信达证券 CINDA SECURITIES

Research and Development Center

关注网安行业需求改善，看好 AI 带来的行业新机遇

—网络安全行业深度报告

2023 年 6 月 2 日

庞倩倩 计算机行业首席分析师
执业编号：S1500522110006
邮箱：
pangqianqian@cindasc.com

郑祥 计算机行业研究助理
邮箱：zhengxiang@cindasc.com

证券研究报告

行业研究

行业深度报告

计算机 行业

投资评级： 看好

上次评级： 看好

庞倩倩 计算机行业首席分析师

执业编号：S1500522110006

邮 箱：pangqianqian@cindasc.com

郑 祥 计算机行业研究助理

邮箱：zhengxiang@cindasc.com

相关研究

信达证券股份有限公司

CINDA SECURITIES CO.,LTD

北京市西城区闹市口大街9号院1号楼

邮编：100031

关注网安行业需求改善，看好AI带来的行业新机遇

2023 年 6 月 2 日

本期内容提要：

- **需求从网关类向内网数据、安全管理、安全服务类产品延伸。**目前国内信息安全市场上的主流安全产品还是以硬件形态呈现的网络边界层安全产品。随着政企上云，服务器等终端设备频繁交互，网络边界开始变得模糊，任何连接到数据中心的智能终端设备都可能带来潜在威胁。我们认为，单纯强调网络边界层防护已难以满足需求，用户对数据安全、安全管理、安全服务等需求或将快速增长。
- **国内网安市场：行业增速快，天花板高：**据 IDC 发布的《全球网络安全支出指南》，预计 2026 年中国网络安全 IT 支出规模将达到 318.6 亿美元，五年 CAGR 约为 21.2%，接近全球平均 CAGR 的两倍。
- **国内信息安全行业的下游客户以政府、电信、金融等关基领域客户为主，该类客户受政策驱动因素的影响相对较大。**据 IDC 预测，到 2026 年，政府、电信、金融三类客户在网安领域的支出将占国内网络安全总支出的 60%。随着《网络安全法》、《数据安全法》、《个人信息保护法》等法律及相关条例落地，政府、关键基础设施行业客户对网安重视度将进一步提高，行业投入有望持续加大。
- **由于用户日渐重视安全，对安全公司技术和品牌愈发看重，近年来行业的集中度逐渐向头部集中。**我们认为，头部公司整体具备研发、销售积累的优势不易被超越，且未来或将形成规模效应，头部效应有望进一步显现。若行业整体需求得到改善，头部公司有望充分受益。
- **人工智能利好网安行业的发展。**（1）人工智能对网安需求的刺激：若将人工智能运用于网络攻击，将降低网络攻击的门槛与成本，企业将遭受更频繁的网络攻击；同时，人工智能将带来许多新型威胁场景，如深度伪造。（2）若将人工智能赋能于网安产品，有助于提升安全工具使用效率、提高威胁监测准确度、降低安全运营成本。
- **2022 年网安公司整体业绩不佳，未来向上弹性较大。**受下游客户需求侧紧缩等因素影响，网安厂商 2022 年收入增速相较于 2020 年、2021 年明显放缓。同时，网安厂商维持高投入，导致盈利能力显著下降。2023 年是“十四五”规划的第三年，政府开支有望一定程度改善；2023 年也是党政信创向八大关键行业拓展的关键年。我们认为，随着政府及重点行业央国企加大投入力度，网安公司收入侧有望得到改善，叠加网安公司开始实施降本增效，未来两年网安企业业绩向上弹性较大。
- **建议关注：**安恒信息、深信服、启明星辰、绿盟科技、天融信、迪普科技、奇安信、山石网科、亚信安全、安博通、美亚柏科、三六零。
- **风险提示：（1）当前形势下公共财政压力或有所增大、不少下游领域景气度亦会受影响，因此下游客户投入力度是否会有改善仍需观察；（2）网安行业下游客户以政企、央国企为主，若相关政策推进不及预期，可能导致该类客户投入力度减弱；（3）若行业竞争加剧，可能导致行业内公司进行持续价格战，进而影响行业公司的盈利能力改善进度。**

目 录

一.网络安全行业需求变化 4
1.1 需求从网关类向内网数据、安全管理、安全服务类产品延伸 4
1.2 目前以硬件为主，未来软件和服务的规模有望进一步提升 5
二.国内网安市场：行业增速快，天花板高，网安厂商利润弹性高 7
2.1 国内网安市场：预计 2026 年规模达 318.6 亿美元，期间 CAGR 达 21.2% 7
2.2 目前行业竞争格局较为分散，后续有望逐渐向头部集中 7
三.网安行业下游客户以政府、央国企为主，该类客户受政策驱动影响较大 9
3.1 网安行业下游客户以政府、关基行业央国企为主 9
3.2 政府对信息安全重视程度显著提升 9
3.3 行业重要规范等保 2.0 有望带来投入增加 11
3.4 2022 年网安公司业绩普遍承压，未来两年利润弹性大 12
四.人工智能发展为网安行业带来新机遇 14
4.1 若将人工智能运用于网络攻击，将带来新型威胁场景 14
4.2 人工智能为安全防御赋能，将提升安全工具使用效率 14
4.3 AI 反诈催生新的安全需求 16
五.国内安全厂商对比分析 19
5.1 头部网安公司对比分析 19
5.2 头部网安公司盈利指标有望回归合理区间 23
六.投资建议 25
七.风险提示 26

表 目 录

表 1：近年来涉及网络安全行业的有关法律法规 10
表 2：等保 2.0 与等保 1.0 比的等级划分区别 11
表 3：头部网安公司对比：主要产品、下游客户、销售模式（2022 年数据） 20
表 4：部分网安公司主要财务指标（2022 年数据） 22
表 5：部分网安公司单季节收入占比 22
表 6：2022 年头部网安公司三费率情况 23
表 7：表 7：2019-2022 头部网安公司净利率与恒生电子等公司净利率对比 24

图 目 录

图 1：网络安全产品的主要类别 4
图 2：数据生命周期中各阶段对应的安全防护要求 4
图 3：安恒信息云安全产品矩阵 6
图 4：中国 IT 安全市场规模及规模预测（单位，百万美元） 7
图 5：中国网络安全行业集中度分析 8
图 6：2021 年中国网络安全主要企业市占率 8
图 7：中国网络安全市场行业占比预测（2026 年） 9
图 8：部分网安公司营收同比增长率 12
图 9：部分网安公司销售净利率 13
图 10：部分网安公司销售费用（亿元） 13
图 11：部分网安公司管理费用（亿元） 13
图 12：部分网安公司研发费用（亿元） 13
图 13：Microsoft Security Copilot 以机器速度和规模实现防御 15
图 14：深信服安全 GPT 演示界面 16
图 15：美亚柏科 AI-3300 慧眼视频图像鉴真工作站 17
图 16：美亚柏科 AIGC 内容检测平台 17
图 17：2022 年中国 UTM 防火墙硬件市场份额 19
图 18：2022 年中国统一威胁管理硬件市场份额 19
图 19：2022 年中国安全内容管理市场份额 19
图 20：2022 年中国入侵检测与防御硬件市场份额 19

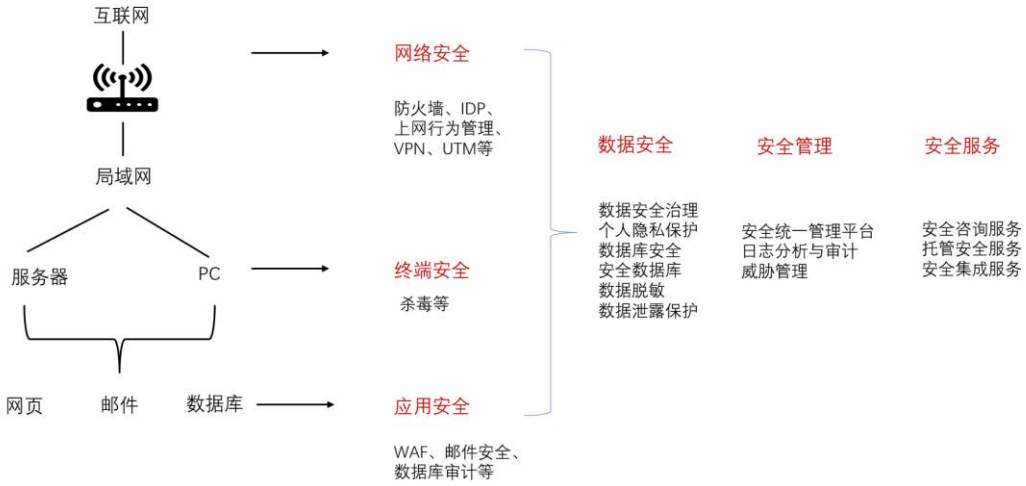
一. 网络安全行业需求变化

1.1 需求从网关类向内网数据、安全管理、安全服务类产品延伸

目前国内信息安全市场上的主流安全产品还是以硬件形态呈现的网络边界层安全产品。主要产品包括防火墙、统一威胁管理平台（UTM）、入侵检测和入侵防御（IDP）、虚拟专用网络（VPN）、安全内容管理（SCM）等。

