信息安全深度剖析6：海外巨头引领安全大模型，安全产业是AI价值洼地

行业研究 · 深度报告

投资评级：超配（维持评级）

证券分析师：熊 莉 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 kuhongyao@guosen.com.cn 证券投资咨询执业资格证书编码：S0980520010001

报告摘要

- **生成式AI在网络安全里的应用成为业界共识。**根据IDC数据，业界普遍认为在IT领域，生成式AI对网络安全、IT运维等领域影响最大。尤其是大模型和安全知识库的结合，对耗时耗人的安全运维将产生巨大变革。AI对网络安全攻防两端均带来影响，一方面降低了攻击者成本，一方面也提供了安全检测和运维的有利工具。从安全厂商角度来看，当前AI主要带来三大类产品：安全检测产品（EDR、防火墙等）、自动化智能运维（Copilot、XDR、SOC等）、使用大模型的数据安全产品（DLP等）。

- **海外巨头厂商持续投入AI+安全，大模型将大幅提升运维能力。**微软、谷歌这类大模型厂商，也均推出安全领域里的AI大模型产品，进一步验证大模型在安全领域的应用价值。以Palo Alto Networks、Crowdstrike等厂商为代表，海外龙头安全厂商一直保持高强度AI投入，即使在早期的检测类模型应用背景，Crowdstrike 也凭借AI技术颠覆了端点安全的市场格局。当前各大厂商的AI创新均以安全运维为核心，如Palo Alto 的XSIAM是面向AI重构的SOC平台；Crowdstrike也推出了Charlotte AI 运维助手。Cloudflare 推出了保护用户使用大模型的数据安全产品Cloudflare One for AI；同时基于其向边缘云的持续拓展，也在致力成为边缘端 AI 推理的工作负责。

- **国内安全厂商积极探索大模型应用，已形成初步案例。**奇安信推出了Q-GPT和大模型卫士，形成客户签约；深信服快速迭代，推出了安全GPT2.0，已有50多家客户试用；安恒信息推出了恒脑·安全垂域大模型，已经过大运会、亚运会检验；绿盟科技推出风云卫安全大模型，进一步提升智慧安全3.0能力；启明星辰、天融信等厂商也推出相关产品。与海外方向一致，国内厂商也致力提升安全运维能力。

- **投资建议：看好AI提升网络安全产业价值，维持“超配”评级。**AI 在安全运维里为甲乙双方节省的时间和人员成本是显而易见的，且拓展了传统安全的能力边界，不管是利用AI检测未知威胁，还是处理海量事件，均是AI带来的崭新价值，因此我们持续看好网络安全产业，维持“超配”评级。重点关注在AI大模型积极投入的厂商，奇安信、深信服、安恒信息、绿盟科技、启明星辰、天融信等。

- **风险提示**：宏观经济下行风险；行业竞争加剧风险；AI大模型和算力等产业发展不及预期；AI相关政策推进不及预期。

目录

网络安全是 AI 大模型在IT领域的最具期待的应用场景

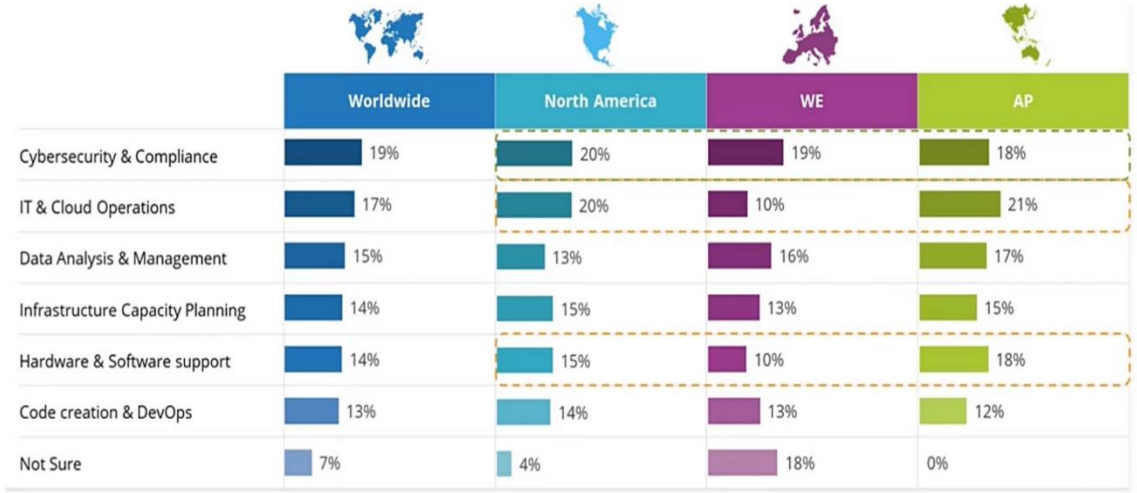
国信证券 GUOSEN SECURITIES

- **网络安全是 IT 领域生成式 AI 应用的共识。**根据 IDC 关于“GenAI 对哪些 IT 技术带来颠覆影响”的最新数据研究，世界范围来看均认为生成式 AI 对网络安全和合规的影响最大，还包括 IT 和云的运维、硬件和软件支持领域，整体上均可涵盖在IT 和安全运维方向。通过 AI 和自动化技术实现安全运维，在本轮大模型热潮之前，也是产业持续探索的方向。

- **多个安全领域均需要 AI 和自动化加成。**根据 IDC 关于“组织中哪些安全流程和功能需要更高级别的自动化”的最新数据研究，安全监管、数据安全和隐私管理、防火墙管理、事件检测和响应等环节均是业内关注的应用重点。业内对 AI 技术的应用已有积极探索，如早期的下一代防火墙上 AIops 的引入，以及当前安全领域 XDR 等产品的发展方向。

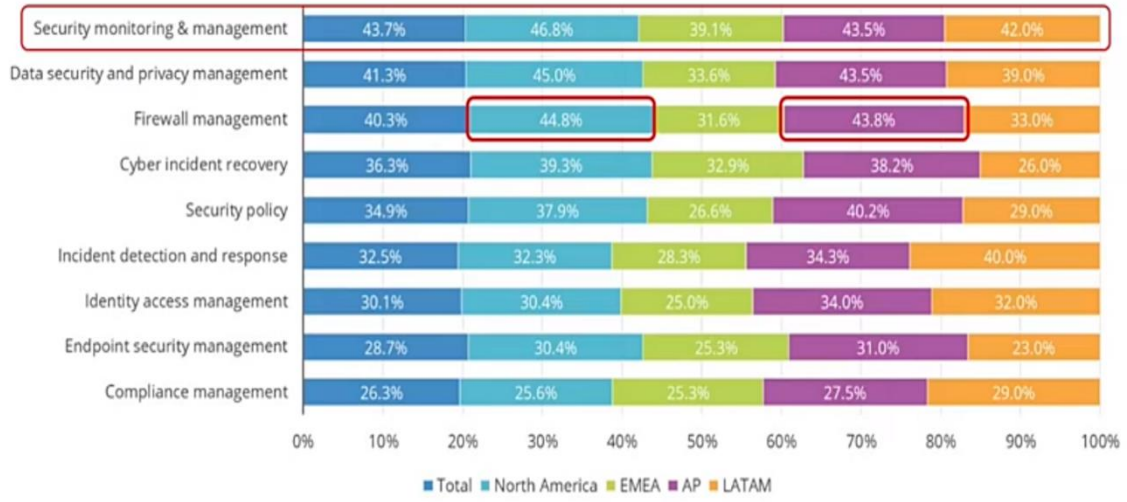
- **AI 影响网络安全攻防两端，市场空间广阔。**Gartner 曾警告称，“到 2025 年，利用生成式人工智能的攻击将迫使具有安全意识的组织降低检测可疑活动的阈值，产生更多错误警报，从而需要更多（而不是更少）人工响应。”根据 Precedence Research 数据，2022年全球基于AI的网络安全市场规模为174亿美元，预计2032年将达1027.8亿美元，2022-2032年复合年均增长率约 19.43%。

GenAI 对哪些 IT 技术带来颠覆影响



资料来源：IDC 2023、国信证券经济研究所整理

组织中哪些安全流程和功能需要更高级别的自动化



资料来源：IDC 2023、国信证券经济研究所整理

AI带来网络安全的思考——攻守两方均迎来升级

国信证券 GUOSEN SECURITIES

- **AI大模型和应用本身的安全问题**：和任何新的IT应用一样，如智能汽车、物联网带来的新安全问题，AI大模型本身也会存在漏洞，数据泄露等问题。常规的IT网络安全建设也是必不可少的，这部分和所有IT系统一样，模型厂商需要加强自身的安全建设。

- **AI大模型应用双方的数据安全**：模型方，训练数据必须脱敏、合规，与人类道德对齐等，这里需要传统数据安全的建设。用户方，也要建设合规使用场景，如不能投喂敏感数据，三星集团就曾因向ChatGPT提问中包含敏感信息，导致公司数据泄露。这部分更多也是传统安全建设，而且更依赖模型方（如训练数据的广义安全）、用户方自身的管理和合规（如DLP和访问控制等措施）。

- **AI诈骗等安全问题**：需要严格的内容审核机制，监管和模型方主要负责。例如，对于AI生成内容可以通过水印等方式标注，通过反生成式AI技术来鉴别是否由AI生成的产品。基于 AI 生成内容可能引发的问题，需要全社会多方角色共同治理。

- **AI降低了网络攻击成本，网络犯罪将增加。**其一、ChatGPT可以让一些几乎没有编程经验人编写可用于间谍、勒索软件、恶意垃圾邮件的软件；根据网络安全公司 Darktrace 公布的数据，攻击者使用 ChatGPT 造成社会工程攻击量增加了 135%。其二、AI大模型被黑客训练后的“黑化”，如黑客组织训练的WormGPT，集中在恶意软件相关的数据上训练，专为恶意活动而设计，输出没有道德限制，可以被要求执行各种恶意任务，收费标准是每月 60 欧元。网络安全属于一种社会工程学，当攻击成本下降后，也必然推动防守方安全建设的投资加大。

- **AI也加强了传统防护技术，大模型提供了新的运维范式。**AI 技术引入网络安全已经应用多年，多为小模型在检测类应用中的场景。在检测网络威胁上，AI比传统特征库匹配技术更进一步，能在特征被提取入库之前发现病毒或者威胁存在。在运维方面，大数据和AI分析帮助企业实现安全运维自动化。对于网络安全行业，AI技术的引入是提升自身能力的新方法，已有像Crowdstrike以AI技术颠覆传统终端安全市场。当前AI大模型已经引发了安全界广泛投入，AI 运维成为未来新范式。

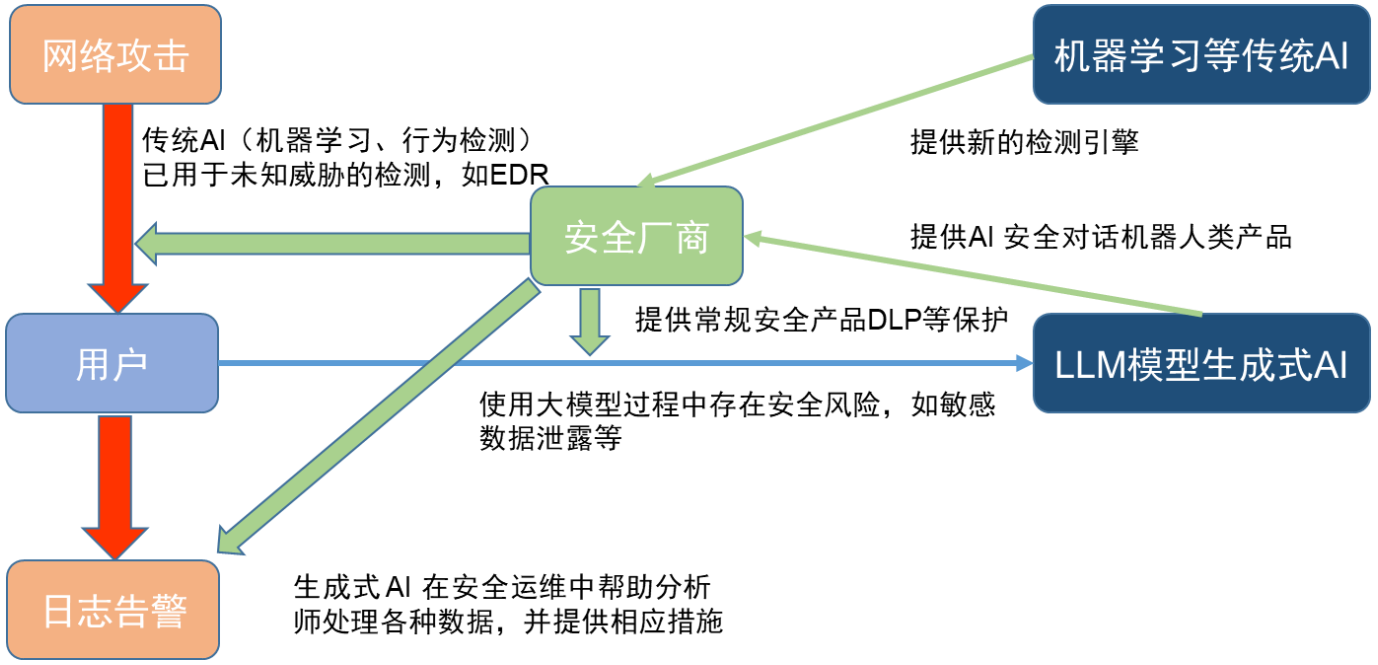
安全厂商能提供三类基于AI 应用的能力

- **检测模型类产品，提升安全检测能力。**在传统病毒引擎基础上，AI 基于机器学习，行为分析，结合海量威胁情报后能实现未知威胁的检测，大幅提升了传统产品的检测能力，主要应用在 EDR、防火墙、APT等产品。大模型出现后，未来 AI 检测能力将进一步提升。

- **运维模型类产品，目标实现自动化智能运维。**传统 AI 技术一直在安全运维里持续投入，比如XDR希望实现自动化检测和响应。大语言模型结合安全知识库，首先可以形成 Copilot 助手类产品，提供中级安全分析师的能力，减轻告警疲劳。大模型也能和XDR、SOC等结合，形成自动化日志、告警、事件的处理能力，大幅提升运维效率。

- **安全厂商提供用户在使用大模型过程中的数据安全能力。**用户在大模型使用中，存在敏感数据泄露等风险，安全厂商可以提供传统安全技术来进行规避，如DLP、访问控制等。

安全厂商能提供的三类AI安全能力



资料来源：Palo Alto Networks、国信证券经济研究所整理

网络安全技术中AI能力的应用——检测和响应是核心，早期AI应用已有探索

国信证券 GUOSEN SECURITIES

- **网络安全技术逻辑**：网络安全本质是发现问题和响应问题（包括解决），最好是在问题出现之前予以解决。

- **发现问题**：传统技术是病毒库、特征库、威胁库匹配，基于已知信息。利用AI技术，可以提升检测能力，在大量数据训练后，可以识别出未被标记的特征，实现未知威胁的检测。这部分能力主要是依赖传统 AI 小模型（如监督学习等），当前已在各类安全产品中有成熟应用，如端点安全，沙箱，各类安全厂商均有布局。

- **解决问题**：传统发现问题后，只能告警、日志，部分攻击也可以直接进行阻断。但依然有大量的人力工作，即处理大量各种不够准确的告警和复杂的日志，各种网络管理的规范和运维，依靠人力判断网络运行的潜在安全问题，因此业界一直在探索SOAR（安全编排、自动化和响应）、SIEM（安全信息和事件管理）、SOC（安全运营中心）等产品和方案，并不断加入AI技术以实现自动化安全。

