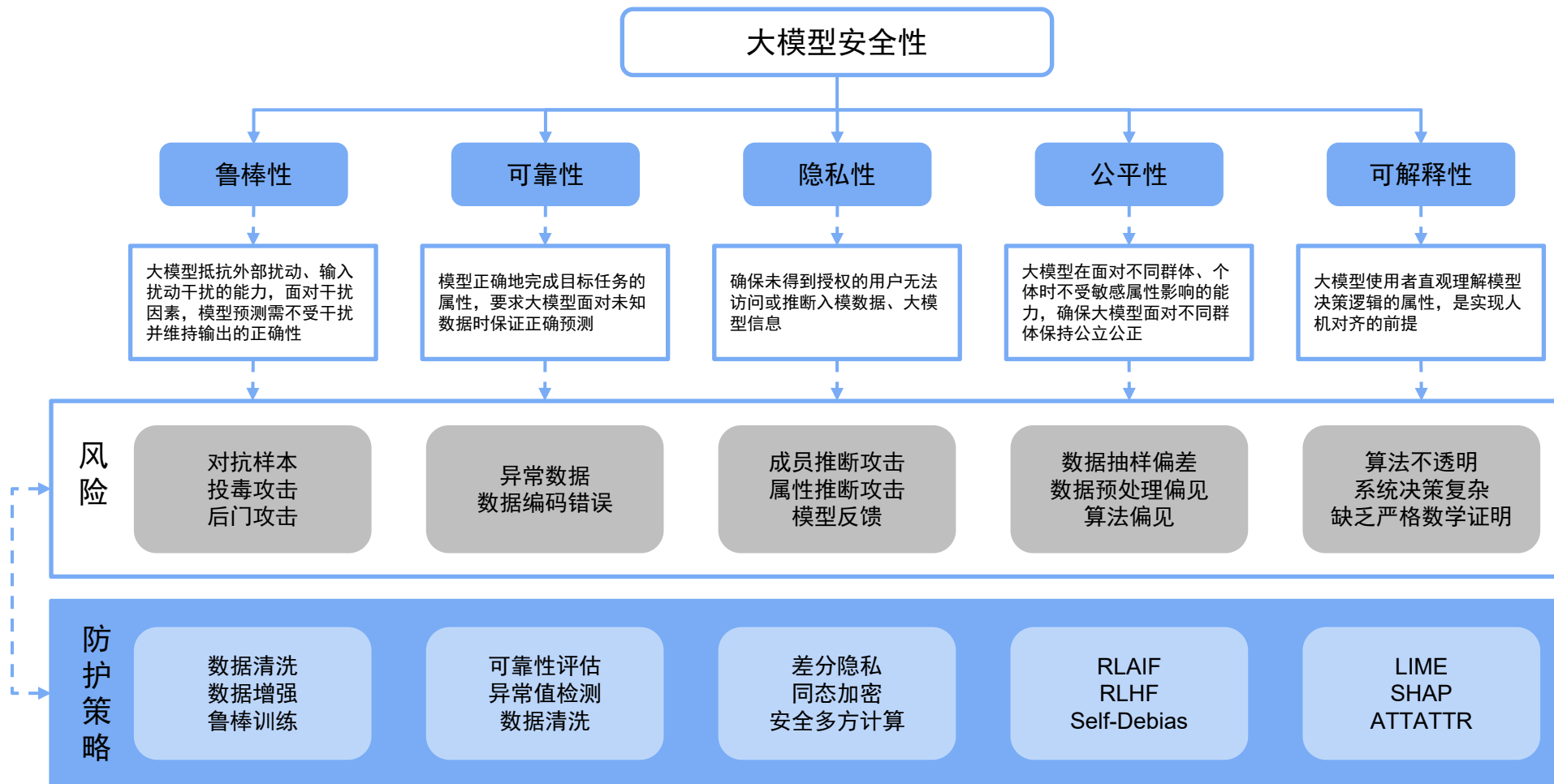
1) 1个月计划定价为200美元；2) 3月计划定价450美元；3) 6个月计划定价1000美元；4) 一年计划定价1700美元。

图表：AI大模型赋能安全攻击侧的几种方式



AI/大模型存在原生安全问题，其中对安全投入影响最大的为数据安全和AI工程化领域。数据安全既包括了训练阶段数据采集不当、存在偏见或标签错误、数据被投毒等，也包括了模型在应用的过程中，面临数据泄露、隐私曝光等风险隐私曝光等风险。通常需要采取包括数据加密、隐私计算、数据清晰等数据安全保障手段。

图表：AI/大模型存在原生安全问题



01

AI+安全驱动需求侧：AI加剧安全威胁

02

AI+安全变革产品侧：安全运营自动化

03

AI+安全的长期思考：竞争格局改变

04

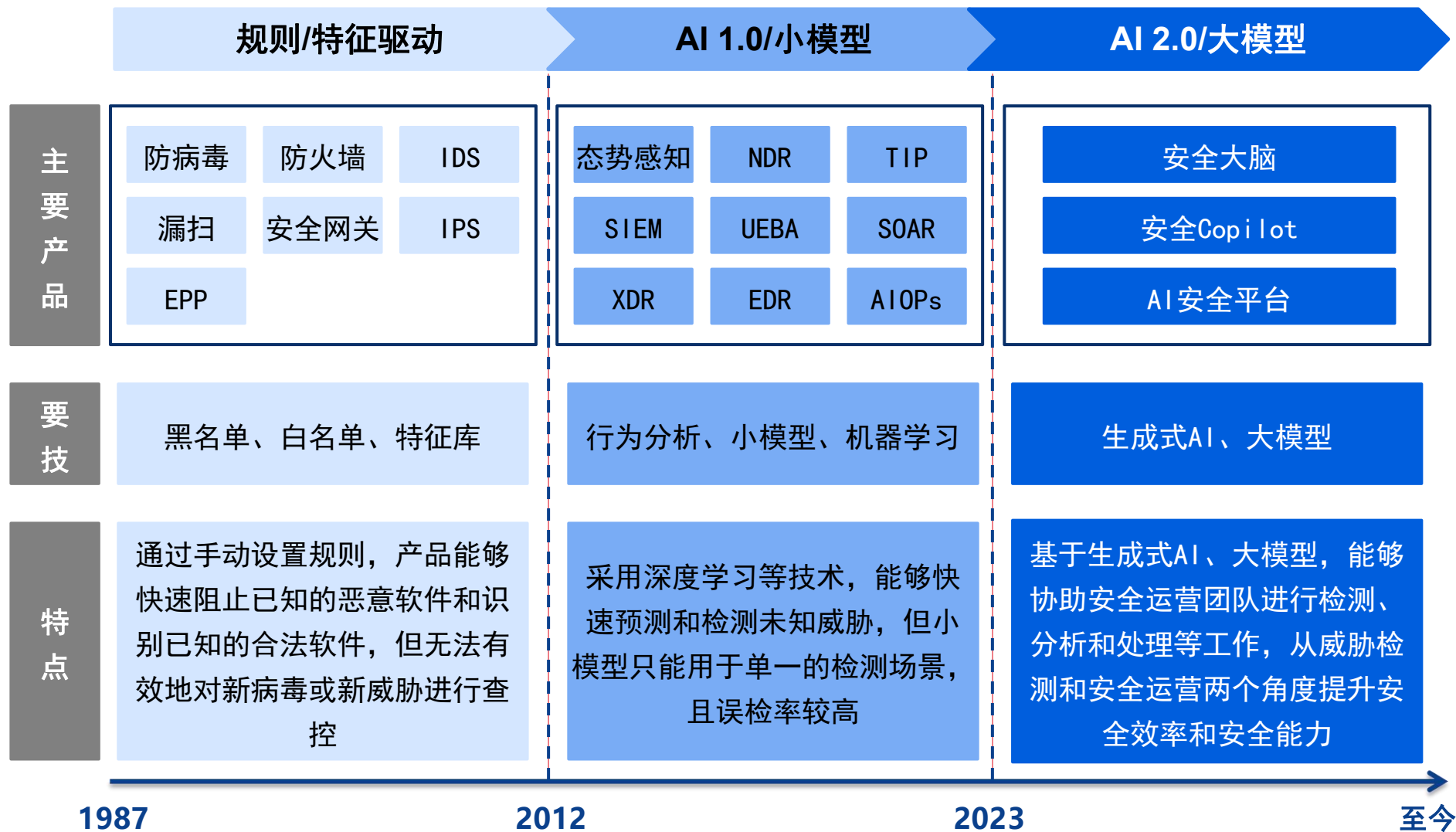
国内AI+安全现状：明年产品有望放量

05

投资策略

AI 2.0：安全能力的又一次进化

图表：AI 2.0时代安全能力再次进化



今年3月微软发布了首个生成式AI安全产品Security Copilot后，多家头部厂商包括CrowdStrike、Google均推出了对应安全Copilot类产品。安全Copilot类产品的主要功能包括基于自然语言和AI辅助的安全状态查询、威胁搜寻、安全事件响应等。

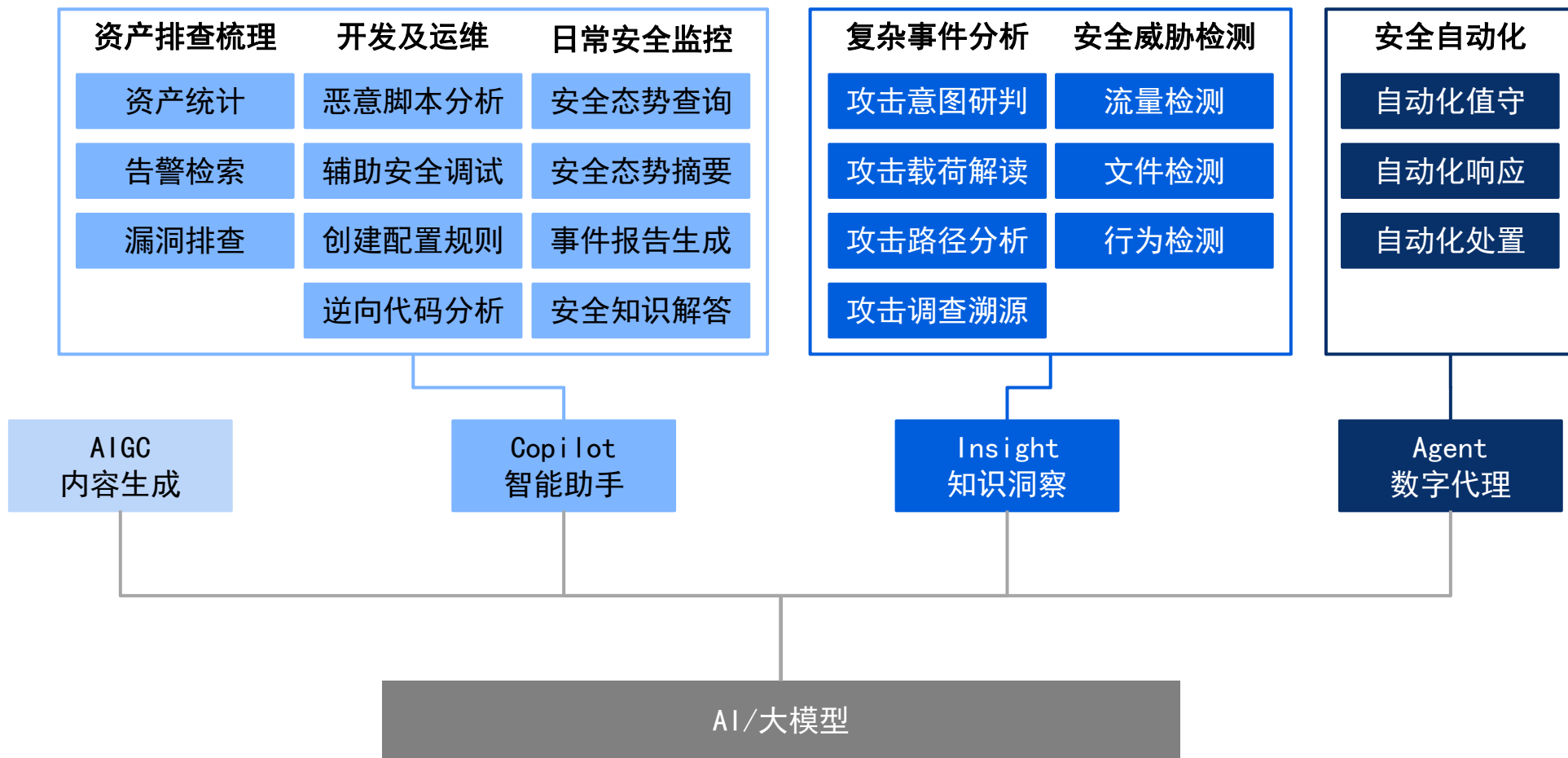
图表： 主要AI+网络安全产品

产品	厂商	功能特性
Security Copilot	Microsoft	Security Copilot将GPT-4内置于产品中，并与微软的安全模型库结合，为用户提供恶意代码防护、隐私合规监控等生成式AI服务。在使用上，Security Copilot类似于聊天机器人，用户用自然语言输入安全问题，Security Copilot输出可操作的回答，并展示来源。
Network Security Copilot	Palo Alto Networks	Network Security Copilot是一款生成式AI安全助手，能够通过自然语言对话的形式给出安全问题的答案。Network Security Copilot将首先集成在Cortex系列产品中。
Charlotte AI	CrowdStrike	Charlotte AI是一款生成式AI安全助手，用户可以用自然语言与其对话，使其回答特定的安全问题，并提供操作建议。CrowdStrike通过Falcon OverWatch、Falcon Complete、Services、Intelligence等产品收集多维数据，用以训练Charlotte AI的AI引擎。
Zscaler Navigator	Zscaler	Zscaler Navigator是一个简化的自然语言交互界面，用户能够使用自然语言与Zscaler产品交互并获取相关的文档信息。
Cursor	Cloudflare	Cursor是一款生成式AI对话机器人，通过Cloudflare Workers和Durable Objects提供技术支持，用户可以使用自然语言与其对话，获取关于Cloudflare开发者平台的知识。
Splunk AI Assistant	Splunk	Splunk AI Assistant是一款人工智能聊天机器人，用户可以使用自然语言与其对话，使其编写或解释定制的SPL（Splunk处理语言）查询语句，从而高效地从企业数据中获得洞察力。
Recorded Future AI	Recorded Future	Recorded Future AI集成在Recorded Future智能云平台中，将OpenAI的GPT模型与公司的智能云相结合，帮助安全分析师提高效率，主要功能包括：1）通过自然语言互动回答安全分析师的提问，2）总结提炼一段信息重点，3）进行实时分析并生成分析报告。
Chronicle AI	Google	Chronicle AI是一款采用生成式AI技术的安全运营工具，用户能够以自然语言对话的方式搜索、分析和调查安全事件，帮助安全分析师提升效率。
ExposureAI	Tenable	ExposureAI是一款生成式AI服务，集成于One Exposure Management Platform平台上。ExposureAI提供了三个基于生成式AI的安全功能：1）允许用户使用自然语言查询分析资产和潜在风险，2）提供缓解威胁的安全指导，3）对风险进行优先级评估。
Purple AI	SentinelOne	Purple AI是一款威胁搜索和响应工具。类似于聊天机器人，用户可以用自然语言要求其查找某类威胁、生成报告，并自动执行补救措施。Purple AI使用了GPT-4等技术来加速威胁调查和响应。