随着政企上云，服务器等终端设备频繁交互，网络边界开始变得模糊，任何连接到数据中心的智能终端设备都可能带来潜在威胁。加之数据集中管控，安全攻击事件可能造成潜在危害大。我们认为，单纯强调网络边界层防护已难以满足需求，用户对数据安全、安全管理、安全服务等需求或将快速增长。

图1：网络安全产品的主要类别



资料来源：深圳网络与信息安全协会、IDC、信达证券研发中心

1.1.1 数据安全

数据安全是以数据为中心的安全体系。数据安全主要产品包括：数据安全治理、分类分级、个人隐私保护、数据库安全、数据脱敏等。同时，《数据安全法》、《个人信息保护法》等法律的出台也将驱动我国数据安全市场的发展。我们认为，数据安全相关的体系建设与规划、数据分类分级等咨询服务有望迎来黄金发展期。

数说安全研究院指出，2021 年我国数据安全市场规模约为 53 亿元，同比增长 30.7%。

图2：数据生命周期中各阶段对应的安全防护要求

资料来源：工信部，信达证券研发中心

1.1.2 安全服务

目前，网络安全服务市场主要由安全咨询服务、IT 安全教育与培训服务、托管安全服务、安全集成服务四个子市场构成。

安全咨询服务：属于专业服务的范畴，主要包括安全战略与规划、合规与审计等多个咨询类别；

IT 安全教育与培训服务：IT 安全教育与培训服务是一套教育活动和过程，主要包括企业级培训服务、教育认证、高校教育等子市场；

安全托管服务（MSS）：安全托管服务指服务提供商通过安全运营中心（SOC）进行全天候远程管理或监控的 IT 安全服务。目前，除驻场类的安全服务外，远程托管服务效率更高、成本更低，倍受中小企业青睐。未来，“驻场+远程”的云地结合模式有望成为主流。2021 年，我国托管安全服务市场规模较 2020 年实现了 61.2%的同比增长；

安全集成服务：安全集成服务指服务提供商通过规划、设计、实施、项目管理四个步骤形成完整安全解决方案的服务，其涉及系统和应用程序的定制化开发、集成企业打包的安全硬件、软件服务等；

据 IDC 报告显示，2021 年中国 IT 安全服务市场厂商整体收入约 28.61 亿美元（约合 184.6 亿元人民币），厂商收入规模较 2020 年同比增长 41.7%。

1.2 目前以硬件为主，未来软件和服务的规模有望进一步提升

从产品的形态来看，网络安全产品可分为硬件、软件、服务三大类。目前，国内网络安全的主要产品仍以硬件为主。根据 IDC 数据显示，2020 年，安全硬件在中国整体网络安全支出中仍占据主导地位，占比高达 47.2%；安全软件支出占比为 20.8%，安全服务支出占比为 32%。

看未来发展趋势，伴随云计算的快速发展，我国网络安全市场的软件化趋势在不断增强。据 IDC 预测，2021-2026 年期间，**安全软件市场规模将以 25%的复合增速快速增长**，安全软件子市场中的信息和数据安全软件（Information and Data Security Software），网络安全软件（Network Security Software），安全分析、情报、响应和编排（SAIRO）有望成为高速增

长的主要技术领域，其中信息和数据安全软件作为软件最大的子市场，将以 29.9%的五年 CAGR 引领软件市场增长；**安全硬件市场规模将保持 17.0%的复合增速；安全服务市场将保持 21.6%的复合增速**，其中托管安全服务（MSS）将达到 34.0%的五年复合增速。据 IDC 预测，2026 年安全软件市场将占国内网络安全市场总支出的 40%。

订阅模式的安全云服务的占比提升是趋势。相较于传统一次性收费的方式，订阅模式通常采取按一定时间收费的模式(通常按每月/每年)。在订阅模式下，客户可减少一次性高额付费，取而代之的是较为温和的平均支出；相应的，对于厂商来说，有助于企业改善现金流、提升客户粘性。网安厂商都在尽可能多的提供 SaaS 化的安全服务，以安恒信息为例，安恒信息基于云安全，为客户提供包括云 Web 应用防火墙、云主机安全、云堡垒机、云网站检测、云漏洞扫描等 SaaS 订阅服务。

图3：安恒信息云安全产品矩阵

资料来源：安恒信息官网，信达证券研发中心

我们认为，随着虚拟化、云化理念的渗透，客户未来安全软件及服务的占比有望持续提升；同时，随着安全厂商 SaaS 化服务能力的增强，订阅模式收入有望增长。相较于传统以硬件销售为主的业务模式，软件化、服务化、订阅化的业务模式有望改善安全厂商的现金流及毛利率。

二. 国内网安市场：行业增速快，天花板高，网安厂商利润弹性高

2.1 国内网安市场：预计 2026 年规模达 318.6 亿美元，期间 CAGR 达 21.2%

中国网络安全市场增速持续领跑全球，行业增速快，且天花板高。据 IDC 发布的《全球网络安全支出指南》，2021 年全球网络安全 IT 总投资规模为 1687.7 亿美元，并有望在 2026 年增至 2875.7 亿美元，五年 CAGR 为 11.3%。聚焦中国市场，随着《网络安全法》、《数据安全法》、《个人信息保护法》等法律法规悉数落地、《数据出境安全评估办法》、《网络安全审查办法》等条例颁布实施，我国网络安全法律法规体系化、纵深化态势明显，叠加数字化需求攀升，网络安全市场持续扩大，2026 年中国网络安全 IT 支出规模将达到 318.6 亿美元，全球占比约为 11.1%，五年 CAGR 约为 21.2%，接近全球平均 CAGR 的两倍。

图4：中国IT安全市场规模及规模预测（单位，百万美元）

资料来源：IDC 中国，信达证券研发中心

2.2 目前行业竞争格局较为分散，后续有望逐渐向头部集中

整体来看，目前网安行业竞争格局仍较为分散，我们认为，主要原因是：1.网安产品类型较多，产品线复杂；2.从下游客户来看，各行业客户都有网安需求，客户市场较为分散。不过，从趋势来看，近几年集中度有所提升。根据 CCIA 统计，2021 年，我国网络安全市场 CR1/CR4/CR8 分别为 9.5%/28.07%/43.96%，与前几年相比，行业集中度呈逐渐上升势头，形成低集中寡占型格局。我们认为，**未来我国网安市场集中度或将持续向头部靠拢，主要原因有以下几点：**

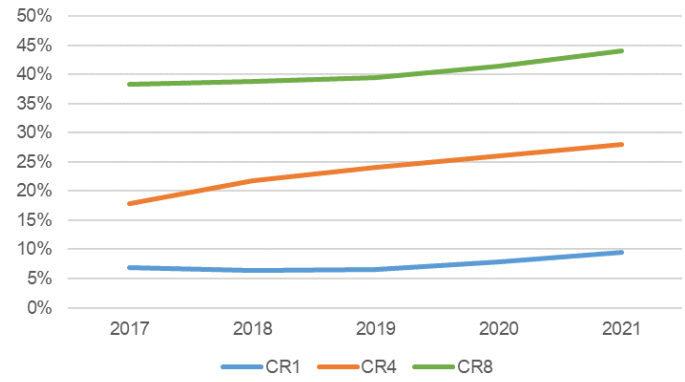
（1）研发体系壁垒：网安行业的技术积累是通解决各种攻击手段不断积累而来的，过去的攻击手段还会再现，所以相应的技术积累是有效积累。

在网安行业能看到很多公司基于新的技术创新生存，但是很难成长，原因就在于这些公司需要把以前的技术点补齐，还需要投入大量人员精力做产品研发，需要时间以根据实际使用反馈进行持续调优。反过来，这些就是头部公司研发上的壁垒。

