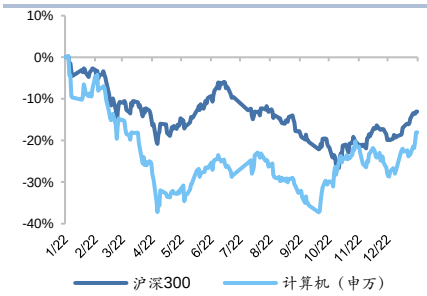
AI 既是网安需求来源，也是网安下一形态

行业评级：增持

报告日期：2023-03-29

行业指数与沪深 300 走势比较



分析师：尹沿技

执业证书号：S0010520020001

邮箱：yinyj@hazq.com

分析师：王奇珏

执业证书号：S0010522060002

邮箱：wangqj@hazq.com

联系人：张旭光

执业证书号：S0010121090040

邮箱：zhangxg@hazq.com

相关报告

1.《华安证券_公司研究_计算机行业_行业深度_存量改造+数据安全，商密处于上升期》2023-1-20

2.《华安证券_行业研究_计算机行业_行业深度_多角度对比美国网安，我国网安前景广阔》2022-05-16

主要观点：

AI 及算力发展，带来网络安全的直接需求

目前 AI 和大模型带来了算力搭建需求，以服务器插八张 GPU 来计算，两万片 GPU 的 AI 训练带来的服务器增量，即 1250 台服务器。而两万片 GPU，以 trendforce 预计约为 chatGPT3.5 所需数量，未来可能超过 3 万颗。考虑到国内各大互联网、IT 厂商相继投入大模型，未来服务器、数据中心的建设已是高确定性事件。数据中心由于骨干网、云端数据中心其自身 1）边界访问安全需求；2）数据保护需求；3）运行状态检测运营需求，对于网络安全设备有天然需求。**我们认为**，AI 乃至大模型时代，网安设备的硬需求为同向增长状态。

AI 能力增加了网络进攻，催生事件性驱动

网络安全的本质是攻防，攻击者盗取破坏信息，防护者保护信息。由于防守者永远是被动，即使是态势感知也无法阻止最开始的破坏入侵， AI 带来的降本增效首先受益方是攻击者。根据 MIT Technology Review 对于 300 个网安公司人员的采访数据，2021 年 60%的采访对象已经难以应对自动化的网络攻击，96%的人已经在开始遭受 AI 网络攻击，部分使用了 AI 进行防御。近期发布的腾讯《2023 产业互联网安全十大趋势》也指出，chatGPT 类技术辅助写代码的能力大大降低了攻击者的技术门槛，而可以对于漏洞攻击、钓鱼攻击、鱼叉攻击等常用的攻击方式进行快速上手和创新。我们认为，AI 的成长，会带来攻击量增长，网安的技术性需求会由于攻击事件的催化而得到释放。

AI 能力融入网络安全，性能表现可观

网络安全的攻防，基础之一在于网络流量的分析识别，也包括了 dns 日志、HTTP/S 日志等数据。这些数据在网络上被探针感知到传送到安全厂商集成了 AI 能力的监测中心时，危险的探知识别以及随后的发送防御信号也随之进行。AI 大模型在学习、分析、识别乃至发送命令上相对于人类具有高效的优势，如 3 月 29 日发布的 Microsoft Secure Copilot 可以将耗时几小时甚至十几小时的勒索软件事件处理降至秒级。因此，在近期国际争端中，网络安全大国也会对于盟友进行相应的 AI 类网络安全能力帮助，如 AI 监控运营商流量。

投资建议

AI 赋能网络安全，从需求和供给改革行业生态。我们认为可关注以下标的：1） 传统厂商，如奇安信、深信服、启明星辰等；2） 密码类厂商，信安世纪、吉大正元、电科网安等；3）数据要素类厂商，美亚柏科、熙菱信息等。

风险提示

1）技术研发不及预期；2）政策支持不及预期；3）下游需求不及预期。

正文目录

图表目录

引言：AI 既是网安需求来源，也是网安下一形态

在《关于构建数据基础制度更好发挥数据要素作用的意见》等政策助推下，数据要素市场成为接下来重点发展的主题，而数据要素对应的前提就是数据安全。工信部等 16 部门发布的《关于促进数据安全产业发展的指导意见》，提到 2025 年我国数据安全产业规模将达 1500 亿元，同比增速 30%。网络安全仍是目前数字经济中一条不可忽视的主线。

- **观点一：AI 及算力发展，带来网络安全的直接需求。**目前 AI 和大模型带来了算力搭建需求，以服务器插八张 GPU 来计算，两万片 GPU 的 AI 训练带来的服务器增量，即 1250 台服务器。而两万片 GPU，以 trendforce 预计约为 chatGPT3.5 所需数量，未来可能超过 3 万颗。考虑到国内各大互联网、IT 厂商相继投入大模型，未来服务器、数据中心的建设已是高确定性事件。数据中心由于骨干网、云端数据中心其自身 1）边界访问安全需求；2）数据保护需求；3）运行状态检测运营需求，对于网络安全设备有天然需求。我们认为，AI 乃至大模型时代，网安设备的硬需求为同向增长状态。

- **观点二：AI 能力增加了网络进攻，催生事件性驱动。**网络安全的本质是攻防，攻击者盗取破坏信息，防护者保护信息。由于防守者永远是被动，即使是态势感知也无法阻止最开始的破坏入侵， AI 带来的降本增效首先受益方是攻击者。根据 MIT Technology Review 对于 300 个网安公司人员的采访数据，2021 年 60%的采访对象已经难以应对自动化的网络攻击，96%的人已经在开始遭受 AI 网络攻击，部分使用了 AI 进行防御。近期发布的腾讯《2023 产业互联网安全十大趋势》也指出，chatGPT 类技术辅助写代码的能力大大降低了攻击者的技术门槛，而可以对于漏洞攻击、钓鱼攻击、鱼叉攻击等常用的攻击方式进行快速上手和创新。我们认为，AI 的成长，会带来攻击量增长，网安的技术性需求会由于攻击事件的催化而得到释放。

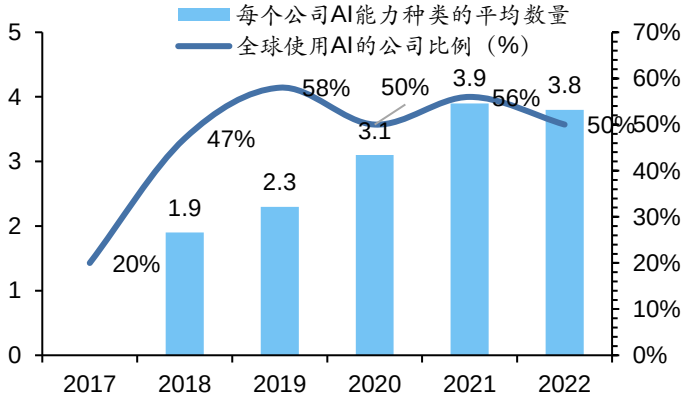
- **观点三：AI 能力融入网络安全，性能表现可观。**网络安全的攻防，基础之一在于网络流量的分析识别，也包括了 dns 日志、HTTP/S 日志等数据。这些数据在网络上被探针感知到传送到安全厂商集成了 AI 能力的监测中心时，危险的探知识别以及随后的发送防御信号也随之进行。AI 大模型在学习、分析、识别乃至发送命令上相对于人类都有高速的优势，目前对于创新程度不高的攻击都具有较好的防护能力。因此，在近期国际争端中，网络安全大国也会对于盟友进行相应的 AI 类网络安全能力帮助，如 AI 监控运营商流量。

