

# 中国网络安全产业分析报告

## (2023 年)



中国网络安全产业联盟  
2023 年 9 月

## 版 权 声 明

本报告版权属于中国网络安全产业联盟（CCIA），并受法律保护。转载、摘编或利用其它方式使用本报告文字或者观点的，应注明“来源：中国网络安全产业联盟”。违反上述声明者，CCIA 将追究其相关法律责任。

## 前 言

习近平总书记在党的二十大报告中强调，必须坚定不移贯彻总体国家安全观，要坚定维护国家政权安全、制度安全、意识形态安全，加强重点领域安全能力建设，强化网络、数据等安全保障体系建设。作为国家安全的重要组成部分，网络安全与其它各领域安全相互交融、相互影响，已经成为我国面临的最复杂、最现实、最严峻的非传统安全问题之一。近年来，《网络安全法》《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》等一系列法律法规和政策文件相继颁布实施，构建起网络安全政策法规体系的“四梁八柱”，网络综合治理体系基本建成；网络空间国际话语权和影响力明显增强，网络强国建设迈出新步伐；网络产品和服务层出不穷，产业规模持续增长，产业综合实力不断提高。但与此同时，我国网络安全在技术、资源、人才、管理等方面与发达国家相比差距较大，仍存在自主创新不足、网络安全防护技术体系尚不健全等问题。习近平总书记在2023年全国网络安全和信息化工作会议上作出重要指示，提出了网信工作的使命任务，明确“十个坚持”的重要原则，为做好新时代新征程网信工作指明了方向。

本报告是中国网络安全产业联盟（CCIA）连续第六年发布。CCIA继续联合我国网络安全领域专业研究机构“数说

安全”，以数据为基础，按照客观中立原则展开了数据调研、收集整理和分析研究工作。

本报告的市场规模采用收入法统计，统计范围为在国内销售网络安全产品或提供网络安全服务的企业，不包括产业链上游硬件供应商和下游销售渠道（代理商和分销商）。

本次调研延续前五次产业调研模式，仍然以具备网络安全产品、服务和解决方案销售收入的我国网络安全企业为目标研究对象，调研企业 296 家，最终收集到 192 家企业有效数据，基本覆盖了国内主要的网络安全企业。

本报告首先介绍了 2023 年我国网络安全产业面临的总体形势，既面临网络安全治理日臻完善、网络安全技术加快迭代升级、数字安全再提层级以及全球网络安全战略布局加快的发展机遇，也遭遇全球经济下行、大国博弈加剧的环境下网络安全产业发展动能放缓、竞争激烈度增强等挑战，新技术的不当应用也造成网络安全挑战更加复杂艰巨的局面。

在市场分析部分，报告以客户及厂商调研数据为基础，面向产业链结构的供需两侧探求市场全貌。从供给侧，报告分析了我国网络安全企业的总体构成及分布情况，对 2022 年我国网络安全产业规模进行了测算，并对行业集中度、市场区域分布等进行了分析；在需求侧，对客户行业分布及网络安全需求数据进行了分析，定位当前市场热点；同时基于对网络安全市场分类的划分，更新绘制了我国网络安全产业

全景图。

在企业竞争力和产业格局部分，报告按照企业发展阶段对网络安全企业竞争力进行了全面评估，并将我国网络安全企业划分为领导者、战略布局者、成长者和创新者，分析各类企业特点，展望产业格局的演变趋势。

在资本市场部分，报告基于采集的样本公司经营数据，对 2022 年我国网络安全主要企业经营情况进行了综合分析，刻画了总体现金流量画像。同时，报告评价了我国网络安全产业资本市场表现，回顾了 2022 年以来的 IPO 动态和投融资情况，对创投市场的整体环境变化情况及产业内的资本动态进行回溯分析。

在产业发展热点部分，报告从网络安全技术、服务和治理三个维度，重点列举了 10 个发展热点，分别是生成式人工智能、人工智能对抗攻防技术、量子安全技术、云原生安全、网络安全保险服务、安全审计和合规性服务、网络安全防护有效性验证服务、云密码服务、数据安全治理，以及软件供应链安全治理。