（2）解决方案壁垒：我国当前的网安市场还是以硬件为主，主要集中在网络边界层的防护上，随着攻击的日益复杂以及用户对安全的重视程度日益提升，以往仅购买点状的安全产品已经难以满足用户需求，需要公司形成一整套智能、全面的安全防护方案。客户会愈加看重安全厂商的综合技术实力、解决各种安全问题的能力。相比尾部公司，头部公司在提供全套解决方案的能力上具有一定竞争优势。

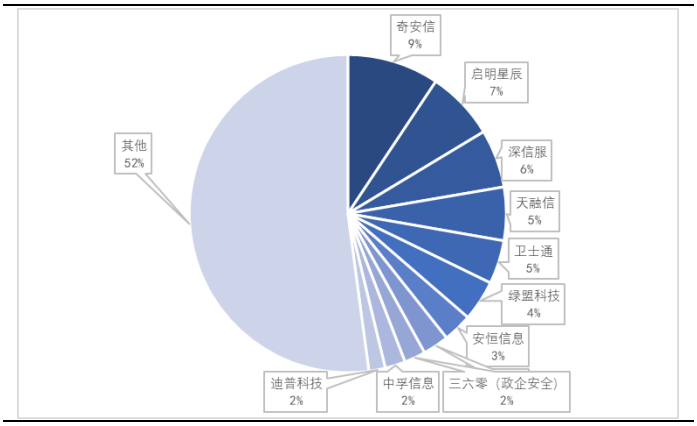
（3）销售渠道壁垒：网安行业的下游客户以政府或 B 端客户为主，需要通过直销或者分销渠道触及客户，渠道的建立需要时间。

图5：中国网络安全行业集中度分析



资料来源：CCIA 网安产业联盟，信达证券研发中心

图6：2021年中国网络安全主要企业市占率



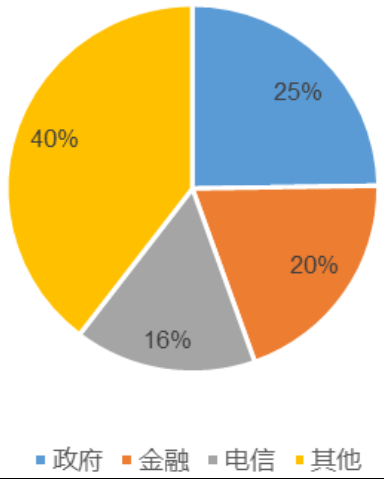
资料来源：CCIA 网安产业联盟，信达证券研发中心

三. 网安行业下游客户以政府、央国企为主，该类客户受政策驱动影响较大

3.1 网安行业下游客户以政府、关基行业央国企为主

从下游客户分布来看，据 IDC 预测，中国网络安全终端行业客户结构相对稳定，其中政府、金融和电信行业占比最大；预计到 2026 年，三者合计支出规模将超 192.2 亿美元，占比超中国网络安全总支出的 60%。**我们认为，中国网安行业客户主要分布在政府、金融、电信等关键领域，该类型客户受政策驱动因素影响相对较大。近年来，国家对于网络安全重视程度显著提升，行业整体投入有望逐渐加大。**

图7：中国网络安全市场行业占比预测（2026年）



资料来源：IDC 中国、信达证券研发中心

3.2 政府对信息安全重视程度显著提升

近年来，政府对信息安全的重视程度、战略定位大幅提升。先后于 2017 年 6 月实施《网络安全法》（首次立法）、于 2017 年 7 月发布《关键信息基础设施安全保护条例》，于 2019 年 5 月发布《信息安全技术网络安全等级保护基本要求》（等保 2.0）。未来几年，由于《网络安全法》及相关法律法规落地、等保 2.0 的实施，客户对安全愈加重视，行业投入有望持续加大。主要体现在：

- 《中央企业负责人经营业绩考核办法》于19年4月1日实施，将网络安全纳入央企负责人考核内容，可以理解成安全责任从信息部主任提升到央企一把手，重视程度提升会带来相关投入的增加。
- 等保 2.0 于 19 年 12 月 1 日实施，有望带来较大的整改投入，行业景气度有望进一步提升，头部公司业绩提速确定性较强；
- 《关键信息基础设施安全保护条例》于2021年7月开始实施，该条例明晰了关键信息基础设施的定义，明确了保护工作部门的职责，强化了运营者的安全管理主体责任，规定了国家保障和促进措施，确立了监督管理体制。该条例是对《网络安全法》确立的关键信息基础设施安全保护制度的细化完善，有助于构建多方尽责，共同协作的关键信息基础设施安全防护体系，更好地应对网络安全风险挑战。

- 《中华人民共和国数据安全法》于2021年9月开始实施，该法律规定，开展数据活动，应当遵守法律、法规、尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，旅行数据安全保护义务，承担社会责任，不得危害国家安全、公共利益，不得损害个人、组织的合法权益。该法律为我国数据安全领域的基础性法律，其完善了国家数据安全工作体制机制，标志着我国在数据安全领域有法可依，为各行业数据安全提供监管依据。

表 1：近年来涉及网络安全行业的有关法律法规

发布时间	文件名称	发布部门	重点内容
2016.11	《中华人民共和国网络安全法》	全国人大常委会	我国网络安全领域的基本大法，适应了我国网络安全工作新形势、新任务，落实中央决策部署、保障网络安全。
2021.06	《中华人民共和国数据安全法》	全国人大常委会	我国数据安全领域的基础性法律，其完善了国家数据安全工作体制机制，标志着我国在数据安全领域有法可依，为各行业数据安全提供监管依据。
2021.08	《中华人民共和国个人信息保护法》	全国人大常委会	对自然人关于个人信息的权利、个人信息处理者对于个人信息的义务、相关部门对于个人信息的保护职责个人信息处理具体要求、个人信息跨境、法律责任等做出了明确和可操作的规定。
2021.07	《关键信息基础设施安全保护条例》	国务院	《条例》是对《网络安全法》确立的关键信息基础设施安全保护制度的细化完善，有助干构建多方尽责，共同协作的关键信息基础设施安全防护体系，更好地应对网络安全风险挑战。
2021.11	《网络数据安全管理条例（征求意见稿）》	网信办	规定了国家建立数据分类分级保护制度。明确了在中华人民共和国境内利用网络开展数据处理活动的一般规定、个人信息保护、重要数据安全、数据跨境安全管理、互联网平台运营者义务、监督管理

			及法律责任等安全管理要求。
2022.7	《数据出境安全评估办法》	网信办	指出数据出境安全评估坚持事前评估和持续监督相结合，风险自评估与安全评估相结合，防范数据出境安全风险，保障数据依法有序自由流动。
2023.02	《个人信息出境标准合同办法》	国家互联网信息办公室	旨在保护个人信息权益，规范个人信息出境活动。

资料来源：国务院、中国人大网、网信办、信达证券研发中心

3.3 行业重要规范等保 2.0 有望带来投入增加

相比等保1.0（GB/T 22239-2008《信息安全技术 信息系统安全等级保护基本要求》），等保2.0中高标准的覆盖范围更广、增加对新场景的安全要求、本身法规性更强，下游客户或将加大投入：

（1）等保2.0针对新技术新增扩展要求

等保2.0在等保1.0资产防护的基础上，就云计算、物联网、移动互联网和工业控制系统提出安全防护要求。可以理解成监管对象从传统的政府、事业单位、国企，延伸到“有数据的民企”，我们预计会带来可观市场。扩展要求就新技术领域提出针对性要求，深信服、启明星辰等领先公司积极布局云安全、移动互联网安全及工控安全领域，并与阿里、腾讯等云计算厂商就云安全开展技术合作。预计深信服、启明星辰等公司有望受益于等保2.0。

（2）等保2.0三级对象覆盖范围增加，三级安全防范要求显著多于二级

等保2.0根据等级保护对象受到破坏时所侵害的客体和对客体造成侵害的程度，将信息系统的安全保护等级分为5个等级。相比等保1.0，等保2.0三级覆盖范围大幅扩展，“受到破坏会对相关公民、法人和其他组织的合法权益造成特别严重损害的重要网络”从二级上升到三级对象。相比二级对象，等保2.0对三级监管对象有定期开展测评的要求，被监管对象的重视程度更高，会有更多安全投入。

