国金证券 SINOLINK SECURITIES

2023 年 06 月 10 日

AI 应用端行业研究

买入（首次评级）

行业深度研究

证券研究报告

计算机组
联系人：纪超
jichao@gjzq.com.cn

分析师：孟灿（执业 S1130522050001）
mengcan@gjzq.com.cn

AI+网络安全的“矛”与“盾”

行业观点

- **全球市场基于 AI 带来的网络安全投资进入爆发期。**AI 应用落地带来新安全风险，安全防护难度大幅上升，但 AI 同时赋能网络安全，促进攻防技术升级，因此越来越多的安全厂商加速布局网络安全与 AI 技术的融合，驱动 AI 安全市场加速爆发。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 CAGR 约 19.43%。我们认为可以从两条线切入 AI+网络安全：一方面是利用 AI 技术为网络安全产品赋能，这是从攻防对抗的逻辑来提升产品攻防效果；另一方面是针对 AI 应用场景打造新的安全防护产品，这是从新业务场景的逻辑来满足新的安全需求。
- **AI 促进攻防技术升级，提升产品力。**网络安全的本质为攻防对抗，AI 在攻防两端提供了显著的赋能效应，使攻防技术向主动化、自动化、智能化方向演进，网安产品在技术变革中迭代升级。之于攻，攻击者可通过 AI 完善攻击方案，网络安全威胁趋向复杂化和智能化；之于防，防御者可基于 AI 构建多产品协同联动的防御体系，实现对网络安全威胁的预先研判、智能防护和自动抵御。
- **AI 助力行业降本提效，改善盈利能力。**网安厂商与其他软件厂商相比在投入方面更大，主要还是在于人员方面的投入。因此解决降本增效问题成为网安行业当务之急。AI 可有效提升安全运营的智能化和自动化程度，使得安服人员需求明显下降，从而带来显著降本增效空间，网安厂商的盈利能力进而有望改善。
- **AI 应用带来新安全挑战，新安全需求同步增加。**AI 红利接踵而至，安全风险如影随形。首先模型算法本身不可靠、不安全，AI 算法可解释性不足且鲁棒性较差；其次是数据安全问题，大数据是 AI 技术研发和落地的基础，随着海量数据被生成、采集、存储和利用，数据安全和隐私保护领域的安全风险加剧；最后 AI 技术滥用风险极高，AI 网络攻击、AI 欺诈等新安全威胁持续增加。

投资建议

- AI 发展催生安全防护需求，同时助力攻防技术升级，为网安行业带来显著降本增效空间，我们重点推荐奇安信、安恒信息、启明星辰、永信至诚、深信服等网络安全厂商。

风险提示

- 国内宏观经济环境波动的风险、政策落地不及预期、技术应用普及不及预期。

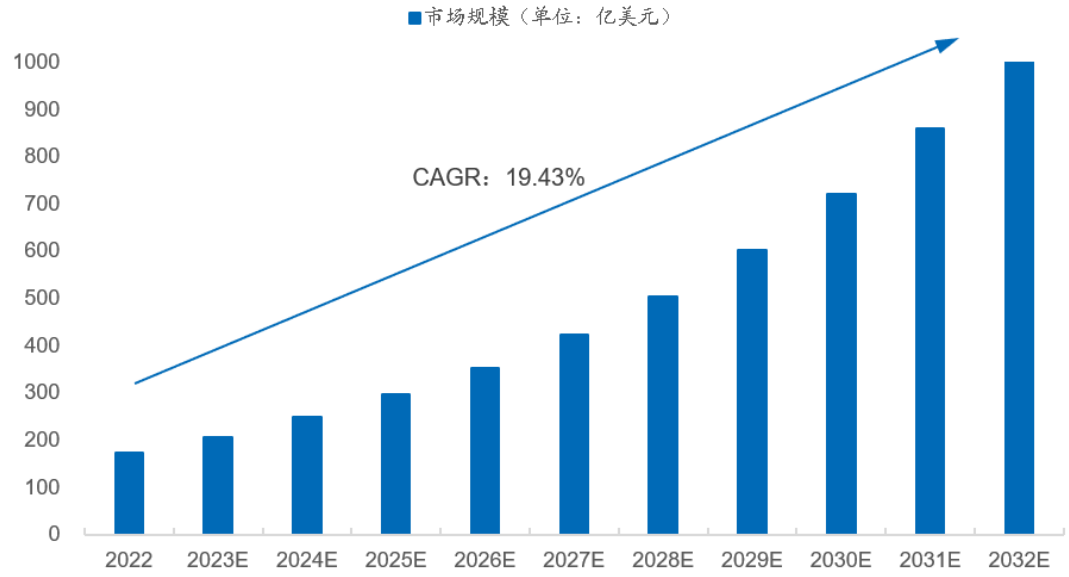
内容目录

图表目录

1. 基于 AI 的网络安全投资进入爆发期

- 全球市场基于 AI 带来的网络安全投资进入爆发期。AI 应用落地带来新安全风险，安全防护难度大幅上升，但 AI 同时赋能网络安全，促进攻防技术升级，因此越来越多的安全厂商加速布局网络安全与 AI 技术的融合，用 AI 对抗 AI 成为行业共识，驱动 AI 安全市场加速爆发。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 CAGR 约 19.43%。

图表1：2022-2032 年全球基于 AI 的网安市场规模 CAGR 约 19.43%



来源：Precedence Research，国金证券研究所

- 安全厂商加速布局“AI 军备竞赛”，AI 产品应用不断落地。亚马逊、CrowdStrike、谷歌、IBM、微软、Palo Alto Networks 等网安头部厂商加速布局 AI/ML 研发，以应对日益复杂的安全威胁和企业客户对新功能的需求。具体来看，部分头部网安厂商已将 AI 能力嵌入其核心产品。例如 CrowdStrike 的云安全平台 Falcon，通过 AI 技术识别和应对潜在威胁；Palo Alto Networks 业界首创 AIOps for NGFW，革新防火墙运营并提升其安全防护能力。随着生成式 AI 技术快速发展，国内外网安厂商对 AI 的布局正在提速。微软今年 3 月发布 Security Copilot，结合 GPT-4 与微软安全模型以更快更准确地检测和响应安全威胁;谷歌云今年 4 月发布 Security AI Workbench，谷歌安全大模型 Sec-PaLM 加持下帮助用户缓解安全运营压力，IBM 则在同月推出新安全套件 Security QRadar Suite，以加快威胁检测、调查和响应的速度；国内安全厂商方面，深信服今年 5 月推出国内首款安全 GPT 大模型，提升安全检测效果的同时提高了安全运营的效率。
- 总的来看，可以从两条线切入 AI+网络安全：一方面是利用 AI 技术为网络安全产品赋能，这是从攻防对抗的逻辑来提升产品攻防效果；另一方面是针对 AI 应用场景打造新的安全防护产品，这是从新业务场景的逻辑来满足新的安全需求。从这两个维度出发，建议关注积极布局数据安全、云安全、物联网安全等新安全场景、积极应用 AI 技术提升安全防护效果的创新型公司。

2. AI 对于网络安全行业的赋能是把双刃剑

2.1 AI 促进攻防技术升级，提升产品力

- AI 助力安全产品升级迭代，大幅提升安全防护效果。网络安全的本质为攻防对抗，AI 在攻防两端提供了显著的赋能效应，使攻防技术向主动化、自动化、智能化方向演进，网安产品在技术变革中迭代升级。之于攻，攻击者可通过 AI 完善攻击方案，网络安全威胁趋向复杂化和智能化；之于防，防御者可基于 AI 构建多产品协同联动的防御体系，实现对网络安全威胁的预先研判、智能防护和自动抵御。随着 AI 逐渐融入各类网络安全产品和解决方案，其安全防护能力已在威胁分析、态势感知、攻防对抗等多个场景得到充分验证。