在产业发展趋势部分，报告提出对网络安全产业未来发展的五大趋势研判，展望了网络安全产业的发展前景，为网络安全产业发展规划提供参考。

鉴于产业全口径统计数据获取实际情况，本报告中涉及网络安全产业规模及增速等分析所用数据截至 2022 年底；

网络安全企业经营数据更新至 2023 年上半年。产业基本情况、企业竞争力与产业格局以及资本市场分析涉及的数据均为 CCIA 和数说安全基于调研或公开资料整理。本报告观点及数据仅供参考，不作为投资依据。

中国网络安全产业联盟 (CCIA)

# 目 录

前 言.....	1
一、2023 年网络安全产业发展面临的新形势.....	9
（一）发展机遇.....	9
（二）面临挑战.....	14
二、我国网络安全产业基本情况.....	17
（一）我国网络安全企业总体表现.....	17
（二）我国网络安全产业规模及市场集中度分析.....	20
（三）我国网络安全市场区域分布及增速分析.....	22
（四）我国网络安全客户所属行业分布及增速分析.....	24
（五）我国网络安全客户产品需求热度分析.....	25
（六）我国网络安全市场分类及全景图.....	26
三、我国网络安全企业竞争力与产业格局.....	30
（一）我国网络安全企业竞争力评估.....	30
（二）我国网络安全产业竞争格局.....	31
四、我国网络安全资本市场分析.....	33
（一）我国主要网络安全企业经营情况分析.....	33
（二）我国网络安全产业资本市场表现.....	38
（三）我国网络安全企业 IPO 动态.....	39
（四）我国网络安全产业投融资情况.....	40

五、我国网络安全产业发展热点分析.....	42
（一）生成式人工智能.....	43
（二）人工智能对抗攻防技术.....	44
（三）量子安全技术.....	46
（四）云原生安全.....	48
（五）网络安全保险服务.....	49
（六）安全审计和合规性服务.....	50
（七）网络安全防护有效性验证服务.....	52
（八）云密码服务.....	53
（九）数据安全治理.....	54
（十）软件供应链安全治理.....	55
六、我国网络安全产业发展展望.....	57
（一）政策驱动、需求拉动的发展趋势将更加明显.....	57
（二）产业自主可控的发展趋势将更加明显.....	58
（三）“产品+服务”双轮驱动的发展趋势将更加明显.....	59
（四）领军企业带动、产业链协同的发展趋势将更加明显.....	59
（五）技术服务“智能化+主动化”的发展趋势将更加明显.....	60
附件一 2022.9-2023.9 网络安全相关法律法规和政策列表.....	62
附件二 网络安全企业竞争力评估指标和分析方法.....	64



## 图目录

图 1	2023 年我国网络安全企业的总体构成.....	17
图 2	2022Q4-2023H1 我国网络安全上市公司营业收入同比增长率.....	18
图 3	2022 年中国网络安全市场规模及增速.....	20
图 4	近五年中国网络安全行业集中度分析.....	21
图 5	2022 年中国网络安全行业主要企业市占率情况.....	22
图 6	2022 年中国网络安全市场区域分布.....	23
图 7	2022 年中国网络安全项目数量省市分布及增速.....	23
图 8	中国网络安全客户地图.....	24
图 9	2022 年中国网络安全项目数量行业分布及增速.....	25
图 10	2022 年中国网络安全产品采购趋势.....	26
图 11	中国网络安全市场分类架构示意图.....	27
图 12	2023 年中国网络安全市场全景图.....	29
图 13	CCIA 50 强企业画像.....	31
图 14	2022 年中国网络安全产业竞争格局.....	32
图 15	2020-2022 年样本网络安全企业安全业务营业收入.....	35
图 16	2022 年样本企业安全业务营业收入及营收增长情况.....	36
图 17	2022 年样本网络安全企业安全业务盈亏状况.....	36
图 18	2022 年样本企业费用以及四项费用率构成.....	37
图 19	2022 年样本企业现金流净额.....	38
图 20	2013-2023 年中国上市网络安全企业市值动态.....	38