- **大模型与知识库结合是应用落地趋势，安全知识库具备极佳场景。**大模型在医疗、法律等领域的应用已经初见成效，其行业特别是有大量的文本知识积累，具备较强的专业壁垒，依赖从业人员的经验等；大模型的能力能极大提升知识使用的效率。同样地，大模型也能在安全运营领域充分发挥作用，例如大量的日志、告警、事件、情报等信息数据，均是标准化的“类安全语言”，也是行业持续积累的知识库；各云、网、端不同设备和软硬件产生的数据，亟待进行上下文分析，并对企业整体网络运营产生推理作用，大幅减少甲乙双方安全运维人力。所以安全运维是非常适合大模型落地的AI赋能场景，微软推出安全copilot，谷歌推出Sec-PaLM安全大模型，均是目标在解决问题方面，实现自动化、智能化，减少运维压力。

AI 算法在网络安全中的应用

机器学习类型	训练目的	网络安全应用
监督学习	以标记数据训练，目标教它在遇到新数据时执行任务	在良性和恶意样本上训练模型，以教会它们预测新样本是否是恶意的
无监督学习	以无标记数据训练，目标寻找数据中的结构关系和模式	用于发现大型数据池中的新攻击模式或对手行为（例如异常检测）
强化学习	反复试验来学习，目标在最大化累积奖励，对于识别解决问题的创造性和创新方法特别有用	可应用于网络物理系统、自主入侵检测和分布式拒绝服务（DDOS）攻击的解决方案

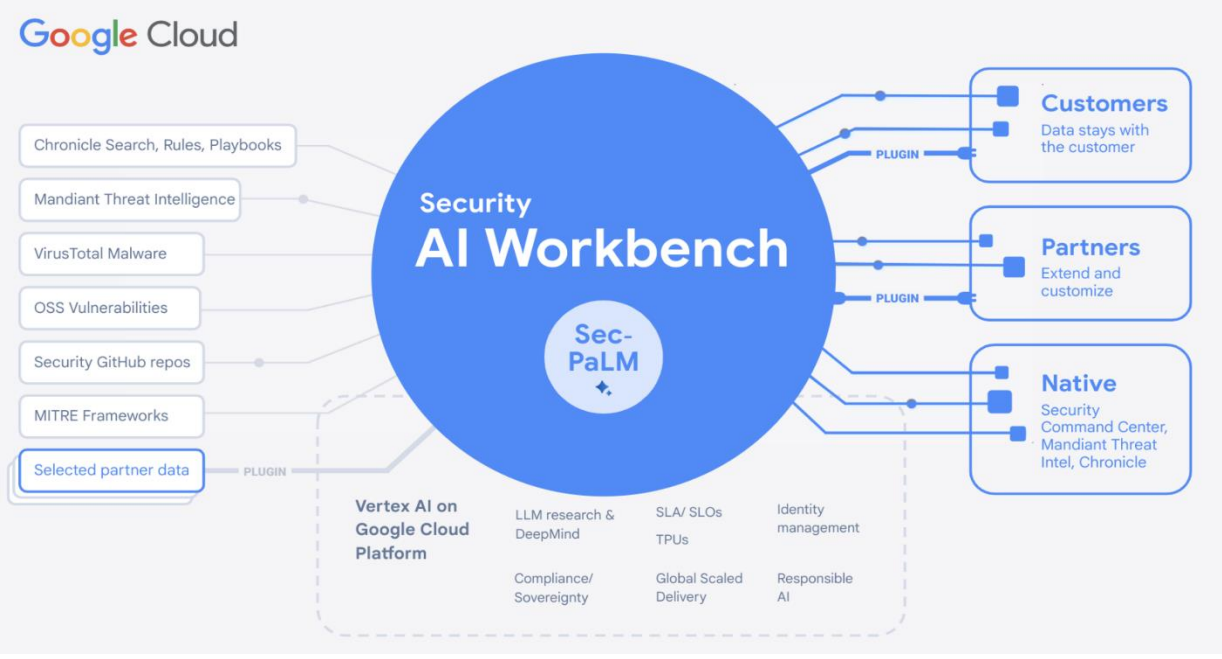
资料来源：Crowdstrike 、国信证券经济研究所整理

目录

谷歌安全大模型——Sec-PaLM2集AI安全能力大成

- **谷歌PaIM2模型也推出安全垂直应用模型Sec-PaLM2。**在 2023 年 RSA 大会上，谷歌推出了Google Cloud Security AI Workbench，这是由Sec-PaLM 提供支持的可扩展平台。Sec-PaLM 是谷歌PaLM模型的一个分支，针对安全用例和数据对其进行微调，如关于漏洞、恶意软件、威胁指标和攻击者档案的一线情报。其中，谷歌在22年9月收购威胁情报厂商Mandiant，提供了大量数据。埃森哲成为第一个合作伙伴。
- **Sec-PaLM2安全模型集各类AI安全应用于一身。**Sec-PaLM 解决三大安全挑战：威胁过载、繁琐的工具和人才缺口。**1）威胁过载**：利用AI及时检测威胁并做出响应，避免威胁感受后蔓延。**2）繁琐的工具**：生成式AI减少组织的安全工具和控制手段，如Assured OSS利用AI更好的集成漏洞管理方案，soc实时在线检测组织的恶意脚本并警报，Sec-PaLM 快速查找威胁情报并采取行动，最终减轻组织的安全工作量。**3）人才缺口**：Sec-PaLM让安全更易于理解，提升安全民主化，让初级安全分析师能力快速提升，如Chronicle AI类似于Crowdstrike的Charlotte AI，用对话交互实现对安全的运维；AI安全指挥中心将复杂攻击转化成人类可读的显性解释，给出相应措施。

谷歌安全 AI Workbench



资料来源：Google Cloud、国信证券经济研究所整理

微软——Security Copilot辅助而非取代安全分析师

- **微软推出基于AI的安全分析工具——Security Copilot，提供类ChatGPT的助理功能。**微软一直是网络安全领域收入最高的厂商，22年安全业务创历史新高超过200亿美元，同比增长33%，增速超过集团旗下其他主流产品。本次推出的Security Copilot，是基于GPT-4和微软自身安全相关模型的融合，是本轮AI大模型驱动的安全产品代表。在微软强大的安全业务基础上，安全大模型融入了其强大的威胁情报能力，每日65万亿个安全信号，微软Sentinel、Defender、Intune多个安全工具的数据和功能。Security Copilot运行在Azure云上，可以提供企业级的安全和隐私体验。
- **Security Copilot 以辅助安全分析师为核心。**Security Copilot 像聊天机器人一样提供对话框，辅助安全分析师的运维工作，可以在几分钟内评估风险敞口。Security Copilot 具备生成式AI带来的多个优势：**1）更好交互**：其如同随时接受问题的助手，用户可以直接询问企业的安全风险，攻击事件等。**2）总结问题，快速响应**：其通过总结、理解威胁情报，快速梳理出攻击事件和信息，优先处理重要事件，并推荐最佳行动方案。**3）修复常见攻击**：Security Copilot 与 Sentinel 和 Defender 等微软安全产品集成，能够自动阻断一些常见攻击，修复错误安全配置。其能展示安全威胁路径，目标也是帮助甲方运维，解决安全人才缺口问题，并不能完全取代安全分析师。
- **Security Copilot 在交互和应用上比ChatGPT具备更多尝试 。** Security Copilot 产品更类似于安全运维版的ChatGPT，且具备共享属性，包括相当多的便捷工具。其具备一个供同事合作和分享信息的便签板功能，可以用安全同事们就能在同一背景下开展威胁分析和调查；还具备一个提示簿，是一组步骤或自动化操作，可以将操作绑定到提示中。 Security Copilot 目前为预览版，尚未正式发布。

微软 Security Copilot

资料来源：微软、国信证券经济研究所整理

Security Copilot 工作界面

资料来源：微软、国信证券经济研究所整理

Palo Alto Networs——防火墙龙头云转型成功，AI贯穿安全能力始终

国信证券 GUOSEN SECURITIES

- **Palo Alto认为自己最有能力利用AI提供安全成果，用户对本轮安全领域AI应用兴趣提升。**Palo Alto 认为AI价值的充分发挥，在安全方面，需要大量**全面且实时**的数据，并具备足够的技术准备阻止威胁发生，公司每天有数PB的事件、会话、文件数据在其云、网、端节点上流经。Palo Alto 认为**本轮AIGC在安全中的应用逻辑有三**：第一、进一步推动此前已经应用的AI能力，提升底层检测和防护能力。第二、提升产品交互能力，即利用已收集的大型网络安全数据，提供更直观、更自然的语言驱动体验。第三、企业员工自身在AI应用中，提升流程和运营效率。伴随着ChatGPT的成功，越来越多的用户开始咨询在安全产品中能否部署AI，而此前用户对AI并不关心。Palo Alto也计划在未来数月内，将生成式AI融入解决方案中。

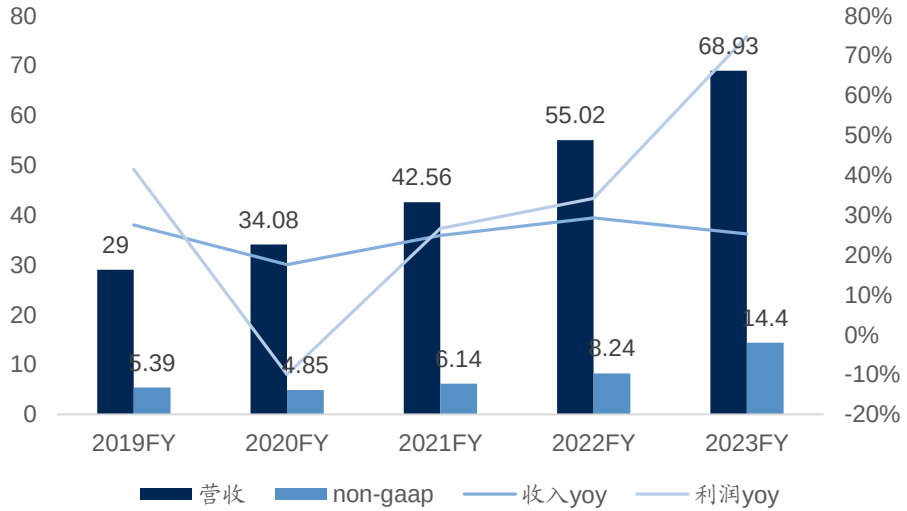
- **Palo Alto 是网络安全企业云和AI转型的典范，AI 能力始终是产品重心之一。**公司是下一代防火墙的开创者和领导者，将基于硬件为主的传统安全带到新的高度。同时，公司也是云安全、AI应用等创新技术的引领者，顺应 IT 架构云化、无边界化、零信任化、安全运营智能化等多方向发展，持续取得突破。公司始终坚持 AI 在安全领域里创新应用，从早期利用AI在检测端、运维端的尝试，到进一步以AI驱动的新一代SOC平台，生成式AI方面也积极跟进 Copilot 产品。公司各方面转型顺利，23财年SASE、Cortex订单量均超过10亿美金，Prisma 也超过了5亿美金，下一代安全（NGS）ARR增长了56%。公司23财年首次实现表观盈利，24财年收入指引达到81.5-82亿美金，增长18-19%，超出华尔街预期；未来三年预期收入和订单增长复合增速在17-19%之间，26年硬件占比将下降至10%。

Palo Alto 在安全产品中的AI应用

领域	AI应用产品	AI价值体现
检测端	云沙箱WildFire	本地无法判断的文件上传云端，通过机器学习在沙箱中识别恶意程序
	下一代防火墙	防火墙内联深度学习检测，可防止零日攻击，超越了基于传统签名的检测
运维端	AIOPS（基于防火墙）	通过机器学习检测防火墙设备健康状态，减少设备中端时间等
	AIOPS（基于SASE）	通过AI自动化实现网络连接的复杂操作，降低网络运营复杂性
检测与响应端	Cortex自动化安全平台	早期基于精准式AI的人工智能持续安全平台，包括XDR、XSOAR、XPANSE三大产品，结合AI技术面向检测、响应、运维，推动SOC的AI转型
	XSIAM（扩展安全智能和自动化管理）	面向AI视角重建了SOC平台，集成了Crotex核心功能，实现了智能数据、自动化运维、主动安全能力，是AI安全运营最突出代表
生成式AI	Network Security Copilot	将精准AI和生成式AI进行结合，共同消除安全的复杂性。通过自然语言对话，得到安全状况和相应策略

资料来源：Palo Alto Networks、国信证券经济研究所整理

公司近年来业绩表现（亿美元）



资料来源： Palo Alto Networks 、国信证券经济研究所整理

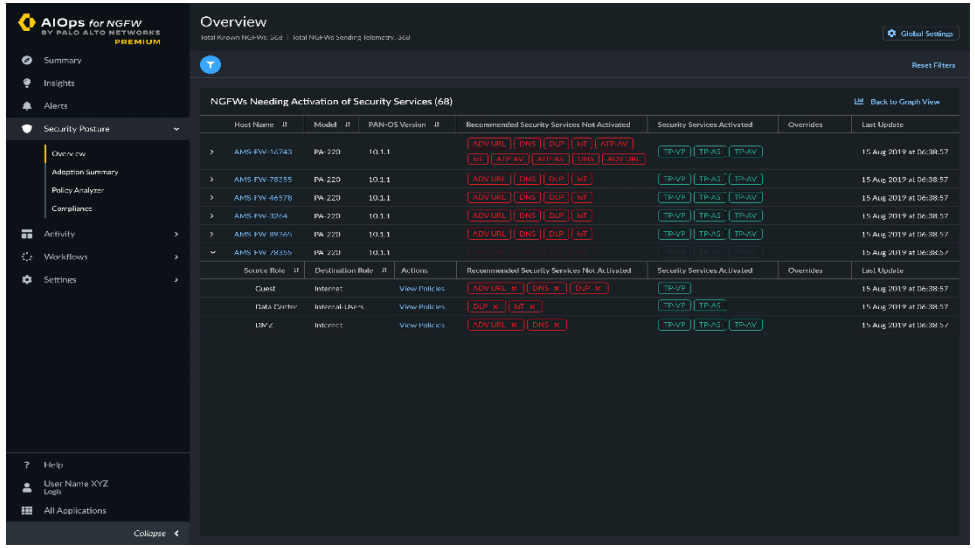
Palo Alto Networs——传统AI在安全中的应用

- **云沙箱通过AI对恶意程序进行分析判断。**Palo Alto 在2016年首次将机器学习功能作为 WildFire 产品的一部分引入，WildFire 是威胁情报云，或者是云上的沙箱。对于如防火墙等本地设备无法判断的文件，上传到WildFire，在虚拟环境中观察，采用了机器学习技术，识别快速变化的恶意程序；在对样本打上“恶意”标签后，可以迅速推送给所有订阅WildFire的用户，即实现众包智能。在最新的 Advanced WildFire 中，其也内联了机器学习引擎，可防止常见文件类型中的恶意内容，无需进行云分析。
- **Palo Alto将深度学习引入防火墙，能够检测未知威胁。**2020年推出了业界首款由机器学习驱动的下一代防火墙，其中内联深度学习检测可防止零日攻击，超越了基于传统签名的检测。深度学习技术可实现快速分类，在下载时检测文件，并在感染前阻止他们。该技术可以分析实时流量，包括可移植可执行文件、网络钓鱼、无文件攻击等，且无需对大多数恶意程序进行云端或者离线分析。AI能帮助防火墙将识别和阻止未知威胁的时间减少到几乎为零，而之前必须手动添加签名来实现防护。
- **AIOPS提升防火墙智能化水平和网络运维。**Palo Alto 防火墙具备AIOPS功能，通过机器学习提升设备整体的安全状况，即减少新设备采购；预测防火墙中断时间（最多提前77天），对于错误配置、软硬件故障等给出修复建议，即减少停机时间；主动分析和修复策略。AIOPS可以快速部署，且与ServiceNow 集成，以直观的仪表盘实现高可见性。AIOPS是安全运营的必然发展方向。