■ 我们认为 AI 促进攻防技术升级主要体现在以下四个方面：

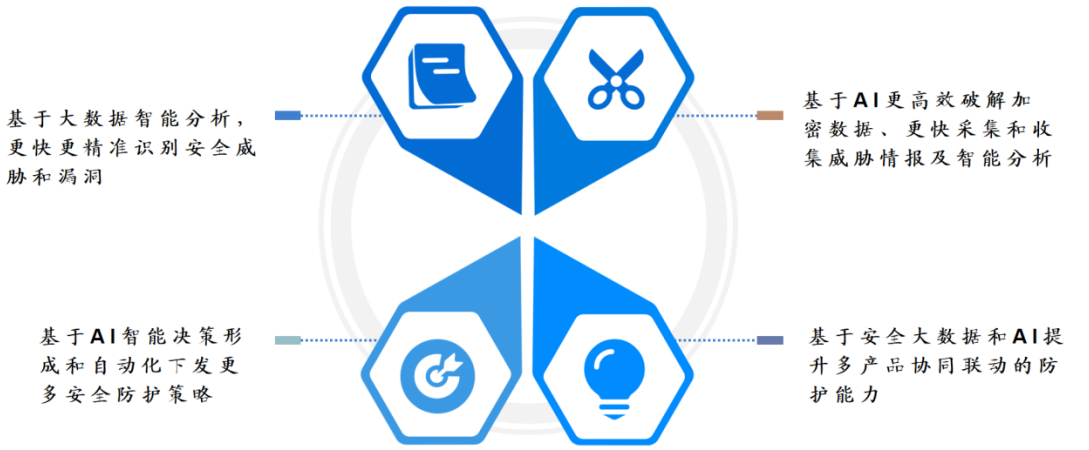
1）基于大数据智能分析，更快更精准识别安全威胁和漏洞。基于安全大数据的智能分析与决策，可以有效提升安全威胁和漏洞识别的速度和准确性，目前有大量的网安厂商都在利用 AI 技术赋能威胁检测、漏洞挖掘、漏洞扫描等场景，GPT-4 等大模型的发布将加速相关产品落地进程。

2）基于 AI 更高效破解加密数据、更快采集和收集威胁情报及智能分析。依托强大的算力和算法能力支持，AI 可以快速破解加密数据，对来自不同来源和渠道的网络威胁情报进行智能化的收集、整理、分析和共享，从而更好地了解和分析当前网络安全状况。

3）基于 AI 智能决策形成和自动化下发更多安全防护策略。网络安全领域经常涉及攻防对抗场景，重大节日、国家重要活动、攻防演练、护网演习等敏感节点均是攻击高发期，安全部门的全天候值守已经成为了重保标配，给一线安全值守人员带来了极大压力。AI 可以通过大数据分析自动化地制定、执行和动态调整安全防护策略，以更高的效率和更智能化的分析研判应对已知和未知的网络攻击。

4）基于安全大数据和 AI 提升多产品协同联动的防护能力。网络安全本质是攻防对抗，安全防御与安全攻击的不同点在于，安全攻击只要找到任何一个突破点就能够取得攻击成果，安全防御需要尽可能地覆盖所有场景才能防御成功，随着安全威胁日趋复杂化和多样化，传统单点防御逐渐失效。AI 可以实现多产品高效协同联动，帮助构建全方位、立体化的安全防御体系，AI 赋能下未来会有越来越多的安全厂商由一个单品发展至多个产品，最终形成网络安全整体解决方案。

图表2：AI 促进攻防技术升级



来源：国金证券研究所

2.2 AI 助力行业降本提效，改善盈利能力

■ AI 助力网安行业降本提效。网安厂商与其他软件厂商相比在投入方面更大，主要还是在于人员方面的投入。一方面是研发人员，网络安全与信息化建设紧密相关，“十四五”期间我国信息化发展以数字经济为主线，在各行各业加速推进数字化、智能化、云化转型的背景下，网安产品需要同步更新和升级迭代，导致研发投入非常大；另一方面是安全服务人员，全球网安市场安全服务占比达到 50%以上，网安厂商如果不发展安全服务业务，收入增速会承压，但如果发展安全服务业务，收入增速上升但毛利率又不断下降，因此解决降本增效问题成为网安行业当务之急。AI 可有效提升安全运营的智能化和自动化程度，使得安服人员需求明显下降，从而带来显著降本增效空间，网安厂商的盈利能力进而有望改善。

■ 我们认为 AI 助力网安行业降本提效主要体现在以下三个方面：

1）基于自动化流程和工具高效执行安全测试。新产品开发出来后往往需要靠人反复迭代测试，而 AI 可以自动执行许多网络安全测试流程，例如辅助安全测试脚本编写、生成安全测试工具等，进而减轻了安全测试人员的工作量、降低人力成本。

2）基于 AI 和安全大数据实现机器永续运营值守。安全运营中最重要的因素是人，但网络攻击随时都可能发生，单纯依靠人无法做到 24 小时不间断值守。AI 可以实现自动化地永续运营值守，让安服人员能够通过自然语言交互的方式实现漏洞识别、威胁检测、安全响应等多种操作，从而降低安服人员需求、提升安全运营效率。

3）通用代码编写效率提升，助力研发降本增效。从研发层面来看，生成式 AI 技术可以实现编码任务自动化，并迅速识别和修复代码中的错误，从而提升开发效率、减少开发成本。例如 GitHub 于今年 3 月发布的新一代编程辅助工具 Copilot X，在 GPT-4 模型的加持下可将开发人员的代码编写效率提升近 10 倍。然而客观来讲，虽然 AI 能辅助生成代码，但是仅限于技术壁垒较低的通用型应用，网络攻防与协议分析等高精尖领域不大可能由 AI 代替，同时这些领域的研发人员几乎占研发团队的绝大多数，因此 AI 实际上只能替代少部分的人员成本。

图表3：AI 助力网安行业降本提效

来源：国金证券研究所

2.3 AI 应用带来新安全挑战，新安全需求同步增加

- AI 的快速发展和应用引发新安全风险，催生大量安全防护需求。AI 红利接踵而至，安全风险如影随形，网络安全新需求快速提升。首先，模型算法本身不可靠、不安全，AI 算法可解释性不足且鲁棒性较差，带来数据投毒攻击、恶意样本攻击等新安全挑战；其次是数据安全问题，大数据是 AI 技术研发和落地的基础，随着海量数据被生成、采集、存储和利用，数据安全和隐私保护领域的安全风险加剧；此外 AI 技术滥用风险极高，AI 网络攻击、AI 欺诈等新安全威胁持续增加。
- 我们认为 AI 应用场景的风险与治理主要体现在以下三个方面：

1）AI 攻击工具增加防护成本，防御侧亟需产品和技术方案升级。传统网络攻防为人与人的对抗，AI 赋能网络攻击后将彻底改变过去劳动密集型、成本高昂的攻击手法，从而衍生出更为精准和快速的自动化攻击方式，网络攻防真正进入智能化对抗时代。随着攻击侧技术和手段不断升级，将倒逼安全防护体系进一步强化，防御侧客户需求也将不断扩大。

2）大模型带来更多安全威胁，如数据泄露、欺诈攻击、社会治理安全等。以 ChatGPT 为代表的生成式 AI 技术可以快速生成钓鱼邮件、编写恶意软件与代码等，当网络攻击的技术门槛和成本下降后，攻击数量则呈现爆发式增长，AI 欺诈事件频繁发生。根据 Darktrace 数据，ChatGPT 等生成式 AI 导致网络钓鱼邮件攻击增长 135%。同时，生成式 AI 还带来了数据非法获取、数据泄露及恶意滥用等数据安全问题，例如 ChatGPT 在对话交互过程中能够获取用户数据或输出训练数据，这可能涉及到个人隐私数据、业务数据等敏感信息，从而加剧了数据泄露的风险，未来 AI 应用场景将催生广泛的数据安全需求。