AI+安全的结合点：安全运营

AI+安全的主要结合点集中在安全运营+安全平台领域，目前AI2.0+安全产品主要可分为两类：1) 安全Copilot产品：代表为Microsoft Security Copilot和CrowdStrike Charlotte AI；2) AI驱动的安全平台：代表为Palo Alto Networks推出的基于AI驱动的新产品XSIAM（扩展安全智能和自动化管理）。

图表： AI+安全的主要产品形态

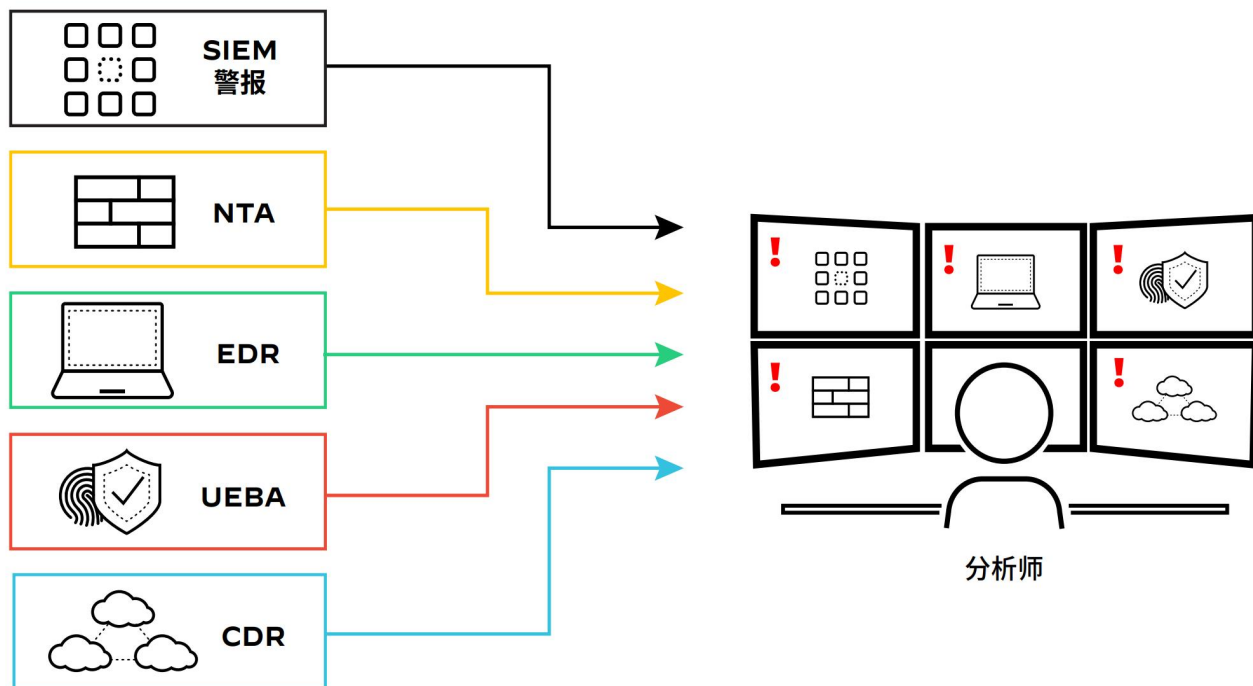


为什么是安全运营？

安全运营是安全行业自动化程度最低的领域：在一个网络安全系统的各个组成中，防火墙、端点安全等单点的安全产品已经具备了较高的自动化水平，而安全运营本是自动化程度最低的一环。这是由安全的复杂性决定的。

安全运营是安全行业最需要AI深度改造的环节：1) 传统安全设备是第三方的，多且杂，数据混乱，导致误报率高，变成了真实风险看不到，出现威胁防不了；2) 安全运营工作压力太大，上万威胁，且90%非真实威胁，效率低下。

图表：安全运营是安全自动化最低的领域

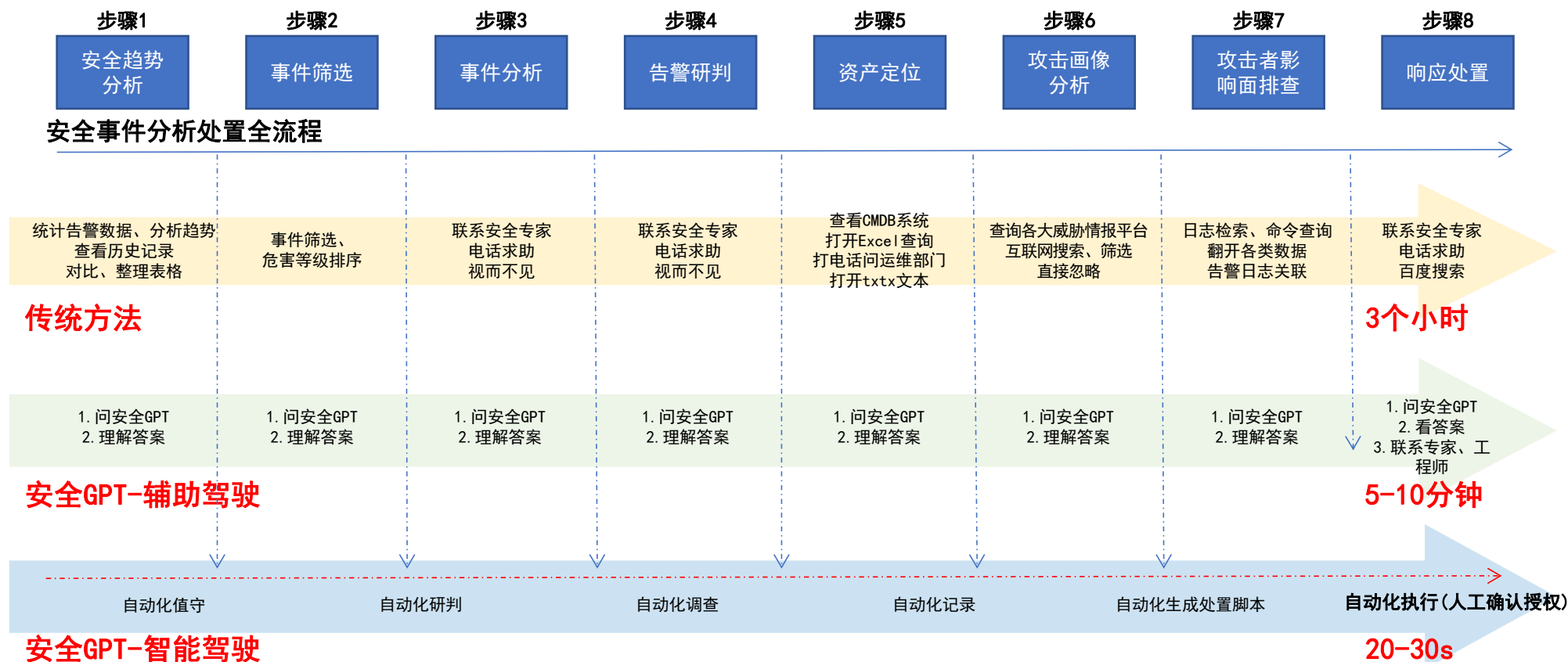


AI将带来安全运营效率的飞跃

能力提升（从一线运营到安全专家）：对于经验不足的IT和安全专业人员，AI可以帮助他们更快地做出更好的决策，让更高级的安全操作变得更加容易，能够迅速达到中高级安全人员的处置能力，降低安全运营门槛；

效率提升（响应处置时间从天/小时到秒）：安全人员水平可自动执行数据收集、提取以及威胁搜索和检测等重复且繁琐的任务，缩短对关键事件的响应时间，同时通过简单的自然语言提示实现任何检测、调查或响应工作流程，降低安全运营的时间和人力成本。

图表：AI+安全的最大机会来自于提升安全运营的自动化程度

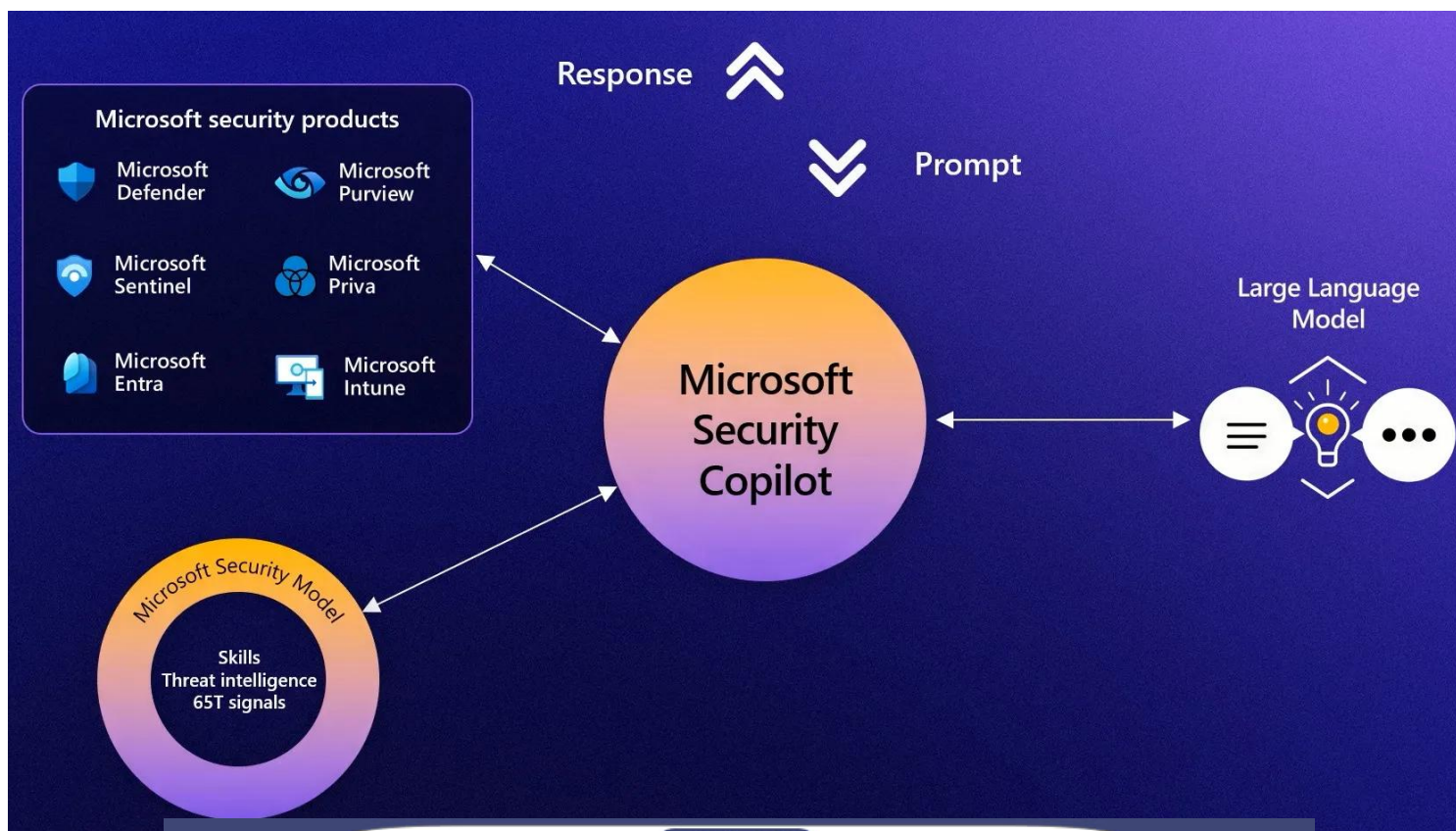


微软Security Copilot: 首个生成式AI安全产品

微软3月发布的Security Copilot是全球首个生成式AI安全工具，底层模型由ChatGPT-4驱动，并结合了微软的安全专用模型。模型每天持续学习微软在其威胁情报中收集的超过65万亿个信号数据，为Security Copilot幕后的安全专业人员提供支持。

Security Copilot拥有一个极其简洁的界面，能够接受自然语言输入，用户只需向其发送提示——可以是问题和请求，也可以是文件、URL、代码片段或威胁指标——Security Copilot会动用安全模型的全部功能来分析事件或执行任务。

图表：微软的Security Copilot是全球首个生成式AI安全工具



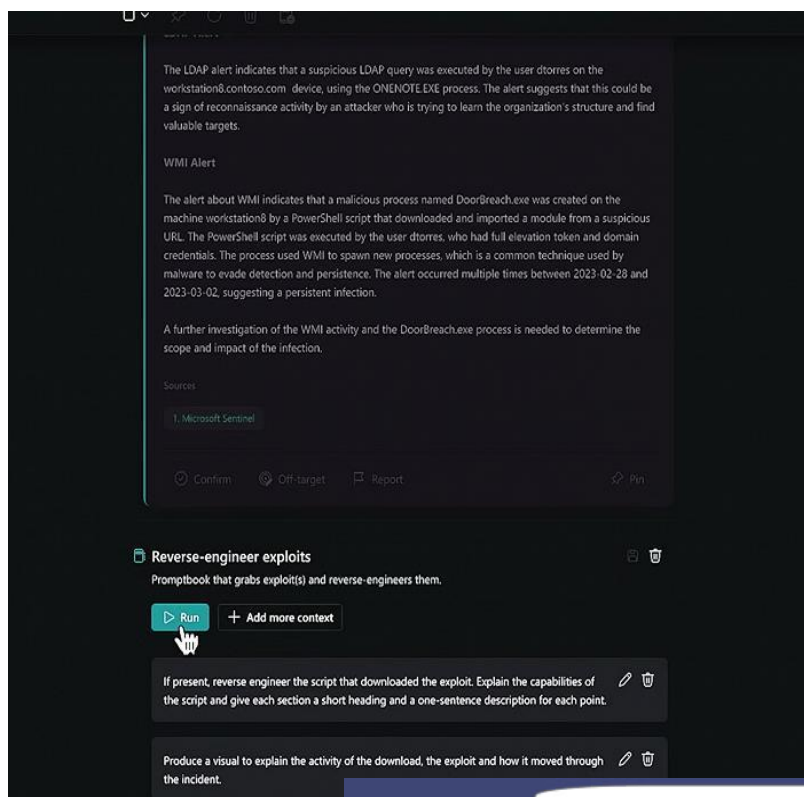
微软Security Copilot: 首个生成式AI安全产品

Microsoft Security Copilot的几个关键应用功能包括：安全事件解读与分析、优先级排序与深度分析、安全知识助手、内部态势评估总结、创建汇报文档等。