表 2：等保 2.0 与等保 1.0 比的等级划分区别

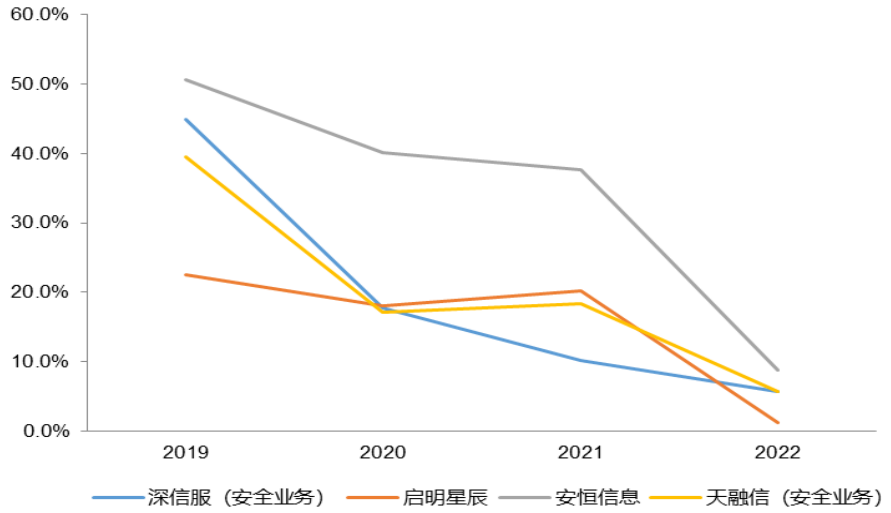
受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	**第二级变为第三级**
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

资料来源：全国信息安全标准化技术委员会、网络安全等级保护网、信达证券研发中心

3.4 2022 年网安公司业绩普遍承压，未来两年利润弹性大

从头部公司的收入增速来看，2022 年收入端短期承压。网安厂商 2022 年收入增速相较于 2020 年、2021 年明显放缓。

图8：部分网安公司营收同比增长率



资料来源：IFIND、信达证券研发中心

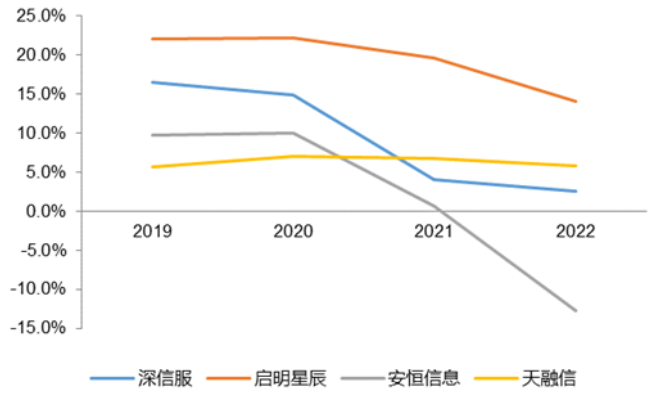
2022 年大部分网安公司收入与利润均表现不佳的主要原因：

1.受外部环境不佳致使下游客户需求侧紧缩、客户短期内采购需求减少等原因，网安公司收入侧增速放缓。

2.同时，网安厂商维持高投入，导致盈利能力显著下降。

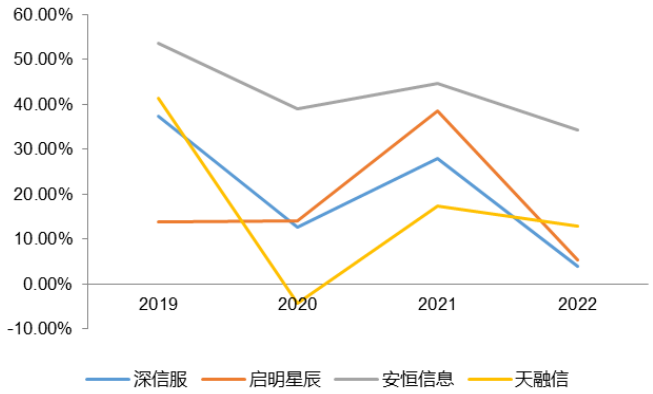
分析深信服、启明星辰、安恒信息等网络安全龙头公司的费用投入，可以看到大部分网安公司于 2022 年开始实施降本增效，进入控费周期。**展望 2023 年，2023 年是“十四五”规划的第三年，政府开支有望一定程度改善；2023 年也是党政信创向八大关键行业拓展的关键年。我们认为，随着政府及重点行业央国企加大投入力度，网安公司收入侧有望得到改善，叠加网安公司开始实施降本增效，未来两年网安企业业绩向上弹性较大。**

图9：部分网安公司销售净利率



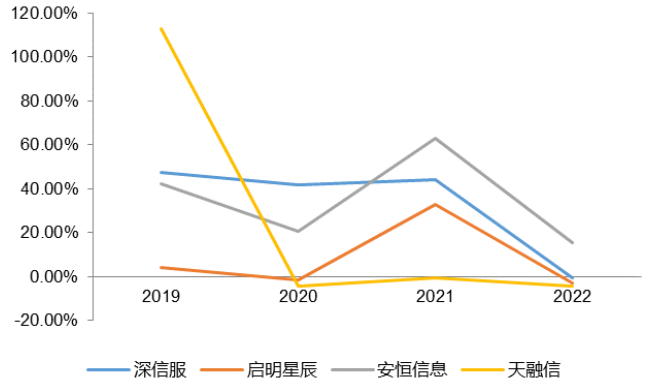
资料来源：IFIND，信达证券研发中心

图10：部分网安公司销售费用增速



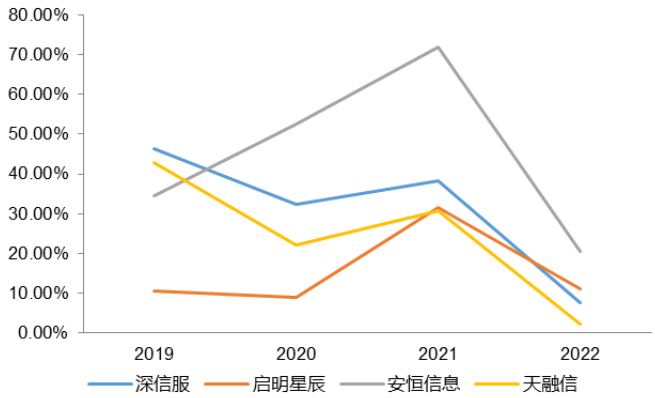
资料来源：IFIND，信达证券研发中心

图11：部分网安公司管理费用增速



资料来源：IFIND，信达证券研发中心

图12：部分网安公司研发费用增速



资料来源：IFIND，信达证券研发中心

四. 人工智能发展为网安行业带来新机遇

生成式人工智能（AIGC）是指基于算法、模型、规则生成文本、图片、声音、视频、代码等内容的技术，作为一种前沿技术，该机器学习方法从其数据中学习内容或对象，并通过原始数据生成全新、原创的实际工件。

人工智能对网安行业的影响在于，一方面，若将人工智能应用于网络攻击，将降低网络攻击的门槛、增加网络威胁的数量，同时提升网络攻击的复杂程度，客户对网络安全的需求也将随之增加。另一方面，若将人工智能赋能于网络安全，有助于提升安全工具的使用效率以及安全监测的准确率。

4.1 若将人工智能运用于网络攻击，将带来新型威胁场景

就网络安全领域而言，人工智能的恶意使用可以创建更复杂的攻击，比如用于恶意代码威胁、DDoS 攻击、生成虚假数据、恶意软件威胁等。

（1）自主化、规模化的拒绝服务攻击威胁：人工智能技术扩大了恶意软件同时攻击多个目标的能力，并且利用自我学习能力，以前所未有的规模对脆弱系统实施自主攻击，发动大规模 DDoS 攻击并造成网络阻塞和瘫痪。

（2）智能化、高仿真的社会工程学攻击威胁：随着人工智能的发展，社会工程学攻击逐渐呈现智能化、高仿真的特征。人工智能使攻击者利用社交媒体等个人隐私数据，自动学习并构造虚假信息，让受攻击目标在无意间上钩。

（3）智能化、精准化的恶意代码威胁：攻击者倾向于针对恶意代码攻击链的各个攻击环节进行赋能，增强攻击的精准性，提升攻击的效率与成功率，突破网络安全防护体系。

（4）自主化、复杂化的恶意软件威胁：基于人工智能的自适应恶意软件将具有一种态势感知技术，可以识别网络空间环境，并对下一步做出慎重的决定，它搜索目标、识别目标、选择渗透路线并自动避开智能检测。

我们认为，随着人工智能技术的突飞猛进，未来或将带来数量更多、模式更复杂的网络攻击，因此，网络安全的需求有望随着各类技术的发展而增长，技术发展的越快，网络安全需求增长的越快。