AIOPS对防火墙设备健康程度的管理

资料来源：Palo Alto Networks、国信证券经济研究所整理

AIOPS对防火墙产品各功能启用的管理

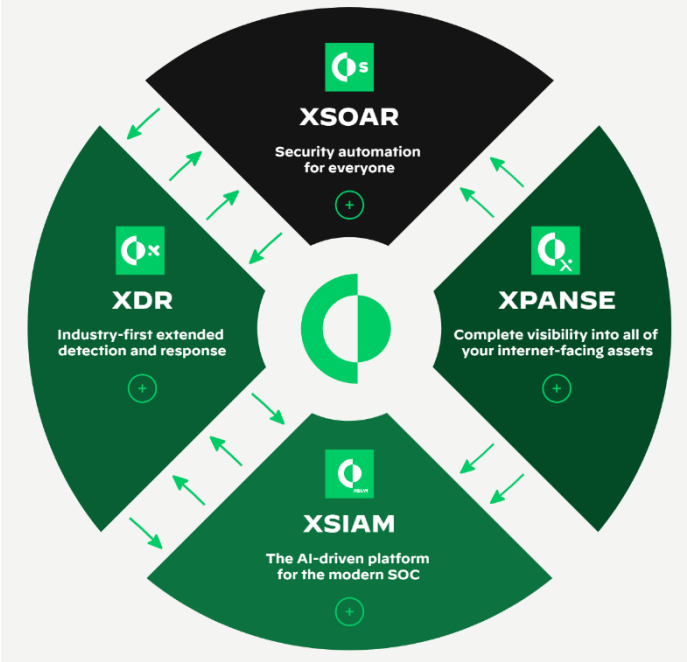


资料来源： Palo Alto Networks 、国信证券经济研究所整理

Palo Alto Networs——Cortex是前期AI融入安全的代表，致力于AI驱动安全

- **公司Cortex是业界首个开放集成的人工智能持续安全平台，探索智能化安全运维。**公司推出Cortex旨在充分发挥AI优势，简化安全运维和管理工作。Cortex部署于全球性可扩展公有云平台，能提高海量数据分析速度。Cortex数据湖可安全存储客户私有数据并分析，以AI技术发现威胁并快速编排响应策略。Cortex XDR于19年3月推出，业内首次将检测、调查、响应与网络、端点及云数据实现了原生集成。目前Cortex平台包含XDR、XSOAR、XPANSE（XSIAM的基本模块），均结合AI技术面向检测、响应、运维，推动SOC的AI转型。截止4月底的12个月，Cortex实现了 10 亿美元的预订（19年为1.5亿美元）。XSIAM是Cortex最新推出的产品，全面推动人工智能驱动的安全转型。
- **Palo Alto将AIOPS添加至SASE业务中，已于23年5月上线。**SASE是当前公司持续成长引擎，在最新功能中添加了AIOPS，以自动化网络连接的复杂操作，公司定义为业界首个针对 SASE 的“用于 IT 运营的原生集成人工智能”。SASE汇集了SDN、零信任安全、软件定义的安全 Web 网关等多种组件，AIOPS降低IT 和网络运营的复杂性，减少网络管理成本。

人工智能持续安全平台——Cortex



资料来源：Palo Alto Networks、国信证券经济研究所整理

Cortex四大模块功能

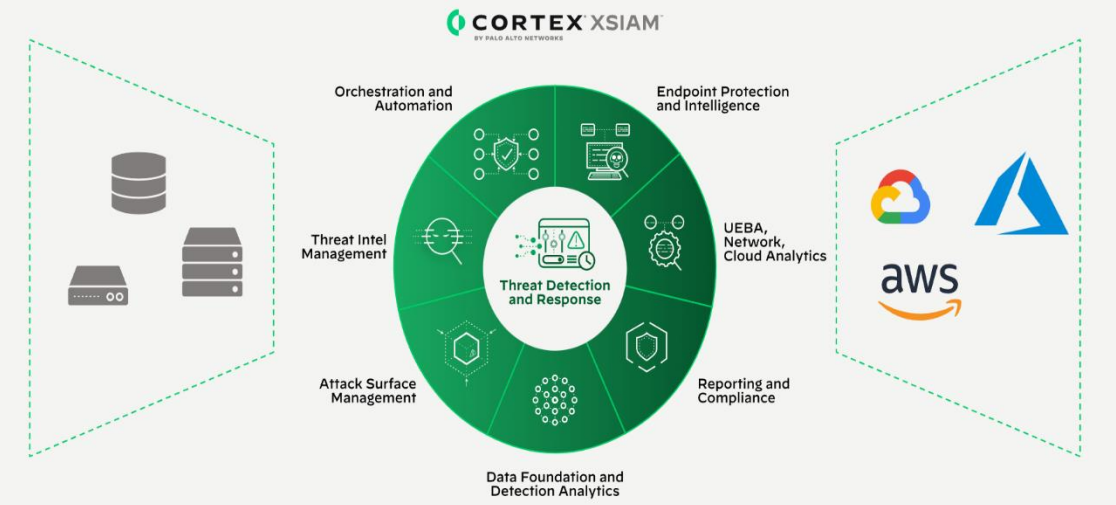
Cortex四大核心产品	主要功能	AI应用
XDR（扩展检测和响应）	不只是传统的端点数据收集，也扩展至网络、云、第三方数据，基于所有数据进行检测和响应。	使用行为分析发现隐藏的威胁，例如内部滥用、凭据攻击、恶意软件和数据外泄。
XSOAR（安全编排、自动化和响应）	帮助任何人，安全区域实现安全自动化流程。XSOAR也集成了威胁情况，解决事件速度提高 90%，处理事件减少 75%，为所有安全用例实现安全运营转型。	通过机器学习平台，可根据过去的事件和分析师的行为，为安全分析师决策提供指导
XPANSE（攻击面管理）	以攻击者角度从外向内查看企业所拥有的资产，以及可能存在暴露风险的资产，让用户能及时发现、评估和减轻网络攻击面风险，这比用户自己手动盘点的资产多35%。	使用监督式机器学习模型不断绘制客户的攻击面，并确定修复工作的优先级。在不增加人力的情况，减少威胁检测和响应时间。
XSIAM(扩展安全智能和自动化管理)	更自主智能的SOC平台，将大量基础架构产生的数据、威胁情报和外部攻击面数据转化为智能数据，为高级机器学习模型提供动力，实现全面有效的自动检测和威胁响应	设计之初即以AI驱动，目标使整个SOC达到一个更加智能的程度。除了日志和告警，还有更多细粒度数据来驱动AI，实现交叉关联分析，自动化响应操作

资料来源： Palo Alto Networks 、国信证券经济研究所整理

Palo Alto Networs——XSIAM用 AI 颠覆安全运营SOC

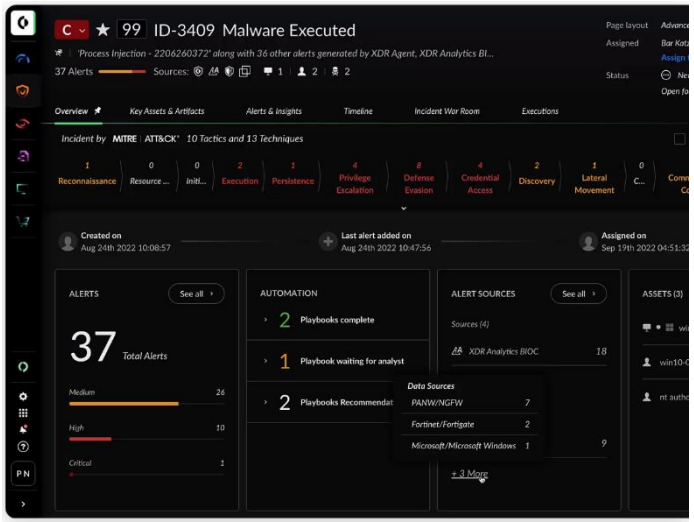
- **XSIAM是当前Palo Alto在本轮AI浪潮的重点产品。**XSIAM 汇集了 Cortex 的核心功能，为客户带来了AI驱动的应用成果。公司能收集10亿个事件，通过ai可以将事件告警下降到100多个。通过AI和自动化技术的应用，XSIAM 可以在几秒钟内检测到事件，并在一分钟内响应高优先级事件。公司使用 1000 个AI模型来检测攻击以实现加速调查响应。
- **SOC需要基于AI的重建。**传统SIEM围绕人类分析师构建（93%的soc处理需要人工流程），大量信息存在孤岛管理问题，且依赖人的处理；同时，安全工程师和架构师深陷于集成单点产品和数据源，以此进行检测和响应。最终导致传统SIEM以警报、日志为核心保障安全运营，但收效甚微。而AI是实现实时攻击检测和修复的唯一选择，因此要实现自动化处理，下一代SOC必须以AI视角重建。
- **AI驱动的XSIAM 将颠覆SOC，是网络安全“解决问题”的最理想答案。**现代SOC的转型，需要处理 EDR、NDR、云、身份、威胁情报和其他类型的数据，而所有数据处于孤岛，并非传统SIEM覆盖范围。公司将 Cortex 平台与 XSIAM 结合使用，以高保真数据源、人工智能和自动化为核心，对安全运营中心能力重组：**1）智能数据**：XSIAM 必须对各类数据进行规范化、理解并集成（即将其缝合在一起），实现AI级的相关性理解，使用事件上下文来驱动检测、调查和响应能力。**2）自动化**：XSIAM 对于攻击形成的事件链，利用AI学习形成自动化处理的检测器，或者响应策略。**3）主动安全：**XSIAM 还嵌入了威胁情报和攻击面管理功能，使安全分析师能够更主动地思考和采取行动。因此XSIAM将以AI重构整个安全运营模式。

AI驱动的全新 SOC 平台——XSIAM



资料来源：Palo Alto Networks、国信证券经济研究所整理

XSIAM 功能应用

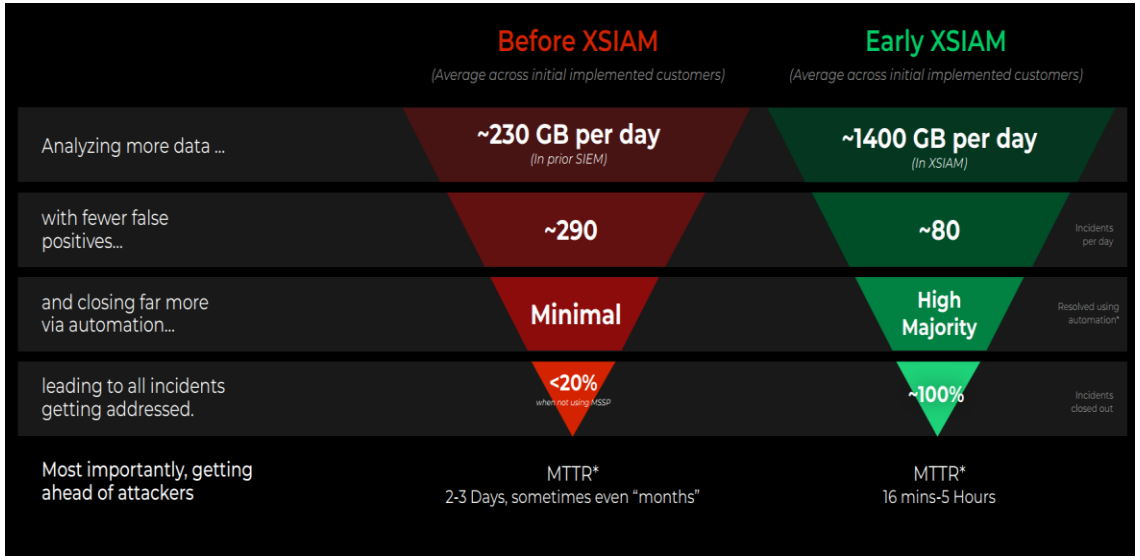


资料来源： Palo Alto Networks 、国信证券经济研究所整理

Palo Alto Networs——XSIAM 表现超公司预期，安全运维的AI需求迫切

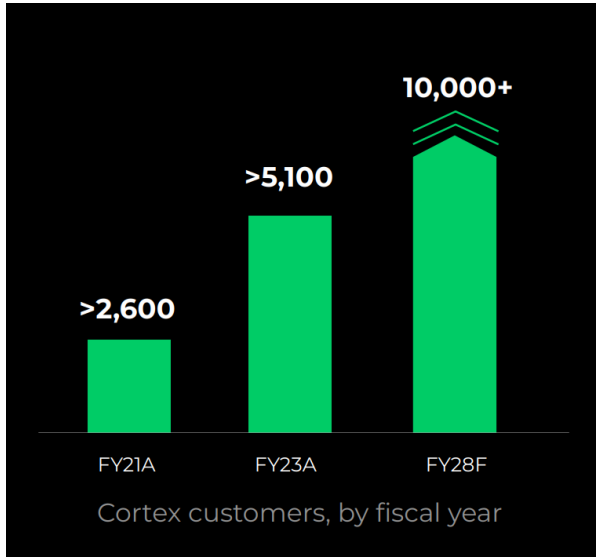
- **XSIAM 对客户已产生卓越价值。**XSIAM 不仅具备庞大的数据基础，利用AI将警报进行连接和标准化，同时添加上下文数据，取得了极好的效果。在部署 XSIAM 之后，客户安全价值显著提升：数据分析量提升到每天1400G；错误告警减少至每天80个；可以通过自动化关闭的告警达到更大占比；导致事件得以解决的概率接近100%；最终事件从创建到解决时间缩减至16分钟至5小时以内。
- **XSIAM 订单迅速超2亿美金，大订单成为趋势。**XSIAM于22年10月开始面向部分客户提供，截止23年1月底的Q2，已经实现了3000万美金订单，并已签署了首个8位数的解决方案协议，同时只有购买 XDR 才能获得 XSIAM。公司认为XSIAM将比过去所有产品更快达到1亿美元订单，事实上，不到1年已突破2亿美元，并且连续两个季度签署了8位数的协议。XSIAM 显著提升了订单规模，每笔 XSIAM 交易的规模都超过100万美元，23财年有4个订单超过2000万美金，而原 Cortex 客户迁移到 XSIAM的 ARR都提升了3倍以上。未来3-5年，Palo Alto 以及合作伙伴还会在 XSIAM 上增加10个以上模块，持续提升AI 驱动安全运维能力，Cortex 客户数量也将突破1万家。
- **客户也表现出对于AI能力SOC转型的积极需求。**公司XSIAM表现出极强的竞争力，在一家大型零售商客户中，公司以XSIAM为核心获取了超4000万美金的订单，并取代了现有的SIEM产品，增加了威胁情报和攻击面管理功能。需求方面，客户对AI提升运营能力较为迫切，尤其美国证券交易委员会新规要求上市公司必须在4个工作日内报告重大违规行为，客户需要大幅提升其安全效率。