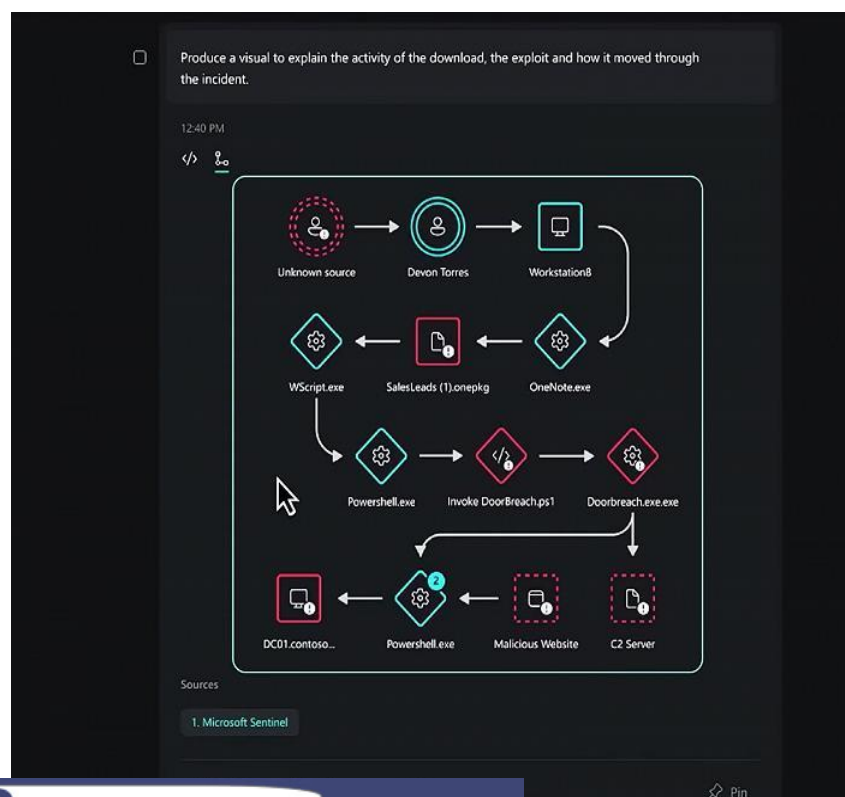
例如：安全管理人员可以使用自然语言询问与安全相关的问题，例如“公司中发生了哪些安全事件？”。Security Copilot 可以总结出由公司网络安全系统和外部数据生成的威胁报告，同时聊天机器人还可用于帮助安全管理人员进行安全调查、创建报告和总结事件。

Security Copilot在10月份已经开启测试，11月20日在微软Ignite大会上，推出首款集成Security Copilot的统一安全运营平台，数据安全、身份、设备管理等领域产品全面集成Security Copilot。

图表：Security Copilot: 安全知识解答



图表：Security Copilot: 安全事件调查

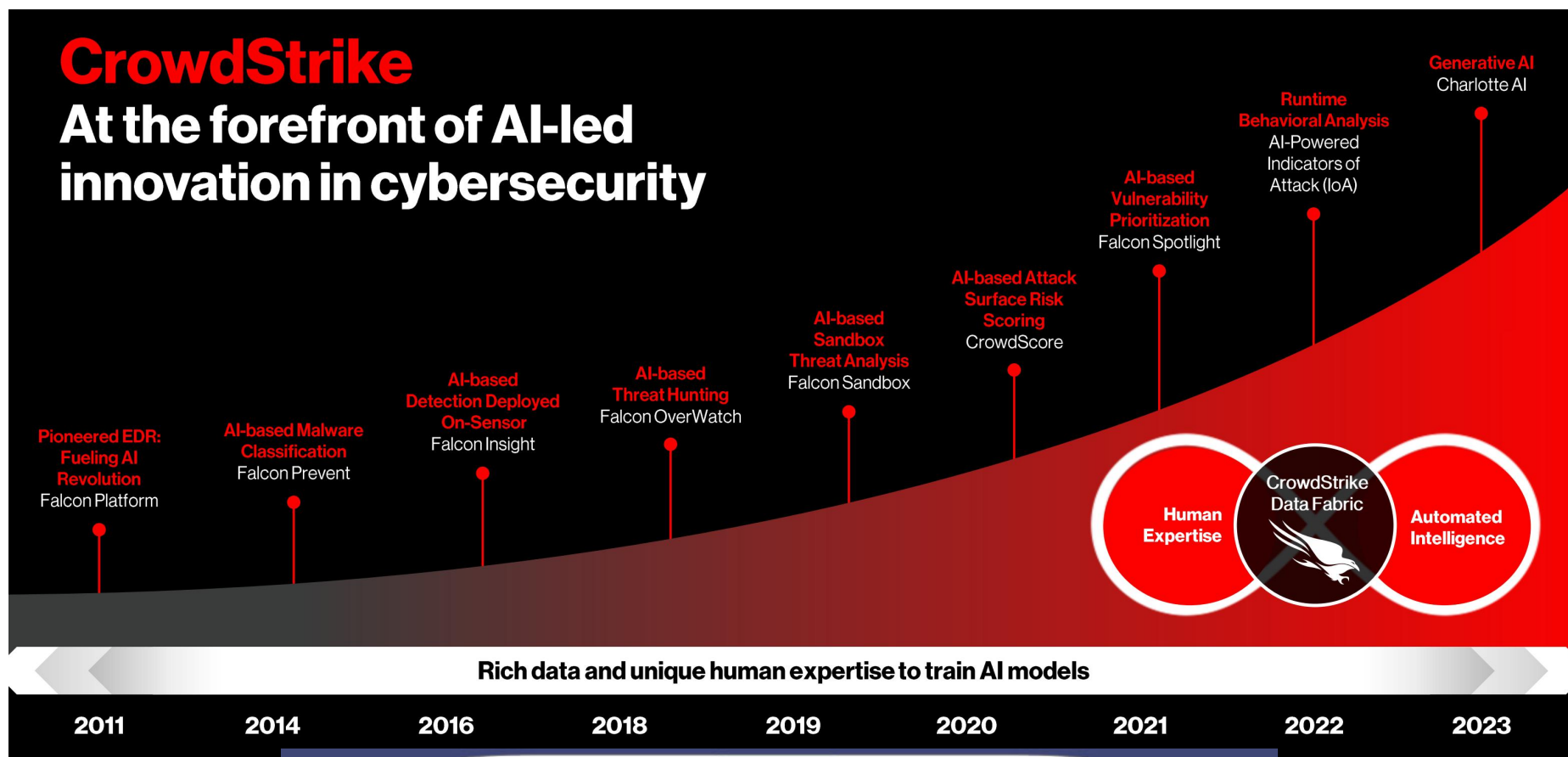


CrowdStrike的生成式AI产品Charlotte AI

CrowdStrike今年5月发布了生成式AI产品Charlotte AI，定位为虚拟安全分析师，可以帮助安全运营中心(SOC)的分析师自动化履行职责。安全分析师可以与Charlotte AI进行对话，询问有关环境中的安全威胁、如何应用于其行业、哪些资产面临风险、如何修复这些资产的问题，甚至可以创建有关情况的报告。

CrowdStrike自成立以来就一直处于AI+安全创新的前沿，作为EDR的开创者，CrowdStrike借助Charlotte AI，正在将AI+安全的领先优势扩大到生成式AI。

图表：CrowdStrike自成立以来就处于AI+安全创新的前沿



CrowdStrike Charlotte AI 主要功能

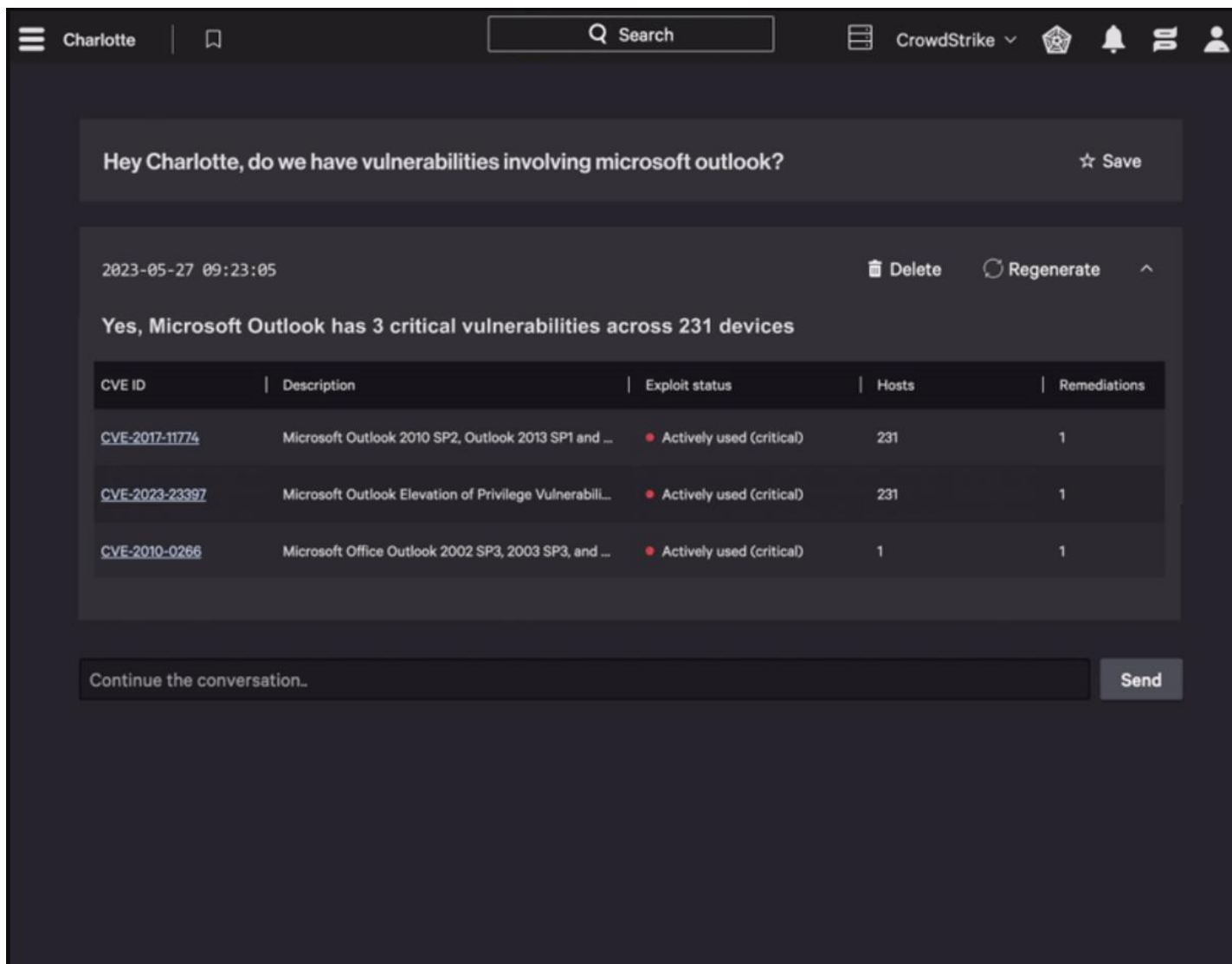
图表：Charlotte AI功能1:安全管理和安全态势感知

功能1：安全管理和安全态势感知

通过提出一些简单、直接的问题，实时洞察组织的风险状况，包括其威胁状况、关键漏洞的风险级别、当前的安全状况、合规性要求、网络安全性能指标等等。

比如：

- 1) 我们是否存在涉及 MS Outlook的漏洞？
- 2) 我们的业务关键资产面临的^{最大}风险是什么？
- 3) 我们是否能够免受 Log4j 漏洞的影响？我们哪里有危险？



Hey Charlotte, do we have vulnerabilities involving microsoft outlook? ☆ Save

2023-05-27 09:23:05 Delete Regenerate ^

Yes, Microsoft Outlook has 3 critical vulnerabilities across 231 devices

CVE ID	Description	Exploit status	Hosts	Remediations
CVE-2017-11774	Microsoft Outlook 2010 SP2, Outlook 2013 SP1 and ...	Actively used (critical)	231	1
CVE-2023-23397	Microsoft Outlook Elevation of Privilege Vulnerabil...	Actively used (critical)	231	1
CVE-2010-0266	Microsoft Office Outlook 2002 SP3, 2003 SP3, and ...	Actively used (critical)	1	1