1 AI 带来网络安全的内生与外部推动需求

1.1 AI 风潮与大数据并行，chatGPT 带出高算力时代

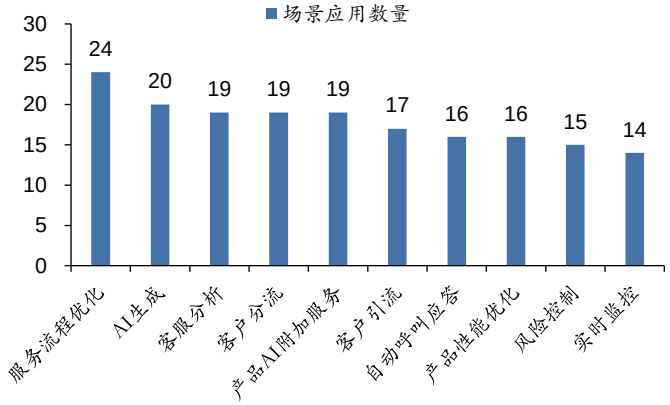
AI 时代赋能多应用场景，数据价值体现。自 2017 年以来，全球企业对于 AI 的使用已到达了一个稳定高峰。根据麦肯锡数据，近四年，全球使用 AI 的企业数量占比在 50-60%之间，较 2017 年 20%的水平已提升 2.5X。平均每个公司都会使用近四种 AI 能力，比起 2018 年的 1.9 种也近翻倍。其中，流程自动化、计算机视觉、自然语言分析、对话界面和深度学习已经成为前五大 AI 用途。而从训练到应用的逻辑来说，AI 的广泛应用，其核心基础是高质量、与应用场景贴合的海量数据资源。

图表 1 2017-2022 全球公司应用 AI 比例及使用数量



资料来源：McKinsey，华安证券研究所

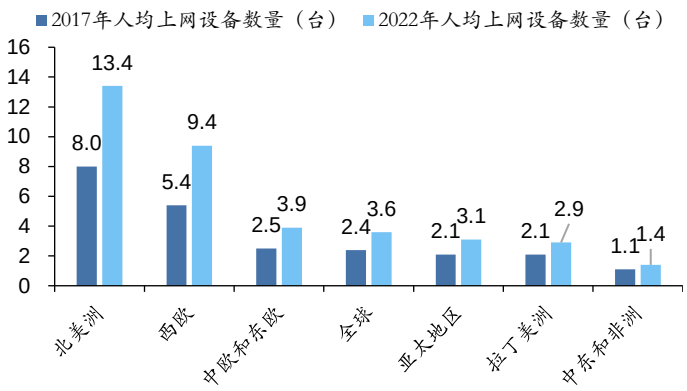
图表 2 2022 年 AI 应用次数最高场景



资料来源：McKinsey，华安证券研究所

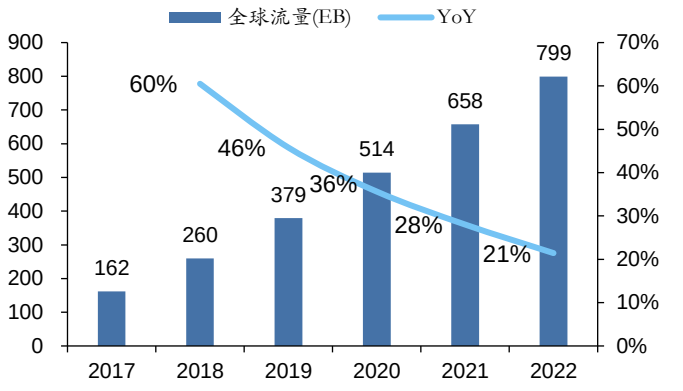
数据量随设备增长，“量价齐升”带动大数据。根据思科的《年度互联网报告》，2023 年地球上的**连网设备数量**将是全球人口的大约三倍，从 2017 年的人均 2.4 台提升至 3.6 台。IP 地址即网络地址+主机地址，网络站点所连接的 IP 数量也由于练级设备增长而处于爆发的阶段。根据 IDC 的《中国物联网连接规模预测，2020-2025》，仅我国物联网 IP 连接量已在 2020 年达 45.3 亿，有望在 2025 年达到 102.7 亿，CAGR 为 17.8%。由于每一个设备联网后开始产生数据流量， 其独有的 IP 地址的数量增长即代表全网数据也将继续大增。根据思科的《年度互联网报告》，2022 年全球网络数据流量将达 799EB（1EB=十亿 GB），同比增长 21%。在数据总量增长的大环境下，总体数据的价值随之提升，有望直接带动大数据产业的发展。

图表 3 2017 与 2022 年人均联网设备数量



资料来源：思科，华安证券研究所

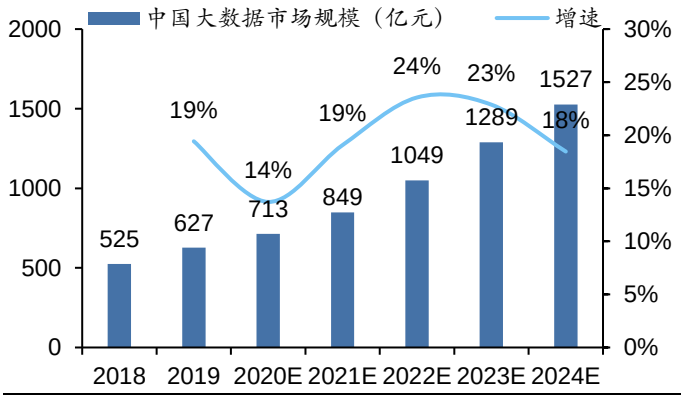
图表 4 2017-2022 全球网络流量



资料来源：思科，华安证券研究所

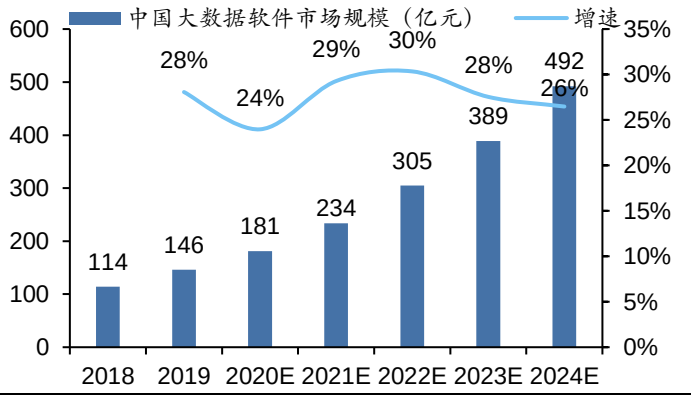
大数据市场规模可观，软件部分增速高。收益于数据量增长，我国大数据市场及相应软件市场规模、增速可观。沙利文研究预计 2022 年我国大数据市场规模为 1049 亿元，同比增速 24%，其中软件约 305 亿元，同比增速 30%，占比约 29%。在大数据行业的高增速之下，数据智能分析工具、大数据管理平台等软件的需求有望进一步提升。