3）针对 AI 算法的攻击层出不穷，如机器视觉攻击、数据源污染等。AI 算法鲁棒性较差，算法运行容易受到数据、模型、训练方法等因素干扰，本身存在被攻击、修改、窃取的安全风险，攻击者可通过对抗样本、数据投毒、模型窃取等多种方式对 AI 算法进行攻击，使其产生错误的预测或决策，同时由于算法黑箱和算法漏洞的存在，这些攻击往往难以检测和防范，导致 AI 在自动驾驶等场景难以大规模落地，强化 AI 监管防护成为大势所趋。

图表4：AI 应用场景的风险与治理

01
AI攻击工具增加防护成本，防御侧亟需产品和技术方案升级

02
大模型带来更多安全威胁，数据泄漏、欺诈攻击、社会治理安全等

03
针对AI算法的攻击层出不穷，机器视觉攻击、数据源污染等

来源：国金证券研究所

3. 投资建议

■ AI 发展催生安全防护需求，同时助力攻防技术升级，为网安行业带来显著降本增效空间，我们建议关注奇安信、安恒信息、启明星辰、永信至诚、深信服、绿盟科技、三未信安等网络安全厂商。

图表5：推荐 AI+网络安全相关标的

公司名称	股票代码	推荐理由
奇安信	688561.SH	奇安信是国内网安行业龙头，数据安全、态势感知等新赛道产品持续领跑，公司基于 ChatGPT 相关技术和自身积累的海量安全知识和数据，正开展专有类 ChatGPT 安全大模型的研发工作。预计 23、24、25 年摊薄 EPS 分别为 0.29、0.8、1.27 元，对应 201X、73X、46X PE。
安恒信息	688023.SH	安恒信息是新兴安全领跑者，“云、大、物、工、智”等新兴安全领域全面布局，已经将类 ChatGPT 的 AI 算法和智能数据分类分级、智能生成检测规则等多个场景相结合，积极推动产品 AI 智能化。预计 23、24、25 年摊薄 EPS 分别为 0.98、2.50、4.65 元，对应 184X、72X、39X PE。
启明星辰	002439.SZ	启明星辰是网安行业老牌厂商，2022 年发布智能辅助工具“PanguBot 盘小古”，基于多年的安全大数据积累以及中国移动在大模型及算力领域的能力，安全运营与服务降本提效未来可期。预计 23、24、25 年的摊薄 EPS 分别为 1、1.26、1.49 元，对应 32X、26X、22X PE。
永信至诚	688244.SH	永信至诚是网络靶场和人才建设领军企业，旗下网络靶场和“数字风洞”产品均是人工智能安全测试评估的基础设施平台，具备对 AI 相关产品和风险进行安全测试评估的能力。Wind 一致预测 23、24、25 年的摊薄 EPS 分别为 1.22、1.82、2.49 元，对应 58X、39X、28X PE。
深信服	300454.SZ	深信服是网络安全和云计算服务提供商，2023 年 5 月发布国内首款安全垂直领域大模型——深信服安全 GPT，大幅提升安全检测效果和安全运营效率，后续安全 GPT 将为所有安全产品赋能。预计 23、24、25 年摊薄 EPS 分别为 0.73、1.39、2.27 元，对应 168X、88X、54X PE。
绿盟科技	300369.SZ	绿盟科技是国内领先的综合性网安厂商，持续布局 AISecOps、SecXOps、安全知识图谱等 AI+安全方向，预计于今年第三季度发布基于类 GPT 技术的智能安全服务机器人，实现对安全运营的智能化支撑。Wind 一致预测 23、24、25 年的摊薄 EPS 分别为 0.39、0.54、0.78 元，对应 36X、26X、18X PE。
三未信安	688489.SH	三未信安是国内领先的商用密码基础设施提供商，“算法”+“芯片”两大硬核技术是三未信安在数据安全与密码领域的竞争优势，能够有效应对 AI 应用带来的数据安全风险与治理挑战。预计 23、24、25 年的摊薄 EPS 分别为 1.32、1.61、2 元，对应 57X、47X、38X PE。

来源：Wind，国金证券研究所（注：永信至诚和绿盟科技盈利预测及估值来自 Wind 一致预期，其他为国金证券研究所预测）

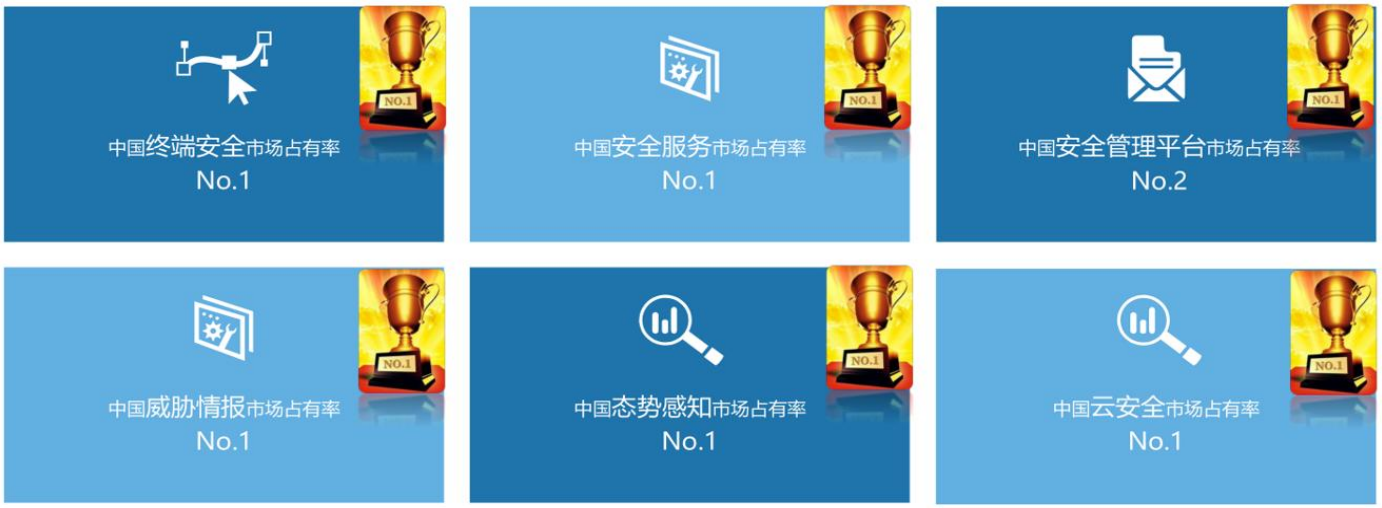
3.1 奇安信：AI 安全先行者，人工智能国家队

■ 奇安信是国内网络安全行业龙头，网络安全国家队，相关产品和服务已覆盖 90%以上

的中央政府部门、中央企业和大型银行，提供从规划到建设再到运行的全过程安全服务，以全链条安服能力提升客户粘性。奇安信目前安全产品品类超过百种，其中核心产品分为终端安全、边界安全、数据安全、实战型态势感知四大类。

- 新赛道产品增势强劲，竞争力市场领先。新赛道产品一类是指面向“云、大、工、移”新场景的安全产品，另一类是指使用“大数据、人工智能”等新技术提升威胁检测与安全防护能力的产品，高度迎合下游客户网络安全建设新需求。奇安信多款新赛道产品的市场占有率和竞争力持续领跑，数据安全、态势感知、终端安全等领域位居行业第一，未来有望持续贡献增量。根据奇安信 2022 年年报，其新赛道产品收入保持高速增长，数据安全产品收入同比增速超 55%，实战化态势感知产品同比增长超 20%。