XSIAM 在安全运维上产生明显价值



资料来源：Palo Alto Networks、国信证券经济研究所整理

Cortex 客户增长预期



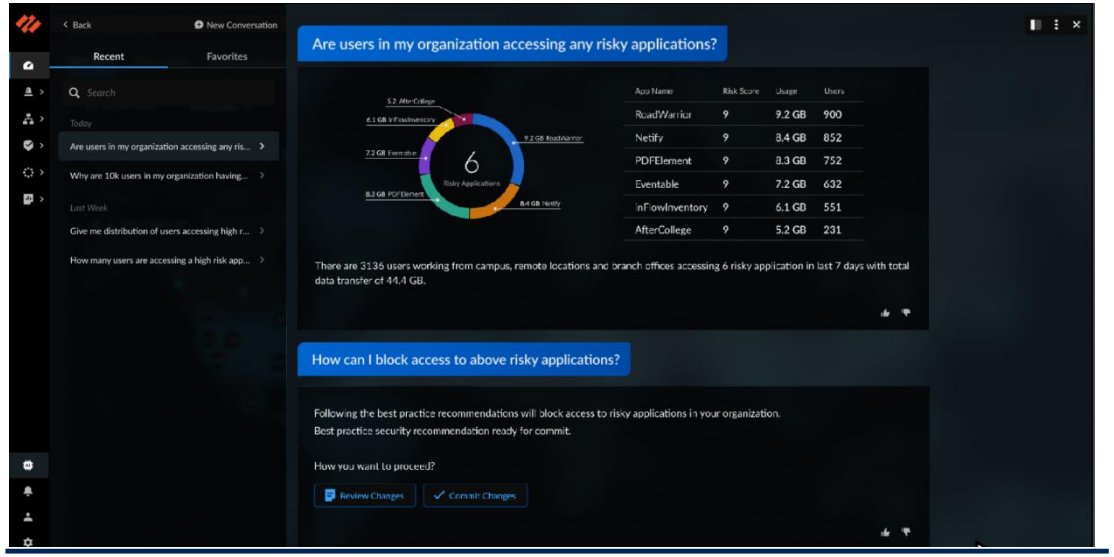
资料来源： Palo Alto Networks 、国信证券经济研究所整理

Palo Alto Networs——AI能力持续创新，也推出安全Copilot产品，关注代码安全

国信证券 GUOSEN SECURITIES

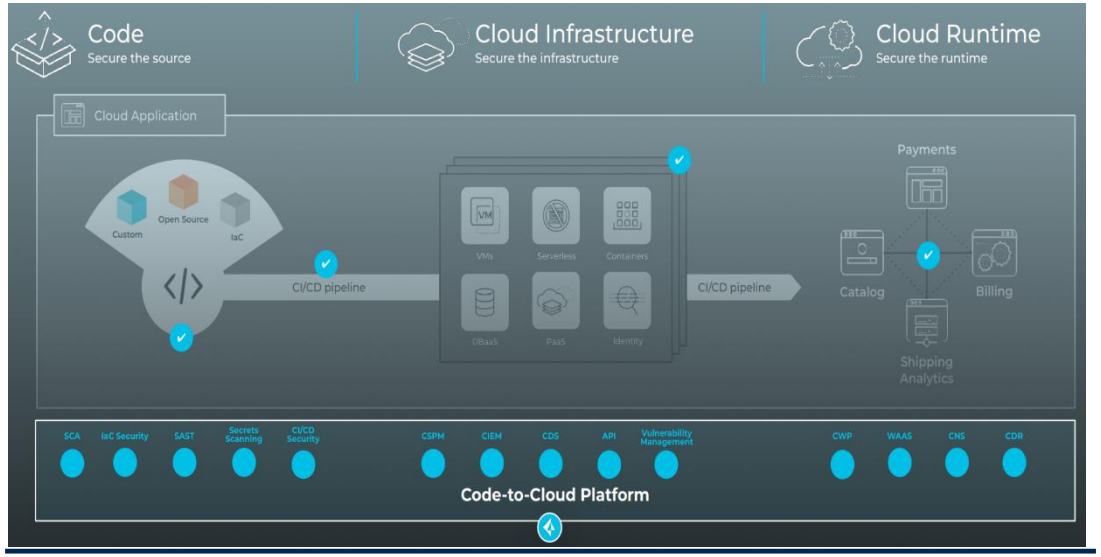
- **Palo Alto Networks 致力于在在每个安全产品中，利用AI copilot实现简单性和可用性。**此前公司在AI上一直保持投入，公司称为精准AI，有超过 100 个机器学习模型在产品中运行。但本轮生成式AI，也是具备极强的应用潜力，如产品开发人员和客户之间存在交流障碍，生成式AI能让客户用自然语言操作产品并解决问题。未来公司将精准AI和生成式AI进行结合，共同消除安全的复杂性。因此公司也推出Network Security Copilot，以自然语言对话的形式给出答案，如“组织中正在访问哪些风险程序？”，凭借 Palo Alto 硬件防火墙、软件防火墙、SASE等云网端的优势，给出了6大风险情况，并相应策略。公司也认为安全领域不能承受“错误答案”的代价，因此在持续研究如何降低 Copilot 的错误率。与此同时，交互模式的改变，也要让产品实现更好的 UI 设计和集成。公司计划产品集成在零信任平台，在年底前进行客户小范围测试，以获得真实客户反馈。
- **公司也关注到安全左移趋势，以及代码安全，但还未将AI大模型能力融入。**公司已经发现开源代码、AI主导开发的代码已经成为趋势，而这些代码在数十万个容器和程序中运行，代码阶段引入的漏洞、风险在云中是成倍增加的。 Palo Alto 关注的是传统解决方法，是为每个问题提供单点产品，如代码阶段就有有六种不同的工具来扫描。因此，公司推出了 Code-to-Cloud Platform，一种从代码到云端保护的集成平台，通过扫描程序生命周期的每个阶段，以实现实时保护。公司也有代码安全、基础架构即代码 (IaC) 安全等产品，加大在 DevSecOps 领域的投入，目前还未引入AI大模型能力。但是AI大模型在代码检测和修复上具备较高应用潜力，未来 Palo Alto 也有可能将其引入。

公司推出 Network Security Copilot



资料来源：Palo Alto Networks、国信证券经济研究所整理

安全左移下代码安全也可能引入AI能力

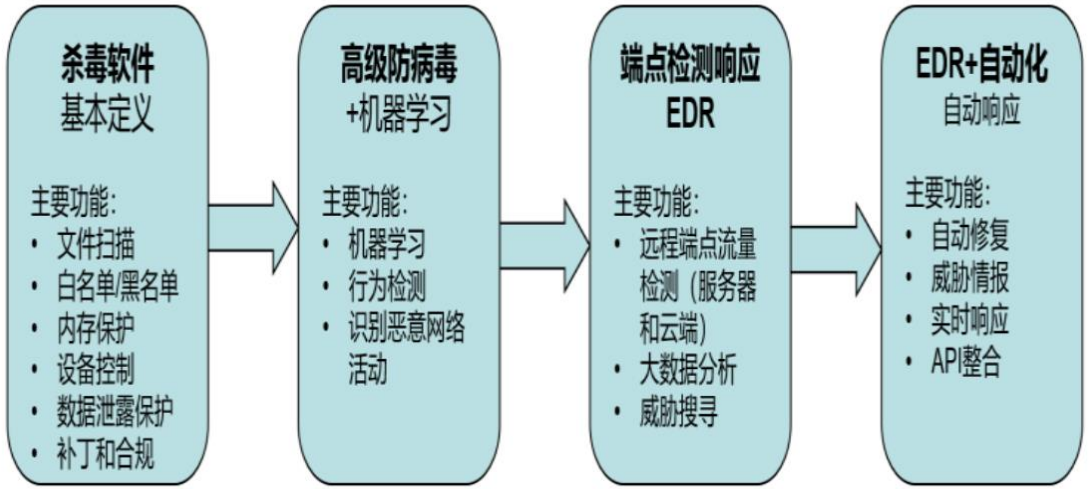


资料来源： Palo Alto Networks 、国信证券经济研究所整理

Crowdstrike——最早将AI技术引入终端安全

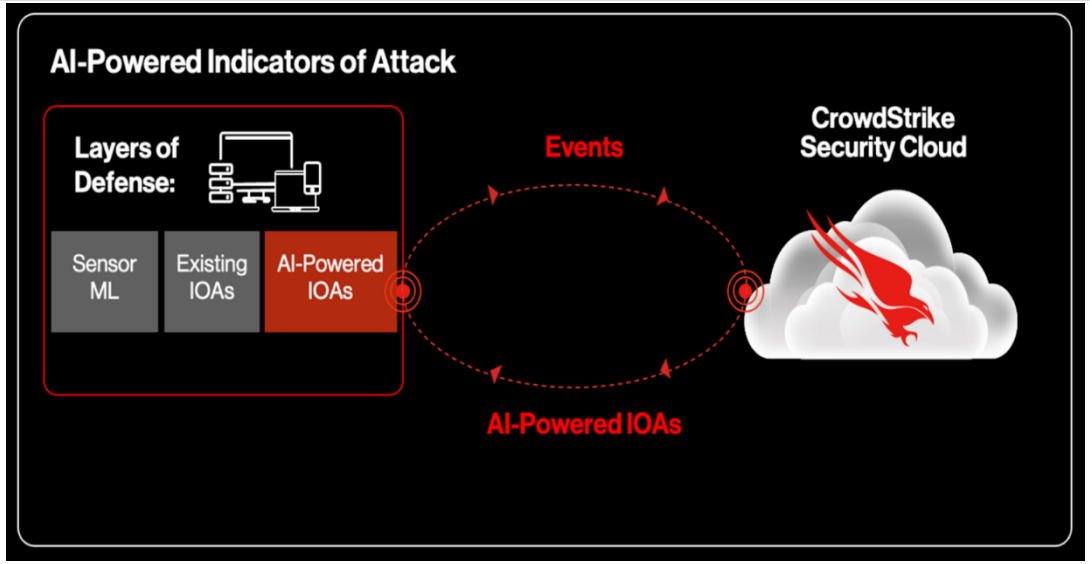
- **Crowdstrike 成立即是以AI和威胁情报颠覆传统终端安全。**2011年公司成立以来就将AI和ML引入终端安全，传统终端安全基于特征库匹配的模式，只能检测已知威胁；基于AI技术，通过机器学习、行为检测，实现对未知威胁的检测。CrowdStrike 的机器学习引擎成为第一个集成到 VirusTotal 中的无签名引擎。Crowdstrike 进一步以AI为基础，推动EDR、自动化等新的终端安全迭代。此时，AI对于公司主要应用三大场景：**1）检测**：通过AI识别攻击方行为和威胁模式。**2）分析**：快速、大规模地分析情报和数据。**3）自动化响应**：利用AI自动化执行重复的安全任务，自动检测和响应解决安全问题。
- **22年率先提出AI驱动的IOA，更快地预测和阻止威胁。**攻击指标（IOA）是Crowdstrike提出的概念，是一系列观察到的事件序列，显示正在进行或尝试入侵系统的活动（例如代码执行、持续横向移动等）。IOA让安全分析员能按顺序跟踪事件，识别攻击方如何获得最初权限，并推断出其动机和目标。IOA 还应用先进的行为分析来建模和预测对手模式，从而增强对未来攻击的预防。传统IOA生成依赖于全世界的专家模式，公司将人类专业知识与机器学习相结合，在云原生的CrowdStrike Falcon® 平台上训练这些模型，该模型可以在大量经过专业管理的恶意威胁和良性活动数据集上检测可疑活动。AI 驱动的 IOA有三大优势：**1）时效**：更快地检测新出现的威胁类别，与本地联动，领先对手一步。**2）共享**：实现自动化防护，云端与终端共享实时 IOA ，以阻止攻击。**3）精度**：减少误报并提高生产力，最大限度地提高分析师的工作效率。公司一直以AI驱动建立安全方案，每天产生2万亿事件用于训练，每秒180+百万IOA决策，颠覆和创新了大量新安全领域。

端点安全引入AI能力后的进化



资料来源：Crowdstrike、国信证券经济研究所整理

密码法相关要点

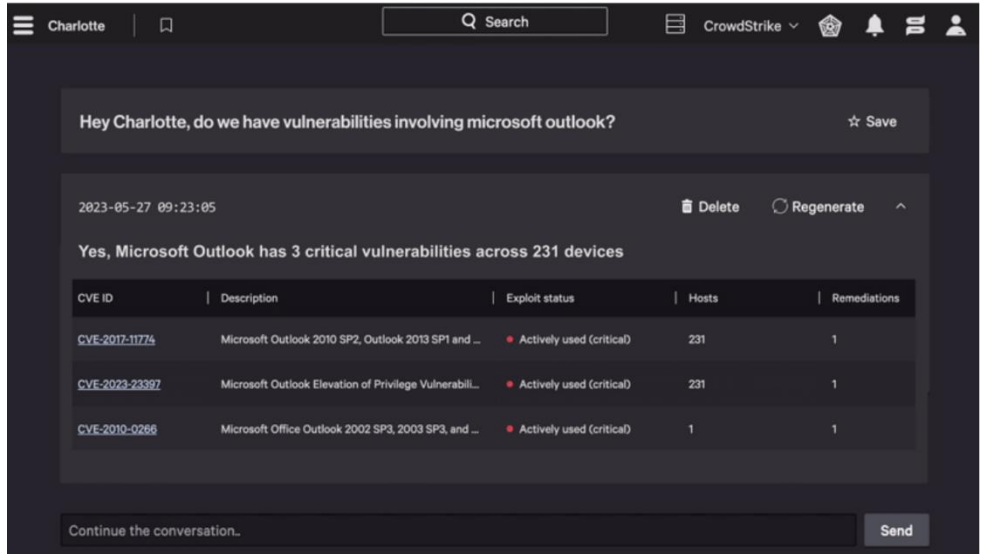


资料来源： Crowdstrike、国信证券经济研究所整理

Crowdstrike——Charlotte AI，生成式 AI 安全分析师

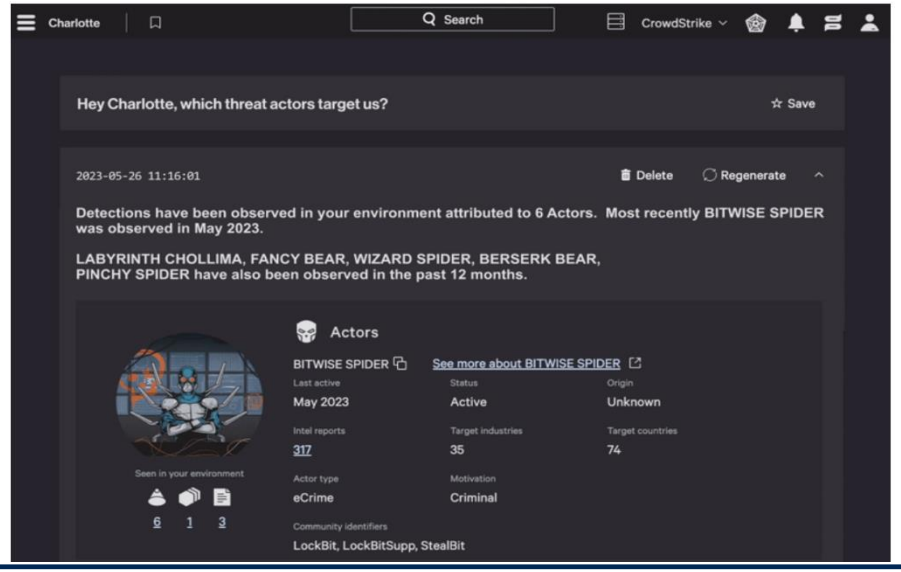
- **Crowdstrike 推出安全分析师Charlotte AI，提升人类分析师水平。**公司通过积累的大量安全数据，以及大量检测与响应的运维专家，在不断循环反馈改进中训练得到Charlotte AI。她将帮助任何技能水平的用户提高阻止威胁的能力，同时降低安全操作的复杂性。用户可以用简单的英语和数十种其他语言提出问题，并获得直观答案，让新手用户也能像Falcon 平台的高级用户一样操作，快速提升网络安全技能。
- **Charlotte AI核心是帮助任何用户更好的理解和运维安全。**目前Charlotte AI有三大用例：**1）更好的洞察**：任何用户都具备洞察组织安全状况，例如可以询问是否存在涉及 Microsoft Outlook 的漏洞。**2）更好的决策**：给予分析师更好决策，缩短对关键事件的响应时间，例如可以询问最推荐的补救措施是什么。**3）更好的执行**：帮助用户执行更高级的安全操作，可以在整个企业或特定区域内大规模自动化检测和响应操作，例如询问查找涉及 Windows 主机的横向移动。
- **Charlotte AI是本轮生成式AI的应用典型，类似于微软Copilot，致力于安全技术民主化。**在安全AI助手方面，Crowdstrike优势有三：**1）威胁情报**：公司是威胁情报领导者，Charlotte AI利用该知识库，可以推理和理解世界各地的对手活动。**2）XDR提供的丰富数据**：各种平台和来源的万亿个安全事件、环境和资产数据、漏洞等，形成Charlotte AI追捕和修复威胁的能力。**3）专家知识**：公司认为真正改变行业并领先攻击者的能力，是人类智慧和AI的结合，因此将专家经验编入 Charlotte AI 使用的数据集中。最终减轻任何安全分析师的工作量。