4.2 人工智能为安全防御赋能，将提升安全工具使用效率

人工智能作为一把“双刃剑”，若将其应用于安全防御领域，有助于提升安全运营效率、反制其带来的不良影响，通过“魔法”打败“魔法”。

（1）Microsoft Security Copilot

美国微软公司于 2023 年 3 月发布其新一代安全产品 Microsoft Security Copilot。Microsoft Security Copilot 将大语言模型（LLM）于微软专用的安全模型结合，成为一款让安全人员能够以 AI 的速度和规模做出相应的安全产品。该产品具有持续增长的安全技能，并获得由微软独特的全球威胁情报和每天超过 65 万亿个信号所提供的信息支持。通过 Security Copilot，使用者将：

a.简化工作，提升效率

安全注重时效性，往往需要在短时间内做出相应。借助 Security Copilot，安全人员可以在几分钟内响应安全事件，无需像过去一样花费数小时或数天。

b.提前发现网络安全威胁

网络安全攻击者往往会隐匿在各种噪音（Noise）后面，通过 Security Copilot，安全人员可以发现那些原本可能未被发现的恶意行为和威胁。

c.缓解专业人才紧缺的问题

据微软预测，全球安全领域约有 340 万个职位空缺，而专业的安全运营人员需要大量的成本投入。Security Copilot 能够回答与安全相关的问题，提高安全人员的技能。同时，Security Copilot 将不断从用户交互中学习，适应企业偏好，并就最佳行动方案向安全人员提供建议，以实现更安全的结果。

图13：Microsoft Security Copilot以机器速度和规模实现防御

资料来源：微软官网，信达证券研发中心

（2）深信服安全 GPT

深信服于 2023 年 5 月 18 日举行产品发布会，发布深信服安全 GPT。该产品为安全行业垂直领域大模型，且不依赖其他开源模型，由深信服自主训练，并部署于深信服托管云，实现完全自主可控。

深信服安全 GPT 基于“大模型算法+威胁情报+安全知识”训练而成，目前可应用于高级威胁检测、安全监测调查、热门漏洞排查等场景。

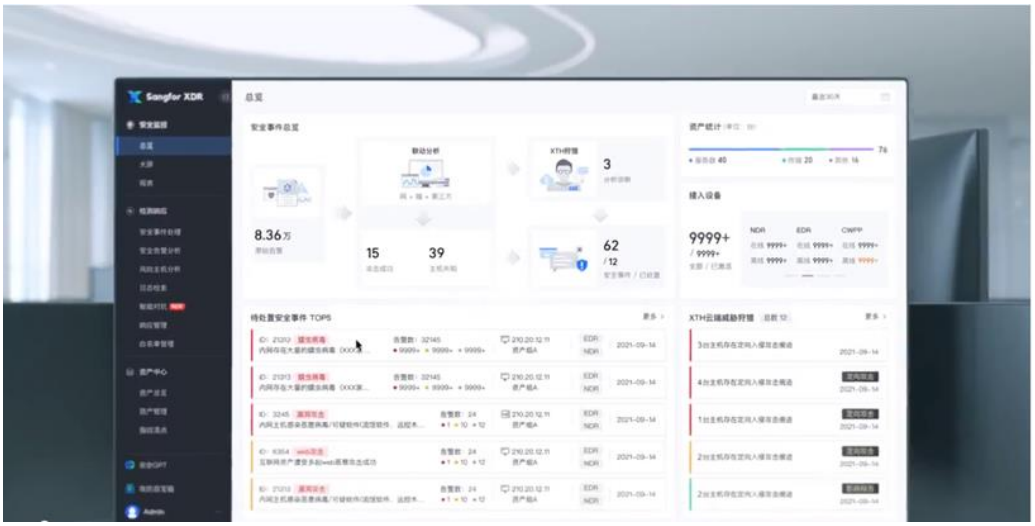
高级威胁检测场景：目前，已经出现攻击者利用 AI 大模型快速发动攻击，经测试，主流传统安全产品难以识别该类攻击。深信服 XDR 通过安全 GPT 技术，可以直接在安全事件页面，精准识别出利用 AI 大模型生成的攻击告警，并形成近乎一致的攻击 Payload。通过使用 5kw 样本集、500w 混淆类的攻击手法，将安全 GPT 的能力和传统产品进行对比，检测率上升至 95.7%，误报率下降至 4.3%。经过公司测试，安全 GPT 对安全攻击的理解已经达到 5 年从业经验安全专家的水平。

安全监测调查场景：当前大部分传统产品对安全攻击的理解都是初级的，但安全 GPT 能够图文显示监测结果，在海量信息中筛选有价值的报警信息，解读复杂的数据包内容，确定具体的风险以及事件受害者资产的责任人，并提供攻击者信息、攻击意图，给出解决方案。在过去，需要花费 3-6 个小时才能完成检测任务。资产定位、影响面排查、查询 CMDB（配置

管理数据库）、手动关联数据等流程需要耗费大量时间。现在，使用安全 GPT 只需要进行几次简单对话，花费 5-10 分钟即可完成同样任务，实现了生产力的飞跃。

热门漏洞排查场景：进行漏洞排查，需要知道其原理和目的，安全 GPT 能显示 CVSS 评分、漏洞潜在威胁、并且显示过去被攻击的次数，详细给出风险资产名称，并以表格形式输出，本来需要进行多步骤才能查询到的结果，现在通过安全 GPT 可以在较短时间内完成。

图14：深信服安全GPT演示界面



资料来源：深信服官微视频号，信达证券研发中心

（3）除安全垂直领域大模型外，国内网安厂商也在积极布局人工智能与网络安全结合的相关技术。以启明星辰为例，公司针对 LiveAction 的加密分析（Cryptanalysis）技术展开研究，围绕采用加密的 DNS 隧道、HTTP 隧道及 HTTPS 隧道通信的攻击流量，设计出高效的 AI 检测技术，并在 NFT 及 TAR 等产品中实现落地应用；除此之外，基于 AI 赋能的 AIOps 平台，启明星辰自主研发的人工智能安全建模和赋能平台，将 AIOps 自动化运营的能力加持到 AI 安全建模的全过程中，全面提升数据获取、数据处理、算法配置、模型训练、模型部署等步骤的效率，让 AI 检测分析模型更加触手可及。

4.3 AI 反诈催生新的安全需求

4.3.1 深度伪造技术带来的安全威胁

深度合成和生成式 AI 技术作为人工智能领域的创新应用技术，因其具备应用门槛较低、娱乐属性较强、应用场景丰富等特征而备受关注。随着深度合成和生成式 AI 技术逐渐开放开源，相关产品和服务增多。通过深度合成和生成式 AI 技术伪造文本、音频、视频，进行诈骗、勒索、诽谤等违法犯罪的行为已屡见不鲜。据哈尔滨网警官方百家号报道，2021 年 6 月，某位受害人遭受欺诈，诈骗人员不仅拦截了受害人的手机验证码，还攻破了银行人脸识别系统，在受害者没有参与操作的情况下，远程 6 次“扫脸”验证成功。无独有偶，据包头市公安局官微报道，2023 年 4 月，福州市某科技公司法人郭先生遭受 AI 诈骗，诈骗人员利用 AI 换脸技术，通过微信视频的方式伪装受害人的好友，并对其实施诈骗，涉案金额高达 430 万元。

4.3.2 针对深度伪造与生成式 AI 的应对措施

美亚柏科作为国内电子数据取证龙头，公司 2017 年就成立了 AI 研发中心，相关技术布局较早，为了应对人工智能可能带来的安全问题，公司于 2019 年专门针对深度合成等技术成立了专项研究团队。通过对深度合成和生成式 AI 技术的深入研究，美亚柏科推出针对视频图像检测鉴定的一体化装备“AI-3300 慧眼视频图像鉴真工作站”，以及针对人工智能（如 ChatGPT）生成文本内容的检测工具“AIGC 内容检测平台”。