图表6：奇安信新赛道产品及安全服务在国内市占率领先

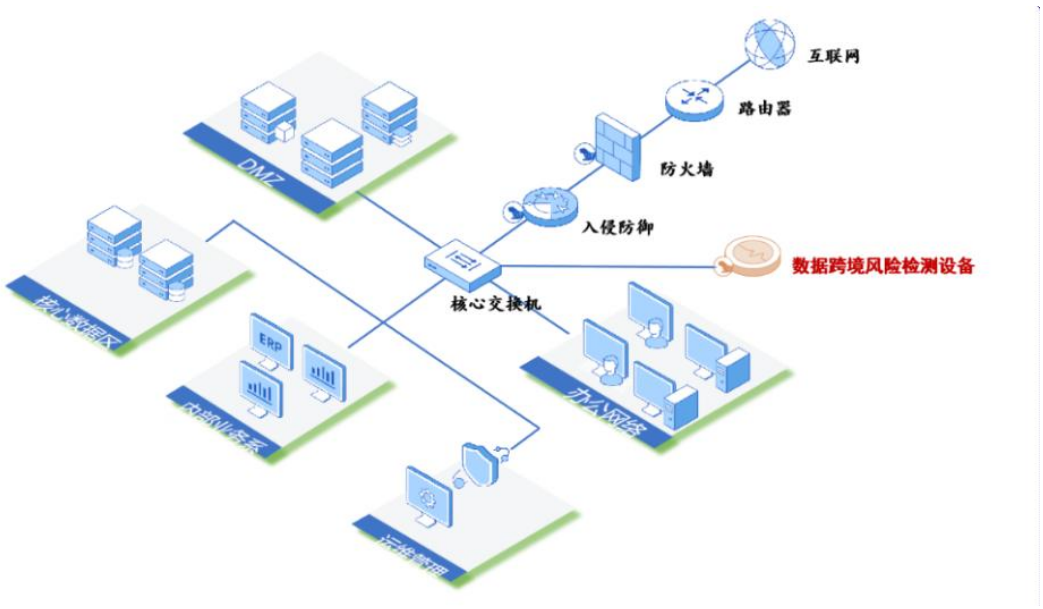


来源：IDC，赛迪，国金证券研究所

- AI 快速发展催生数据安全需求，持续领跑数据安全赛道。奇安信数据安全创新产品五件套包含特权卫士、权限卫士、API 卫士、隐私卫士和数据安全态势运营中心，帮助客户构建“一中心四卫士”的全场景数据安全闭环体系；使用境外的类 ChatGPT 产品，首先要解决数据跨境合规问题，奇安信领先行业发布数据跨境卫士，不仅使企业跨境传输的数据能够满足《数据安全法》、《个人信息保护法》、数据跨境监管等合规要求，还能对敏感数据的跨境流动情况进行全局掌控。此外，2022 年奇安信旗下数据安全产品通过了信通院的七大品类测评认证，是首家获得全套数据安全产品测评资质证书的网络安全企业，可有效应对 AI 应用所导致的数据安全风险与治理挑战。

- AI 技术赋能网络安全。奇安信高度重视 AI 技术在网络安全领域的应用，并在网络安全、计算机视觉、自然语言处理、恶意样本识别等方向提升产品智能化水平。基于 ChatGPT 相关技术和自身积累的海量安全知识和数据，其正在训练专有的类 ChatGPT 安全大模型，未来将广泛应用于安全产品开发、威胁检测、漏洞挖掘、安全运营及自动化等领域。2022 年奇安信获批建设“软件安全国家新一代人工智能开放创新平台”，正式跻身“人工智能国家队”。目前，奇安信人工智能研究院在深度伪造、深度鉴伪等技术上已取得重大突破，可以做到准确识别多种前沿 AI 伪造技术生成的虚假图片视频，成为防止 AIGC 技术生成虚假信息的有力武器。

图表7：数据跨境卫士有效保障 ChatGPT 运作中的数据跨境安全



来源：奇安信微信公众号，国金证券研究所

3.2 安恒信息：深度探索 AI+安全，赋能众多应用场景

- 发力新兴技术安全，打造平台化产品。安恒信息立足“云、大、物、智、工”发展战略，安恒云产品集多云安全和多云管理于一体，截至 2022 年已累计为 700 朵私有云、20000+云租户提供云安全服务，其中包含 200+省市级政务云、30+省级运营商。安恒信息是态势感知国家标准的核心起草单位，AiLPHA 态势感知产品目前已服务于全球 3000+客户，满足中大型政企客户对安全分析和安全运营的实战化、常态化需求，被 IDC 评为态势感知领导者。安恒信息形成了聚焦身份安全、数据流通、数据保护和咨询规划四大方向的“安恒数盾”品牌，其中 AiGuard 产品保障全生命周期、全链路、全场景数据安全，AiLand 数据安全岛实现数据共享过程的可靠、可控和可溯。此外，安恒信息从“云、边、管、端”四个层面共建物联网领域安全生态体系，赋能智慧物联服务。

图表8：安恒数盾数据安全全景图

来源：安恒信息微信公众号，国金证券研究所

- MSS 业务快速发展，海量安全数据为 AI 应用提供助力。安恒信息 MSS 业务已形成千万级体量，在教育、医疗、企业和政务市场打造了 100+标杆案例，根据 Frost&Sullivan

数据，安恒信息以 17.3%的市场份额位列 2021 年中国地区安全托管服务第一。云端安全运营中心每日采集 10 亿级安全告警数据，通过机器学习、大数据分析和 AI 等技术并结合实际攻防对抗经验，积累了 2000+ Usecase 规则，同时将用户网络攻击的平均检测时间（MTTD）和平均响应时间（MTTR）由业界普遍的数天级缩短到分钟级，实现安全检测及告警分析的自动化和智能化水平大幅提升。随着 MSS 业务持续增长，云端积累的数据和经验也将不断增加，安恒信息将加速投入打造“AI+安全大脑”，持续输出 AI 技术+情报数据链的实战化成果。

- 深度探索“AI+安全”，积极推动产品 AI 智能化。基于 AI 技术和海量安全数据，安恒信息打造了基于深度学习的 AI+恶意软件检测、基于 AI 的加密流量威胁检测引擎、基于人工智能和集成学习的 UEBA 分析流程、MSS 云平台 AI 威胁分析引擎、ChatGPT 违规使用检测等多项安全产品及服务，有效提升安全防护能力及运营效率。目前已经将类 ChatGPT 的 AI 算法和智能数据分类分级、智能生成检测规则、智能告警处置分析、智能客服问答系统、智能钓鱼邮件分析、智能加密流量检测等多个场景进行结合，积极布局 AI 前沿研究并加速 AI 产品落地进程。