Continue the conversation... Send

CrowdStrike Charlotte AI 主要功能

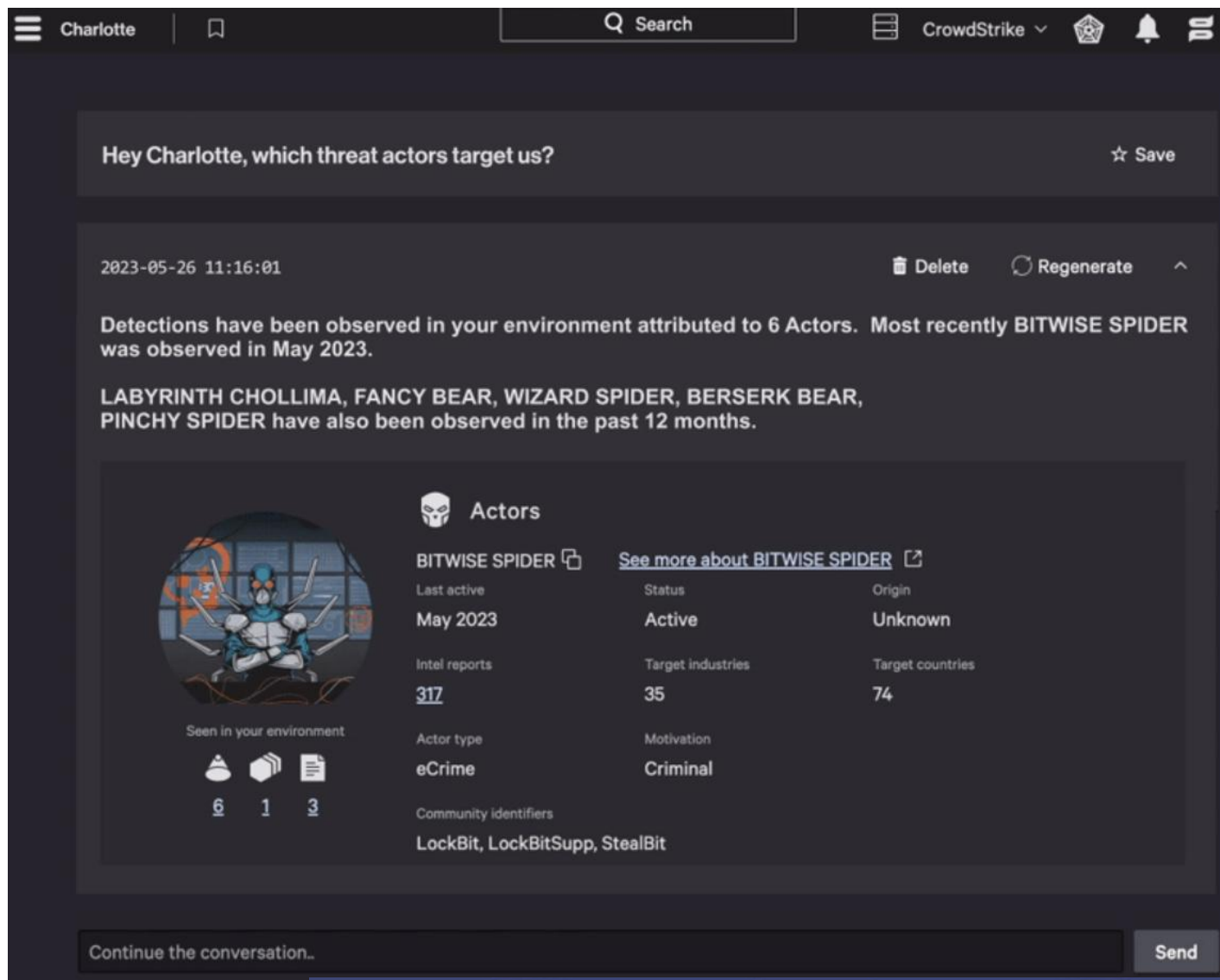
图表: Charlotte AI功能2:威胁搜索与威胁狩猎

功能2: 威胁搜索与威胁狩猎

对于经验不足的IT和安全人员,可以帮助他们更快地做出更好的决策,缩短对关键事件的响应时间,像高级的分析师一样进行简单的查询

比如:

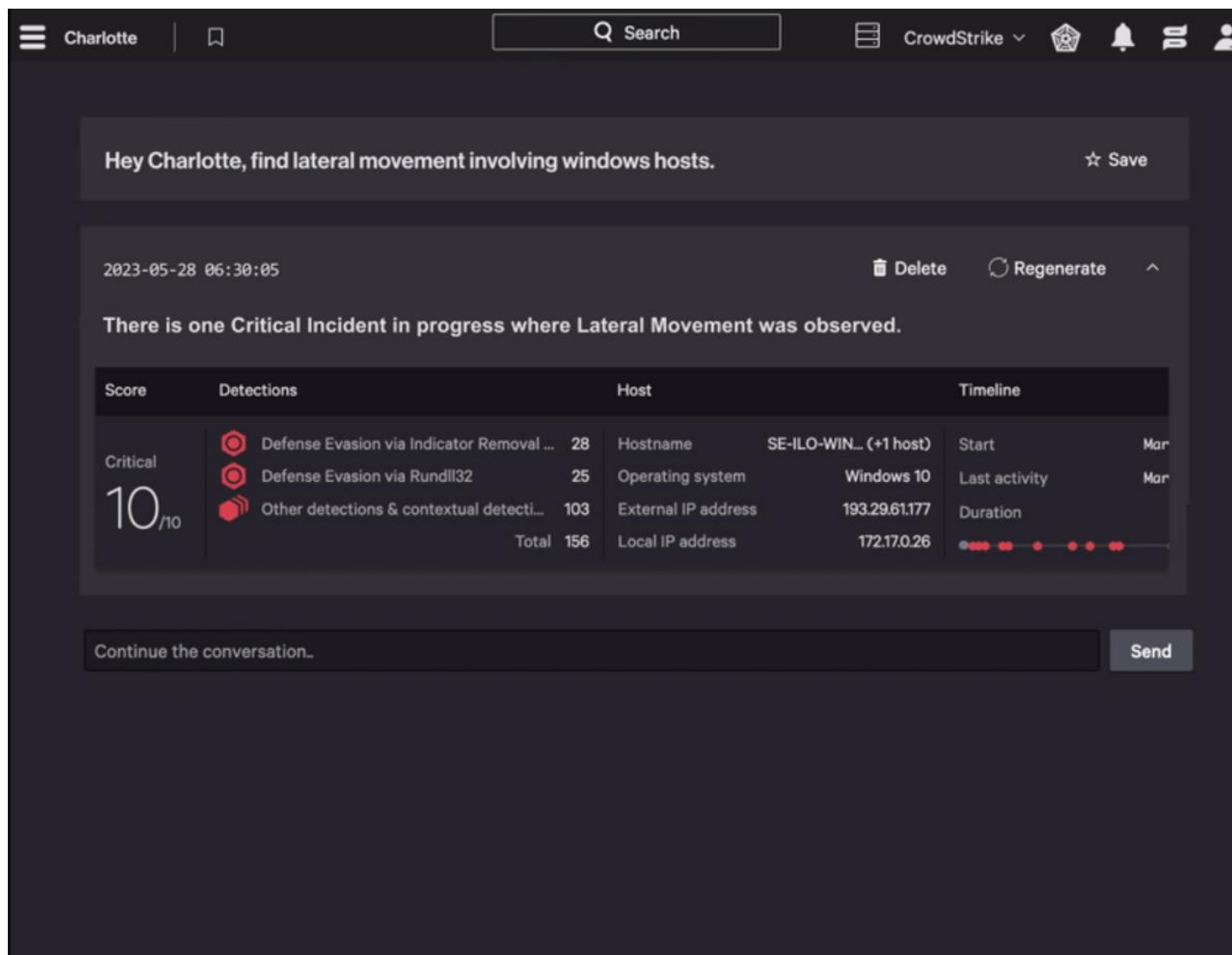
- 1) 哪些威胁行为者针对我们?
- 2) 这些对手正在利用哪些关键漏洞?
- 3) 您可以扫描我的端点资产以查找您发现的任何 IOC 吗?
- 4) 针对受影响的端点最推荐的补救措施是什么?



CrowdStrike Charlotte AI 主要功能

图表：Charlotte AI功能3:安全流程的自动化

功能3：安全流程的自动化



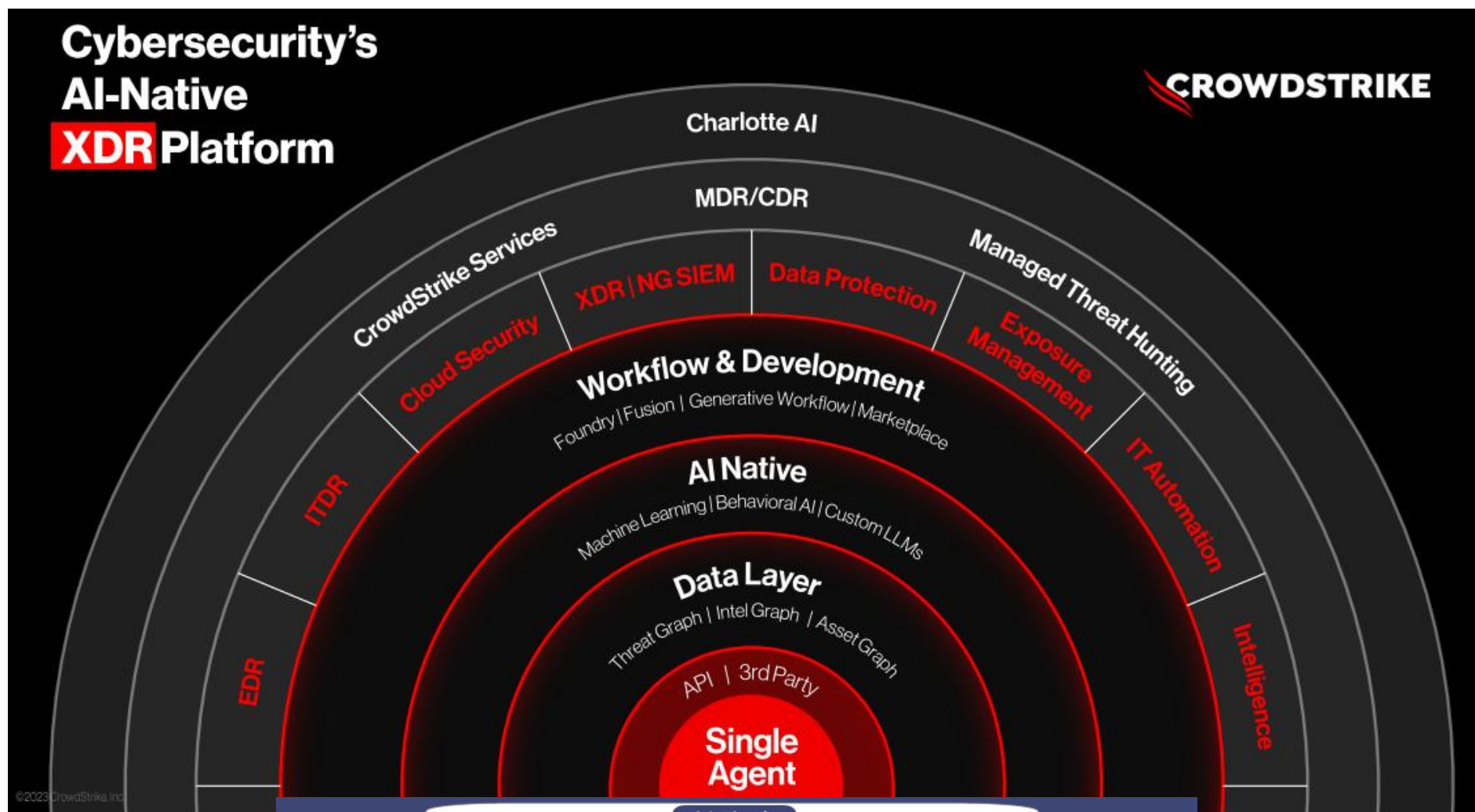
可自动执行数据收集、提取以及基本威胁搜索和检测等重复且繁琐的任务，同时使执行更高级的安全操作变得更加容易。进行任何检测、调查或响应工作流程，以增强平台体验-无需编写任何代码。

比如：
查找涉及 ows 主机的
横向移动

CrowdStrike基于AI驱动的XDR平台框架

除了生成式AI安全工具Charlotte AI之前，目前CrowdStrike已经将大模型能力作为XDR平台的重要组成部分。基于多个基础模型，利用CrowdStrike的高保真数据优势，能够为整个Falcon平台提供生成式AI功能。

图表：CrowdStrike基于AI驱动的XDR平台框架



CrowdStrike Charlotte AI定价公布

CrowdStrike在推出Charlotte AI之后，在Q3推出数据产品Raptor（把所有数据从过去的分在不同终端统一通过raptor整合进charlotte），通过AI+数据+平台，可以将过去8hrs的运营时间降低到几分钟，同时交互和易用性大幅提升。

Charlotte AI的定价是20美元/终端，公司管理层认为未来将达到70亿美金的市场规模，不亚于目前的几条核心产品线（比如Falcon IT）。

图表：CrowdStrike公布Charlotte AI定价方案



CrowdStrike业绩指引大幅上修

CrowdStrike在今年第二财季大幅上调对未来业务空间和盈利模型，同时预计未来五到七年内实现100亿美元ARR，公司预计未来3-5年的营业利润率达到28-32%，原目标是20-22%，是近期最强的美股业绩预期上修之一，同时在第三财季公司继续保持第二财季的高预期。

图表：CrowdStrike业绩指引大幅上修

New Target Model		
Non-GAAP Measure	Target (% of Revenue)	Change from Prior Target (At Midpoint)
Subscription GM %	82 – 85%	+400 Basis Points
✓ S&M	28 – 33%	-200 Basis Points
✓ R&D	15-20%	No Change
✓ G&A	5 – 7%	-200 Basis Points
Operating Margin %	28 – 32%	+900 Basis Points
Free Cash Flow %	34 – 38%	+500 Basis Points

网络安全龙头厂商Palo Alto Networks在去年底推出了基于AI驱动的新产品XSIAM（扩展安全智能和自动化管理）。XSIAM是一个云交付的集成SOC平台，统一了EDR、XDR、SOAR、ASM、UEBA、TIP和SIEM等模块，将威胁检测、事件管理、威胁情报、自动化、攻击面管理等将多个产品整合到一个集成平台中。

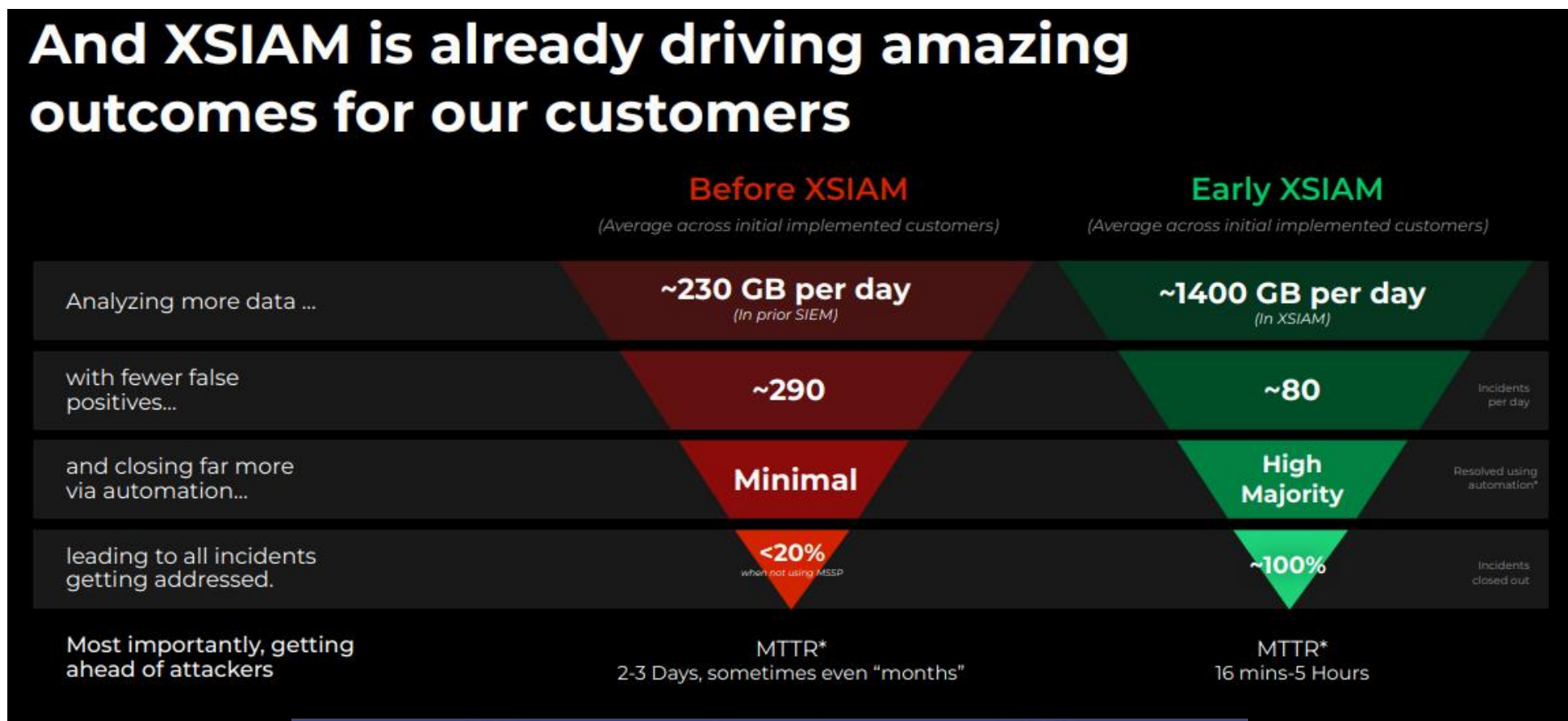
图表：XSIAM是集成了AI的基于云交付的集成SOC平台



XSIAM是未来安全平台的雏形

XSIAM的背后是精准AI（精准检索和响应）和生成式AI（便捷交互和理解），强调用AI&ML重塑安全，处理数据量6X、误报率减少70%、自动化率大幅提升、响应速度从2-3天变成16mins-5hrs。