图表 5 我国大数据市场规模



资料来源：沙利文研究，华安证券研究所

图表 6 我国大数据软件市场规模



资料来源：沙利文研究，华安证券研究所

chatGPT 出世，加速了高质量大数据和高算力时代进程。相比传统 AI 算法，GPT 模型的区别在于通过**海量参数**，进一步提升了模型的精确度。

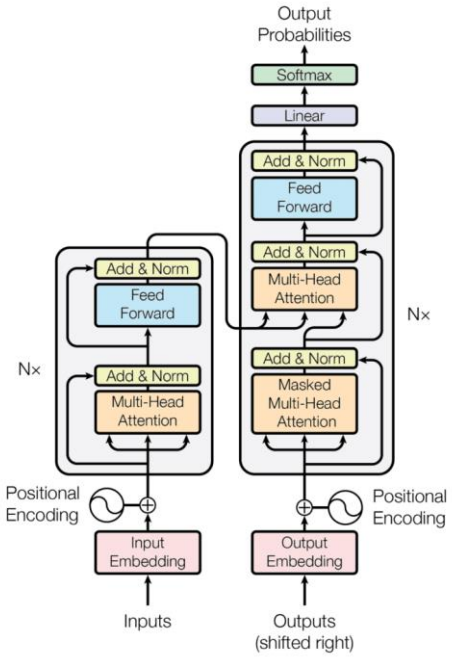
初代的 GPT 模型参数是 1.17 亿，而 GPT2 的模型有 15 亿个参数，参数增加了 10 倍之多。第三代的 GPT3 模型，参数达到了 1750 亿，是 GPT2 参数的 100 倍。正是由于参数的指数级提升，使得模型的使用效果大幅提升。**而此类参数上亿的模型，通常称之为“大模型”。**

GPT 模型基于 Transformer 架构，这是一种由谷歌的 Vaswani 等人于 2017 年引入的神经网络类型。Transformer 架构特别擅长对序列数据中的长距离依赖进行建模，这使其非常适合自然语言处理任务。

为了训练 GPT 模型，OpenAI 使用了来自互联网的大量文本数据，包括书籍、文章和网站。该模型使用一种称为无监督学习的技术进行训练，这意味着它学会了在没有人类监督的情况下预测文本序列中的下一个单词。

GPT 模型能够生成连贯和语法正确的文本，已被用于广泛的自然语言处理任务，包括语言翻译、文本补全和文本生成。

图表 7 transformer 模型工作流程



资料来源：machine learning mastery，华安证券研究所

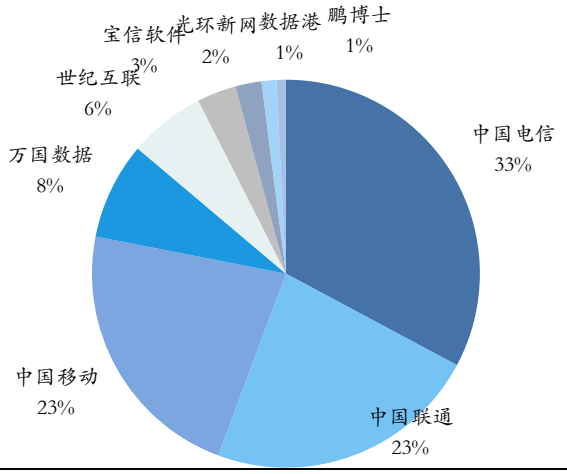
AI 及大模型带来高算力需求，即硬件建设需求。根据 lambdalabs 报导的数据，GPT3 若使用 V100 需要训练 355gpu 年，就是建立在理论数据下，以 V100 理论算力 28 TFLOPS 计算的（直接将 FP 32 的理论算力 14TFLOPS 乘以 2，以得到 FP16 的理论算力）。若使用 RTX8000，假设 15TFLOPS，将花费 665GPU 年 （资料来源：OpenAI's GPT-3 Language Model: A Technical Overview (lambdalabs.com)） 。由此计算的 GPT3 的训练算力，整体达到 3.14E23 FLOPS。若仍然以 V100 就算，若要将训练一次的周期降低至 1 周内，则**需要 2 万片** V100GPU。大量的 GPU 算力，意味着数据中心的大举建设。

1.2 大数据高算力，意味着安全市场增长

算力即数据中心，运营商加大支出带来市场爆发。以服务器插八张 GPU 来计算，两万片 GPU 的 AI 训练带来的服务器增量，即 1250 台服务器。而两万片 GPU，以 trendforce 预计约为 chatGPT3.5 所需数量，未来可能超过 3 万颗。考虑到国内各大互联网、IT 厂商相继投入大模型，**未来服务器、数据中心的建设已是高确定性事件**。

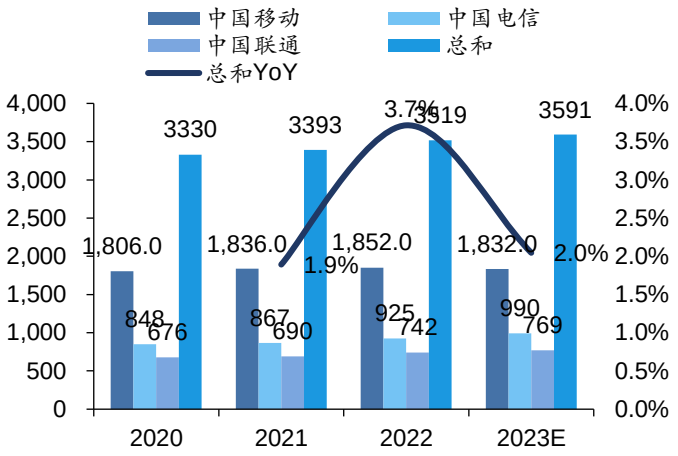
根据三大运营商 2022 年年报计划，1）中国移动：2023 年，对算力网络的资本开支预算提高到 452 亿元，同比增长近 35%。新增投产云服务器超过 24 万台、新增投产对外可用 IDC 机架超 4 万架；2）中国电信：2023 年在 IDC 方面将投资 95 亿元，实现 IDC 机架规模超过 56 万架；在算力投资 195 亿元，使算力总规模达到 6.2EFLOPS；3）中国联通：2023 年算力网络资本开支将达到 149 亿元，占总资本开支达 19.4%，同比增长超 20%。IDC 机架规模达到 39 万架。