图表9：安恒信息将AI技术和安全领域的众多场景相结合

应用场景	主要内容
智能数据分类分级	基于强化学习的人工智能模型已经在 AiSort 数据安全分级产品中部署应用，AiSort 能够精准识别数据业务含义，进行自动分类分级，大幅提高数据梳理的工作效率。
智能生成检测规则	针对内网环境，ChatGPT 可以根据客户现场对误报的处理，从大量的原始日志、告警信息、误报中自动学习，自动生成检测规则； 针对云上环境，依托 MSS 平台积累的大量数据，在此基础上研究场景，利用强化学习训练模型和人工反馈不断调试优化。开发运营反馈模块，将告警排查过程中的各种日志证据录入上报，利用 ChatGPT 学习其中的模式并自动生成告警规则，在降低误报的同时也可以对新产生的攻击方式和手法自动生成检测规则。
智能告警处置分析	针对告警处置，ChatGPT 可以学习安全分析师对各类风险场景的处置动作，自动生成处置规则。借助运营反馈模块，将告警排查过程中的各种日志证据进行录入上报； 针对云上环境，可以利用 MSS 平台收集全国数据，在此基础上训练用于风险研判的 ChatGPT 模型。
智能客服问答系统	公司初步训练的模型已在内部试用，可以实现常见系统问题的应答，未来将在智能语音问答方面积极探索。
智能钓鱼邮件分析	基于多年积累的攻防实践经验，公司将 AI 技术与邮件附件智能沙箱技术、邮件正文语言分析技术和邮件收发账号 UEBA 技术相结合，可以准确识别可疑邮件、及时做出钓鱼邮件预警，未来将积极探索 Bard、ChatGPT 等大型语言模型，全方位守护用户的邮件安全。
智能加密流量检测	EMT 智能流量检测系统支持大规模网络全流量捕获、检索，网络攻击检测、分析，威胁行为评估、溯源，可以结合 ChatGPT 技术进行深度分析，加速网络威胁检测，实时发现并响应攻击行为。

来源：安恒信息微信公众号，国金证券研究所

3.3 启明星辰：“盘小古”助力安全运营与服务降本增效

- 产品线覆盖齐全，新安全业务持续放量。启明星辰是网络安全产品、服务和解决方案综合提供商，深耕网络安全领域 27 年，除了基础安全产品市场份额持续多年领先外，启明星辰在数据安全、工控安全和物联网安全等新兴安全领域中多项产品市占率第一。面对数字化场景带来的新发展机遇和新安全挑战，启明星辰以数据安全、涉云安全和安全运营业务作为三大顶级业务战略，打造业务增长新引擎。2022 年启明星辰涉云安全、数据安全 2.0&3.0、工业数字化安全、安全运营等新业务板块实现收入 18.8 亿元，同比增长 21.1%，其中涉云安全和数据安全 2.0&3.0 业务收入均同比增长 40%以上。

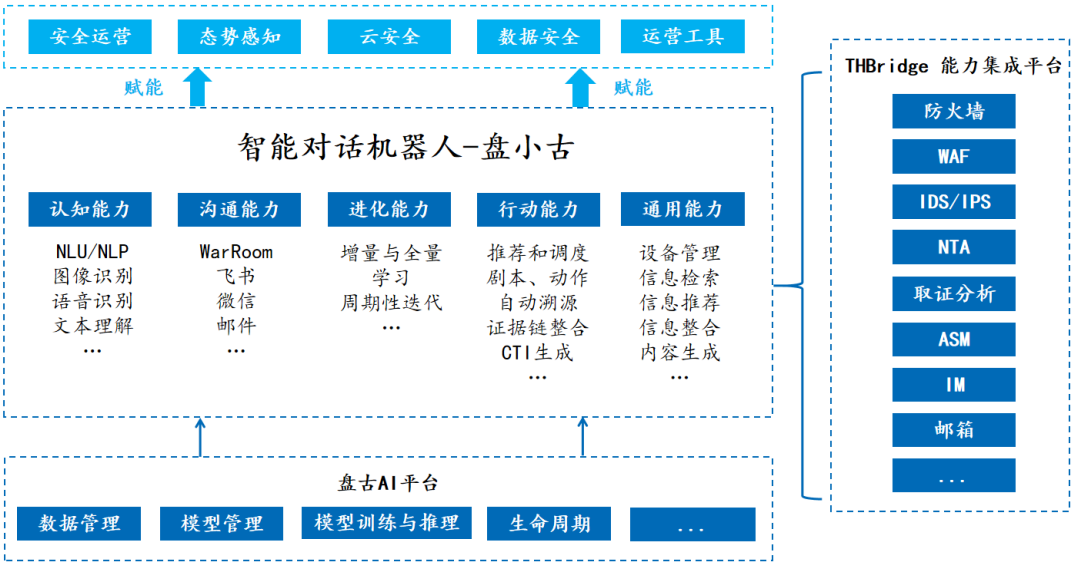
图表10：“数据绿洲”数据安全能力全景图

来源：启明星辰微信公众号，国金证券研究所

- “盘小古”赋能安全运营智能化和自动化。启明星辰2022年发布“PanguBot 盘小古”，盘小古是启明星辰自主研发的针对安全领域的智能助手类产品组件，主要是作为安全运营中心的辅助智能工具，通过AI技术为前端运维人员提供支持。盘小古的核心大脑为专门应用在安全领域的AI模型，基于安全运营专用语料库训练而成，相当于安全运营领域的专家，一方面整合各种运营工具，并通过会话方式为安全运营人员提供支持，实现运营的自动化；另一方面具有内容检索、整合、推荐和内容生成能力，自动生成可用的CTI威胁情报，实现运营的智能化。此外，盘古人工智能平台为模型运行提供算力和环境，并通过全生命周期的建模和模型迭代更新管理能力使模型不断学习和进化，进而提升作战能力，提高整体运营效率。

- 依托中国移动大模型能力及算力，安全运营降本提效未来可期。大模型训练往往需要海量数据和强大算力支撑，中国移动自主研发了“九天”人工智能平台，并与中国移动通信联合会、中国电信、中国联通和中国广电等单位合作成立GPT产业联盟，加码布局AI大模型。未来启明星辰有望借助中国移动的大模型能力及算力支撑，基于通用大模型和自身二十多年来积累的海量安全数据，训练安全垂直领域大模型。从AI赋能网络安全的角度来看，未来安全运营业务全面融入大模型能力后，一方面有助于提前发现潜在威胁特征，进行漏洞自动挖掘，大幅提升威胁检测和分析能力；另一方面对于安全运营智能助手等新应用，可以通过自然语言交互的方式实现安全运营全流程的自动化，从而大幅减少安服等人员需求，降低人员成本，提高安全运营效率。目前启明星辰安全运营中心已经覆盖了全国1/3地级市，后续“盘小古”的升级迭代有望带来显著降本增效。

图表11：“PanguBot 盘小古”赋能安全运营与服务

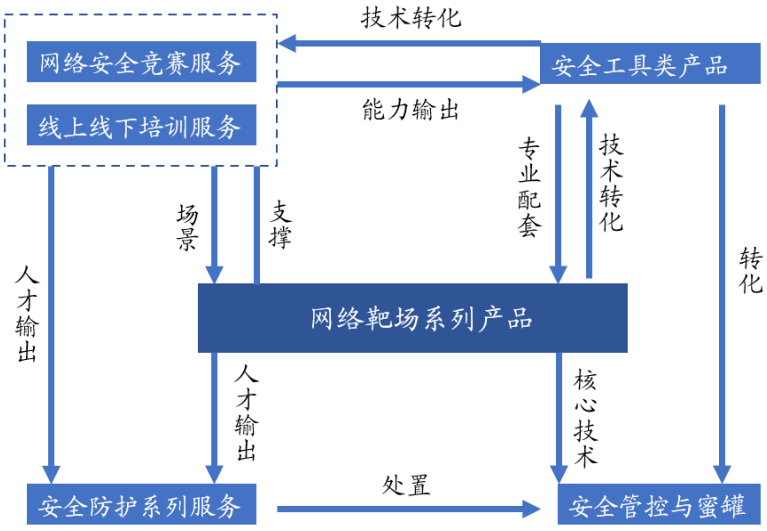


来源：启明星辰微信公众号，国金证券研究所

3.4 永信至诚：为 AI 安全测试和评估提供基础设施平台

- 永信至诚是网络靶场和人才建设领军企业。基于网络空间平行仿真及攻防对抗类技术，永信至诚推出了网络靶场系列产品、安全管控与蜜罐产品、安全工具类产品、安全防护系列服务、网络安全竞赛服务和其他服务。其中，网络靶场系列产品是核心业务，其核心技术为蜜罐产品奠定了技术基础；网络安全竞赛服务和线上线下培训服务作为流量入口，积累行业化经验、储备安全人才以及提升公司影响力。