图 21 2013-2023 年中国上市网络安全企业估值动态..... 39

图 22 2018-2022 年中国网络安全领域融资事件数量金额比较..... 41

表目录

表 1 2023 年上半年已公开上市的网络安全企业经营数据..... 19

表 2 公开上市的网络安全企业 2022 年经营情况.....34

表 3 2020-2023 年网络安全企业上市进程情况..... 40

表 4 2022 年-2023 年上半年度网络安全企业（一级市场）融资情况  
..... 41

## 一、2023 年网络安全产业发展面临的新形势

2023 年，世界百年未有之大变局加速演进，在通胀压力继续攀升、地缘政治冲突升级、供应链挑战加剧等多重冲击下，全球经济增长乏力，网络安全产业发展面临的国际形势依然复杂严峻，网络安全成为大国角力和科技竞争主攻方向的趋势更加明显。从国内看，2023 年是全面贯彻落实党的二十大精神开局之年，随着疫情防控平稳转段，我国国民经济持续恢复，网络安全产业逐步恢复稳定增长的发展态势。在网络安全法律体系更趋完善、政策愈加落地，以及技术迭代、数字经济注入新发展动力的加持下，网络安全产业应对国际变局动荡的心态更稳、能力更强，从政府到企业凝聚合力、攻坚克难、开拓创新，正加快构筑产业发展新优势，共同夯实网络空间命运共同体的安全基石。

### （一）发展机遇

#### 1. 网络安全治理日臻完善，产业发展更加有据可依

一是法律法规趋严趋细，合规要求更加全面深入。近年来，随着关键信息基础设施安全保护、网络安全审查、云计算服务安全评估、数据安全法、个人信息保护法等领域一系列法律法规相继出台，我国网络安全法规体系的“四梁八柱”基本建成。2022 年以来，网络安全治理更加全面深入，国家在一体推进网络安全立法、执法、司法、普法道路上不断向

前迈进。2022 年第四季度，《网络安全法》首次修订，对违反网络运行安全一般规定和网络信息安全法律责任制度进行了调整，增加了从业禁止措施，网络空间治理法治化依据更加明确；《反电信网络诈骗法》正式施行，针对电信网络犯罪行为构建全方位治理体系。《未成年人网络保护条例（草案）》修改审议，加快步入立法进程；《商用密码管理条例》发布并施行，在《密码法》框架下完善了商用密码有关的系列重要制度；《网信部门行政执法程序规定》发布，对进一步规范和保障网信部门依法履行职责、实施行政执法等方面提出要求。此外，线上金融服务的合规监管日益严格，泸州银行泸贝尔 APP、山西银行 APP、兰州银行 APP 等超十家银行 APP 因侵犯用户权益、违规获取个人信息，被有关部门点名通报和限期整改。

二是政策标准密集发布，行业健康规范发展生态更加健全。《关于促进网络安全保险规范健康发展的意见》《关于推进 IPv6 技术演进和应用创新发展的实施意见》《关于开展网络安全服务认证工作的实施意见》等政策为规范网络安全行业细分领域提出了具体要求；在互联网信息服务、互联网广告、证券期货业、寄递服务、在线旅游、政务大数据等重点行业提出了网络安全管理具体措施（详见附件一）。《生成式人工智能服务管理暂行办法》发布，对生成式人工智能技术的发展与治理做出明确规定。首个关键信息基础设施安

全保护的国家标准《信息安全技术 关键信息基础设施安全保护要求》正式实施，《汽车整车信息安全技术要求》等强制性国家标准征求意见，生成式人工智能数据安全规范、大型网络平台网络安全评估指南、数据分类分级保护要求等标准列入 2023 年度网络安全国家标准计划，工业互联网、车联网密码支撑标准体系建设指南发布，在助推网络安全产业高质量发展方面的基础性、规范性、引领性作用更加凸显。

## 2. 网络安全技术加快迭代升级，为产业发展注入更强动力

近年来，全球持续加大对新兴技术的投资和研发力度，零信任、生成式人工智能、量子信息技术等网络安全技术布局及应用持续提速。2022 年以来，零信任架构加快落地，美国正式发布《国防部零信任战略》，将零信任部署为网络安全最高优先事项，美网络安全和基础设施安全局（CISA）发布零信任成熟度模型第二版，更新了政府范围内采用零信任安全架构的关键定义和指标。随着美国开放人工智能公司（OpenAI）推出了聊天生成预训练转换器（ChatGPT）并在全球范围内广泛应用，生成式人工智能（AIGC）再次成为焦点，谷歌、微软、百度、阿里、科大讯飞、腾讯等企业相继推出应用 AIGC 和大语言模型技术产品。在网络安全领域，AIGC 技术浪潮加快了网络安全知识和经验的大规模复制速度，提升了安全代码生成、智能研判等领域的实现效率，为