图表：XSIAM的效果显著优于公司过去的SIEM平台产品

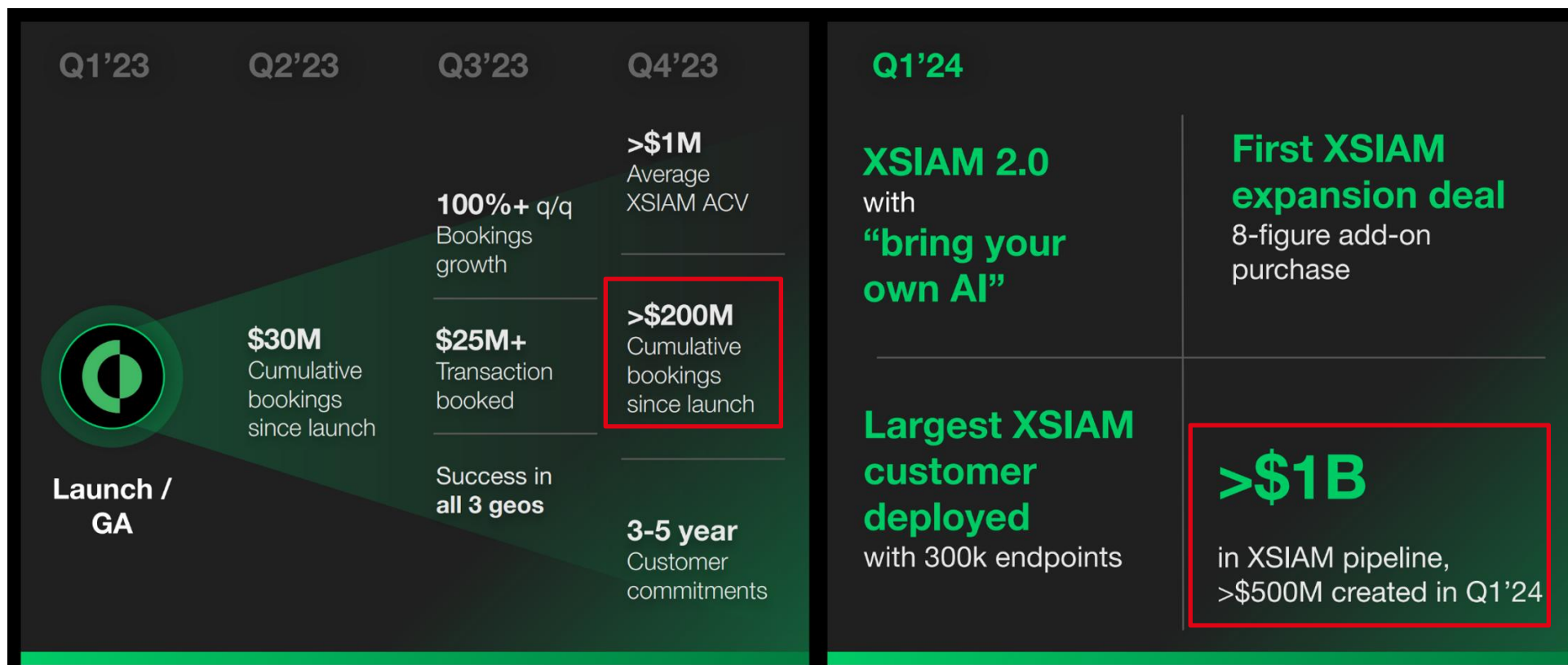


XSIAM是未来安全平台的雏形

XSIAM商业化取得极大成功：自全面推出了XSIAM以来，Palo Alto Networks制定了第一年收入达1亿美元的目标，从实际情况来看，公司连续两个季度内均获得了千万美元级大单，推出第一年XSIAM收入已达2亿美元，远远超出了此前设立的目标。

XSIAM有望在短时间内达到10亿美元体量：公司计划在XSIAM现在功能基础上，未来3-5年将推出10个以上的新增的XSIAM模块（包括自有和合作伙伴模块），进一步扩大AI大平台的能力边界。同时公司披露XSIAM的Pipeline在最新财季已经达到10亿美元体量，有望成为公司增长最快且体量最大的产品线。

图表：XSIAM商业化取得极大成功

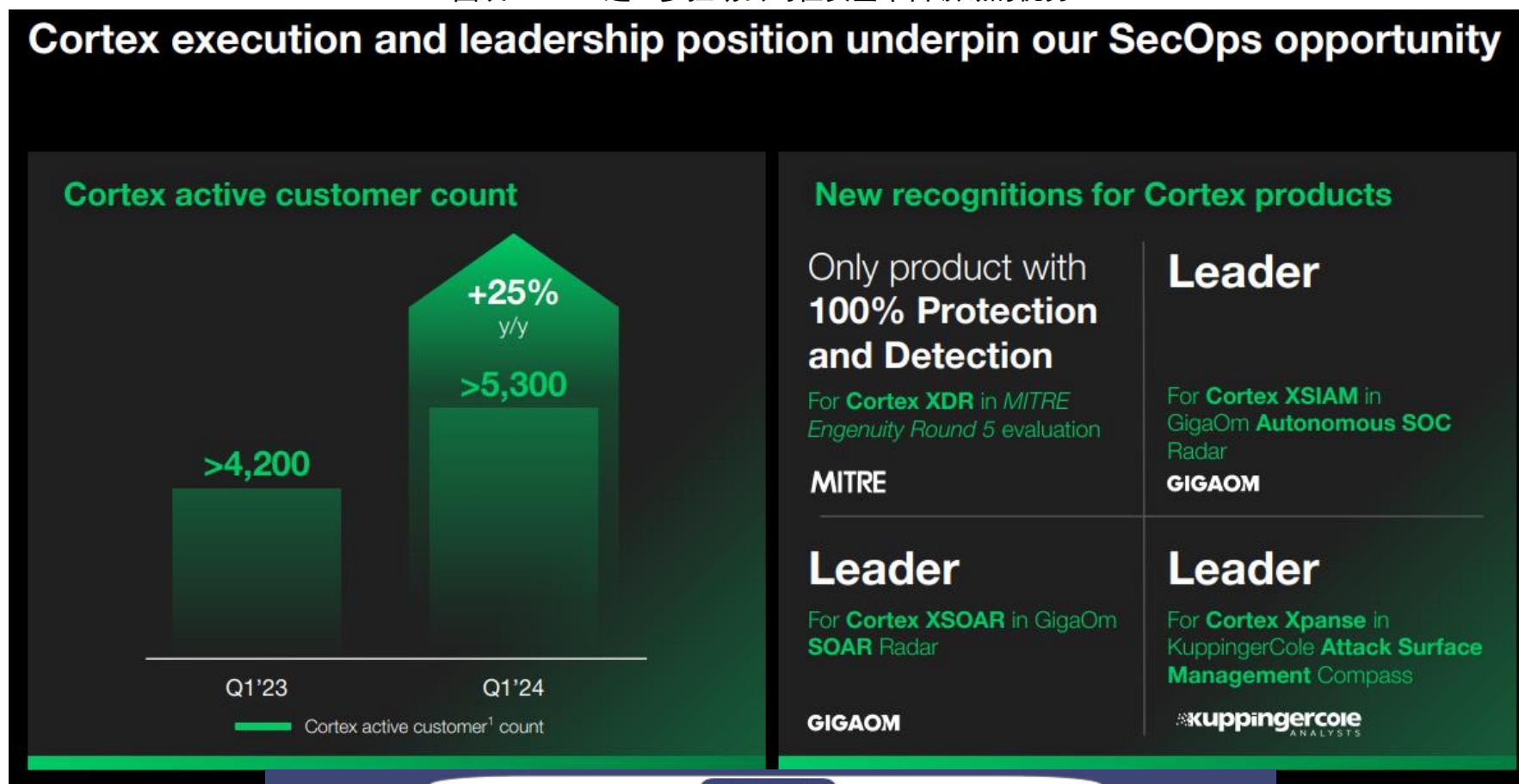


XSIAM进一步拉动公司在安全平台领域的优势

根据最新财报数据，公司Cortex活跃客户数量增长了25%，达到5300多家。Cortex中XDR、XSOAR、Xpanse和XSIAM产品均获得多项行业认可，其中，Cortex XDR是业内唯一在第一轮MITRE评估中实现100%保护和检测的产品，而XSOAR、Xpanse和XSIAM都在GigaOm等第三方评选中处于领导者位置。

Cortex板块的持续增长将巩固公司在安全运营领域的竞争优势。根据公司CEO Nikesh Arora，目前在SOC领域公司主要竞争对手有4-5个，未来随着逐渐集成AI、安全管理、端点安全能力，主要竞争对手将会缩减到2-3个。

图表：XSIAM进一步拉动公司在安全平台领域的优势



AI+安全运营的市场空间测算

AI+安全运营的未来潜在空间主要来自于机器换人逻辑，可分为两个层面：1) 甲方视角，即自身的安全服务团队的人员投入得到精简，一般没有纳入安全市场统计口径；2) 乙方视角，即购买第三方安全厂商的安全服务，目前安全服务市场总规模约800亿美金，乐观估计AI替代安全服务50%，且节省的人力成本损耗50%，即规模为 $800 \times 50\% \times 50\% = 200$ 亿美金左右。同时假设未来甲方：乙方投入在1:1，则AI安全运营总规模在 $200 \times 2 = 400$ 亿美金。

图表：网络安全细分市场支出规模（亿美元）及增速（%）

细分市场	2021年支出（）	2021年增长率（%）	2022年支出	2022年增长率（%）	2023年支出	2023年增长率（%）
应用安全	49.63	20.8	60.18	21.3	75.03	24.7
云安全	43.23	36.3	52.76	22.0	66.88	26.8
数据隐私	11.40	14.2	12.64	10.8	14.77	16.9
数据安全	31.93	6.0	3500人	9.6	39.97	14.2
身份访问管理	158.65	22.3	180.19	13.6	207.46	15.1
基础设施保护	241.09	22.5	274.08	13.7	318.10	16.1
综合风险管理	56.47	15.4	62.21	10.1	70.34	13.1
网络安全设备	175.58	12.3	190.76	8.6	209.36	9.7
其他信息安全软件	17.67	26.2	20.32	15.0	2305人	13.4
安全服务	710.81	9.2	716.84	0.8	764.68	6.7
消费者安全软件	81.03	13.7	86.59	6.9	93.74	8.3
合计	1577.50	14.3	1691.56	7.2	1883.36	11.3

01

AI+安全驱动需求侧：AI加剧安全威胁

02

AI+安全变革产品侧：安全运营自动化

03

AI+安全的长期思考：竞争格局改变

04

国内AI+安全现状：明年产品有望放量

05

投资策略

关注安全行业格局长期提升的机会

安全行业格局现状：主要子赛道各自为王，底层技术栈的差异，导致不同赛道的头部厂商优势产品各有不同，没有出现能统一分散安全能力的大平台大公司；同时，用户在各个领域选择最好/最便宜/关系最好的厂商，然后做大集成，单一安全厂商很难在所有领域都占据头部位置。