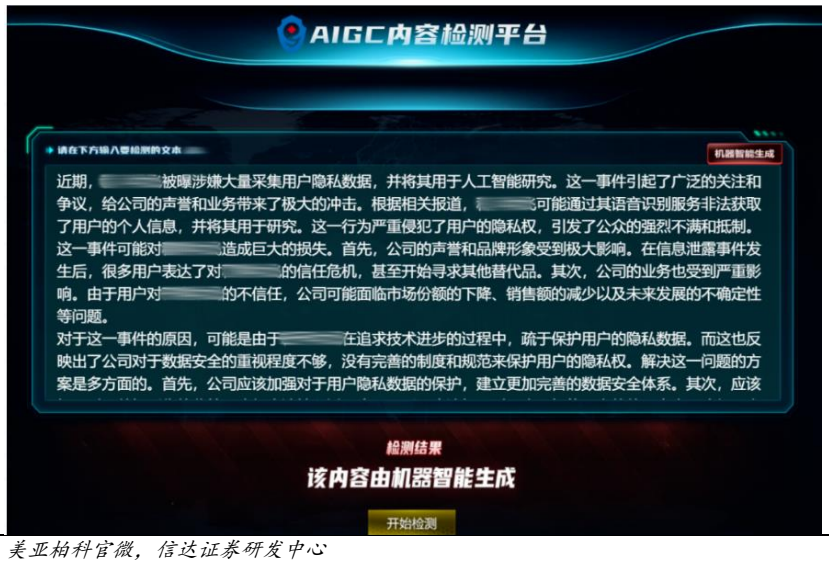
AI-3300"慧眼"视频图像鉴真工作站是一款以人工智能技术为核心的视频图像检验鉴定设备，配备了美亚柏科人工智能团队自主研发的核心 AI 智能检测引擎，支持当前绝大部分深伪视频图像篡改方法的检测，检测精度处于国内领先水平。同时，“慧眼”涵盖了 40 余种视频图像真伪鉴定算法，近 10 种深伪鉴定算法，同时具有智能鉴定和专业鉴定两种鉴定模式，支持卷宗管理和三种鉴定文书生成，为司法鉴定人员提供一站式视频图像检验鉴定服务。

图15：美亚柏科AI-3300慧眼视频图像鉴真工作站

资料来源：美亚柏科官微，信达证券研发中心

针对生成式 AI 鉴真，美亚柏科基于在电子数据取证和公共安全大数据多年的行业积累，研究推出的针对人工智能（如 ChatGPT）生成文本内容的检测工具。该工具对中文生成文本检测的准确率超过 90%。

图16：美亚柏科AIGC内容检测平台



资料来源：美亚柏科官微，信达证券研发中心

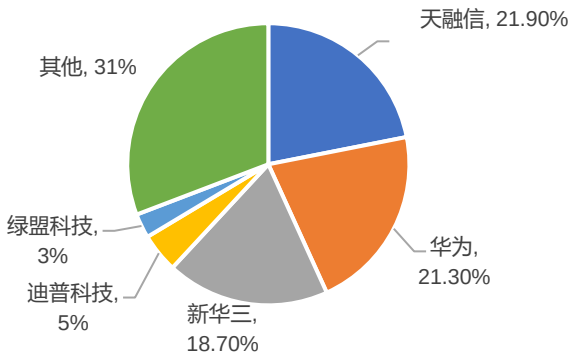
五. 国内安全厂商对比分析

5.1 头部网安公司对比分析

（1）头部公司主打产品都涉及网关类安全产品

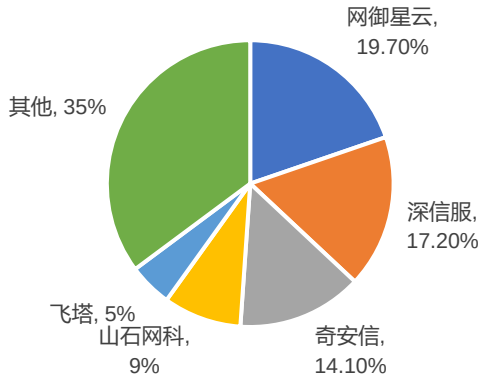
主要有：防火墙、统一威胁管理平台（UTM）、入侵检测和入侵防御（IDP）、虚拟专用网络（VPN），安全内容管理（SCM）。可以看到各细分领域的厂商基本都是深信服、启明星辰、绿盟科技、天融信等头部公司，以及华为、新华三两大数通厂商。

图17：2022年中国UTM防火墙硬件市场份额



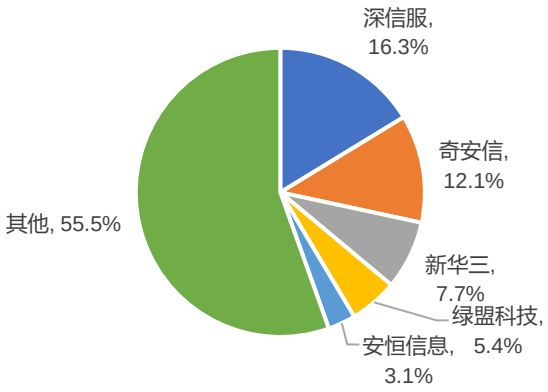
资料来源：IDC 中国、信达证券研发中心

图18：2022年中国统一威胁管理硬件市场份额



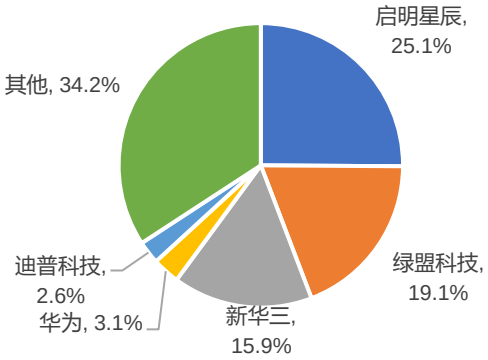
资料来源：IDC 中国、信达证券研发中心

图19：2022年中国安全内容管理硬件市场份额



资料来源：IDC 中国、信达证券研发中心

图20：2022年中国入侵检测与防御硬件市场份额



资料来源：IDC 中国、信达证券研发中心

（2）选择好赛道是公司迅速成长的前提条件

这些头部公司之所以能长大，从产品选择角度来看，此前均重点在市场容量较大的细分领域发力，如防火墙、UTM（含下一代防火墙）、入侵检测、上网行为管理领域。但各家侧重点和优势产品又有所区别。

（3）下游客户占比

这些头部网安公司的下游客户类别差异不大，主要是政府及事业单位、运营商、金融、能源等行业，从各行业客户的占比来看，各网安公司之间存在一定差异。其中最主要的区别在于：

相较于其他网安厂商，在深信服的下游客户中，以企业为代表的中小客户占比较大，而其他网安厂商的下游客户以政府、央国企等大客户为主。

（3）销售模式

深信服以渠道销售为主，2022 年渠道销售收入占总收入的 96.32%。相比其他安全公司，深信服面向的客户体量相对较小，近年来公司着力进行行业纵深，拓展政府部委、银行等大客户。

绿盟科技近年来实施渠道战略转型，截至 2022 年末，绿盟科技共签约超 3500 家合作伙伴，其中战略合作伙伴与生态合作伙伴超过 30 家，并累计服务超过 50000 家的全国客户。

安恒信息采用渠道销售和直销相结合的方式，直销和渠道占比相对均衡。主要原因是因为公司产品的目标用户群多、用户的地域及行业分布广，采用渠道与直销结合的方式能够最大程度实现市场覆盖、最高效率为客户提供网络信息安全产品及服务。

亚信安全采取渠道与直销相结合的方式，对于电信运营商、金融、能源等领域的头部大型客户，公司一般采用直销的方式，安排专门的销售及业务团队为其进行服务。对于其他客户，公司一般采取渠道代理销售的方式。

迪普科技、山石网科采用渠道销售和直销相结合的方式，并以渠道销售为主。截至 2022 年末，迪普科技在全国设立了 28 个办事处并根据各地情况增设二级办事处，有效渠道合作伙伴 2,500 余家；山石网科代理商签约数量约 1932 家。

启明星辰、天融信、奇安信、安博通以直销为主，面向的客户体量相对较大，由于行业景气度提升、地方性客户需求增加，也开始强化渠道建设，拓展中小客户。

两种销售模式是在面向不同体量客户下的适应性选择，无明显优劣，未来是否能在对方领域取得突破性进展还需持续关注。

表 3：头部网安公司对比：主要产品、下游客户、销售模式（2022 年数据）

公司名称	优势产品	下游客户占比	销售模式
深信服	下一代防火墙、上网行为管理、VPN 等	政府及事业单位 49% 企业 39% 金融及其他 13%	渠道为主，直销为辅
启明星辰	统一威胁管理平台（UTM）、入侵检测和防御产品（IDP）、安全管理平台（SOC）、数据安全等	公司未披露最新下游客户占比	直销为主，建设渠道拓展中小客户
天融信	防火墙、安全管理平台（SOC）、IDP、数据安全等	政府及事业单位 37%； 国有企业 34%；	直销为主，建设渠道拓展中小客户