数据安全防护路径提供新的解决思路。2023 年，以量子计算、量子通信为代表的量子信息技术（QIS）逐步由实验阶段走向落地应用，为网络安全技术的发展注入新动力，美德等国家均加快研究不受量子技术攻击的加密技术以保障网络通信安全；我国首个量子通信领域国家标准《量子保密通信应用基本要求》发布，有关量子信息技术应用有望加速落地。全球范围内网络安全技术迅速迭代升级和推陈出新进而产生的知识和技术外溢对网络安全产业的创新发展产生客观的推动作用，同时也倒逼国内企业和研究机构在重点领域和细分环节加快技术突破、专利布局 and 标准转化，打造更强技术优势。

### **3. 数字安全再提层级，数据安全产业将迎来爆发期**

近一年来，数字安全国家立法和战略规划并行推进，《中华人民共和国数字经济促进法（专家建议稿）》的公布标志着数字经济启动首次立法，即将步入有法可依的新阶段；《数字中国建设整体布局规划》正式发布，提出夯实数字基础设施和数据资源体系“两大基础”，强化数字技术创新体系和数字安全屏障“两大能力”，将数字安全提高到战略层级；中共中央、国务院印发《关于构建数据基础制度更好发挥数据要素作用的意见》（简称“数据二十条”），从数据产权、流通交易、收益分配、安全治理等方面构建数据基础制度；《工业和信息化部等十六部门关于促进数据安全产业发展的指

导意见》聚焦数据安全保护及相关数据资源开发利用需求，明确了发展目标和重点任务，为产业发展规划出清晰路线图；《数据出境安全评估办法》规定了数据出境安全评估的范围、条件和程序，为数据出境安全评估工作提供了具体指引，体现出维护数字安全的国际视角。此外，国家数据局的组建有利于加快国内数据流通，有助于快速推进数据要素市场建设。可以预见，在数字安全相关制度建设和机构建设日趋完备的“双轮”驱动下，相关行业对数据安全的投入将持续增加，数据安全产业将迎来增长爆发期。

#### **4. 全球网络安全战略布局加快，对产业提出更高要求**

2022年下半年以来，美国陆续发布《2023—2025年战略计划》《国家网络安全战略》《2023年美国防部网络战略》《美国政府关键和新兴技术国家标准战略》等政策文件，从网络空间安全、关键信息基础设施安全、数字安全等方面提出具体的战略举措，强化网络安全保护和网络空间作战能力。欧盟陆续发布《网络弹性法案》《关于在欧盟全境实现高度统一网络安全措施的指令》（NIS 2指令）、《关于GDPR下的个人数据泄露通知的第9/2022号指南》《网络团结法案》等法律法规，力图通过强监管巩固网络安全管理和网络空间防御。美欧在网络安全领域的系列战略举措显示了其在强化网络空间防御、提高关键信息基础设施安全水平、加强数字监管等方面的决心，预计后续将陆续推出的具体措施将显著

增强其维护国家网络安全，打击所谓“敌对势力”，限制竞争对手发展的能力，这给我们敲响警钟；另一方面，我国“出海”企业将面临更高的合规要求，在满足数字合规、合法权益维护、保持业务安全不宕机等方面需要增强投入。要实现以上两点，需要加强研判，提前布局。

## （二）面临挑战

### 1. 全球经济下行削弱政府财力和企业盈利能力，网络安全产业受到冲击

2023 年，通胀压力继续攀升，全球经济步入中低速增长轨道。世界银行的预测显示，全球增长预计将从 2022 年的 3.1% 放缓至 2023 年的 2.1%。美欧等发达经济体的银行业危机发酵，金融形势险象环生，信贷条件日趋收紧，新兴市场和发展中经济体当中有四分之一实际已无法通过国际债券市场融资<sup>1</sup>。从国内看，疫情防控平稳转段后，我国经济恢复呈现波浪式发展、曲折式前进的过程。宏观经济表现不佳削弱了政府财力，压缩了企业盈利空间，政府和企业网络安全方面的投入不可避免地受到波及，给网络安全业务拓展和产品交付造成了较大的负面影响。大量企业在网络安全建设上“有心无力”，基础网络业务影响较大，部分企业经营困难，再加上政府和企业网络安全方面的预算和投入普遍降低