图表 8 2021 年中国数据中心市场占比



资料来源：中国信通院，华安证券研究所

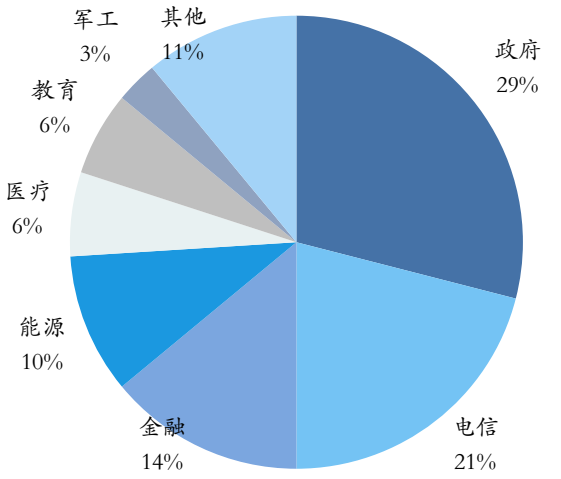
图表 9 三大运营商资本开支及增速（亿元）



资料来源：公司公告，华安证券研究所

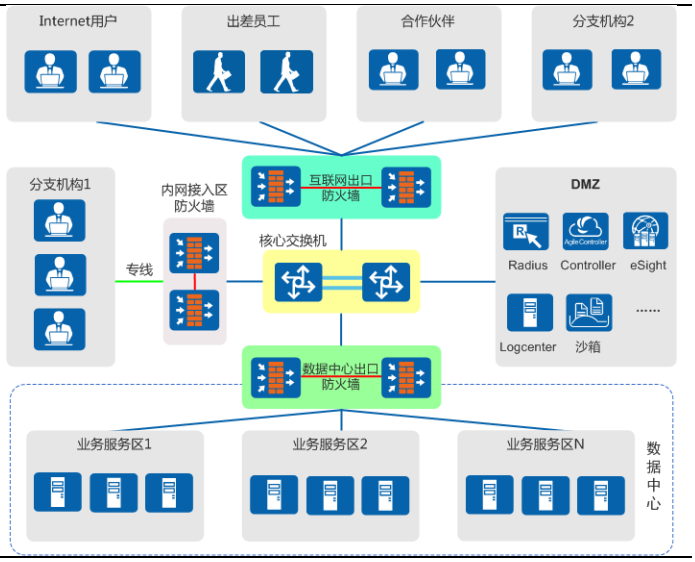
数据中心建设，存在内生网安需求。由于骨干网、云端数据中心其自身 1）边界访问安全需求；2）数据保护需求；3）运行状态检测运营需求，对于网络安全设备有天然需求，首要包括：1）防火墙、交换机、WAF、负载均衡、上网行为管理等网关类需求；2）漏洞扫描、IDS\IPS（即态势感知）、抗 DDoS 等传统抗攻击需求；3）SIEM、数据库审计、运维审计等运维检测类产品；4）vpn、邮件安全等租户需要的设备产品。因此，运营商也是网络安全传统的一大收入来源。此外，金融、互联网等存在自建数据中心需求的客户，其网安需求增长逻辑类似。因此，**我们认为，AI 乃至大模型时代，网安设备的硬需求为同向增长状态。**

图表 10 2020 年网络安全行业营收结构



资料来源：中国信通院，华安证券研究所

图表 11 华为数据中心组网架构中防火墙等设备



资料来源：华为，华安证券研究所

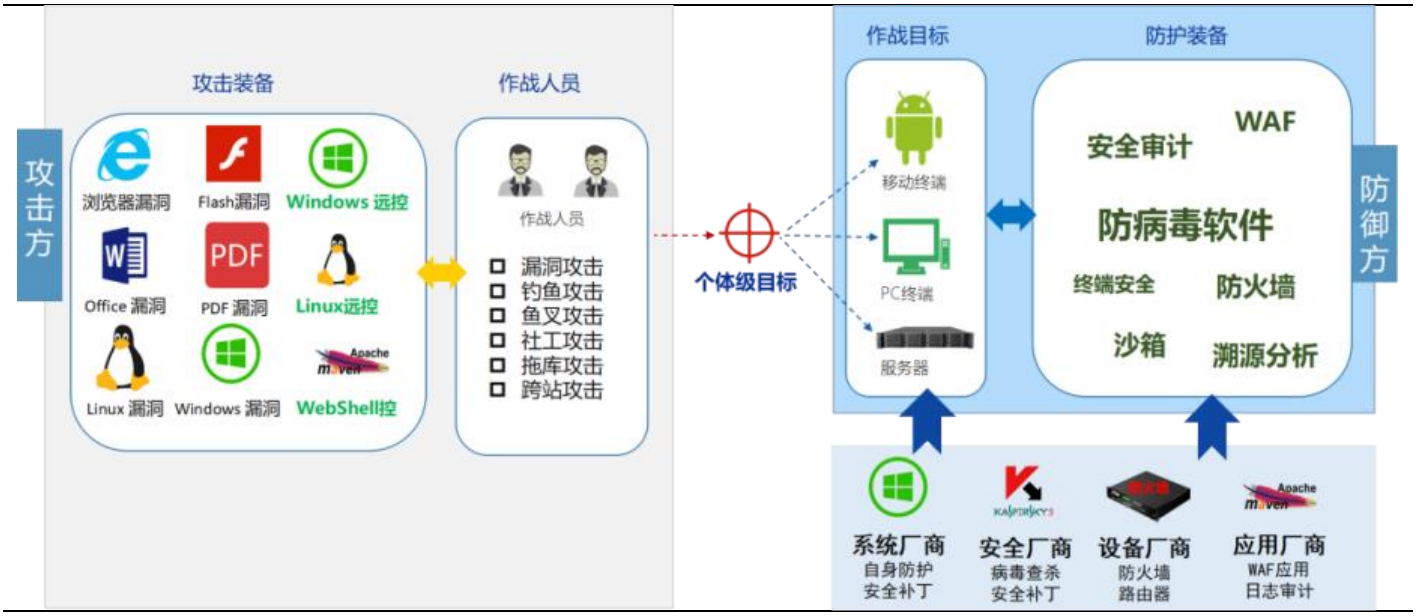
1.3 AI 加持攻击，带来危险增长“第二曲线”

AI 的存在，也赋能了网络攻击。网络安全乃至数据安全的本质是攻防，攻击者盗取破坏信息，防护者保护信息。由于防守者永远是被动，即使是态势感知也无法阻止最开始的破坏入侵， AI 带来的降本增效首先受益方是攻击者。根据 MIT Technology

Review 对于 300 个网安公司人员的采访数据，2021 年 60%的采访对象已经难以应对自动化的网络攻击，96%的人已经在开始遭受 AI 网络攻击，部分使用了 AI 进行防御。

近期发布的腾讯《2023 产业互联网安全十大趋势》也指出，chatGPT 类技术辅助写代码的能力大大**降低了攻击者的技术门槛**，而可以对于漏洞攻击、钓鱼攻击、鱼叉攻击等常用的攻击方式进行**快速上手和创新**。我们认为，**AI 的成长，会带来攻击量增长，网安的技术性需求会由于攻击事件的催化而得到释放**。