		商业及其他 29%	
绿盟科技	入侵检测和防御产品（IDP）、web 应用防火墙（WAF）、抗拒绝服务系统（ADS）、漏扫产品等	金融 15% 电信 22% 能源及企业 28% 政府、事业单位及其他 35%	渠道转型后，渠道收入为主；渠道成为公司业务增长的放大器
迪普科技	终端安全、云端威胁情报、零信任、大数据安全检测与管控、应用开发安全、安全服务等	政府 47%； 运营商 47%； 公共事业 24%	渠道为主，直销为辅
安恒信息	数据安全、应用安全、云托管安全服务等	公司未披露最新下游客户占比	多级渠道经销和直销相结合
奇安信	数据安全、终端安全、IT 安全咨询服务、托管安全服务等	政府 29%； 公检法司 16%； 企业级客户 54%	直销与渠道相结合
亚信安全	终端安全、云安全、身份安全等	运营商 49.33% 非运营商（金融、能源等）50.67%	对于头部大型客户，采取直销；对于其他客户，采取渠道销售
山石网科	统一威胁管理平台（UTM）、下一代防火墙、云安全等	公司未披露最新下游客户占比	直销与渠道相结合，且渠道为主
安博通	安全网关、安全管理、数据安全等	下游客户为网安公司	直销为主

资料来源：各公司年报，IFIND，信达证券研发中心

（4）头部公司财务指标

营业收入：

尽管 22 年网安行业受外部因素影响较大，普遍表现不佳；拉长时间看，18-22 年头部公司的安全业务复合收入增速大部分在 20%左右。

经营性净现金流：

深信服采用渠道销售模式，渠道垫资形成预收款，相比直销形成应付款为主，有更好的经营性净现金流表现。

毛利率：

渠道模式的深信服安全业务毛利率较高，直销为主的公司毛利率较低。我们认为，其主要原因为：（1）深信服销售产品后的实施、调参等工作交由渠道完成，在直销模式下这类人工计入成本项使得毛利率相对略低；（2）深信服产品在中小客户领域或享有一定品牌溢价。

长期来看，我们认为网安公司长期毛利率有望保持稳定，其主要原因是：

（1）网安公司的研发、销售支出刚性，合理的毛利率水平是企业生存的必要条件。

（2）对于网安厂商来说持续绑定客户的关键在于优质的产品和服务，若持续打价格战，难以保证提供比竞争对手更好的技术和服务。技术和服务若不能保证，则难以持久占据市场，因此，我们认为网安厂商之间打价格战的意义不大。

表4：部分网安公司主要财务指标（2022年数据）

公司名称	收入（亿元）	18-22 年收入复合增速	归母净利润（亿元）	经营性净现金流（亿元）	毛利率	净利率	ROE
深信服	整体 74.13 安全 38.93	整体 24.9% 安全 19.8%	1.94	7.46	整体 63.82% 安全 80.50%	2.62%	2.58%
启明星辰	整体 44.37	整体 15.2%	6.26	-0.11	整体 62.66%	14.12%	8.87%
天融信	整体 35.43	整体 19.6%（仅考虑安全行业收入）	2.05	-2.71	整体 59.72%	5.79%	2.13%
绿盟科技	整体 26.29	整体 18.2%	0.28	0.6	整体 62.28%	1.08%	0.87%
迪普科技	整体 8.93	整体 6.1%	1.5	1.81	整体 67.79%	16.77%	4.68%
安恒信息	整体 19.80	整体 33.3%	-2.53	-1.79	整体 64.20%	-12.79%	-8.45%
奇安信	整体 62.23	整体 36.0%	0.57	-12.61	整体 64.34%	0.93%	0.57%
亚信安全	整体 17.21	整体 18.5%	0.99	-2.61	整体 52.79%	5.67%	4.80%
山石网科	整体 8.12	整体 9.6%	-1.83	-3.32	整体 68.32%	-22.67%	-12.92%
安博通	整体 4.56	整体 23.7%	-0.08	-1.69	整体 56.03%	-1.75%	-0.74%

资料来源：IFIND，各公司年报，信达证券研发中心

收入季节性强：

信息安全公司收入有较明显的季节性，由于下游客户主要包括政府、运营商等客户，上述客户通常实行预算管理制度和集中采购制度，在上半年审批当年的年度预算和固定资产投资计划，在年中或下半年安排设备采购招标，设备交货、安装、调试和验收则集中在下半年尤其是第四季度，所以行业公司普遍存在季节性销售特征；下半年尤其是第四季度收入在全年收入中占比较高。

表5：部分网安公司单季节收入占比

公司名称	2022Q1	2022Q2	2022Q3	2022Q4
深信服	15.43%	22.54%	26.07%	35.96%
启明星辰	12.72%	14.64%	21.51%	51.13%
天融信	10.68%	14.16%	16.46%	58.70%
绿盟科技	12.42%	19.32%	21.05%	47.21%
迪普科技	23.93%	17.27%	26.69%	32.10%
安恒信息	11.79%	15.21%	25.50%	47.49%
奇安信	10.59%	21.03%	19.67%	48.71%
亚信安全	16.55%	17.91%	25.33%	40.22%

山石网科	17.83%	29.55%	40.56%	12.06%
安博通	11.56%	20.00%	23.15%	45.29%

资料来源：IFIND、信达证券研发中心

研发投入：

各家公司普遍重视研发投入，研发费用率普遍在22%以上。

销售费用率：

深信服、绿盟科技、迪普科技三家公司销售费用率较高，我们推测，是由于这三家公司以渠道销售为主，相比于直销需要指出更多营销费用所致。类比国内其他大B端软件行业，可以预见，国内网安公司销售费用率长期看或有下降趋势。如ERP也是面向全行业的b端客户，且以大B客户为主，ERP龙头公司用友网络（成立时间是1988年，较启明星辰、绿盟科技、深信服等网安头部公司成立早10年左右时间），随着用友网络收入体量增加、客户覆盖度变高，销售费用率从早期2003年的41%降到2020年的18%。一定程度上可借鉴用友网络的销售费用率变化趋势，前瞻网安头部公司的销售费用率变化趋势。相比ERP行业，网安公司高度产品化的销售模式，更有利于毛利率稳定，在销售费用率得到控制的情况下，更容易看到合理的净利率表现。

表6：2022年头部网安公司三费率情况

公司名称	研发费用率	销售费用率	管理费用率
深信服	30.33%	32.52%	5.26%
启明星辰	21.16%	26.19%	4.71%
天融信	23.17%	22.92%	9.09%
绿盟科技	22.78%	33.28%	7.11%
迪普科技	26.99%	33.93%	3.70%
安恒信息	32.63%	43.08%	9.65%
奇安信	27.22%	30.45%	10.99%
亚信安全	18.71%	28.01%	8.72%
山石网科	41.75%	7.64%	46.18%
安博通	23.03%	12.72%	19.52%

资料来源：IFIND、信达证券研发中心

5.2 头部网安公司盈利指标有望回归合理区间

（1）受外部因素影响，下游客户需求侧紧缩，2022年大部分网安公司收入增速不达预期，同时费用支出较高，因此导致22年行业大部分公司净利率偏低。**我们认为，在宏观环境逐渐改善的大环境下，下游客户需求侧有望改善，叠加网安厂商逐步进入控费周期，网安公司盈利能力有望恢复。**

（2）**我们认为，网安行业的净利率有望维持在10-20%的合理区间。**网安行业由于产品种类多，单一公司难以在全产品线上都超越同行；且需要根据攻击不断持续进行技术产品升级，

难以在研发上拉开代际差距。这些行业特性，使得一家公司想通过进行持续高强度的投入，以实现与其他头部公司在市占率、产品、技术上都拉开差距是比较困难的。想要拉开差距需要打持久战，打持久战长期来看需要有健康的财务回报和可以满足发展的现金流。因此，长期来看网安公司还是会选择追求合理的利润回报。**我们预计网安头部公司净利率会低于寡头垄断的行业的头部公司，比如恒生电子、海康威视。会高于以人数计费为主的银行 IT 头部公司，如长亮科技、宇信科技。预计网安公司长期的净利率区间或在：10%-20%，中值为 15%。**

表 7：2019-2022 头部网安公司净利率与恒生电子等公司净利率对比

	2019	2020	2021	2022
恒生电子	36.56%	32.67%	27.11%	17.22%
海康威视	21.62%	21.54%	21.51%	16.30%
安恒信息	9.76%	9.96%	0.61%	-12.79%
深信服	16.53%	14.83%	4.01%	2.62%
启明星辰	22.07%	22.21%	19.67%	14.12%
绿盟科技	13.54%	14.99%	13.22%	1.08%
长亮科技	10.64%	15.34%	8.11%	1.28%
宇信科技	10.30%	15.19%	10.61%	5.91%