图表12：永信至诚产品服务体系生态链条



来源：永信至诚招股说明书，国金证券研究所

- 永信至诚的网络靶场和数字风洞产品是人工智能安全测试评估的基础设施平台。人工智能在不同行业和领域的应用有不同形态，例如 ChatGPT 类的人工智能平台，一般会出现接口类、越权类等网络安全风险，还可能存在隐私泄露、数据泄露等数据安全风险，永信至诚网络靶场和数字风洞产品具备对该类产品和风险进行安全测试评估的能力。
- 春秋云境网络靶场平台为永信至诚核心产品，基于平行仿真技术体系构建而成，是进行网络安全研究、人才培养、实战演练、安全测试、效能分析及态势推演等的专业试验平台，目前已支撑国家多个部委主办的数十场网络安全演练活动及多个行业的靶场建设工程，覆盖“7+1”业务场景。根据 IDC 数据，2021 年春秋云境网络靶场以 20.4%的市场份额位居第一。

图表13：春秋云境网络靶场覆盖“7+1”业务场景

网络靶场业务场景	模式	主要内容
赛事演练靶场	“外打内”模式	赛事演练靶场平台提供完备的赛前、赛中、赛后管理功能，支持多种可选的比赛模式、积分计算模式以及配套大屏展示效果。
业务模拟仿真靶场		提供完善的仿真场景构建能力，基于多年来积累的靶标库和基础场景库、行业仿真场景库等，利用模拟仿真的靶场场景提供测试测评、攻防演练、效能评估、科研研发等。
智慧城市安全测试靶场	“内打外”模式	能够对测试人员的测试流程、测试手段等进行标准化和精细化管控，也需要能够在测试中及时辨认和终止这些危险操作并进行自动化的控制。
案件线索追踪实战靶场		为了使案件线索追踪实战制式化、装备化，并提升自我防护难题，结合客户业务特性和需求研发了案件线索追踪实战靶场。
人才培养靶场	“内打内”模式	教师和学生分别用自己账号登录平台，教师在靶场进行教学和考核任务下发；学员在靶场进行学习和实验训练，以及技能考核。
人工智能攻防靶场		在人工智能攻防研究中，靶场提供了安全可靠和灵活的测试环境，还可以自动记录测试参数判断是否达到研制预期效果。
复杂业务安全推演靶场		复杂业务安全推演靶场的特点在于自动进行的规模化测试和推演能力。
综合应用型网络靶场		是网络靶场中多种应用场景融合的业务形态，基于公司多项关键技术及产品构建虚拟网络仿真场景，融合核心技术形成多种形态的靶场模块。

来源：永信至诚招股说明书，国金证券研究所

- “数字风洞”开启安全测试评估专业赛道，实现数据安全可知、可视、可验、可量化。基于安全“证无”理念和 3×3×3×(产品×服务)安全感公式，永信至诚 2023 年推出数据安全“数字风洞”产品，目前已形成面向全场景、全要素、全生命周期的安全测试评估解决方案。“数字风洞”产品通过对人、系统、数据等进行持续性测试评估，督促和帮助系统不断迭代优化，助力网络和数据安全由“形式合规”转向“实质合规”。

图表14：数字风洞打造数据安全测试评估标准平台

来源：永信至诚微信公众号，国金证券研究所

- 在人工智能攻防研究领域，永信至诚的人工智能攻防靶场和 RHG 智能靶场平台是验证人工智能网络攻防对抗可行性、可用性的重要设施。永信至诚人工智能攻防靶场提供了安全可靠和灵活的测试环境，可以自动记录测试参数判断是否达到研制预期效果，为人工智能相关技术在网络安全领域的突破融合和实践测试等提供了基础的试验床和数据集，为漏洞挖掘与利用、综合智能攻防等人工智能安全技术的发展及效能验证提供了平台和测试数据集，是人工智能技术在网络安全领域实践的有效基础设施。
- 永信至诚自主研发了国内首个人工智能网络安全攻防平台 RHG(Robo Hacking Game)，

是人工智能在网络安全攻防领域具有创新性的、技术领先的竞赛平台。网络安全竞赛是人工智能在安全领域探索实践的重要平台，2017 年永信至诚推出了自主研发的 RHG 智能靶场平台，同年启动 RHG 中国首届国际机器人大赛，开启了中国人工智能安全演练的先河，并通过网鼎杯、纵横杯、DEF CON CHINA BCTF 等国际国内重要网络安全演练，不断吸引更多研究者通过公司的 RHG 靶场平台对其研究成果进行测试和验证。

图表15：网络安全竞赛是人工智能在安全领域探索实践的重要平台

来源：永信至诚微信公众号，国金证券研究所

3.5 深信服：国内首发安全垂直领域 GPT 大模型

- 网络安全与“云”同行，坚持 XaaS 战略。深信服是网络安全、云计算及 IT 基础设施、基础网络与物联网等产品和服务提供商，VPN、全网行为管理、下一代防火墙、桌面云、超融合等核心产品多年来保持市占率领先。在数字化、云化、服务化的大背景下，深信服从 2021 年开始实行 XaaS 优先战略，持续加大托管云、MSS、SASE、DaaS 等 XaaS 产品和服务的投入力度，推动业务向“云化+服务化”转型。
- AI 领域布局较早，先发优势显著。深信服从 2016 年开始将 AI 技术应用于终端安全领域，作为网络安全和云计算综合厂商，其核心优势在于拥有海量安全数据和充足云端算力，多年来积累了丰富的 AI 模型和“AI+安全”领域专业人才。深信服已经推出了终端安全 SAVE 引擎、AISecOps 智能安全运营等多款融合 AI 技术的产品和服务，目前在文件检测、行为检测、日志分析等 10+不同领域都结合并运用了 AI 能力。凭借在 AI 领域的前瞻性布局，叠加在网安赛道的多年经验和技术积累，深信服有望持续领跑“AI+安全”领域。

图表16：深信服在 AI+安全领域具备先发优势

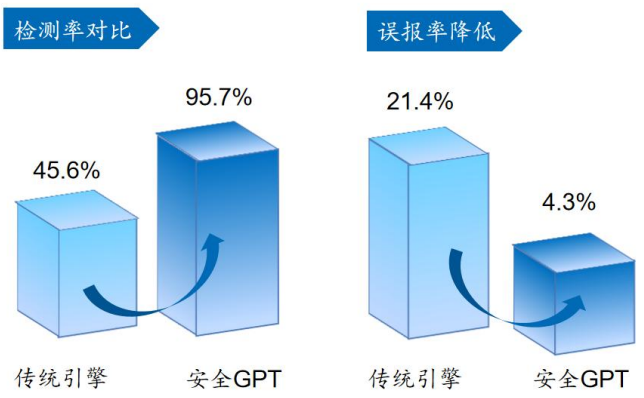
来源：深信服官网，国金证券研究所

- 发布自研大模型安全 GPT，全面布局人工智能。2023 年 5 月深信服发布国内首个安全

垂直领域 GPT 大模型——深信服安全 GPT，安全 GPT 由“大模型算法+威胁情报+安全知识”训练而成，并通过安全专家和原有小模型进行了大量微调，使其同时具有泛化的检测能力和高质量的攻击解释能力，并且能够实现快速迭代。此外安全 GPT 可以针对用户自身的安全日志和产品进行个性化安全分析。作为自研大模型，安全 GPT 不依赖开源模型服务，并被部署至托管云中，保障了数据的安全可控。未来安全 GPT 将为所有产品赋能，目前其已被应用到 XDR 平台和下一代防火墙中。