---

<sup>1</sup> 《世界银行：2023 年 6 月全球经济展望报告》  
<https://finance.sina.com.cn/tech/roll/2023-06-08/doc-imywpprq9744526.shtml>



或延后，大量在建项目资金延期到位，导致网安企业应收账款激增，企业营收和净利润表现不佳，需求侧不振成为网络安全产业发展增速稳中趋缓的重要原因。

## 2. 大国“零和博弈”加剧，网络空间竞争交锋烈度和重点产业供应链风险强度增高

2023 年，大国竞争“零和博弈”趋势更加明显，去全球化的消极互动成为中短期内全球经济与政治互动的主要特征<sup>2</sup>，全球主要国家安全战略将进一步转向大国竞争，叠加地缘政治冲突、全球能源危机等负面因素，网络空间成为现代战争和对抗的重要战场。2022 年以来，国家间网络攻防、供应链攻击、虚假信息传播、勒索软件、数据泄露、黑客攻击等安全事件层出不穷且危害性更强，对国家安全和产业稳定构成威胁。据波耐蒙研究所和 IBM Security 联合发布的报告显示，2022 年全球数据泄露规模和平均成本均创下历史新高，数据泄露事件的平均成本高达 435 万美元；Verizon《2022 年数据泄露调查报告》指出，2022 年针对软件供应商的网络攻击同比增长 146%，其中 62% 的数据泄露归因于供应链安全漏洞。同时，供应链攻击已成为大国角力中主要的网络攻击手段，软件业等国际化程度高、供应链条较长的产业将面临更加严峻的供应链安全风险。网络空间愈发激烈的角逐给全球安全态势带来更多不确定性严重恶化了我国网络安全

---

<sup>2</sup> 中国社科院世界经济与政治研究所《2023 年全球九大趋势展望》  
<https://baijiahao.baidu.com/s?id=1756735326631939871&wfr=spider&for=pc>

形势，对我国加强网络空间安全防护、维护供应链安全稳定提出了更高要求。

### **3. 网络攻击技术加快演进升级，网络安全挑战更加复杂多样**

2023 年，新技术新应用的涌现也为网络安全带来更大挑战。伴随 AI 大语言模型技术发展，网络攻击者通过使用 ChatGPT，用较低的成本通过 AI 技术生成攻击代码或垃圾邮件，从而大大降低网络攻击技术“门槛”；元宇宙相关技术加快应用可能造成更多窃取和仿冒数字身份事件发生，勒索或窃取数字账户将成为数字世界网络犯罪和攻击的主要方面；云原生技术的大量应用可能带来开源代码库漏洞、大量针对 API 接口的网络攻击等网络安全问题；量子计算机能够以更高速度执行复杂计算，可能被应用于操纵或破坏通信网络、导航系统甚至武器军事系统，甚至将改变未来战争形态和战争结果。大量技术的迭代升级带来愈来愈多的网络安全风险和挑战，需要政府和企业不断更新安全理念，形成合力，筑牢网络安全防线。

综上所述，2023 年，我国网络安全产业发展面临的形势依然复杂严峻，既有政策法规细化深入、数字经济赋能、技术迭代创新等发展机遇，也面临宏观经济下行、大国博弈更加复杂、网络攻击愈发多元等诸多挑战，网络安全产业将在暗礁险滩遍布的湍流中探索前行，需要具备更大勇气、更高

智慧、更强动力，以谋求更光明远大发展前景。

## 二、我国网络安全产业基本情况

### （一）我国网络安全企业总体表现

本报告所指网络安全企业包括三类：一是具备网络安全专用产品安全检测或安全认证证书，或者计算机信息系统安全专用产品销售许可证书的企业（即产品型企业）；二是具备中国信息安全测评中心或中国网络安全审查技术与认证中心服务资质证书的企业（即服务型企业）；三是拥有安全检测或安全认证证书，或者产品销售许可证，且拥有服务资质证书的企业（综合性企业）。