资料来源：IFIND，信达证券研发中心

六. 投资建议

国内信息安全行业的典型客户包括党政军、电信、金融、能源、交通、教育等领域，政策驱动因素的影响相对较大。未来几年，由于《网络安全法》及相关条例落地、等保 2.0 的实施，行业投入有望持续加大。

由于用户日渐重视安全，对安全公司技术和品牌愈发看重，过去 2 年行业的集中度从尾部向头部、科创板公司集中。同时。头部公司整体具备研发、销售积累的优势不易被超越，科创板公司由于专注于新型领域有望实现更快增长。

我们认为，头部公司未来 3 年普遍有望实现快于行业的收入增速水平。整体关注下游需求的复苏节奏，除此外不同公司的关注点有差异：

安恒信息：公司在数据安全、安全托管服务（MSS）方向上布局领先，关注公司在数据安全、安全托管服务（MSS）、信创安全等战略新方向的发展。

深信服：关注中小客户的复苏节奏；GPT 的上线节奏和带来的产品功能及效率提升。

启明星辰：中国移动入驻已带来增量业务，关注中国移动持续带来的协同效应。

绿盟科技：公司坚定渠道战略转型，关注后续在研发端的激励调整成效。

天融信：公司研发端前置投入基本完成，关注后续在销售端持续发力带来的效能提升。

迪普科技：公司销售端发力，关注后续业绩提速情况。

奇安信：关注公司持续降本增效的成效。

山石网科：关注渠道体系建设情况；研发端产品补齐情况。

亚信安全：关注产品线的拓展和运营商以外客户的拓展。

安博通：作为安全公司的上游，关注行业增长给公司带来的红利。

美亚柏科：关注 AI 反诈产品的研发和销售进展。

三六零：关注公司 B 端安全业务的布局和大模型的进展。

七. 风险提示

1. 当前形势下公共财政压力或有所增大、不少下游领域景气度亦会受影响，因此下游客户投入力度是否会有改善仍需观察；

2.网安行业下游客户以政企、央国企为主，若相关政策推进不及预期，可能导致该类客户投入力度减弱；

3.若行业竞争加剧，行业内公司进行持续价格战，可能影响各公司的盈利能力改善进度。

研究团队简介

庞倩倩，计算机行业首席分析师，华南理工大学管理学硕士。曾就职于华创证券、广发证券，2022 年加入信达证券研究开发中心。在广发证券期间，所在团队 21 年取得：新财富第四名、金牛奖最佳行业分析师第二名、水晶球第二名、新浪金麒麟最佳分析师第一名、上证报最佳分析师第一名、21 世纪金牌分析师第一名。

郑祥，计算机行业研究助理，北京大学工商管理硕士，武汉大学管理学学士，2021 年 7 月加入信达证券研究所，从事计算机行业研究工作。

机构销售联系人

区域	姓名	手机	邮箱
全国销售总监	韩秋月	13911026534	hanqiuyue@cindasc.com
华北区销售总监	陈明真	15601850398	chenmingzhen@cindasc.com
华北区销售副总监	阙嘉程	18506960410	quejiacheng@cindasc.com
华北区销售	祁丽媛	13051504933	qiliyuan@cindasc.com
华北区销售	陆禹舟	17687659919	luyuzhou@cindasc.com
华北区销售	魏冲	18340820155	weichong@cindasc.com
华北区销售	樊荣	15501091225	fanrong@cindasc.com
华北区销售	秘侨	18513322185	miqiao@cindasc.com
华北区销售	李佳	13552992413	lijia1@cindasc.com
华北区销售	赵岚琦	15690170171	zhaolanqi@cindasc.com
华北区销售	张斓夕	18810718214	zhanglanxi@cindasc.com
华北区销售	王哲毓	18735667112	wangzheyu@cindasc.com
华东区销售总监	杨兴	13718803208	yangxing@cindasc.com
华东区销售副总监	吴国	15800476582	wuguo@cindasc.com
华东区销售	国鹏程	15618358383	guopengcheng@cindasc.com
华东区销售	朱尧	18702173656	zhuyao@cindasc.com
华东区销售	戴剑箫	13524484975	daijianxiao@cindasc.com
华东区销售	方威	18721118359	fangwei@cindasc.com
华东区销售	俞晓	18717938223	yuxiao@cindasc.com
华东区销售	李贤哲	15026867872	lixianzhe@cindasc.com
华东区销售	孙僮	18610826885	suntong@cindasc.com
华东区销售	贾力	15957705777	jiali@cindasc.com
华东区销售	石明杰	15261855608	shimingjie@cindasc.com
华东区销售	曹亦兴	13337798928	caoyixing@cindasc.com
华东区销售	王赫然	15942898375	wangheran@cindasc.com
华南区销售总监	王留阳	13530830620	wangliuyang@cindasc.com
华南区销售副总监	陈晨	15986679987	chenchen3@cindasc.com
华南区销售副总监	王雨霏	17727821880	wangyufei@cindasc.com
华南区销售	刘韵	13620005606	liuyun@cindasc.com
华南区销售	胡洁颖	13794480158	hujieying@cindasc.com
华南区销售	郑庆庆	13570594204	zhengqingqing@cindasc.com
华南区销售	刘莹	15152283256	liuying1@cindasc.com

华南区销售	蔡静	18300030194	caijing1@cindasc.com
华南区销售	聂振坤	15521067883	niezhenkun@cindasc.com
华南区销售	宋王飞逸	15308134748	songwangfeiyi@cindasc.com

分析师声明

负责本报告全部或部分内容的每一位分析师在此申明，本人具有证券投资咨询执业资格，并在中国证券业协会注册登记为证券分析师,以勤勉的职业态度,独立、客观地出具本报告；本报告所表述的所有观点准确反映了分析师本人的研究观点；本人薪酬的任何组成部分不曾与，不与，也将不会与本报告中的具体分析意见或观点直接或间接相关。

免责声明

信达证券股份有限公司(以下简称“信达证券”)具有中国证监会批复的证券投资咨询业务资格。本报告由信达证券制作并发布。

本报告是针对与信达证券签署服务协议的签约客户的专属研究产品，为该类客户进行投资决策时提供辅助和参考，双方对权利与义务均有严格约定。本报告仅提供给上述特定客户，并不面向公众发布。信达证券不会因接收人收到本报告而视其为本公司的当然客户。客户应当认识到有关本报告的电话、短信、邮件提示仅为研究观点的简要沟通，对本报告的参考使用须以本报告的完整版本为准。

本报告是基于信达证券认为可靠的已公开信息编制，但信达证券不保证所载信息的准确性和完整性。本报告所载的意见、评估及预测仅为本报告最初出具日的观点和判断，本报告所指的证券或投资标的的价格、价值及投资收入可能会出现不同程度的波动，涉及证券或投资标的的历史表现不应作为日后表现的保证。在不同时期，或因使用不同假设和标准，采用不同观点和分析方法，致使信达证券发出与本报告所载意见、评估及预测不一致的研究报告，对此信达证券可不发出特别通知。

在任何情况下，本报告中的信息或所表述的意见并不构成对任何人的投资建议，也没有考虑到客户特殊的投资目标、财务状况或需求。客户应考虑本报告中的任何意见或建议是否符合其特定状况，若有必要应寻求专家意见。本报告所载的资料、工具、意见及推测仅供参考，并非作为或被视为出售或购买证券或其他投资标的的邀请或向人做出邀请。

在法律允许的情况下，信达证券或其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，并可能会为这些公司正在提供或争取提供投资银行业务服务。

评级说明

投资建议的比较标准	股票投资评级	行业投资评级
本报告采用的基准指数 ：沪深 300 指数（以下简称基准）； 时间段：报告发布之日起 6 个月内。	**买入：**股价相对强于基准 20%以上；	**看好：**行业指数超越基准；
	增持：股价相对强于基准 5%～20%；	**中性：**行业指数与基准基本持平；
	持有：股价相对基准波动在±5% 之间；	**看淡：**行业指数弱于基准。
	卖出：股价相对弱于基准 5%以下。	

风险提示

证券市场是一个风险无时不在的市场。投资者在进行证券交易时存在赢利的可能，也存在亏损的风险。建议投资者应当充分深入地了解证券市场蕴含的各项风险并谨慎行事。

本报告中所述证券不一定能在所有的国家和地区向所有类型的投资者销售，投资者应当对本报告中的信息和意见进行独立评估，并应同时考量各自的投资目的、财务状况和特定需求，必要时就法律、商业、财务、税收等方面咨询专业顾问的意见。在任何情况下，信达证券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，投资者需自行承担风险。