图表 12 网络空间单点攻击对抗态势



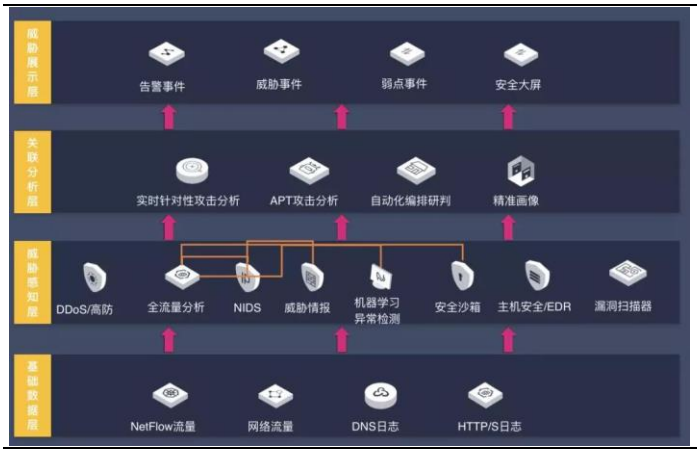
资料来源：安全内参，华安证券研究所

2 AI 解决方案，赋能网安厂商业务

AI 及大模型能力，与网安天然结合。网络安全的攻防，基础之一在于网络流量的分析识别，也包括了 dns 日志、HTTP/S 日志等数据。这些数据在网络上被探针感知到传送到安全厂商集成了 AI 能力的监测中心时，危险的探知识别以及随后的发送防御信号也随之进行。AI 大模型在学习、分析、识别乃至发送命令上相对于人类都有高速的优势，目前对于创新程度不高的攻击都具有较好的防护能力。因此，在近期国际争端中，网络安全大国也会对于盟友进行相应的 AI 类网络安全能力帮助，如 AI 监控运营商流量。

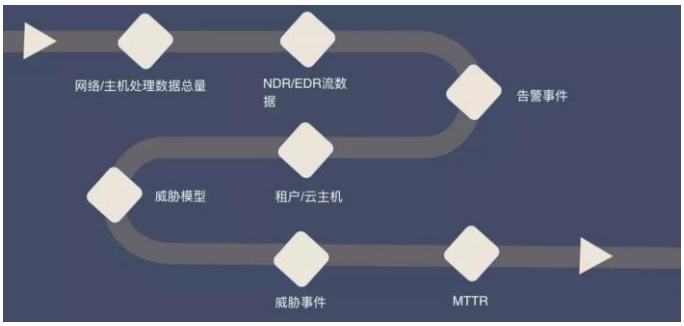
目前各网络安全厂商也将 AI 能力集成至自身平台中。

图表 13 网络安全预测架构



资料来源：京东科技开放平台，华安证券研究所

图表 14 网络安全感知架构



资料来源：京东科技开放平台，华安证券研究所

2.1 美亚柏科:AI 加持取证类产品

公司于 2017 年成立 AI 研发中心，2019 年针对深度合成技术成立专项研究团队，目前已有针对生成式视频图像的真伪识别鉴定的一体化装备产品。AI-3300"慧眼"视频图像鉴真工作站是一款以人工智能技术为核心的视频图像检验鉴定设备，配备了美亚柏科人工智能团队自主研发的核心 AI 智能检测引擎，支持当前绝大部分深伪视频图像篡改方法的检测，检测精度处于国内领先水平。公司将对各类 AIGC 内容的检测、AI 生成文本的检测技术及产品进行布局。

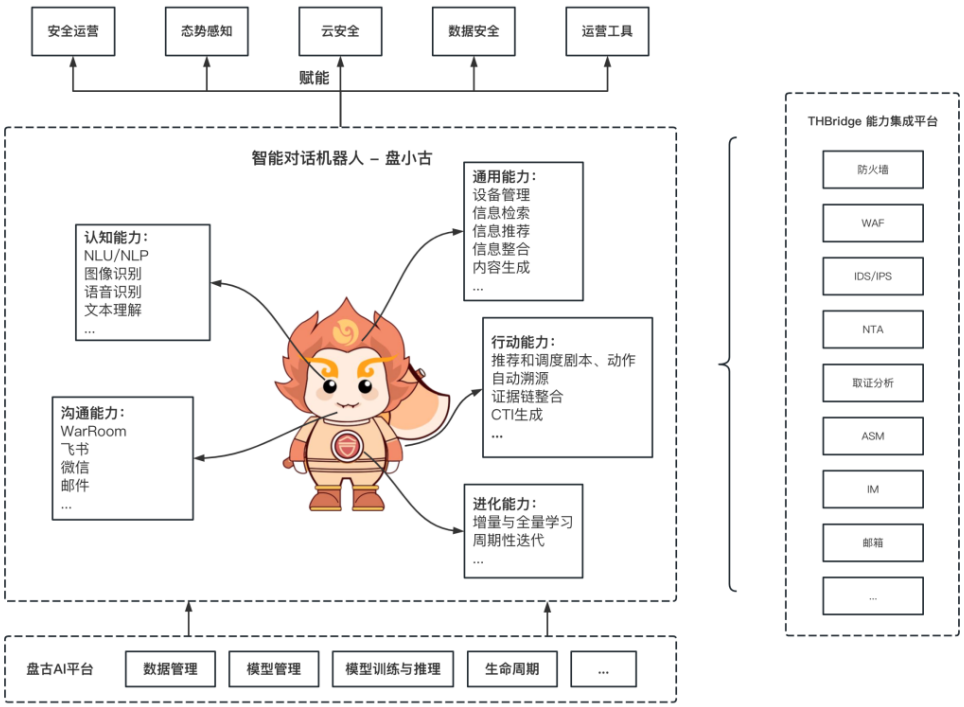
图表 15 美亚柏科 AI-3300"慧眼"

资料来源：美亚柏科官网，华安证券研究所

2.2 启明星辰:AI 助力研发运营

“盘小古”以 Chat 为窗口、以人工智能为核心、以安全分析处置自动化为手段，成为启明星辰新一代智能化安全运营支撑的关键角色，并能在安全运营过程中持续成长。启明星辰盘古人工智能平台作为安全运营的人工智能底座，为安全领域的人工智能应用提供了研发运营的一体化环境，能够实现基于 ModelOps 和 AIOps 的人工智能应用快速搭建、模型全生命周期管理和多重赋能，通过解耦数据治理、AI 建模、模型部署和模型赋能，将复杂的人工智能工程化应用落地问题分解到了多个专业领域中，从而大大简化人工智能应用的工程化难度，提高人工智能应用的开发和上线效率。

图表 16 启明星辰盘古人工智能平台



资料来源：启明星辰官网，华安证券研究所

2.3 奇安信:AI 赋能平台，研究类 ChatGPT 技术

奇安信网神移动环境感知系统，是零信任体系中重要的组件，是解决移动终端环境可信、可靠的重要工具。产品采用大数据分析和**人工智能**技术对用户、设备、环境属性进行感知和建模，实现设备风险和可信状态的持续度量；持续对移动终端进行数据抓取、风险监测、风险分析、风险评估、风险预警、风险处理等功能为一体的移动终端环境感知系统。近期，公司人工智能研究院负责人透露，公司正在基于 ChatGPT 相关技术和自身积累的海量安全知识和数据，训练奇安信专有的类 ChatGPT 安全大模型。