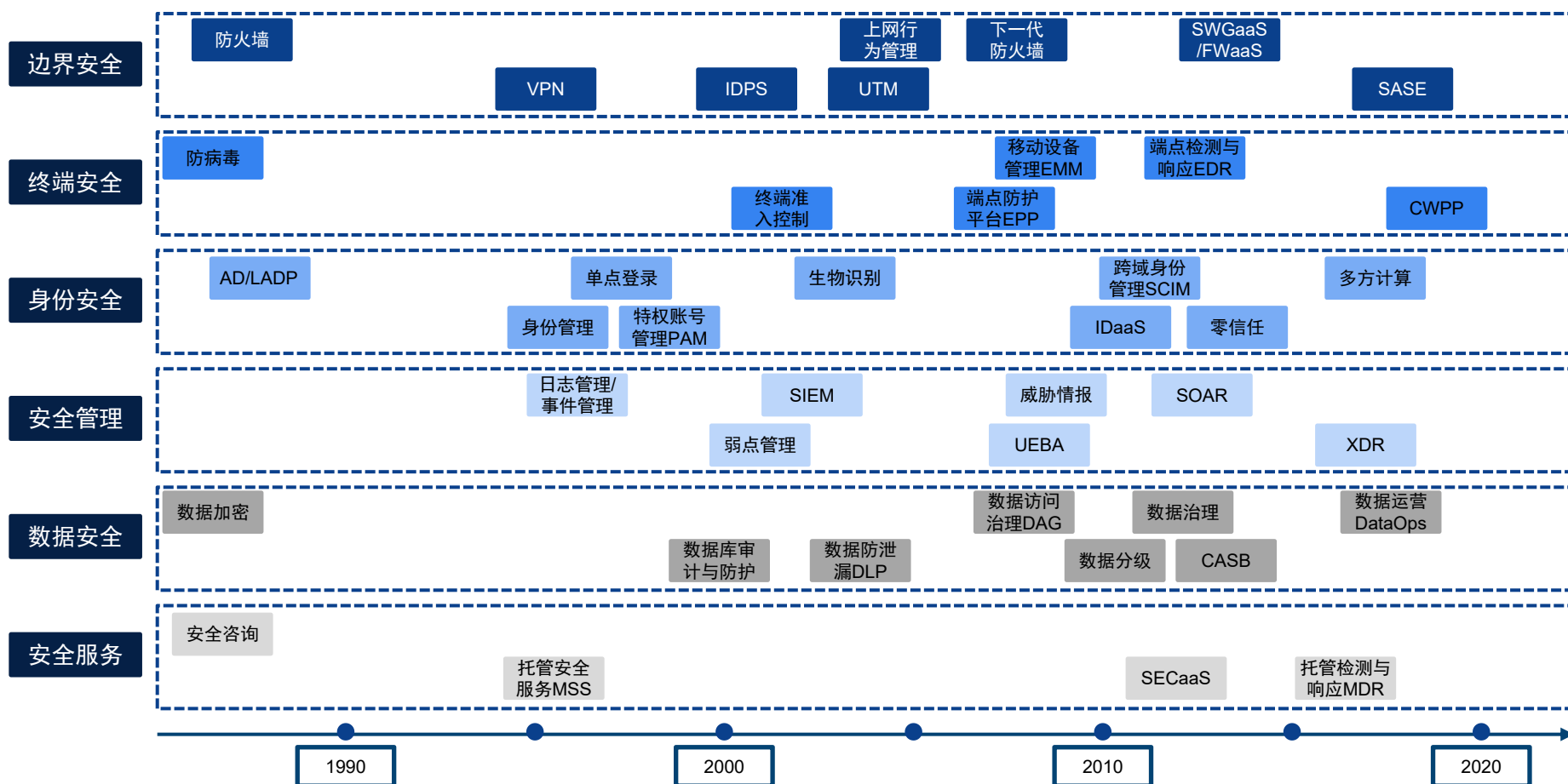
图表：安全行业格局现状

赛道	主要功能	核心技术	主要产品	规模及增速	头部厂商
边界安全	防入侵	网络层协议解析 网络流量分析	防火墙 IDPS VPN 上网行为管理 抗DDoS	250亿元 10%	华为、新华三、天融信、启明星辰、深信服、奇安信、绿盟科技、山石网科、迪普科技
终端安全	反病毒	文件解析 漏洞检测 终端管控	杀毒软件 终端设备管控 端点保护平台EPP 终端检测与响应EDR	45亿元 20%	奇安信、亚信安全、深信服、McAfee、Broadcom、北信源
身份安全	身份与访问管理	加密 身份认证 权限管理 AD/LADP协议	统一管理/4A平台 访问控制/单点登录 特权账号管理/堡垒机 密码/令牌/生物识别 零信任	30亿元 20%	亚信安全、数字认证、吉大正元、上海格尔、IBM、安恒信息、启明星辰、奇安信、齐治科技、飞天诚信
安全管理	安全态势分析	可视化 关联分析 数据挖掘 用户行为分析 编排与自动化响应	SIEM/SOC 态势感知 威胁情报 XDR 漏洞管理	50亿元 35%	奇安信、启明星辰、安恒信息、深信服、绿盟科技、天融信
数据安全	防止数据泄露	文件透明加解密 文件沙箱 数据访问隔离	数据库安全 数据防泄露DLP 文档加密 数据治理	100亿元 25%	启明星辰、安恒信息、绿盟科技、安华金和、Imperva、优炫软件、明朝万达、北信源、联软科技
应用安全	防WEB攻击	WEB漏洞扫描与防御 流量清洗 反向代理	Web应用防火墙 Web扫描器 网页防篡改	35亿元 15%	绿盟科技、安恒信息、阿里云、启明星辰、远江盛邦、新华三、长亭科技、知道创宇
安全服务	完善安全体系	安全框架和体系 安全人员梯队及培养 安全编排与自动化响应 陪跑业务布局及支撑	安全咨询 托管安全服务 安全实施与集成 安全培训与教育	270亿元 25%	启明星辰、奇安信、安恒信息、绿盟科技、天融信、安信天行、德勤、普华永道

过去技术创新是否改变了行业格局？

安全行业是一个技术创新非常频繁的行业，通常而言平均每3年时间就会有一轮小的技术迭代，但大多数情况下，新技术并不能形成独立赛道或催生出大公司，而是被过去的产品所内化。比如：UEBA、SOAR等功能逐渐融入SIEM。从投资的维度我们希望寻找的是：1）技术变革产生于足够大的赛道；2）能够对格局产生影响的重大技术创新。比如：下一代防火墙（Palo alto Networks）、端点检测与响应EDR（CrowdStrike）。

图表：安全行业技术创新频繁



AI+安全：小变革还是大变革？

长周期看，安全行业并不缺少景气度（全球安全市场长期增速维持在7%-15%，国内安全市场短期虽然景气在低位，但长期预期复合增速仍将保持在19%左右），因此安全行业的机会往往来自于格局的变化（能够催生出大公司）。安全行业格局变化的机会大小与两个因素有关，一是技术的颠覆性，即是否能够带来产品的重要变化，二是赛道规模的大小，其中，单赛道级的变革有下一代防火墙、EDR、终端国产化等，而云和AI将对安全产业的影响将大于过去单点的技术和产品创新。

图表：近10年安全产业重要技术变革比较

产业趋势	市场规模	新产品	老产品	时间	厂商	痛点/创新点
下一代防火墙	百亿	下一代防火墙	传统防火墙、UTM	2009	Palo Alto Networks、深信服	应用可视、用户可视、解决UTM在多功能下性能不足问题
终端国产化	十亿	终端安全	国产终端安全	2018	奇安信	党政信创终端全面国产化
AI 1.0	百亿	态势感知、EDR、SOAR等	SOC、SIEM、终端防病毒等	2012	Crowdstrike、安恒信息、深信服	“非黑即白”对未知威胁、复杂攻击手段识别效果不佳
云	百亿以上	SECaaS	本地安全软硬件	2010	Zscaler、Crowdstrike、Okta	边际成本的显著降低，安全大数据的网络效应，安全能力的动态迭代
AI 2.0	数百亿以上	AI安全大脑等	安全管理平台、安全服务	2023	Palo Alto Networks、Crowdstrike	大模型+生成式AI大幅提升安全运营能力、威胁检测能力、自动化处置与响应能力

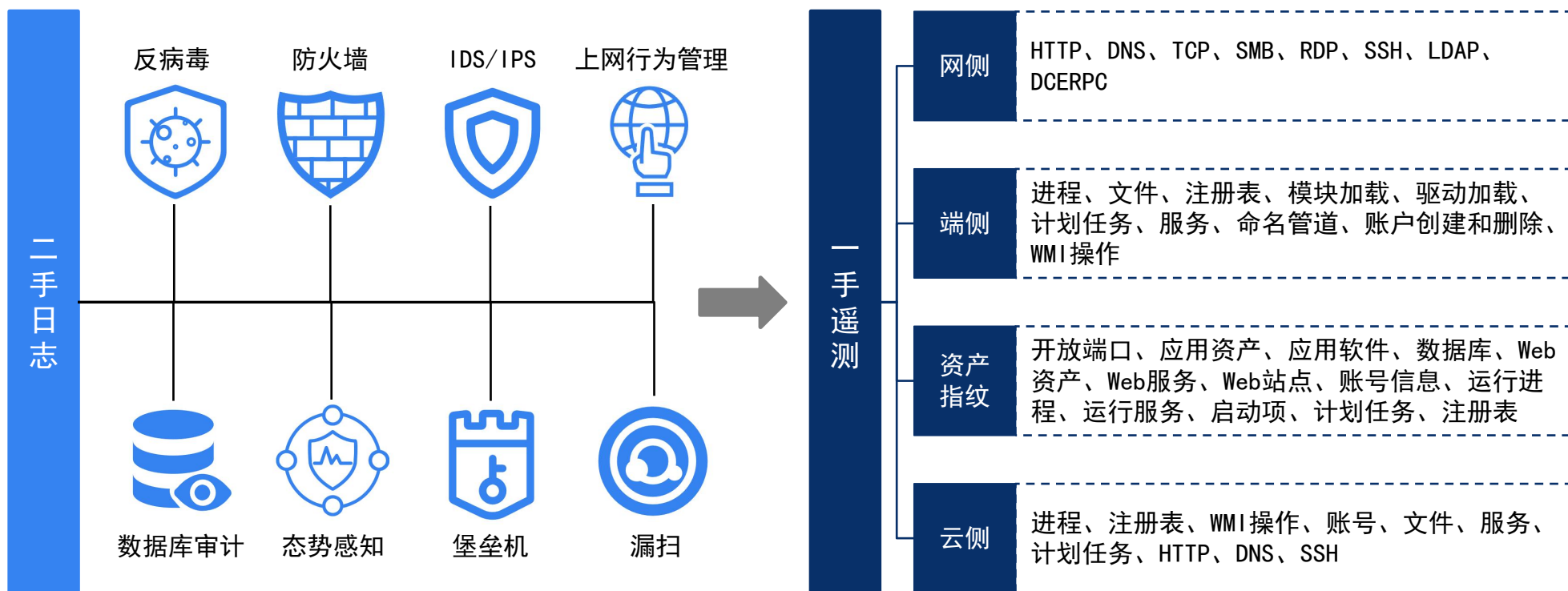
AI对格局的影响：安全大数据的重要性显著提升

AI带来竞争格局改变的可能：安全大数据提升了安全行业的规模效应。数据成为关键竞争要素，数据能力（包括获取/处理数据的能力）决定了安全能力，AI+安全的核心壁垒，是用更强大的模型来挖掘安全大数据

安全大数据的两大底座：云（足够大的数据量）+AI（足够强的数据分析能力），安全数据本质多源异构数据，从安全设备的二手数据到一手遥测数据，包括端点、网络、防火墙、电子邮件、身份和 DNS，分析和关联所有这些本地遥测数据+云端威胁情报，集遥测数据的单独组件，以一致的方式将其组合在一起以识别和阻止威胁。

大模型出现后，海外厂商强调的是AI带来的海量数据分析、理解、自动化处理和生成的能力，特别是那些云安全做的比较好且本身产品体系完善的厂商，用户多、数据多，规模效应更明显。

图表： AI+安全大数据的不同维度



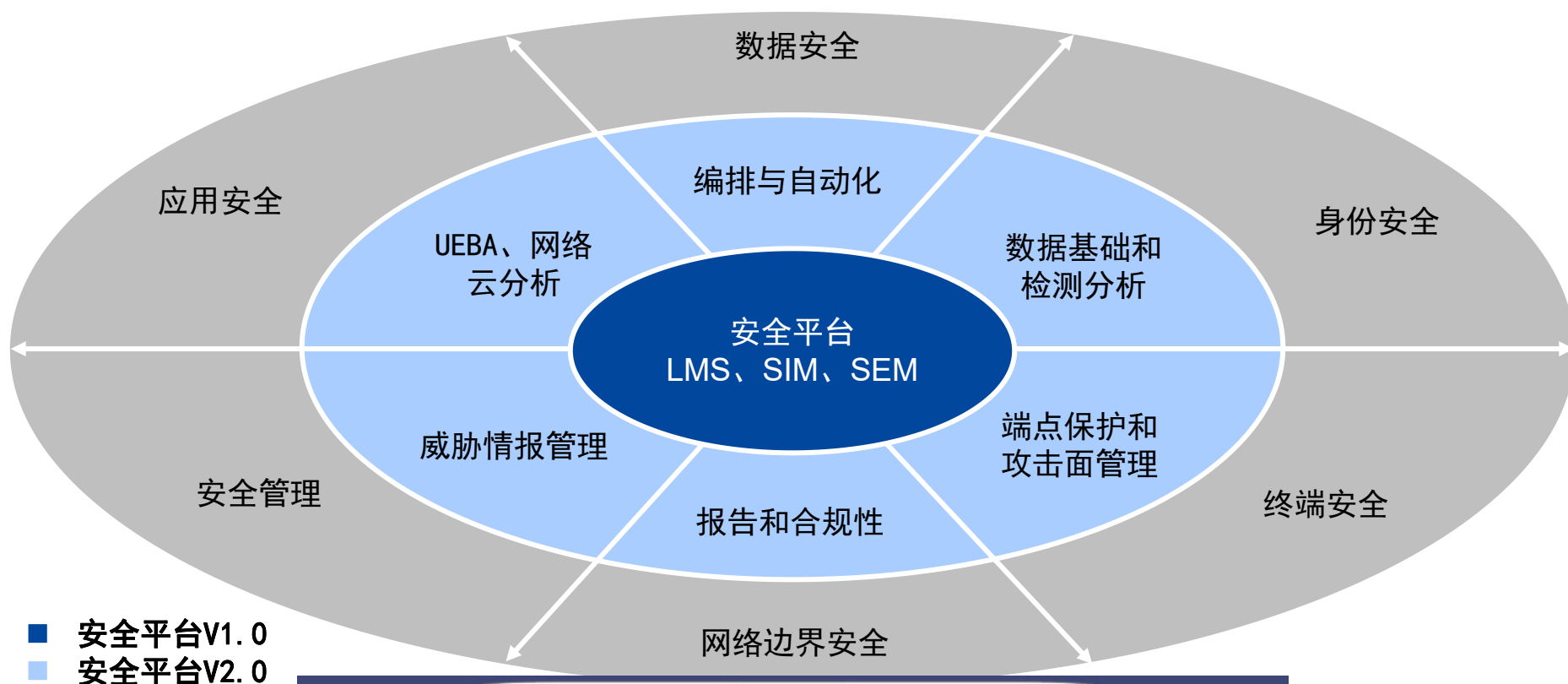
AI将带来安全平台能力的持续进化：

第一代平台（SIEM/SOC）：包含日志管理系统（LMS）、安全信息管理（SIM）、安全事件管理（SEM）三大基础功能，核心是安全日志与安全事件相关功能；

第二代平台（下一代SIEM/XDR）：集成UEBA、SOAR、EDR、威胁情报等多种安全能力，初步打通不同安全子系统的接口，整合各类安全产品的数据进行检测、分析和响应；

第三代平台（AI驱动的安全平台）：平台与整个子安全系统乃至IT、云、网络架构深度耦合，对不同安全域实现全方位纳管，形成整体防御合力，平台的能力边界向外进一步延伸。