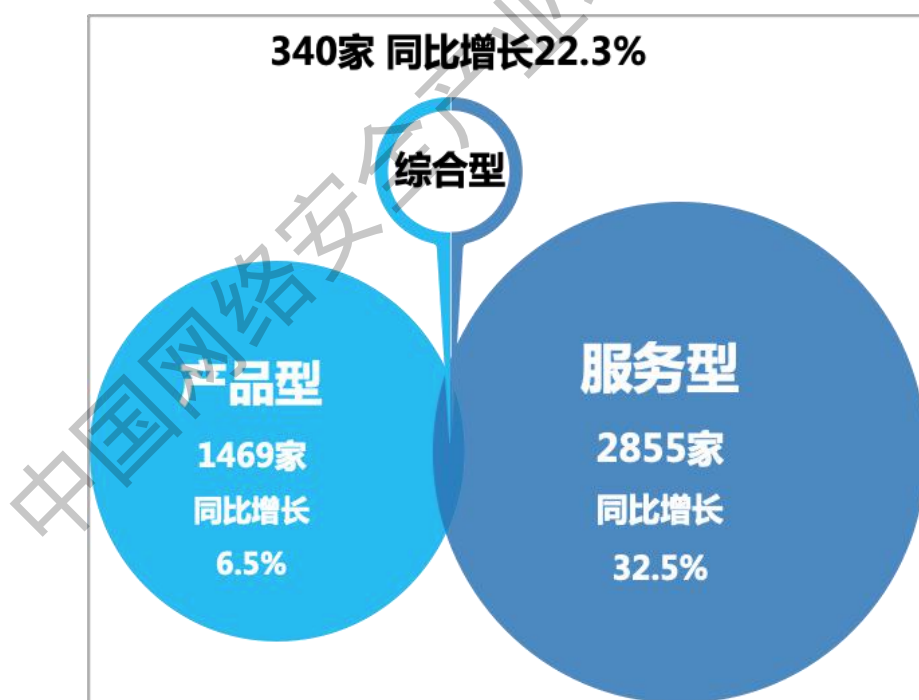


图 1 2023 年我国网络安全企业的总体构成

#### 1. 企业构成及分布

据 CCIA 统计，截至 2023 年上半年，我国共有 3984 家

公司开展网络安全业务，同比增长 22.4%，其中，服务型企  
业数量同比增长 32.5%，是网络安全企业数量增长的主要来  
源。这主要得益于疫情平稳转段后，企业服务资质申请数量  
的增长。

从过去两年来看，国内综合型厂商数量基本恢复到 2021  
年的水平，产品型厂商数量近两年持续上升，2023 年对比  
2021 年增长 15.6%，但服务型厂商数量对比 2021 年，仍然  
下降 25.3%。

## 2. 网络安全企业收入分析

截至 2023 年 6 月 30 日，我国已公开上市的网络安全企  
业共有 26 家。对 26 家上市网络安全企业数据的统计分析显  
示（见图 2），2022 年和 2023 年上半年网络安全上市公司  
营业收入都保持正增长的公司有 11 家。