图表 17 奇安信态势感知平台

资料来源：奇安信官网，华安证券研究所

2.4 深信服:AI+云业务

深信服提出了 AIOps 智能运维一体化技术方案。该方案通过采集桌面云的日志、链路和指标数据，执行故障预测、异常检测、关联推理等算法，为用户提供智能分析服务。AIOps 的数据采集引擎基于 Golang 实现了插件化探针，支持采集 Windows、Linux、Docker 等多类指标数据，可以跨平台、多应用地进行动态采集，也支持 Prometheus 协议和导出，在数据采集上实现了高效和可扩展。

图表 18 深信服 AIOps 智能运维一体化技术方案

资料来源：深信服官网，华安证券研究所

2.5 山石网科:AI 融合传统网安单品

从 2015 年开始不断扩张产品线，山石网科都致力于去引入 AI 的能力。到今天，山石网科已经推出了八大具备 AI 能力的安全产品，除了最早的 iNGFW，还包括云沙箱、山石智·感、数据泄漏防御、WAF、StoneShield、iNGIPS、数据库审计与防护。在现有的几大 AI 产品和服务的基础上，此次山石网科还发布了基于 AI 的三大威胁检测能力：垃圾邮件防御服务，僵尸网络 C2 防御服务，IP 信誉库服务。

在落地 AI 安全的过程中，山石网科不断去提升正负反馈的机器学习能力，这也是 AI 的两大核心技术。山石网科安全防护线产品总监王中斌指出，例如在正反馈训练的异常行为分析方面，基于行为基线的学习可以提前更准确地发现威胁和异常且减少漏报。在负反馈训练方面，进行行为训练、行为聚类、行为归类与威胁判定。

图表 19 山石网科八大人工智能安全产品

资料来源：山石网科官网，华安证券研究所

2.6 中新赛克:AI 赋能态势感知

中新赛克工业互联网安全态势感知平台通过采集与深度解析工业互联网流量数据，获取工业资产的设备类型、固件版本、地理位置、工业云平台等关键信息。利用大数据分析技术，被动监测与主动扫描相结合，对工业互联网安全事件进行监测与预警，为相关政府监管部门提供全天候、多维度的工业互联网安全态势呈现。公司产品能力部分也依托于 NLP 能力。

图表 20 中新赛克工业互联网平台

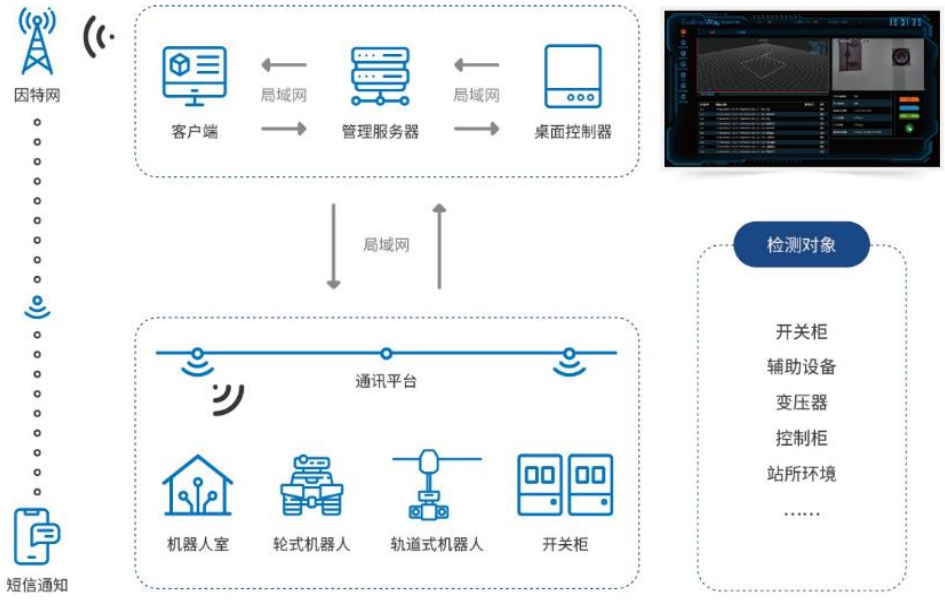
资料来源：中新赛克官网，华安证券研究所

2.7 恒为科技:从可视化到智能巡检

恒为科技凭借多年来在人工智能、边缘计算、嵌入式融合计算、视觉分析、多传感器融合等技术领域的积累，将大数据和 AI 深度学习等技术赋能机器人应用，通过建立“物-物、人-物”相联的网络提升用户业务运营效率，推出智能巡检解决方案，广泛应用于电力、能源、轨道交通、数据中心、智慧园区等领域。

恒为科技智能巡检系统以智能巡检机器人为核心，结合实时通信系统、供电系统、定制化智能巡检管理平台，全面替代人工实现远程巡查，在事故和特殊情况下可以实现特巡和定制性巡检任务，实现在线远程监测及异常情况报警。

图表 21 恒为科技智能巡检系统



资料来源：恒为科技官网，华安证券研究所

2.8 绿盟科技:AI 在隐私计算的实践

“绿盟隐私计算平台(NSFOCUS PCP)”，PCP 是绿盟科技在数据作为生产要素的数字经济时代下，推出的在数据合作过程中保障数据安全和用户隐私的产品。该平台兼容联邦学习(FL)、安全多方计算(MPC)等主流隐私保护技术，在保护数据本身不对外泄露的前提下，高效完成隐私应用场景，达到对数据“可用、不可见”的目的，实现数据价值的转化和释放。

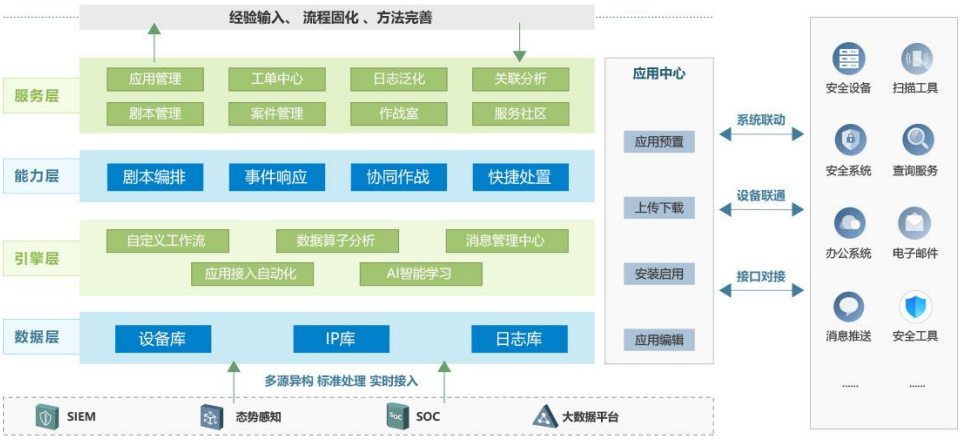
图表 22 绿盟隐私计算平台

资料来源：绿盟科技官网，华安证券研究所

2.9 安博通:AI 抓住安全运营痛点

公司平台策略可帮助企事业单位内部的安全运维团队，脱离低效耗时的纯人工操作，以安全响应和自动化编排技术，提高安全运维管理的效率，保证安全事件处置的及时性和准确性。将人、技术和流程有机地结合起来，形成标准统一、可重复、更高效的安全运营流程。