Charlotte AI 排查系统内的潜在风险



资料来源：Crowdstrike、国信证券经济研究所整理

Charlotte AI 给出攻击溯源和建议



资料来源： Crowdstrike、国信证券经济研究所整理

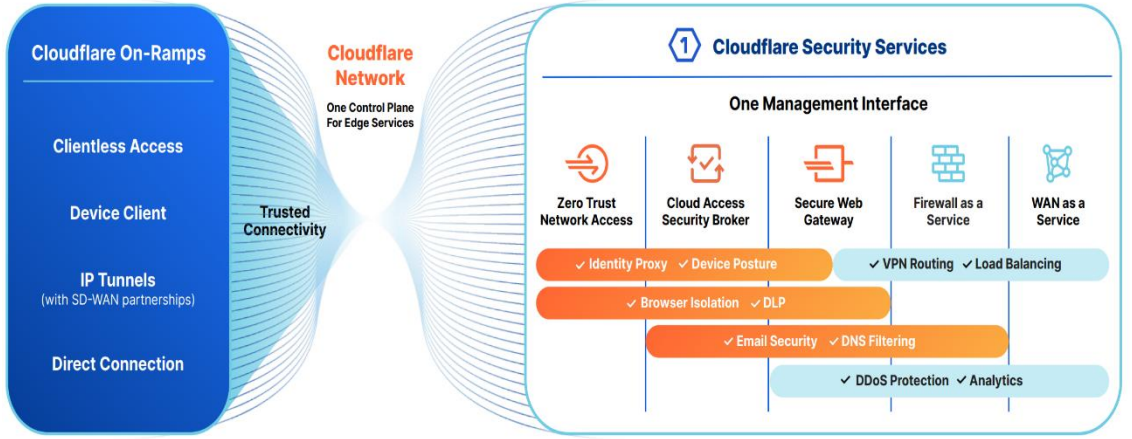
Cloudflare——安全视角：AI模型端的常规安全防护

- **Cloudflare 是当前AI应用安全最直接受益的公司，传统安全能力保护 AI 模型端Web。**全球所有用户在登陆 ChatGPT 的 时候，均需要经过一次“是否为真人”的验证，该服务即由 Cloudflare 提供。公司以安全的CDN业务著称，在全球部署300多个边缘中心，保护着数百万个 Web 资产；公司在提供内容交付加速的同时，也提供了众多安全功能，如DDoS防护，WAF等，深受网站用户的欢迎。得益于当前生成式 AI 的应用基本都在云端，Cloudflare 来自 AI 厂商的收入在季度间都能显示出快速增长，大型 AI 公司季度收入环比增长超过20%，从大到小的 AI 公司客户均呈现增长态势。这些一部分是 Cloudflare 的传统安全业务，即安全和CDN。
- **传统 AI 应用中，Cloudflare 利用机器学习模型来实现流量清洗。**Cloudflare 与其他安全厂商一样，很早就将 AI 技术引入安全产品中。在公司主打的 DDoS 流量清洗业务中，公司每秒处理超过 4600 万个 HTTP 请求，再为流量加速的同时，也需要准确检测威胁。因此，公司在边缘部署机器学习来检测威胁，多个机器学习模型来处理每个请求，公司已平均能每天阻止 1400 亿次。
- **Cloudflare 能提供 AI 应用两端的保护，核心 Cloudflare One 是SASE和零信任结合体。**Cloudflare One 也是当前主流安全公司云转型的SASE 方向产品，让用户无论在哪里，都能将用户动态安全的连接到企业资源。公司依托在 CDN 领域的积累，积极向 SASE 云安全发展，也融入了零信任等众多安全功能。对于 AI 应用，其也提供用户侧的连接安全，因此公司也推出了 Cloudflare One for AI 产品。

访问 Chatgpt 时的安全认证

资料来源：Cloudflare、国信证券经济研究所整理

Cloudflare One 产品融合SASE和零信任

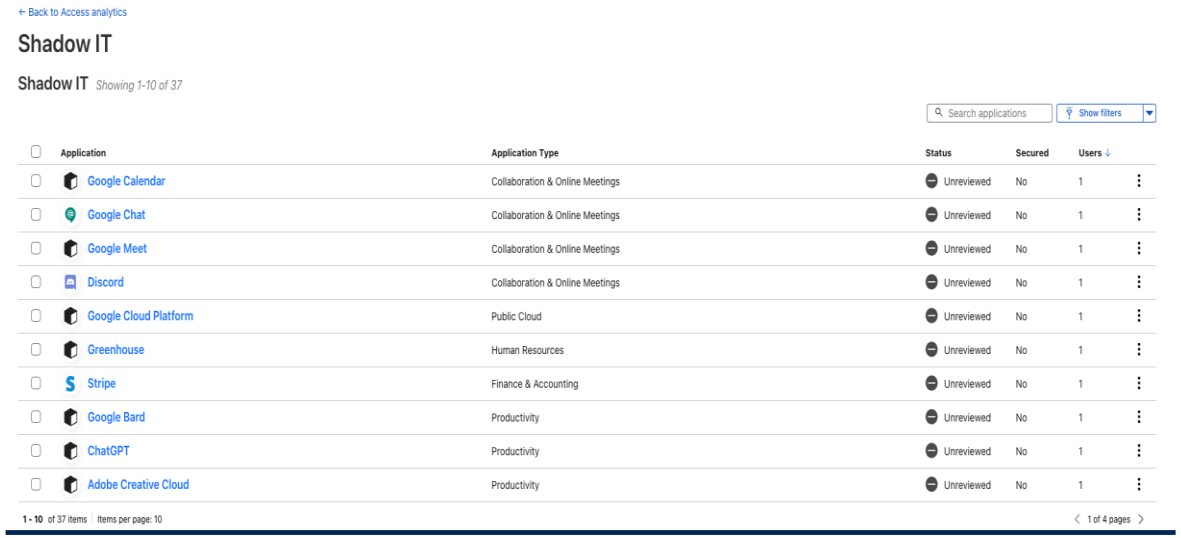


资料来源： Cloudflare 、国信证券经济研究所整理

Cloudflare——安全视角：用户端的 AI 保护，防止数据泄露

- **推出 Cloudflare One for AI，保护用户对于生成式 AI 的安全使用。**生成式 AI 的应用存在用户将敏感数据“投喂”给大模型的可能，导致数据泄露的风险。因此在23年5月，公司推出了Cloudflare One for AI，是一套基于其Cloudflare One 平台的零信任安全控制套件，旨在帮助企业安全地使用生成式 AI 工具，保证数据、知识产权等安全。Cloudflare One for AI 是一种云端服务，本质也是一系列云安全技术，而并非将 AI 功能融入该安全产品中，主要是传统的安全策略、访问控制、加密、DDoS保护等技术组合。该产品也支持各种类型的设备和操作系统，包括Windows、Mac、Linux、iOS和Android等，用户可在任何场景使用，也能根据自己需求灵活扩展。
- **产品基于用户端使用 AI 的保护，实现用户数据和隐私安全。**Cloudflare One for AI 为模型用户端提供了一套简单、快速的安全工具，如 Gateway、DLP等产品，可以了解并衡量 AI 工具的使用情况、防止数据丢失，提供了实时监测和警报机制。例如，企业员工在办公中会使用大量“Shadow IT”，即在企业批准之外，员工自己选用的SaaS或者AI应用等，这些会成为IT 安全的负担。 Cloudflare One for AI 可以看到组织内 AI 使用的情况，也可以阻止对AI的使用。DLP 产品可以提供配置规则，设置好所关心的数据，例如信用卡号码等，以实现对相关数据使用的检查。整体上，该产品主要融入了零信任的理念，更类似于终端和数据安全的结合。

Cloudflare One for AI 监管企业的影子IT



资料来源：Cloudflare、国信证券经济研究所整理

多个组件保护大模型使用的数据安全

Cloudflare One for AI 功能点	主要作用
Cloudflare Gateway	帮助公司观察有多少员工正在尝试 AI 服务，可以在企业做预算和许可数量数量时提供相关信息
Service tokens	为管理员提供清晰的 API 请求日志，控制可以访问 AI 训练数据的特定服务
Cloudflare Tunnel	提供了一个加密的、仅出站连接到Cloudflare网络的通道，每个请求都将接受Cloudflare One配置规则的检查
Cloudflare’s Data Loss Prevention(DLP)	数据防泄漏产品，防止员工向模型投喂敏感数据，可以自定义配置哪些数据类型
Cloudflare's cloud access security broker (CASB)	为SaaS应用程序提供全面的可见性和控制，还能扫描所使用的 AI 工具，检查错误配置和误用

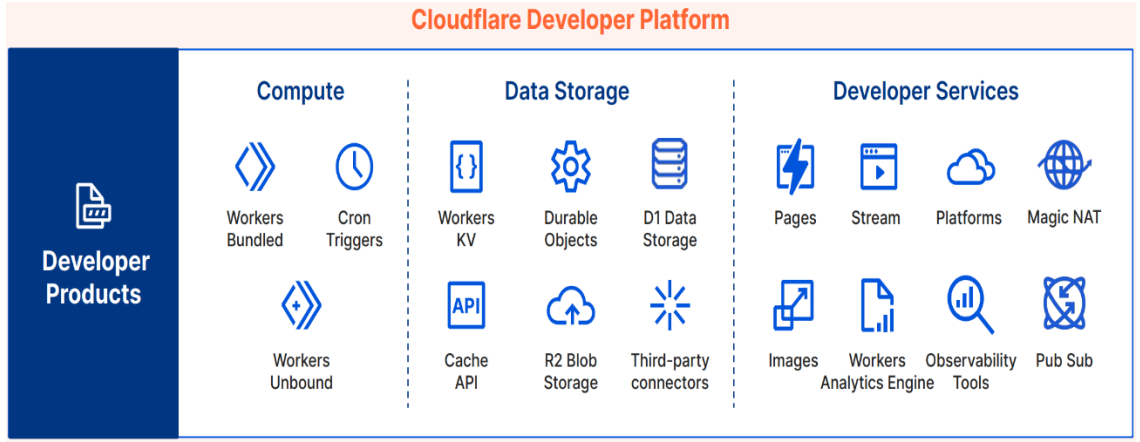
资料来源： Cloudflare 、国信证券经济研究所整理

Cloudflare——云视角：以网络安全能力撬动边缘云发展，成为 AI 开发的工作负载

国信证券 GUOSEN SECURITIES

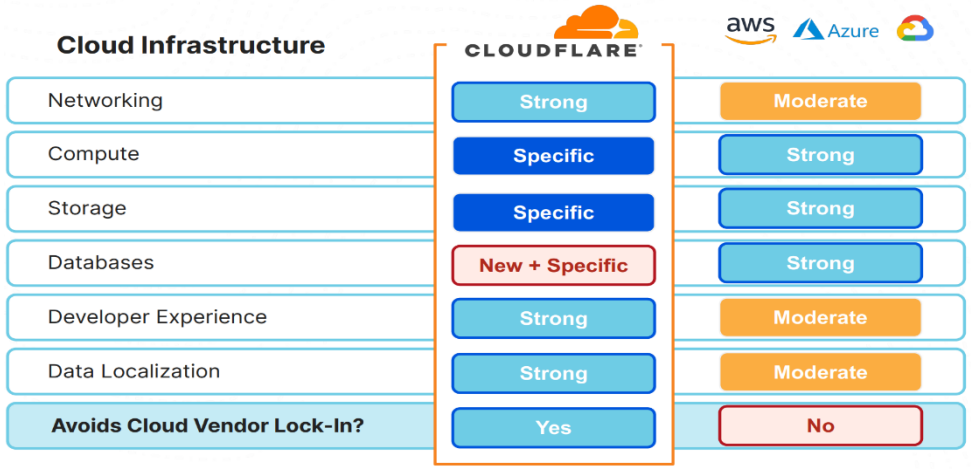
- **Cloudflare 已发展为边缘开发平台领导者，已与公有云厂商竞争。**随着 Cloudflare 网络安全业务的发展，公司在全球部署了300个数据中心，并逐步向边缘计算领域发展。公司推出了 Developer Platform（开发者平台）业务，向客户提供无服务器应用程序所需的一切，如计算（Workers等）、存储（R2 对象存储等）、web和应用开发工具（Pages等）。依靠边缘云的能力，平台可以自动将代码部署到全球所有数据中心，与 95% 世界互联网用户延迟仅为 50 毫秒左右。Cloudflare 边缘云业务已经和AWS 等公有云厂商直接竞争，如 R2 可以兼容 AWS S3 的API，且不再需要任何出口费用，实现更低的延迟和更好的吞吐量，让客户更好迁移。
- **R2 成为受益于本轮 AI 高速发展，公司为边缘端提供 AI 推理能力。**开发者平台 Cloudflare Workers 持续呈爆炸式增长，第二季度的活跃Workers 申请数量达到 1000 万，同比增长490%，自12月以来增长250%。R2 存储超过 13 PB 的客户数据，环比增长 85%，R2付费订阅客户达到44000个。本轮生成式 AI 浪潮成功带动了Cloudflare 算力的需求，尤其是 R2 “零出口费用”的优势，帮助客户找到最低的GPU成本来训练他们的模型。因此，Cloudflare 与多个 AI 基础设施公司合作，如CoreWeave、Lambda、MosaicML，均深度依赖 R2 降低成本；Character.ai、Leonardo.ai、Lexica.art 和 SiteGPT.ai 等多个 AI 应用公司也依靠Cloudflare的R2等提供全球推理能力。
- **Cloudflare 成为 AI 厂商最常用的云基础供应商，中立性和 Workers 让其受益本轮 AI 爆发，同时实现与安全的交叉销售。**越来越多的 AI 创业公司选择Cloudflare，因为其作为云厂商的中立性，以及快速灵活的网络和计算环境。除了常规的 AI 的 web 安全应用之外，AI 客户也会选择公司的开发者平台，在Workers 上快速进行 AI 应用开发。同时也能带来安全收入，例如一个使用 Workers 的客户，也选择了公司应用程序安全和零信任产品，签署了为期三年，总值130万美元的合同。