图表：安全平台的进化路线

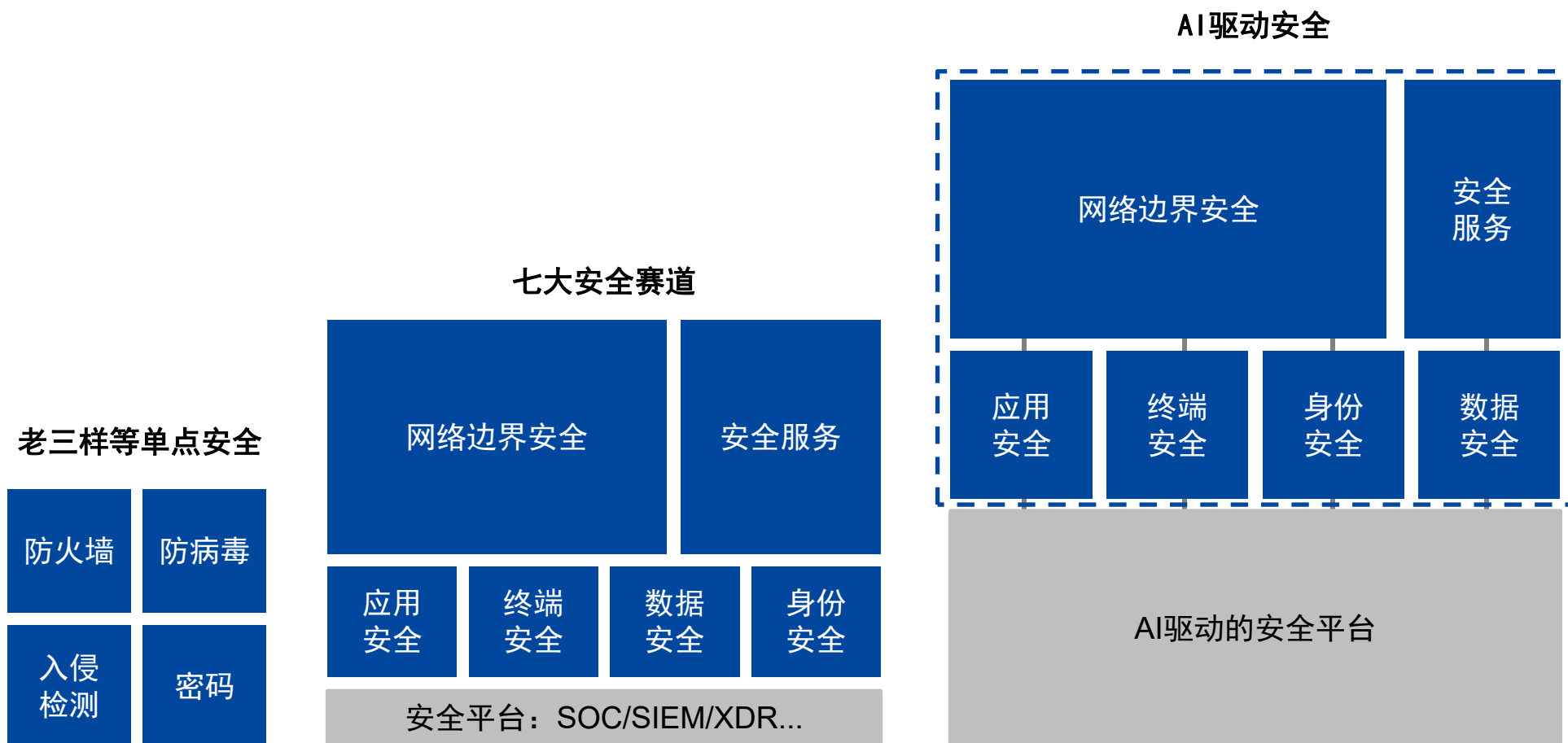


最终行业格局推演：AI能否提升行业集中度？

未来网络安全格局推演：1) AI驱动下，平台的作用提升，平台厂商产业链地位提高；2) 安全大数据是核心壁垒，头部厂商的优势非常明显，格局上强者恒强，头部的份额持续提升；

哪些公司能够受益：1) 拥有核心产品且产品联动做得比较好，具备比较强安全平台能力的厂商直接受益；2) 有比较广泛的客户触手，构建安全数据壁垒；3) 产品创新和执行力强，能够率先推动相关技术的商业化。

图表：网络安全行业格局演进



01

AI+安全驱动需求侧：AI加剧安全威胁

02

AI+安全变革产品侧：安全运营自动化

03

AI+安全的长期思考：竞争格局改变

04

国内AI+安全现状：明年产品有望放量

05

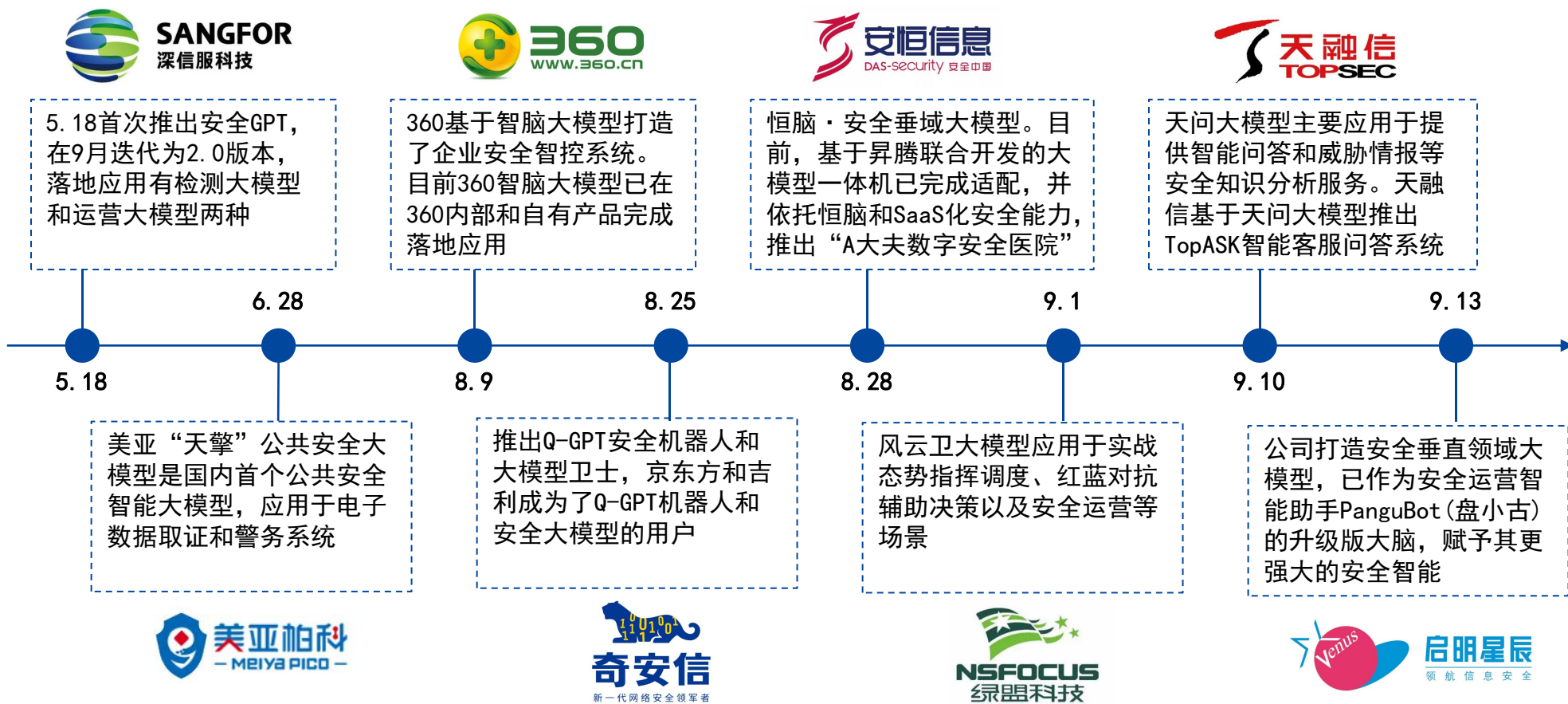
投资策略

国内AI+安全进展：预期不充分、产品还未铺开

国内AI+安全进展：包括深信服、奇安信、安恒等十余家头部厂商已发布AI+安全产品，目前正处于产品测试与市场推广的初期，预计明年产品将全面铺开。

中长期维度对AI带来的安全行业的变化——痛点解决得很明确，既会酝酿出新的大赛道上的新单品，也有希望从根本上改变安全的“复杂性”。

图表：国内网安公司AI+安全进展



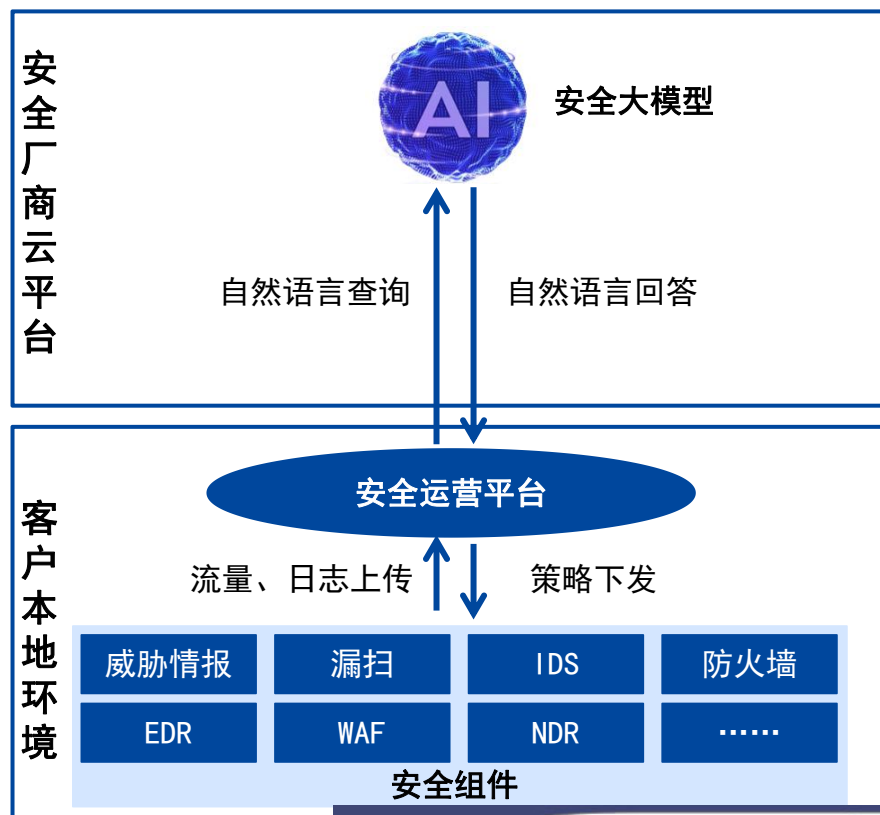
大模型如何落地：云化VS本地化

在大模型落地方式上，目前国内外安全市场存在明显差异。

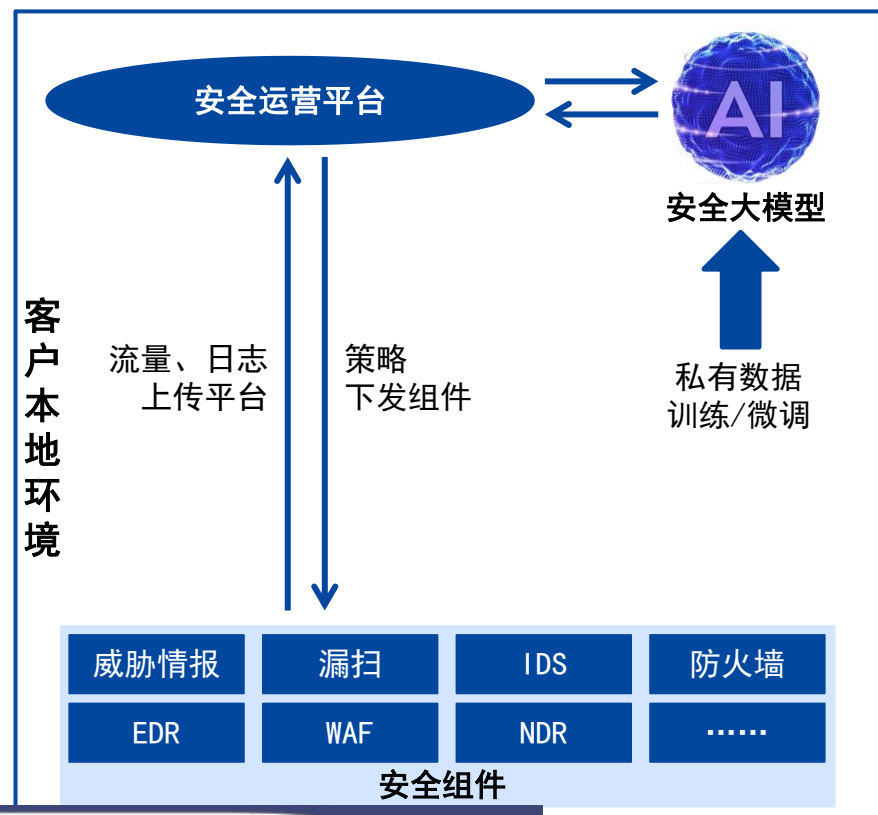
海外市场：云化部署占主导。海外客户对安全SaaS接受度较高，包括CrowdStrike、Panw等头部安全厂商均采用云优先的战略来推AI，头部安全厂商能够基于安全大数据去迭代优化安全能力。

国内市场：私有化本地化部署为主，少数场景也会考虑云化部署的模式。国内政府、金融等头部客户对数据安全要求较高，同时考虑算力成本以及大模型本地实施需求，训练/推理一体机的模式有望成为主流。

图表：大模型云化部署



图表：大模型本地化部署



模式一：深信服安全GPT

深信服在5月18日发布了国内首个安全垂直领域GPT大模型“安全GPT”，在9月22日展示了安全GPT的落地成果与2.0版本的升级，安全GPT2.0在检测和运营能力上得到了进一步提升。安全GPT 2.0升级的能力可分为两种，其一为检测大模型，即作为新一代检测引擎，更准确、更快速地侦测到潜在的入侵活动，如0day漏洞、APT隐蔽威胁入侵等；其二为运营大模型，即作为安全运营智能助手，实现自动化值守，提升安全运营效率和效果。

目前深信服安全GPT支持SaaS化及本地化多种部署方式，满足用户不同需求。在产品端，安全GPT现已全面赋能安全托管服务MSS，服务专家与“数字化助理”。

图表：深信服安全GPT



模式二：安恒恒脑大模型及昇腾一体机

图表：安恒昇腾一体机

安恒信息“恒脑·安全垂域大模型”于8月28日正式对外发布，同时发布了基于“恒脑”的安全运营平台。

“恒脑”平台能够为用户带来安全能力和安全效率的提升。

- 1) **安全能力提升**：能够从各种安全工具和数据源中收集、整合和分析信息，与态势感知、资产管理系统、威胁情报平台、漏洞管理系统等其他产品集成，从而实现全面的威胁情报分析和事件响应；通过大模型自动识别和分析安全事件，学习和适应新的威胁模式，从而提高对未知威胁的检测能力；
- 2) **安全效率提升**：通过智能编排来提高安全团队的效率和响应能力，帮助安全团队减少手动操作的工作量，从而提高响应速度和准确性。