图表 23 网络安全智能运营与协同响应平台



资料来源：安博通官网，华安证券研究所

2.10 安恒信息：AI 加持取证类产品

AiLPHA 安全分析与管理平台（又称为：AiLPHA 大数据智能安全平台）是一款结合大数据技术和人工智能算法的安全运营系统。采用业界领先的大数据分析技术架构和

自研 AI 深度感知引擎，运用用户实体行为分析、安全编排与自动化响应、多维态势感知等技术为企业级用户提供全局安全态势感知能力， 保障其业务不间断稳定运行。 平台部署在用户侧， 通过威胁发现、智能研判和自动化响应处置的流程，提高安全运维工作效率，构建智能安全运营体系，实现安全运营的闭环管理，致力于让安全更智能，更简单。该产品已广泛应用于政府、金融、运营 商、公安、军工、电力能源、税务、工商、社保、交通、卫生、教育等各企事业单位。

图表 24 AiLPHA 安全分析与管理平台

资料来源：安恒信息官网，华安证券研究所

2.11 迪普科技:AI 算法融入态势感知

迪普科技先知威胁感知大数据平台借助 AI 算法构建更为高效精准的安全检测分析模型，极大地提升了平台的网络攻击识别、安全事件研判、安全事件处置等能力。先知威胁感知大数据平台 AI 识别引擎通过内置的 AI 识别引擎，并基于 XGBoost 的冰蝎 webshell 检测算法、基于机器学习的攻击者真实意图 URL 检测算法、基于语义分析的 Web 访问智能检测算法等大量的 AI 算法实现对攻击威胁的精准检测。一款帮助用户发现 APT 攻击、失陷主机、僵木蠕传播等安全威胁，实现精准溯源及应急处置的产品。

平台以安全大数据+AI 智能分析技术为核心，结合主/被动检测、威胁情报、UEBA、攻击行为建模、失陷主机检测等技术，实现安全事件可视化、全网威胁可视化、全网流量可视化、资产及脆弱性可视化等，帮助客户评估安全状态并决策处置。同时平台设计遵循 GBT-20984-2007 及等保 2.0 等相关要求，全面满足合规性需求。

图表 25 迪普科技态势感知平台优势

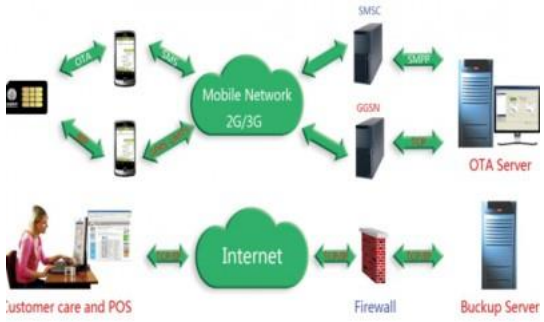
技术优势	功能价值
安全事件监控	支持对僵木蠕传播、漏洞利用、C&C 通道、APT、敏感信息泄漏等各类安全事件的聚合和管理，可基于告警制定进一步的处置策略，并生成黑客档案信息
安全威胁分析	支持多维度多场景建模，可从内部威胁、外部威胁、外联威胁等多个维度展开分析，具备攻击溯源能力，以关系图呈现并包含攻击链信息
威胁情报关联	支持海量威胁情报的获取，探针上报数据可与威胁情报实时关联，增强对高级威胁线索的发现能力
漏洞探测及验证	支持对资产漏洞的全面检测，并可基于模拟人工渗透技术进行漏洞验证，对漏洞的修复结果进行跟踪闭环
异常流量分析	支持对网络流量的常态监测能力，基于流量自学习和用户自定义模型，智能发现网络中异常流量
全网资产监控	支持主动扫描、流量镜像结合的方式进行资产识别，并支持自定义标签及权重设置，对在线资产进行精细化管理
安全态势呈现	支持全方位安全态势呈现能力，将用户业务及行业场景进行深度耦合，在网络安全宏观监管层面和微观运维层面实现双赢
联动处置	展示未处置威胁地址列表，可对威胁地址进行封禁、解封、忽略等处置动作
平台架构	分布式处理框架，支持平滑扩展；支持分布式部署，支持集中式管理，支持灵活组网
专用软硬件平台**	采用飞腾 CPU、盛科交换芯片的专用硬件平台，软件平台拥有麒麟内核使用授权

资料来源：迪普科技官网，华安证券研究所

2.12 东信和平：物联网融合 AI

东信和平 OTA 系统是一个基于 OTA 技术的多功能，多站点的用来验证 SIM 卡/USIM 卡应用配置的解决方案。OTA 系统包括 SIM 卡/ USIM 卡，OTA 的服务器和全套预装的应用、管理工具。移动用户只需要拥有一张 OTA 卡，在手机上进行简单操作，就可以按照个人喜好把网络所提供的各种业务菜单方便地下载到自己的 SIM 卡中，按自己的意愿定制具体业务。

图表 26 东信和平 OTA 系统



资料来源：东信和平官网，华安证券研究所

2.13 信安世纪:AI 加持取证类产品

信安移动安全管控平台(简称：MSMP)是一套基于移动化场景的移动安全跨平台解决方案。该平台以保护企业移动核心数据资产为核心，在提供移动设备管理（MDM)、移动应用管理（MAM)、移动内容管理（MCM）等基础移动终端管理能力的同时，通过移动安全桌面和移动数据防泄漏等移动终端安全技术，实现对移动终端应用和数据地隔离与保护，并通过移动安全接入技术实现端对端的应用级数据传输加密，最终为企业移动信息化提供一站式移动终端安全管理解决方案。

图表 27 信安移动安全管控平台特点

资料来源：信安世纪官网，华安证券研究所

2.14 电科网安:AI 分析文本数据

卫士通人工智能数据安全分析服务平台在智能文档处理的通用能力和 AI 核心能力方面均表现优异。在通用能力方面，该平台在信息抽取、表格文字识别、表格结构识别、版面分析、文档分类等文档处理能力均有较高的支持度。在 AI 核心能力方面，该平台在文本分类、实体识别、关系抽取、事件抽取、光学字符识别等指标上的准确率、召回率、F1 值总体较高。