公司开发者平台主要包含产品



资料来源：Cloudflare、国信证券经济研究所整理

公司边缘云相比传统云厂商的优势

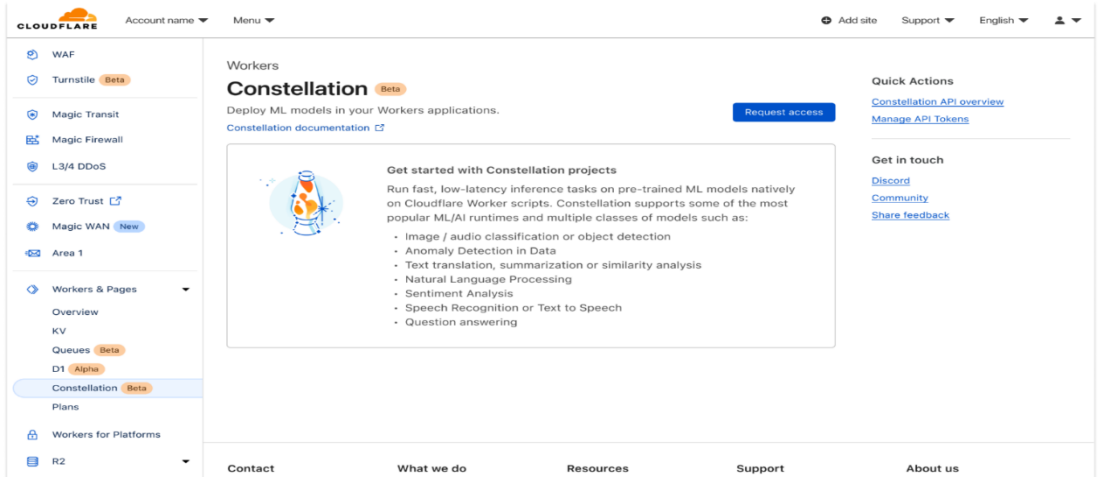


资料来源： Cloudflare 、国信证券经济研究所整理

Cloudflare——云视角：解决生成式AI反馈时间问题，边缘端 AI 推理可期

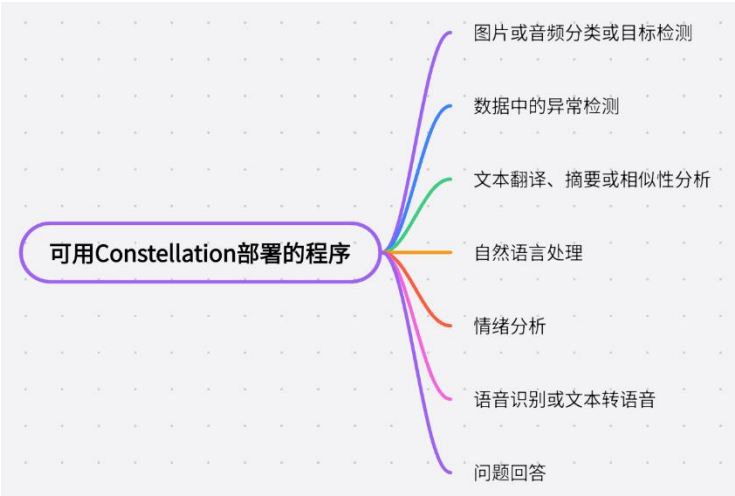
- **Cloudflare 认为边缘端进行 AI 推理具备很好的“位置”和“本地化”优势。**针对生成式 AI 的“提问”和“回答”，这个“推理”的性能表现是至关重要的，尤其是在大量数据和大量并发背景下的反馈的时间，可能决定了各家 AI 大模型的表现。公司认为“推理环节”应该尽可能靠近提出请求的人，如在终端设备上，或者非常接近最终用户的网络边缘上。未来一定有很多推理和模型运行在终端上，但依然有大量较大模型，需要更多GPU、内存等空间，只能运行在网络中。因此，**Cloudflare 具备两大优势：第一、“位置”**：公司将“推理”放在其网络边缘中运行是极具意义的，其可以提供几乎无限的网络、内存、GPU资源，公司已经看到越来越多的 AI 创业公司在如此发展。**第二、“本地化”**：由于各国的监管压力，数据私密性也是 AI 应用的争议点，如意大利限制了某些 AI 工具，因为其将数据发至国外。Cloudflare 可以在本地处理数据，因为其已经覆盖了全球300多个城市。
- **Cloudflare 定位推理算力需求不高，网络是核心优势。**Cloudflare 可以支持在网络中运行大模型，但并非是训练（该任务依然是超大公有云的工作），因此也不需要 H100 这类最先进的 GPU 。因此，高效的网络架构而非算力，才是Cloudflare 抢占推理市场的最大优势。公司多年积累的庞大的全球分布式网络，可以高效处理大量数据，还能处理大量同时请求，形成对 AI 推理的完美适配。
- **推出Constellation，将 AI 加入 Cloudflare 技术栈。**Constellation 是公司于23年5月推出的一组API，集成在 Workers 的生态中，可以让开发人员使用预先训练的机器学习模型运行快速、低延迟的推理任务；开发人员可以将任何受支持的模型上传到 Constellation。现在已经有几千个帐户加入了 Constellation 私人测试版，公司在 6 月也进行了升级更新。 Constellation 有望成为公司在边缘端推理的重要产品。

Constellation 让预训练的AI模型快速运行



资料来源：Cloudflare、国信证券经济研究所整理

Constellation 以融入多种AI能力



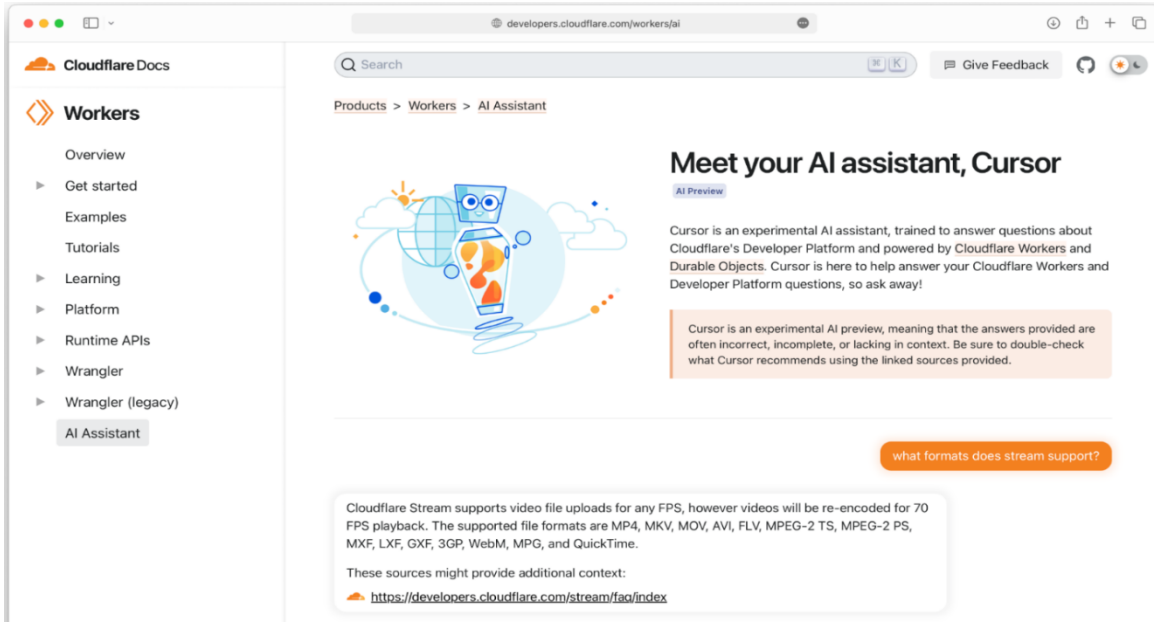
资料来源： Cloudflare 、国信证券经济研究所整理

Cloudflare——云视角：为开发者提供Cloudflare AI 助手 Cursor

国信证券 GUOSEN SECURITIES

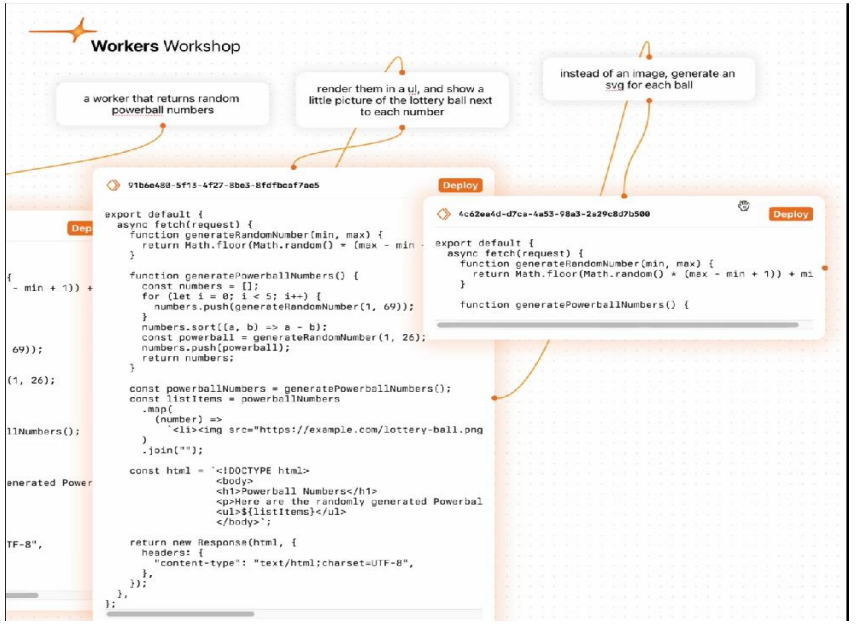
- **Cloudflare 推出AI 助手 Cursor，可以回答开发者平台的问题。**基于生成式 AI 的能力，公司在 Workers 平台上推出了 Cursor AI 对话机器人，旨在帮助开发者更好的使用工具。通过 Cursor，开发者可以迅速找到其需要的接口，提升其开发效率。Cursor 可以回答问题的基于文本的回复，以及指向 Cloudflare 文档中可帮助开发者进一步了解的相关页面的链接，因此 Cursor 也被定义为人工智能辅助文档。目前 Cursor 还是实验性的，目前还处于初级阶段。公司还在探索更深层的 AI 帮助开发者的功能，例如在 UI 上进行操作，将 AI 生成的代码，或者开发者自己写的代码直观的链接在一起，实现更高效的开发。
- **Cloudflare 为 AI 初创公司提供大量免费服务。**公司传统 CDN 业务也有免费服务模式，以此吸引大量早期用户，并逐步转变为付费用户。公司也针对 AI 创业公司推出了 Workers 启动计划，只需要简单的申请和验证就可以得到免费服务。

Workers 平台上推出了 Cursor AI 助手



资料来源：Cloudflare、国信证券经济研究所整理

Cursor AI在测试帮助开发者高效开发工具

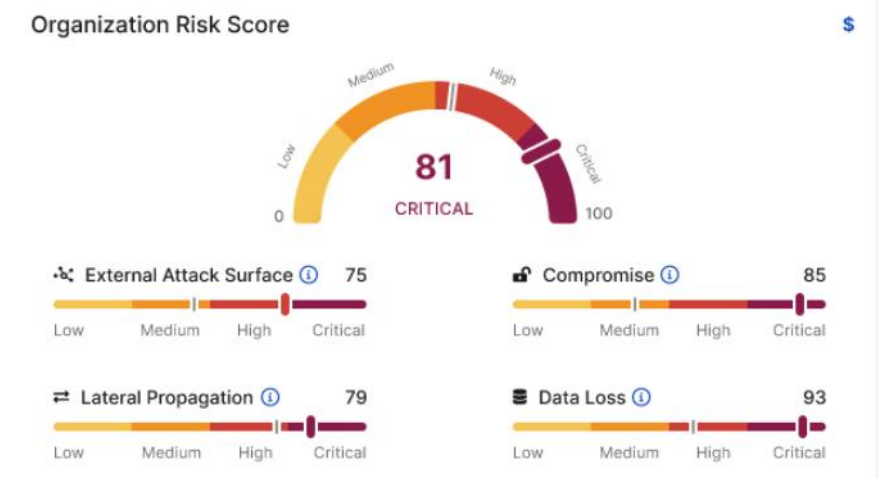


资料来源： Cloudflare 、国信证券经济研究所整理

Zscaler：以生成式 AI 创新产品，推出 Risk360

- **Zscaler：首先让客户安全的拥抱 AI 转型。**传统应用里，公司认为 AI 已经能很好的应用于威胁检测、数据保护，例如公司在2018年就收购了一家 AI/ML 公司，将 AI 与公司积累的数据相结合，实现对零日攻击更好的检测。同时，针对企业员工对 ChatGPT 类大模型使用中涉及的敏感信息，公司的 DLP 和访问控制产品可以保护大模型使用的数据安全（类似 Cloudflare One for AI）。在新一轮 AI 热潮中，凭借公司每天有 3000 亿条日志和数万亿个信号的数据积累，公司可以为安全领域定制和有效训练 LLM 模型。公司认为 AI 的兴起将助推更大的网络风险，同样地，公司也将利用 AI 预测勒索软件的行为以及其他复杂攻击。
- **利用生成式 AI 探索安全产品创新。**在近期举办的Zenith Live ‘23大会上，公司积极拥抱生成式 AI，并开发了3项行业领先的创新。**具有违规预测功能的 Security Autopilot**：一种主动保护数据的方法，通过 AI 持续在变化的策略和日志中学习，以准确推荐策略并分析影响。**Zscaler Navigator**：实现简化且统一的自然语言界面，让用户更简单的与 Zscaler 产品交互。**多模态 DLP**：将生成式 AI 和多模态功能集成到已有的 DLP 产品上，在原来保护文本和图像数据基础上，进一步保护视频、音频等形式的泄露。公司加速在 AI 上的产品创新，这些功能将打包在其高价捆绑销售中。
- **推出 Zscaler Risk360 产品，同样是安全运维视角。**Risk360 是一个风险量化和可视化框架，主要面向企业 CISO，提供组织风险的整体视角，并给出相应措施。 Risk360 从企业外部和内部环境获取数据，描绘网络攻击的 4 个阶段（外部攻击面、受损情况、横向传播、数据丢失），并展现企业 IT 所有实体，如资产、应用程序、员工、第三方。实时性和直观性是 Risk360 的优点，能让安全人员迅速给出措施，尤其是美国SEC等监管机构对事件处理时间要求越来越高。目前， Risk360 已接到大量订单，比公司任何其他产品更受关注。