- 安全 GPT 赋能带来显著降本增效空间。安全 GPT 大模型可以大幅提升流量和日志的安全检测能力，实现用户安全现状自动分析及建议生成，自动化调查、分析、研判能够提升安全运营效率。此外，通过自然语言交互的方式大幅度提升了安全运营的的全流程效率，降低了对安全人员的需求，后续有望大幅降低人力成本。从安全 GPT 赋能 XDR 的效果来看，通过前期 5000 万样本数据测试，安全 GPT 加持的 XDR 高级威胁检测率高达 95.7%，误报率（安全告警里判错的比例）仅 4.3%，同时能够将安全事件的响应效率提升至分钟级，通过对话问答的方式实现安全漏洞快速排查，大幅提升安全运营效率。

图表17：安全 GPT 能够显著增强高级威胁检测能力



来源：深信服微信公众号，国金证券研究所

图表18：安全 GPT 能够大幅提升安全运营效率

来源：深信服微信公众号，国金证券研究所

3.6 绿盟科技：持续投入 AI+安全方向，新产品蓄势待发

- 网络安全行业综合厂商，新兴业务多点开花。绿盟科技是国内领先的综合性网络安全厂商，能够为客户提供全品类网络安全产品、场景化安全解决方案和体系化安全运营服务，其 IPS、ADS、RSAS、WAF 等基础安全产品多年来位居市场第一，云安全、态势感知平台、全流量感知等新兴安全产品位居市场前列。绿盟科技坚持安全技术创新，重点布局数据安全、云安全、工业互联网安全、物联网安全等新兴领域，2022 年数据安全、云安全、工业互联网安全等核心赛道产品订单分别为 2.51、3.95、0.78 亿元，分别同比增长 45%、75%、20%。
- 持续投入 AI+安全方向，积累多项研究成果。绿盟科技天枢实验室专注于 AI 方向的研究，在 AI 模型的鲁棒性增强、AI 系统安全防护、AI 应用安全、AI 系统的安全性评估与测试等领域拥有多年的技术积累，并积极探索 AISecOps、SecXOps、安全知识图谱、针对 Web 攻击的 AI 高性能检测方案等 AI+安全方向。绿盟科技参与编写了中国信通院《人工智能研发运营体系(MLOps)实践指南(2023 年)》，此外，绿盟科技以“智慧安全 3.0”理念体系为指引，不断创新 AI 和大数据等核心技术，从而构建“全场景、可信任、实战化”的安全运营能力，实现“全面防护，智能分析，自动响应”的安全防护效果。

图表19：绿盟科技智慧安全 3.0 理念体系

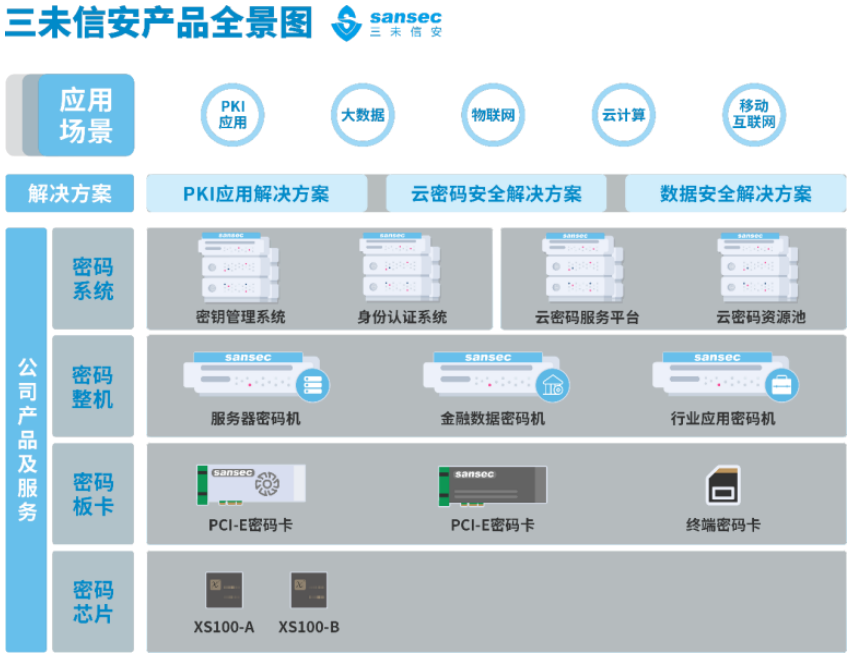
来源：绿盟科技官网，国金证券研究所

- AI+安全产品不断落地，新产品蓄势待发。绿盟科技已将类 GPT 技术应用于安全攻防、安全运营、类 GPT 技术的风险分析和应对等多个领域。此外基于多年积累的攻防知识、运营数据与威胁情报，绿盟科技计划于今年第三季度发布基于类 GPT 技术的智能安全服务机器人，实现对安全运营的智能化支撑，进一步提升安全运营服务效能。此外，根据其 5 月 15 日发布的 2023 年度向特定对象发行股票预案，绿盟科技拟募集资金约 4.76 亿元投入研发总部基地建设项目，其中包括建设支持网络安全行业应用的安全算力大脑平台，从而进一步构建智能安全运营的生态体系，为网络安全领域的 AI 应用提供研发、运营、运维的一体化环境。

3.7 三未信安：密码技术为 AI 安全保驾护航

- 三未信安是国内领先的商用密码基础设施提供商，主要产品包括密码芯片、密码板卡、密码整机和密码系统，可实现各种应用场景的国产密码改造和数据安全保障，为关键信息基础设施和云计算、大数据、物联网、人工智能等新兴领域提供密码服务。

图表20：三未信安产品体系

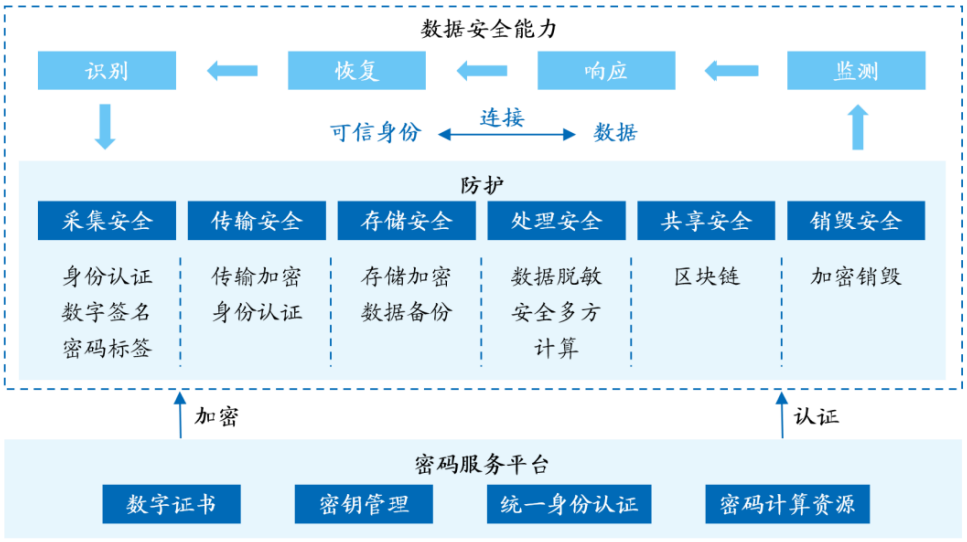


来源：三未信安招股说明书，国金证券研究所

- 密码是实现数据安全的核心技术与基础支撑。数据隐私和安全保护问题是人工智能系统在开发和应用中面临的严峻挑战，AI 训练数据的质量和安全性，将直接影响 AI 算

法、AI 技术的质量和安全性，亟需建设数据安全防护能力，防范数据安全风险。密码安全防护作用贯穿于数据采集、数据传输、数据存储、数据处理、数据交换、数据销毁等全生命周期，在身份认证、访问控制、数字签名、传输加密、存储加密、隐私保护等方面发挥重要作用。AI 浪潮下，数据安全产业高速发展，商用密码紧密同行。