目前恒脑大模型已顺利通过AI框架昇思MindSpore相互兼容性测试认证，基于昇腾联合开发的大模型一体机已完成适配，在国内安全大模型一体机落地上已占据明显先发优势。目前安恒信息已开始向客户交付恒脑大模型和一体机，主要服务于大型央国企客户，与其他厂商相比，公司拥有更早、更快拿货的优先权益。在近日的昇腾AI创新大赛2023浙江赛区决赛中公司凭借该解决方案获得应用赛道金奖，展现与华为昇腾在大模型领域的深入合作。



01

AI+安全驱动需求侧：AI加剧安全威胁

02

AI+安全变革产品侧：安全运营自动化

03

AI+安全的长期思考：竞争格局改变

04

国内AI+安全现状：明年产品有望放量

05

投资策略

今年以来，收入端由于安全行业的后周期性和政策空窗期承压，行业整体景气度处于低位。

中期有望迎来政策驱动下预算恢复，在今年机构调整后，关基、密码相关细则和预算对明年的需求能够起到一定提振效果。

图表：国内网安公司收入、毛利率、利润情况

证券代码	证券简称	市值/亿元	营业收入/亿元				毛利率				归母净利润/亿元			
			2022	yoy	2023Q1-Q3	yoy	2022	同比变化	2023Q3	同比变化	2022	yoy	2023Q1-Q3	yoy
002439.SZ	启明星辰	261.40	44.37	1.16%	25.34	16.84%	62.66%	-3.33%	61.85%	-1.50%	6.26	-27.33%	2.41	196.72%
300369.SZ	绿盟科技	80.15	26.29	0.76%	12.07	13.04%	62.28%	0.89%	54.73%	-5.97%	0.28	-91.77%	-5.24	-106.43%
688023.SH	安恒信息	98.96	19.80	8.77%	12.07	16.14%	64.20%	0.23%	56.03%	-1.37%	-2.53	-1935.70%	-5.36	-17.20%
002212.SZ	天融信	119.18	35.43	5.71%	16.48	12.63%	59.72%	0.31%	62.31%	1.09%	2.05	-10.83%	-2.48	40.85%
688225.SH	亚信安全	75.60	17.21	3.21%	9.92	3.59%	52.79%	-0.56%	52.00%	2.75%	0.99	-44.85%	-2.11	-26.88%
300454.SZ	深信服	336.38	74.13	8.93%	48.08	1.28%	63.82%	-1.67%	65.12%	2.80%	1.94	-28.84%	-5.46	21.69%
688561.SH	奇安信-U	289.55	62.23	7.12%	36.86	15.50%	64.34%	4.33%	60.75%	-0.43%	0.57	110.28%	-12.23	-8.69%
688168.SH	安博通	27.01	4.56	16.61%	2.75	10.29%	56.03%	-4.48%	63.99%	5.84%	-0.08	-111.72%	-0.70	-120.02%
300768.SZ	迪普科技	100.50	8.93	-13.31%	7.20	18.75%	67.79%	-3.66%	68.33%	0.99%	1.50	-51.57%	0.67	-1.60%
688030.SH	山石网科	36.50	8.12	-20.97%	7.00	1.89%	68.32%	-4.92%	61.18%	-12.93%	-1.83	-341.64%	-1.73	-347.53%
688651.SH	盛邦安全	38.95	2.36	16.56%	1.33	32.58%	77.69%	-1.11%	71.94%	-2.44%	0.46	-3.34%	-0.23	-46.30%
300188.SZ	美亚柏科	148.00	22.80	-10.08%	7.50	32.02%	52.24%	-6.14%	48.43%	0.82%	1.48	-52.41%	-3.97	-91.39%
688244.SH	永信至诚	39.08	3.31	3.28%	1.71	37.60%	59.61%	2.85%	56.92%	-4.79%	0.51	7.93%	-0.30	-38.57%
688292.SH	浩瀚深度	47.10	4.49	9.65%	3.69	45.11%	47.39%	-5.59%	51.10%	-0.76%	0.48	-18.74%	0.51	122.31%
603496.SH	恒为科技	101.28	7.71	13.61%	4.98	7.68%	43.03%	7.40%	37.94%	-5.98%	0.76	42.63%	0.32	-29.23%
002912.SZ	中新赛克	50.99	4.36	-37.20%	4.60	75.67%	66.15%	-2.81%	80.30%	6.31%	-1.22	-316.93%	0.74	173.49%
688201.SH	信安世纪	44.16	6.58	25.44%	3.43	10.10%	71.51%	-0.61%	70.40%	-2.69%	1.64	6.36%	-0.12	-122.51%
688489.SH	三未信安	56.42	3.40	25.69%	2.36	37.35%	75.47%	1.85%	72.63%	-3.61%	1.07	43.52%	0.40	33.24%
300579.SZ	数字认证	74.06	10.99	7.13%	5.91	3.67%	54.61%	-1.82%	52.41%	-4.51%	1.01	-12.63%	-0.20	-188.99%
003029.SZ	吉大正元	39.55	4.91	-39.82%	3.23	11.04%	67.24%	8.94%	56.82%	-9.91%	-0.34	-123.03%	-0.83	-28.98%
603232.SH	格尔软件	33.55	6.60	7.93%	3.31	28.83%	39.86%	-11.86%	42.02%	2.97%	-0.09	-110.93%	-0.37	26.11%
002268.SZ	电科网安	202.64	34.38	16.35%	17.21	16.40%	36.68%	-1.24%	43.74%	9.72%	3.07	28.81%	0.76	53.32%

网络安全行业长期成长逻辑不变，同时明后年AI安全、数据安全等安全新需求将带来新的增量。

同时随着预算修复和竞争企稳，叠加头部厂商估值也已经全面回落，当前板块整体投资价值已经逐步开始凸显。

重点推荐：启明星辰、安恒信息、深信服；**关注标的：**奇安信、天融信、绿盟科技、360、美亚柏科、中新赛克、电科网安、亚信安全、迪普科技。

图表：国内网安公司利润及估值

证券代码	证券简称	市值/亿元	三费（销售+管理+研发）				净利润/亿元			PE		
			2022	yoy	2023Q3	yoy	23E	24E	25E	23E	24E	25E
002439.SZ	启明星辰	261.40	23.09	6.75%	16.94	-9.79%	9.97	12.76	16.50	26.22	20.49	15.84
300369.SZ	绿盟科技	80.15	16.61	20.28%	12.19	6.14%	1.60	2.80	4.43	49.96	28.60	18.10
688023.SH	安恒信息	98.96	16.90	26.41%	13.61	14.08%	-0.07	1.49	3.20	-1369.99	66.20	30.88
002212.SZ	天融信	119.18	19.55	5.16%	14.42	-0.12%	4.25	5.81	7.55	28.04	20.50	15.79
688225.SH	亚信安全	75.60	9.54	26.44%	7.93	9.43%	1.10	1.66	2.64	68.73	45.50	28.69
300454.SZ	深信服	336.38	50.49	5.27%	41.14	1.45%	3.45	5.95	9.04	97.42	56.54	37.20
688561.SH	奇安信-U	289.55	42.73	2.68%	34.40	1.40%	2.24	4.78	7.38	129.06	60.55	39.22
688168.SH	安博通	27.01	2.52	25.48%	2.44	37.18%	0.77	1.22	1.64	35.05	22.16	16.42
300768.SZ	迪普科技	100.50	5.77	6.13%	5.12	18.77%	2.11	2.91	3.80	47.52	34.56	26.44
688030.SH	山石网科	36.50	7.76	8.99%	6.23	7.51%	-0.24	0.66	1.51	-151.98	55.54	24.16
688651.SH	盛邦安全	38.95	1.44	20.02%	1.35	30.86%	0.70	0.99	1.40	55.89	39.32	27.84
300188.SZ	美亚柏科	148.00	9.79	-11.00%	7.83	4.29%	2.66	3.51	4.46	55.61	42.14	33.21
688244.SH	永信至诚	39.08	1.48	4.39%	1.50	36.00%	0.86	1.26	1.78	45.70	31.01	21.95
688292.SH	浩瀚深度	47.10	1.61	1.43%	1.47	31.71%	0.71	1.06	1.57	66.45	44.30	29.98
603496.SH	恒为科技	101.28	2.55	14.96%	1.54	-4.39%	1.27	2.14	3.02	79.93	47.42	33.54
002912.SZ	中新赛克	50.99	4.98	8.87%	3.67	-0.23%	1.68	2.41	3.21	30.35	21.13	15.91
688201.SH	信安世纪	44.16	2.83	19.26%	2.57	40.69%	2.06	2.69	3.45	21.45	16.40	12.79
688489.SH	三未信安	56.42	1.49	26.84%	1.57	44.33%	1.51	2.03	2.65	37.42	27.82	21.26
300579.SZ	数字认证	74.06	4.63	2.85%	3.65	23.10%	/	/	/			
003029.SZ	吉大正元	39.55	3.64	14.99%	2.71	-0.10%	1.95	2.82	3.83	20.28	14.03	10.33
603232.SH	格尔软件	33.55	3.03	8.19%	2.14	-16.21%	0.50	1.02	1.51	67.10	32.89	22.22
002268.SZ	电科网安	202.64	8.82	12.61%	7.25	12.52%	4.02	5.22	6.72	50.28	38.82	30.15

数据安全风险：AI需要通过输入大量的数据输入来不断优化自身性能，一方面存在数据泄露和隐私安全问题等，另一方面数据不完备、数据投毒、数据滥用等行为也将将会对相关公司造成严重负面影响。

技术发展风险：生成式人工智能发展迅速，但技术的发展仍存在许多未知的挑战和风险，导致产业变革和应用落地节奏不及预期。

贸易摩擦加剧风险：目前AI训练芯片主要由海外厂商提供，若中美贸易摩擦加剧，将面临“卡脖子”风险，导致相关技术和产品研发不及预期。

道德和伦理风险：AI涉及道德和伦理价值观的问题，在具有重大后果的决策环境中，AI可能表现出意想不到的行为或做出具有不可预见后果的决定。

公司评级体系

收益评级：

- 买入 — 未来6个月的投资收益率领先沪深300指数15%以上；
- 增持 — 未来6个月的投资收益率领先沪深300指数5%至15%；
- 中性 — 未来6个月的投资收益率与沪深300指数的变动幅度相差-5%至5%；
- 减持 — 未来6个月的投资收益率落后沪深300指数5%至15%；
- 卖出 — 未来6个月的投资收益率落后沪深300指数15%以上。

风险评级：

- A — 正常风险，未来6个月投资收益率的波动小于等于沪深300指数波动；
- B — 较高风险，未来6个月投资收益率的波动大于沪深300指数波动。

行业评级体系

收益评级：

领先大市 — 未来6个月的投资收益率领先沪深300指数10%以上；

同步大市 — 未来6个月的投资收益率与沪深300指数的变动幅度相差-10%至10%；

落后大市 — 未来6个月的投资收益率落后沪深300指数10%以上；

风险评级：

A — 正常风险，未来6个月投资收益率的波动小于等于沪深300指数波动；

B — 较高风险，未来6个月投资收益率的波动大于沪深300指数波动。

分析师声明

方闻千声明，本人具有中国证券业协会授予的证券投资咨询执业资格，勤勉尽责、诚实守信。本人对本报告的内容和观点负责，保证信息来源合法合规、研究方法专业审慎、研究观点独立公正、分析结论具有合理依据，特此声明。

本公司具备证券投资咨询业务资格的说明

华金证券股份有限公司（以下简称“本公司”）经中国证券监督管理委员会核准，取得证券投资咨询业务许可。本公司及其投资咨询人员可以为证券投资人或客户提供证券投资分析、预测或者建议等直接或间接的有偿咨询服务。发布证券研究报告，是证券投资咨询业务的一种基本形式，本公司可以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，并向本公司的客户发布。

免责声明：

华金证券股份有限公司（以下简称“本公司”）的客户使用。本公司不会因为任何机构或个人接收到本报告而视其为本公司的当然客户。

本报告基于已公开的资料或信息撰写，但本公司不保证该等信息及资料的完整性、准确性。本报告所载的信息、资料、建议及推测仅反映本公司于本报告发布当日的判断，本报告中的证券或投资标的价格、价值及投资带来的收入可能会波动。在不同时期，本公司可能撰写并发布与本报告所载资料、建议及推测不一致的报告。本公司不保证本报告所含信息及资料保持在最新状态，本公司将随时补充、更新和修订有关信息及资料，但不保证及时公开发布。同时，本公司有权对本报告所含信息在不发出通知的情形下做出修改，投资者应当自行关注相应的更新或修改。任何有关本报告的摘要或节选都不代表本报告正式完整的观点，一切须以本公司向客户发布的本报告完整版本为准。

在法律许可的情况下，本公司及所属关联机构可能会持有报告中提到的公司所发行的证券或期权并进行证券或期权交易，也可能为这些公司提供或者争取提供投资银行、财务顾问或者金融产品等相关服务，提请客户充分注意。客户不应将本报告为作出其投资决策的惟一参考因素，亦不应认为本报告可以取代客户自身的投资判断与决策。在任何情况下，本报告中的信息或所表述的意见均不构成对任何人的投资建议，无论是否已经明示或暗示，本报告不能作为道义的、责任的和法律的依据或者凭证。在任何情况下，本公司亦不对任何人因使用本报告中的任何内容所引致的任何损失负任何责任。

本报告版权仅为本公司所有，未经事先书面许可，任何机构和个人不得以任何形式翻版、复制、发表、转发、篡改或引用本报告的任何部分。如征得本公司同意进行引用、刊发的，需在允许的范围内使用，并注明出处为“华金证券股份有限公司研究所”，且不得对本报告进行任何有悖原意的引用、删节和修改。

华金证券股份有限公司对本声明条款具有惟一修改权和最终解释权。

风险提示:

报告中的内容和意见仅供参考，并不构成对所述证券买卖的出价或询价。投资者对其投资行为负完全责任，我公司及其雇员对使用本报告及其内容所引发的任何直接或间接损失概不负责。

华金证券股份有限公司

办公地址:

上海市浦东新区杨高南路759号陆家嘴世纪金融广场30层

北京市朝阳区建国路108号横琴人寿大厦17层

深圳市福田区益田路6001号太平金融大厦10楼05单元

电话: 021-20655588

网址: www.huajinsc.cn