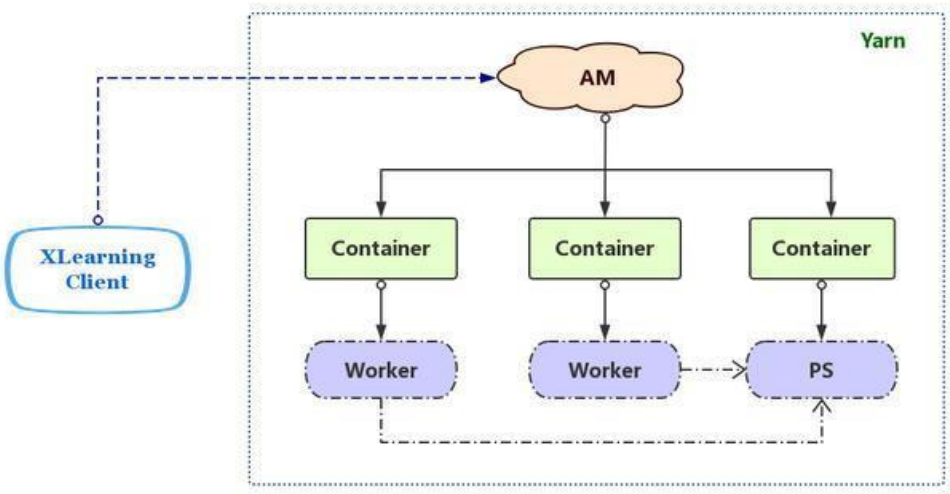
图表 28 卫士通人工智能数据安全分析服务平台

资料来源：电科网安官网，华安证券研究所

2.15 360:提供大数据深度学习平台

XLearning 平台将大数据与深度学习相融合，基于 Hadoop Yarn 完成了 TensorFlow、MXNet、Caffe、Theano、PyTorch、Keras、XGBoost 等常用深度学习框架的集成，是典型的“AIon Hadoop”的实现。XLearning 从今年 4 月份正式开发上线运行，经多次版本迭代更新，为各学习框架的使用者提供了统一、稳定的调度平台，实现了资源共享，极大的提高了资源利用率，并且具有良好的扩展性和兼容性。

图表 29 XLearning 平台



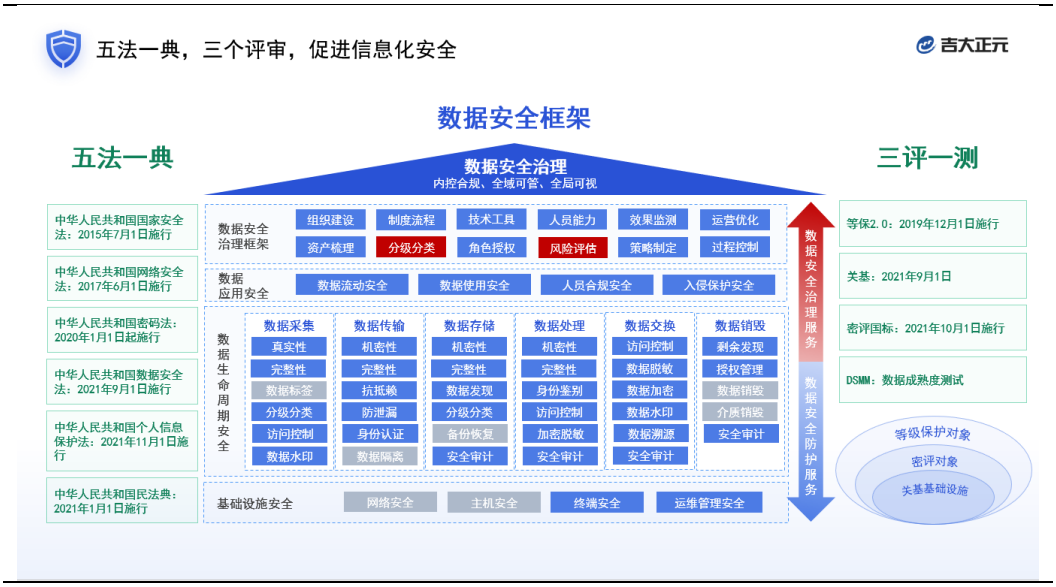
资料来源：360 官网，华安证券研究所

2.16 吉大正元:智能化能力集合至数据安全方案

数据安全方案包含基础设施安全、数据生命周期安全、数据应用安全和数据安全治理框架。吉大正元聚焦数据安全，以体系化、智能化和实战化的思路为指引，以大数据、人工智能、密码技术为支撑，构建面向政务、金融、能源等行业场景，覆盖数据采集、

传输、存储、处理、交换和销毁等数据全生命周期的安全产品和服务体系，从数据安全治理和数据安全防护服务，制定数据安全策略，对数据分级分类，从技术到产品、从策略到管理，提供完整的产品与服务支撑。

图表 30 吉大正元数据安全方案



资料来源：吉大正元官网，华安证券研究所

2.17 熙菱信息:安防图像 AI

熙菱信息以视频图像感知大数据为基础，以高维融合计算及 AI 智能分析技术为依托，推出时空大数据分析一站式解决方案——天启，涵盖了数据湖构建、大数据融合计算建模和大数据融合实战应用等不同层面的关键内容。这款面向警务研判的实战应用系统，使能公安智慧警务。通过全方面的体系架构，天启大数据平台实现从数据汇聚、数据清洗、存储、计算，到数据的碰撞、分析、研判、挖掘，最后到业务应用，形成一体化的统一、高效、便捷的公安大数据平台。

图表 31 时空大数据分析一站式解决方案——天启

资料来源：熙菱信息官网，华安证券研究所

3 投资建议

AI 赋能网络安全，从需求和供给改革行业生态

我们认为可关注以下标的：

1） 传统厂商，如**奇安信、深信服、启明星辰等。**

2） 密码类厂商，信安世纪、吉大正元、电科网安等

3） 数据要素类厂商，美亚柏科、熙菱信息等。

风险提示

1）技术研发突破不及预期；

2）政策支持不及预期；

3）下游需求不及预期。

分析师与研究助理简介

分析师：尹沿技，华安证券研究总监、研究所所长，兼 TMT 首席分析师，曾多次获得新财富、水晶球最佳分析师。

分析师：王奇珏，上海财经大学信息管理学士，上海财经大学资产评估硕士，7 年计算机行业研究经验，曾任职广发证券研究所，2022 年 6 月加入华安证券研究所。

联系人：张旭光，凯斯西储大学金融学硕士，主要覆盖 AI 及行业信息化，2021 年 8 月加入华安证券研究所。

重要声明

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，以勤勉的执业态度、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，本报告所采用的数据和信息均来自市场公开信息，本人对这些信息的准确性或完整性不做任何保证，也不保证所包含的信息和建议不会发生任何变更。报告中的信息和意见仅供参考。本人过去不曾与、现在不与、未来也将不会因本报告中的具体推荐意见或观点而直接或间接收任何形式的补偿，分析结论不受任何第三方的授意或影响，特此声明。

免责声明

投资评级说明

以本报告发布之日起 6 个月内，证券（或行业指数）相对于同期相关证券市场代表性指数的涨跌幅作为基准，A 股以沪深 300 指数为基准；新三板市场以三板成指（针对协议转让标的）或三板做市指数（针对做市转让标的）为基准；香港市场以恒生指数为基准；美国市场以纳斯达克指数或标普 500 指数为基准。定义如下：

行业评级体系

增持—未来 6 个月的投资收益率领先市场基准指数 5%以上；

中性—未来 6 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 个月的投资收益率落后市场基准指数 5%以上;

公司评级体系

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。