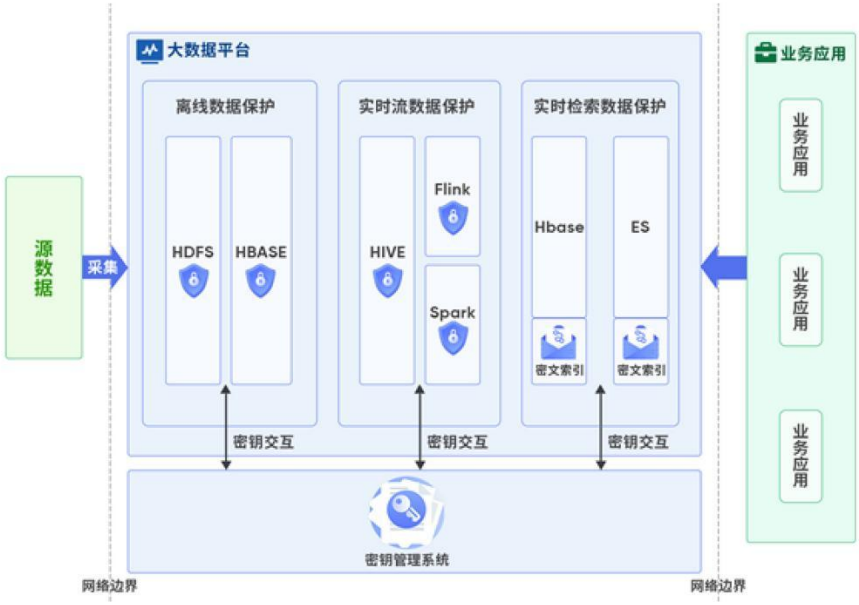
图表21：密码是实现数据安全的核心技术与基础支撑



来源：《信息安全与通信保密》，国金证券研究所

■ 三未信安积极布局数据安全领域，包括数据安全与隐私计算技术、密码硬件加速核心技术两大层面。三未信安将大数据安全与隐私保护技术和产品作为重要发展战略，以安全多方计算、同态加密、隐私计算等新型密码技术为核心，实现密码系统与大数据、人工智能等各种信息系统的深度融合，全面提高大数据安全的保障能力。在密码硬件加速核心技术方面，三未信安重点突破数据安全系统中核心密码运算的效率问题，研发了 XS100 密码芯片、密码板卡、密码机等产品，密码运算性能达到国内领先水平。“算法”+“芯片”两大硬核技术是三未信安在数据安全与密码领域的竞争优势所在，不但能够保障数据全生命周期的高安全性，而且有效解决了数据安全的效率瓶颈问题。

图表22：三未信安大数据加密系统应用场景



来源：三未信安官网，国金证券研究所

4. 风险提示

■ 国内宏观经济环境波动的风险

宏观经济环境的波动可能影响需求落地的意愿、能力、量级和节奏。

■ 政策落地不及预期

AI 在网络安全领域的应用目前还处于初期，部分领域在萌芽和成长前期需要政策的鼓励和扶持。

■ 技术应用普及不及预期

AI 技术对于网络安全产品和服务的赋能需要网安厂商持续投入大量的研发，存在技术应用落地不及预期的风险。

行业投资评级的说明：

买入：预期未来 3—6 个月内该行业上涨幅度超过大盘在 15%以上；

增持：预期未来 3—6 个月内该行业上涨幅度超过大盘在 5%—15%；

中性：预期未来 3—6 个月内该行业变动幅度相对大盘在 -5%—5%；

减持：预期未来 3—6 个月内该行业下跌幅度超过大盘在 5%以上。

特别声明：

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

本报告的产生基于国金证券及其研究人员认为可信的公开资料或实地调研资料，但国金证券及其研究人员对这些信息的准确性和完整性不作任何保证。本报告反映撰写研究人员的不同设想、见解及分析方法，故本报告所载观点可能与其他类似研究报告的观点及市场实际情况不一致，国金证券不对使用本报告所包含的材料产生的任何直接或间接损失或与此有关的其他任何损失承担任何责任。且本报告中的资料、意见、预测均反映报告初次公开发布时的判断，在不作事先通知的情况下，可能会随时调整，亦可因使用不同假设和标准、采用不同观点和分析方法而与国金证券其它业务部门、单位或附属机构在制作类似的其他材料时所给出的意见不同或者相反。

本报告仅为参考之用，在任何地区均不应被视为买卖任何证券、金融工具的要约或要约邀请。本报告提及的任何证券或金融工具均可能含有重大的风险，可能不易变卖以及不适合所有投资者。本报告所提及的证券或金融工具的价格、价值及收益可能会受汇率影响而波动。过往的业绩并不能代表未来的表现。

客户应当考虑到国金证券存在可能影响本报告客观性的利益冲突，而不应视本报告为作出投资决策的唯一因素。证券研究报告是用于服务具备专业知识的投资者和投资顾问的专业产品，使用时必须经专业人士进行解读。国金证券建议获取报告人员应考虑本报告的任何意见或建议是否符合其特定状况，以及（若有必要）咨询独立投资顾问。报告本身、报告中的信息或所表达意见也不构成投资、法律、会计或税务的最终操作建议，国金证券不就报告中的内容对最终操作建议做出任何担保，在任何时候均不构成对任何人的个人推荐。

在法律允许的情况下，国金证券的关联机构可能会持有报告中涉及的公司所发行的证券并进行交易，并可能为这些公司正在提供或争取提供多种金融服务。

本报告并非意图发送、发布给在当地法律或监管规则下不允许向其发送、发布该研究报告的人员。国金证券并不因收件人收到本报告而视其为国金证券的客户。本报告对于收件人而言属高度机密，只有符合条件的收件人才能使用。根据《证券期货投资者适当性管理办法》，本报告仅供国金证券股份有限公司客户中风险评级高于 C3 级（含 C3 级）的投资者使用；本报告所包含的观点及建议并未考虑个别客户的特殊状况、目标或需要，不应被视为对特定客户关于特定证券或金融工具的建议或策略。对于本报告中提及的任何证券或金融工具，本报告的收件人须保持自身的独立判断。使用国金证券研究报告进行投资，遭受任何损失，国金证券不承担相关法律责任。

若国金证券以外的任何机构或个人发送本报告，则由该机构或个人为此发送行为承担全部责任。本报告不构成国金证券向发送本报告机构或个人的收件人提供投资建议，国金证券不为此承担任何责任。

上海
电话：021-60753903
传真：021-61038200
邮箱：researchsh@gjzq.com.cn
邮编：201204
地址：上海浦东新区芳甸路 1088 号
紫竹国际大厦 7 楼

北京
电话：010-85950438
邮箱：researchbj@gjzq.com.cn
邮编：100005
地址：北京市东城区建内大街 26 号
新闻大厦 8 层南侧

深圳
电话：0755-83831378
传真：0755-83830558
邮箱：researchsz@gjzq.com.cn
邮编：518000
地址：深圳市福田区金田路 2028 号皇岗商务中心
18 楼 1806