生成式 AI 创新产品Risk360的运维视角



资料来源：Zscaler、国信证券经济研究所整理

Risk360主要功能

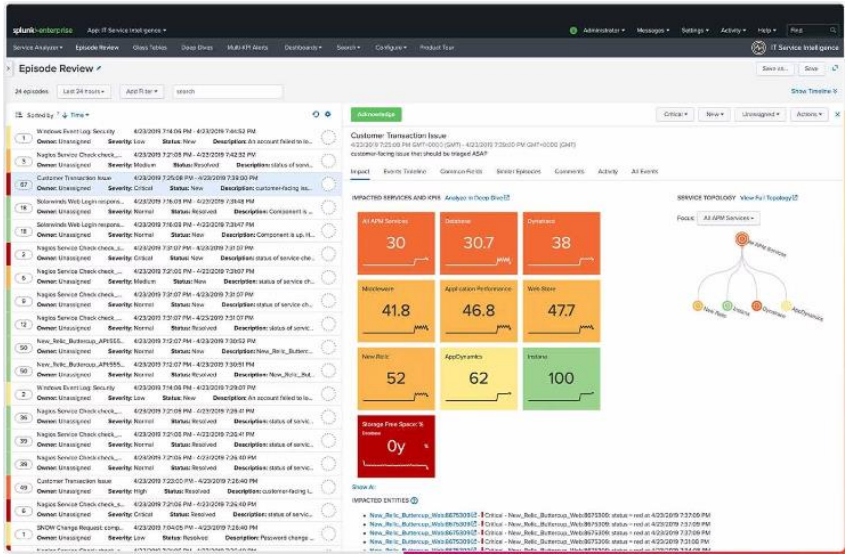
核心价值	具体功能
强大的风险量化	提供针对网络入侵各个阶段的实时风险评分，以及四个实体之间可视化风险展示
直观的可视化和报告	筛选出网络风险的主要驱动因素，并预测财务风险估算，包括财务补救建议，并能创建简洁的董事会级演示材料
可行的补救措施	通过引导工作流程，优先考虑可行建议，以调查和纠正最关键的问题，从而确保组织的安全并保持业务持续运行

资料来源： Zscaler 、国信证券经济研究所整理

Splunk：机器数据分析的天然 AI 应用场景

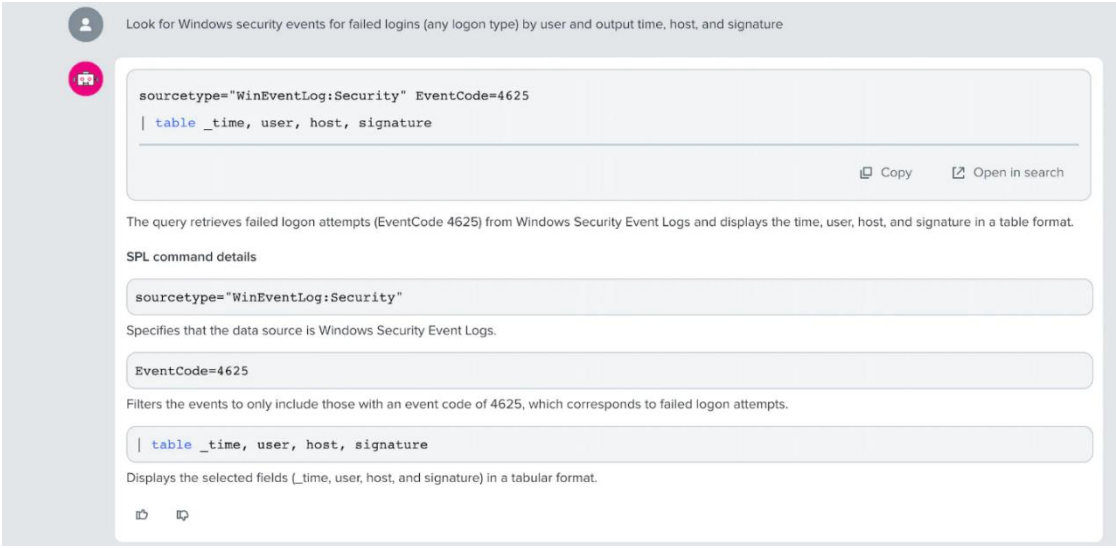
- **Splunk 早期广泛将 AI 应用数据分析。**公司致力于机器数据分析，AI 具备天生的应用场景，从日志分析到安全事件管理SIEM。公司产品的核心搜索功能中采用了机器学习，Splunk 机器学习工具包 (MLTK) 为各级用户提供 ML 的技术支持，下载量超过20万次。公司也认为 AI 并非替代人工，而是人类决策的加速器，以缓解全球网络安全工作者的短缺；AI 通过自动检测异常，并推荐决策、风险评估，让有限的人力投入到更具价值的问题上。尤其是新一轮 AI 推动下，通过对事件、上下文的总结和解释，可以进一步加快学习速度，为 SecOps、ITops 和工程团队带来大量新的机会。公司的智能IT服务产品，自动事件关联和优先级划分，通过集成各IT管理工具，缩短事件解决时间；还有 APM等功能，也可以应用在使用大模型的客户侧，类似于 Datadog 等厂商。
- **推出全新 Splunk AI Assistant 产品。**公司在2022年即推出了基于大型语言模型的 SPL 助手预览版，帮用户通过简单的语言来查询 Splunk 的数据（传统方式需要其搜索处理语言SPL）。2023年7月，公司发布 Splunk AI ，是去年 SPL 助手的改进版。新的生成式 AI 应用 Splunk AI Assistant 将自动化和人机交互相结合，也是让用户通过简单的语言对话来搜索数据，AI 产品将请求转化为可以执行或构建的查询命令，大幅缩短了 SPL 的学习时间。Splunk AI 旨在帮助组织推动更快的检测、调查和响应，以实现更强的可观察性价值，因此其本质依然是 AI 在安全运维里的应用。目前，除 Splunk AI Assistant 和 ML-Assisted Thresholding 为预览版外，Splunk AI 的所有新产品现已全面上市。

基于大语言模型的升级版Splunk AI Assistant



资料来源：Splunk、国信证券经济研究所整理

AI Assistant将请求转化为可执行或构建的查询命令

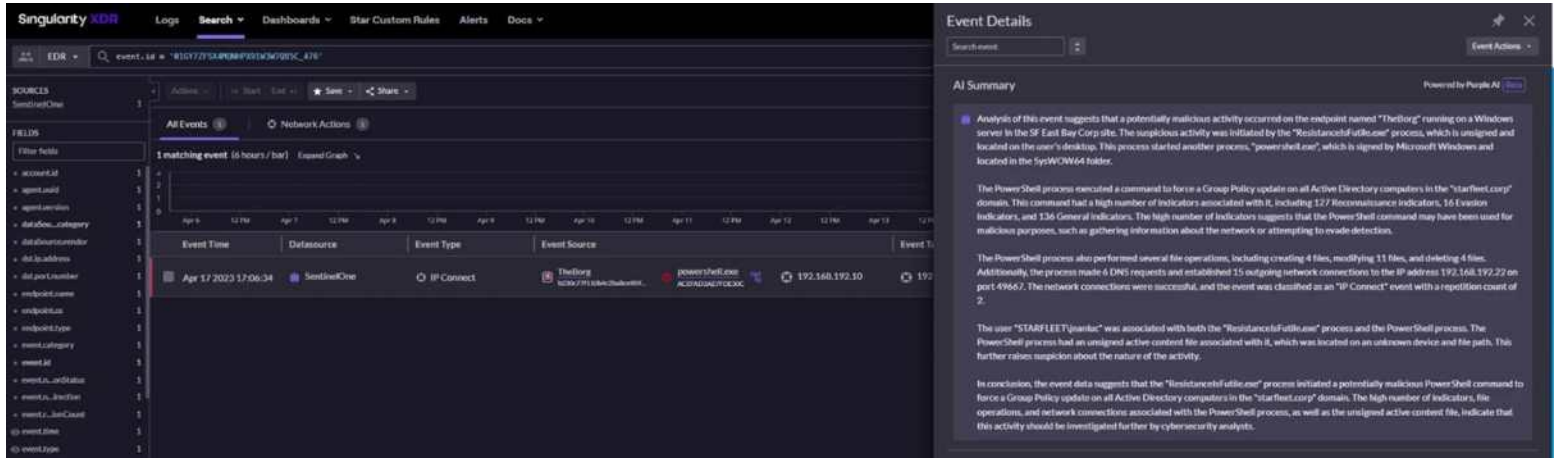


资料来源：Splunk、国信证券经济研究所整理

其他海外安全公司：AI 安全应用也集中在运维领域

- **Fortinet：将 AI 能力融入检测和安全运维，类似Palo Alto Networks。**公司认为 AI 技术可以帮助公司显著提高生产力，可以在恶意软件检测、威胁搜索、事件关联和自动化、安全网络设计和故障排除等领域进行应用。公司第一个AI用例，即虚拟 FortiGuard 威胁分析师，通过机器学习和协调保护实时解决威胁，以AI 来驱动威胁情报。公司将继续在产品中投资 AI 技术，包括生成式 AI ，以增强、简化和自动化客户的安全性。目前已布局 AI 产品也侧重于安全运营领域。
- **SentinelOne：以 AI 能力颠覆终端安全，推出生成式 Purple AI 产品，类似 Crowdstrike。**公司自成立以来，AI 就是其解决终端安全问题的核心方法，将 AI 引擎部署在每个终端，通过行为分析取代传统的病毒特征识别，来实现对未知威胁的保护。公司在业内首创了基于 AI 的 XDR 平台，结合 AI 驱动的 EPP 和 EDR 部署在所有端点，实时和自动化地响应威胁。本轮生成式 AI 背景下，公司在23年4月推出基于 LLM模型的 Purple AI，一种致力于威胁搜寻、分析和响应的生成式 AI。该产品也是面向安全运维，帮助安全分析师通过简单的对话来简化威胁分析，减少SOC团队的告警疲劳，目前已处于有限试用阶段。
- **OKTA：加大 AI 投资，认为当前监管“为时尚早”。**公司计划将年度研发预算的约 4000 万美元用于新的人工智能项目，约占研发总预算的 10%。OKTA 对本轮 AI 价值非常看好，认为 AI 会带来更多的联系和身份，身份安全重要性增加，同时当前对 AI 的监管还较早。同时，当前100多家 AI 公司都在使用 OKTA 的身份安全，如OpenAI、Character.AI、Browse.AI 和 Hypotenuse.AI 等客户。OKTA 本身也一直将 AI 融入安全产品中。**员工身份**：ThreatInsight、电话反欺诈系统、自适应多因素身份验证 (AMFA)，通过机器学习实现更好的威胁洞察，优化身份判断。**客户身份**：机器人检测、身份威胁级别 (ITL) 工具、自适应 MFA，利用 AI 实现对客户登录层面的高效安全管理。

SentinelOne 推出生成式 Purple AI提升安全运维效率



资料来源：SentinelOne、国信证券经济研究所整理

目录

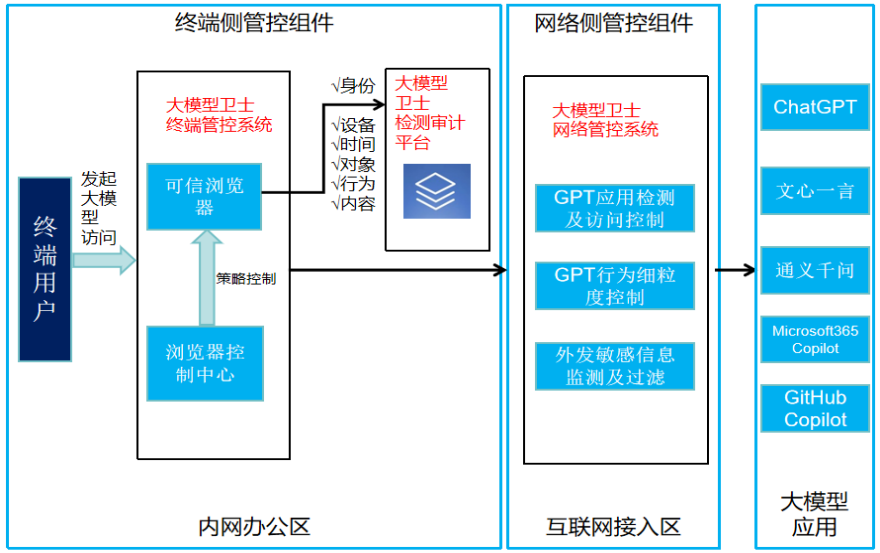
奇安信：安全机器人和大模型卫士双管齐下

- **业界首个工业级大模型应用Q-GPT安全机器人。**面对告警疲劳、专家稀缺、效率瓶颈等现实问题，Q-GPT扮演了“虚拟安全专家”的角色，核心也是帮助安全分析师减轻安全运维的工作。奇安信 AI 研究院已经在6大方向形成100余种 AI 能力，包括三大平台：AI能力平台（奥丁）、AI 对抗平台（洛基）、AI 训练平台（天算）；同时具备业内最大规模的安全专家团队、海量的安全知识数据，让Q-GPT可以通过简单对话，实时、自动为客户研判。在日常产生的海量告警中，通常只有1%的告警被研判，剩余99%无暇顾及。一台 Q-GPT 机器人等于60多位安全专家，可产生约2000万元的运营效益，大幅提升客户侧的运营效率。京东方集团和吉利汽车集团在奇安信产品发布会现场签约，成为国内安全机器人的第一批用户。
- **大模型卫士帮助企业安全使用大模型。**奇安信大模型卫士保障客户在使用端的数据安全，解决企业客户对于大模型“想用不敢用”的顾虑。其主要有 4 重功能：防止数据投喂造成的敏感数据泄露、建立身份识别与溯源机制、避免触发数据跨境安全监管红线、对企业内部大模型应用状况全面分析。大模型卫士也是基于传统的安全技术，部署在终端和网络端，能够完美适配主流大模型应用。大模型卫士目前已获得了国内多家客户的签约意向。

奇安信推出Q-GPT安全机器人

资料来源：奇安信、国信证券经济研究所整理

奇安信大模型卫士工作原理



资料来源：奇安信、国信证券经济研究所整理

安恒信息：恒脑•安全垂域大模型赋能安全运营升级，已经过重大赛事检验

- **安恒发布恒脑•安全垂域大模型，将助力杭州亚运会运维实战。**公司在 23年 8月发布恒脑·安全垂域大模型，并进行了基于大模型的安全运营平台全新升级。安全在大数据安全领域一直处于市场龙头地位，但过去的大数据技术即使可以把告警从400万个处理至8000-9000个，依然是安全专家无法全部处理的状态；AI 大模型的引入让真正要处理的事件再下降至 18个左右，将对安全运营产生质变。在此前举办的成都大运会上，该大模型已经投入应用，并圆满完成任务；在9月举办的杭州亚运会上，这款安全运营平台也将投入使用。在赛前演练中，安全运营成效已提升70%以上。
- **大模型的下半场是智能体，安恒多项产品保持领先。**恒脑·安全垂域大模型与安恒OpenSecurity能力中台结合，实现“感知”、“决策”、“执行”、“反馈”的智能一体化方案，智能体逐步成长为虚拟安全专家。公司WAF、APT、EDR、SOAR等多款产品保持行业领先，早期态势感知也一直侧重各产品联动。AI 大模型进一步从各种安全平台和数据源中收集、整合和分析信息，实现全面的威胁情报分析和事件响应，并通过智能编排来提供问题解决策略。大模型将成为全公司的安全能力底座，为安恒信息数据安全战略、MSS战略、人才战略三大战略提供全面升级的源动力。

安恒发布恒脑安全大模型

资料来源：安恒信息、国信证券经济研究所整理

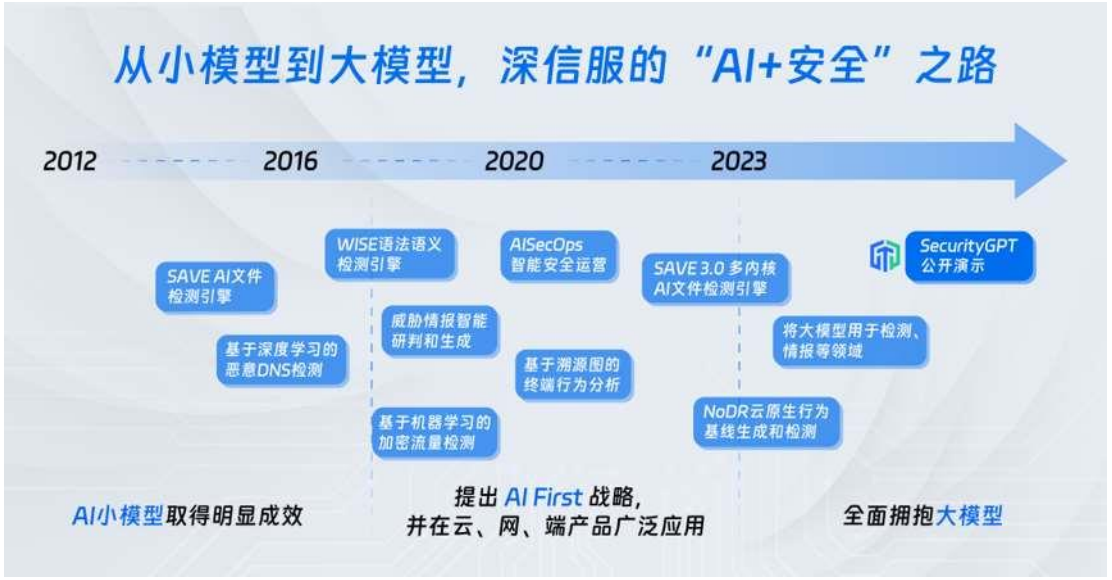
安恒大模型制支撑多种安全功能

资料来源： 安恒信息、国信证券经济研究所整理

深信服：国内首推安全 GPT，迅速迭代 2.0 版再升级

- **坚持 AI First 战略，从小模型到大模型。**深信服在2015年开始投入决策式AI技术的研究和应用，并在2016年确立了AI First的研发战略，也取得了一系列研发成果：未知病毒检出率国内第一的SAVE 3.0引擎、精确度超90%的AIOps 智能运维分析引擎等。公司于 2023年5月业内首发自研安全大模型“安全 GPT”，率先探索生成式 AI 在安全运维里的应用空间。基于公司8年来持续积累的高质量安全语料，安全 GPT 能通过自然语言，深入攻击样本检测、漏洞研判、分析处置等安全细分场景，大幅降低服务和运营人力成本。目前，安全GPT技术应用在XDR平台上，已经达到5年经验的安全专家水平。
- **安全 GPT 已在50多家客户落地试用，2.0 能力进一步提升。**公司产品迭代迅速，成为首批通过《生成式人工智能服务管理暂行办法》备案的安全大模型；并于9月推出升级版安全 GPT，实现了从“1.0 辅助驾驶”到“2.0 智能驾驶”的演进。安全GPT 2.0目前可承载超80%的告警分析、事件调查、资产排查等工作，利用大模型的研判、处置速度，真正实现30秒研判遏制威胁，单一事件平均闭环时间缩减96.6%。目前，安全GPT现已全面赋能安全托管服务MSS，支持SaaS化及本地化多种部署方式。

深信服在AI+安全上的发展历程



资料来源：深信服、国信证券经济研究所整理

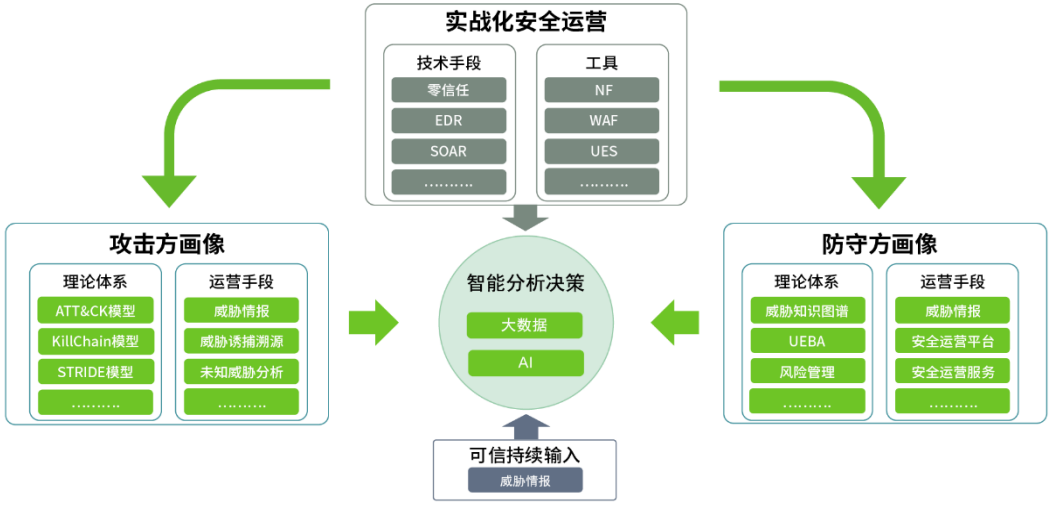
深信服推出安全GPT

资料来源： 深信服、国信证券经济研究所整理

绿盟科技：发布风云卫大模型，聚焦实战攻防

- **绿盟发布 AI 大模型产品风云卫。**公司在 2023年 9月 TechWorld 绿盟科技智慧安全大会上重磅发布了风云卫大模型（NSFGPT），致力于提升网络安全运维效率。该模型基于海量安全专业知识训练，构建一套覆盖安全运营、检测响应、攻防对抗、知识问答等多种场景的网络安全运营辅助决策系统。公司同时也发布了《安全行业大模型SecLLM技术白皮书》等研究成果。
- **大模型为公司实现智慧安全3.0添砖加瓦。**公司多年来坚持安全智能化投入，21年即已发布智慧安全3.0理念体系，目标达到达到“全面防护，智能分析，自动响应”的防护效果。随着大模型能够自动解析和解读复杂的日志数据，并提供智能研判告警信息，推荐最佳响应方案，公司智慧安全3.0 有望更进一步。目前公司积累了高质量语料数据体系，覆盖攻、防、情报、知识等多个方面，也形成了千亿级高质量打标签数据的安全知识图谱。风云卫大模型对安全运营效能也有明显提升，如检测规则自动生成，由原来耗时1天提升至分钟级；分析研判处置自动化，由原来耗时6小时提升至分钟级。凭借公司在 AI 安全领域积累的6大优势，风云卫能解决三大问题：实战态势指挥调度、红蓝对抗辅助决策以及安全运营效能提升。

绿盟智慧安全 3.0致力于提升运维效率



资料来源：绿盟科技、国信证券经济研究所整理

绿盟安全大模型风云卫六大优势

资料来源： 绿盟科技、国信证券经济研究所整理

国内安全行业均在积极探索大模型应用

- **启明星辰：早在 22 年就已发布安全智慧生命体“PanguBot(盘小古)”，积极研发安全垂直领域大模型。**公司在安全运营中心战略以来，一直加强在SOC领域的智能化建设，因此公司在 22年发布了面向安全运营业务的安全智慧生命体“PanguBot(盘小古)”。该产品融合了公司多年对自然语言理解、自然语言处理、大数据分析、智能化处理方面的智算能力和安全运营经验，能够通过聊天式窗口直接与安全运营人员进行样式丰富的交互，并整合各种运营工具，实现安全分析处置自动化。2023年，公司再次启动了安全垂直领域大模型的研发，已经在威胁情报提取、安全日志分析、告警有效性评估等安全业务展现出良好的应用前景；“盘小古”在大模型基础上也进行了升级。除此之外，公司让 AI 赋能多模态安全检测，在流量检测、Web 安全、威胁情报、UEBA 等多个产品中应用 AI 模型实现了能力提升。

- **天融信：发布天问大模型，首先侧重于智能问答。**公司在 23 年 9 月的网络安全博览会上发布了自研的天问大模型，主要包括天问智能客服问答系统、威胁情报查询解读等功能，能有效解决传统的安全防护方法需要依赖大量的专业知识和经验的问题。其中，天问智能客服问答系统针对网安行业知识及天融信的产品知识等进行微调学习，具备较强的语义理解和生成能力，可以进行自动化的网安领域知识问答，大大提高了客户支持效率，减少人工客服工作量。未来大模型还会进一步加强检测、漏洞挖掘等能力。除了大模型之外，公司在多款传统产品上也融合了 AI 能力，如防火墙融入了AI智能检测，EDR、态势感知等产品也引入了 AI 能力。

- **安博通：与百度合作探索 AI Inside。**公司在 23 年 4 月与百度安全达成合作，通过“AI Inside 创新合作模式”共建安全网络空间。公司作为网络安全产业上游领先企业，专注于底层安全能力上的系统和产品研究开发，尤其是基于 ABT SPOS 的可视化网络安全技术，人工智能技术的叠加让其更具可靠性和灵活性。目前双方技术的联合已经实现了IT日常工作的自动化运维，未来将 AI 应用进一步深入核心业务逻辑，从而降低运维人员的技术和经验门槛，后续安博通将陆续发布基于百度AI Inside的产品和解决方案。

- **美亚柏科：发布“天擎”公共安全大模型，侧重监管侧应用。**公司于 23 年 6 月发布国内首个公共安全大模型“天擎”美亚，具备强大的警务意图识别、警务情报分析、案情推理等业务理解和推理能力。同时，以该大模型为基座，公司打造了“MYGPT”取证智能助手，重构电子数据智能分析，变革用户取证交互体验。在监管侧，基于公司在取证和大数据的长期积累，公司也推出了AI-3300“慧眼”视频图像鉴真工作站，可以针对利用深度合成伪造及生成式技术生成的内容进行识别、检测和鉴定。

- **永信至诚：与商汤达成三大战略合作，AI 靶场积累多年。**公司于 23 年 7 月与商汤签署战略合作协议，形成公司的三大战略：第一、公司为商汤大模型的数据安全和网络安全的全生命周期安全提供测试评估服务；第二、公司成为商汤对外提供大模型服务中的安全增值能力提供方；第三、双方共同探索在网络安全攻防对抗和漏洞挖掘领域的大模型应用并形成产品竞争力。公司早期也推出了人工智能靶场，帮助测评 AI 漏洞挖掘技术，同时自主研发国内首个人工智能网络安全攻防平台RHG，将 AI 引入网络对抗。

目录

投资建议

- **看好AI提升网络安全产业价值，维持“超配”评级。**AI 在网络安全行业应用已久，在检测能力上已展现出价值，并诞生了Crowdstrike 这类颠覆性的端点安全公司。本次生成式 AI 带来的机会，业界普遍共识网络安全最具创造价值机会。大模型与安全知识库的融合，形成 Copilot 类助手，迅速成为3-5年经验的安全分析师；结合 XDR、新一代SOC等安全平台，自动化处理海量事件和告警，大幅提升安全运维效率。微软、谷歌等巨头均推出安全领域里的AI大模型产品，Palo Alto Networks、Crowdstrike、Cloudflare等多个海外新兴安全厂商均推出AI安全产品，并已逐步得到市场认可；国内龙头安全厂商也纷纷跟进AI大模型投入，并已进入客户试用阶段。AI 在安全运维里为甲乙双方节省的时间和人员成本是显而易见的，且拓展了传统安全的能力边界，不管是利用AI检测未知威胁，还是处理海量事件，均是AI带来的崭新价值，因此我们持续看好网络安全产业，维持“超配”评级。
- **关注在网络安全产业新发展机会，重点关注在AI大模型积极投入的厂商。**国内多家安全公司已发布了大模型，重点关注奇安信（Q-GPT 机器人，大模型卫士）、深信服（安全GPT 2.0）、安恒信息（恒脑垂域大模型）、绿盟科技（风云卫大模型）、启明星辰（盘小古）、天融信（天问大模型）等，部分产品已进入签约和试用阶段；美亚柏科、安博通、永信至诚等厂商也在积极探索 AI+安全的应用。

风险提示

第一，宏观经济下行风险。若宏观经济波动，产业变革及新技术的落地节奏或将受到影响，宏观经济波动导致下游需求不及预期，可能对 IT 投资产生负面影响，从而导致整体行业增长不及预期。

第二，行业竞争加剧。国内各厂商纷纷加大 AI 相关投入，导致产品陷入同质化竞争。

第三，国内 AI 大模型、算力等技术发展不及预期，影响AI 在安全领域的应用。

第四，相关政策推进不及预期。如生成式 AI 应用需面临相关政策要求等。

免责声明

国信证券 GUOSEN SECURITIES

国信证券投资评级

投资评级标准	类别	级别	说明
报告中投资建议所涉及的评级（如有）分为股票评级和行业评级（另有说明的除外）。评级标准为报告发布日后6到12个月内的相对市场表现，也即报告发布日后的6到12个月内公司股价（或行业指数）相对同期相关证券市场代表性指数的涨跌幅作为基准。A股市场以沪深300指数（000300.SH）作为基准；新三板市场以三板成指（899001.CSI）为基准；香港市场以恒生指数(HSI.HI)作为基准；美国市场以标普500指数(SPX.GI)或纳斯达克指数（IXIC.GI）为基准。	股票投资评级	买入	股价表现优于市场代表性指数20%以上
		增持	股价表现优于市场代表性指数10%-20%之间
		中性	股价表现介于市场代表性指数±10%之间
		卖出	股价表现弱于市场代表性指数10%以上
	行业投资评级	超配	行业指数表现优于市场代表性指数10%以上
		中性	行业指数表现介于市场代表性指数±10%之间
		低配	行业指数表现弱于市场代表性指数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；分析逻辑基于作者的职业理解，通过合理判断并得出结论，力求独立、客观、公正，结论不受任何第三方的授意或影响；作者在过去、现在或未来未就其研究报告所提供的具体建议或所表述的意见直接或间接收取任何报酬，特此声明。

重要声明

本报告由国信证券股份有限公司（已具备中国证监会许可的证券投资咨询业务资格）制作；报告版权归国信证券股份有限公司（以下简称“我公司”）所有。本报告仅供我公司客户使用，本公司不会因接收人收到本报告而视其为客户。未经书面许可，任何机构和个人不得以任何形式使用、复制或传播。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，一切须以我公司向客户发布的本报告完整版本为准。

本报告基于已公开的资料或信息撰写，但我公司不保证该资料及信息的完整性、准确性。本报告所载的信息、资料、建议及推测仅反映我公司于本报告公开发布当日的判断，在不同时期，我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。我公司不保证本报告所含信息及资料处于最新状态；我公司可能随时补充、更新和修订有关信息及资料，投资者应当自行关注相关更新和修订内容。我公司或关联机构可能会持有本报告中所提到的公司所发行的证券并进行交易，还可能为这些公司提供或争取提供投资银行、财务顾问或金融产品等相关服务。本公司的资产管理部门、自营部门以及其他投资业务部门可能独立做出与本报告中意见或建议不一致的投资决策。

本报告仅供参考之用，不构成出售或购买证券或其他投资标的要约或邀请。在任何情况下，本报告中的信息和意见均不构成对任何个人的投资建议。任何形式的分享证券投资收益或者分担证券投资损失的书面或口头承诺均为无效。投资者应结合自己的投资目标和财务状况自行判断是否采用本报告所载内容和信息并自行承担风险，我公司及雇员对投资者使用本报告及其内容而造成的一切后果不承担任何法律责任。

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，是指从事证券投资咨询业务的机构及其投资咨询人员以下列形式为证券投资人或者客户提供证券投资分析、预测或者建议等直接或者间接有偿咨询服务的活动：接受投资人或者客户委托，提供证券投资咨询服务；举办有关证券投资咨询的讲座、报告会、分析会等；在报刊上发表证券投资咨询的文章、评论、报告，以及通过电台、电视台等公众传播媒体提供证券投资咨询服务；通过电话、传真、电脑网络等电信设备系统，提供证券投资咨询服务；中国证监会认定的其他形式。

发布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
GUOSEN SECURITIES

国信证券经济研究所

深圳

深圳市福田区福华一路125号国信金融大厦36层

邮编：518046　　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