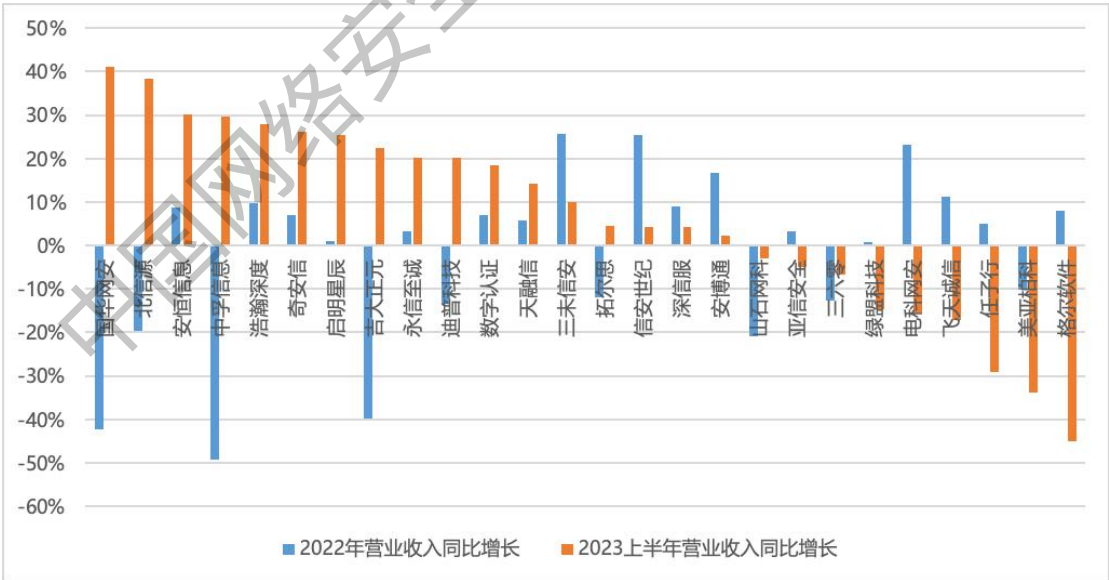


图 2 2022Q4-2023H1 我国网络安全上市公司营业收入同比增长率<sup>3</sup>

2023 年，尽管国内经济逐步复苏，但下游市场需求恢复

<sup>3</sup> 图 2 涉及数据为 CCIA 和数说安全基于巨潮资讯信息整理。

尚需时日。上半年，26家安全上市公司营业收入总和约200亿元（见表1），相较于2022年同期增长2.5%。其中，3家公司收入增速超过30%，7家公司收入增速在20%-30%之间，7家公司收入增速在0-20%之间，9家公司收入增速为负值。

表 1 2023 年上半年已公开上市的网络安全企业经营数据

序号	公司	营业收入 (亿元)	营业收入同比增长 %	扣非净利润 (亿元)	扣非净利润同比增长 %
1.	三六零	45.0	-6.6%	-2.6	49.5%
2.	深信服	29.3	4.2%	-5.9	23.7%
3.	奇安信	24.8	26.2%	-9.8	7.1%
4.	启明星辰	15.2	25.3%	-0.8	71.4%
5.	电科网安	11.4	-12.7%	-0.1	-485.4%
6.	天融信	10.0	14.2%	-2.2	6.8%
7.	绿盟科技	7.1	-14.7%	-4.3	-93.2%
8.	安恒信息	7.0	30.1%	-4.2	-9.7%
9.	亚信安全	5.6	-5.0%	-1.9	2.4%
10.	美亚柏科	4.6	-33.8%	-2.9	-119.2%
11.	拓尔思	4.4	4.6%	0.5	8.5%
12.	迪普科技	4.4	20.2%	0.3	14.3%
13.	数字认证	3.8	18.4%	0.0	14.3%
14.	山石网科	3.7	-2.9%	-1.2	-38.6%
15.	中孚信息	3.3	29.6%	-1.9	32.6%
16.	飞天诚信	3.3	-17.3%	-0.8	-204.8%
17.	北信源	3.2	38.3%	0.0	99.2%
18.	吉大正元	2.6	22.5%	-0.3	-19.6%
19.	浩瀚深度	2.4	28.0%	0.3	12.6%
20.	信安世纪	1.8	4.3%	-0.3	-236.4%
21.	任子行	1.8	-29.1%	-0.7	-38.1%
22.	格尔软件	1.6	-45.0%	-0.8	-24.0%
23.	安博通	1.5	2.2%	-0.8	-122.7%

序号	公司	营业收入 (亿元)	营业收入同比增长 %	扣非净利润 (亿元)	扣非净利润同比增长 %
24.	三未信安	1.0	10.1%	0.1	0.6%
25.	永信至诚	0.8	20.3%	-0.3	-56.3%
26.	国华网安	0.3	41.1%	-0.3	21.1%

## (二) 我国网络安全产业规模及市场集中度分析

### 1. 我国网络安全产业规模与增速情况

据国内网络安全主要企业调研数据分析显示，2022 年，我国网络安全市场规模约为 633 亿元，同比增长 3.1%。近三年行业总体保持增长态势，但受宏观经济等因素影响，网络安全行业增速持续放缓（见图 3）。

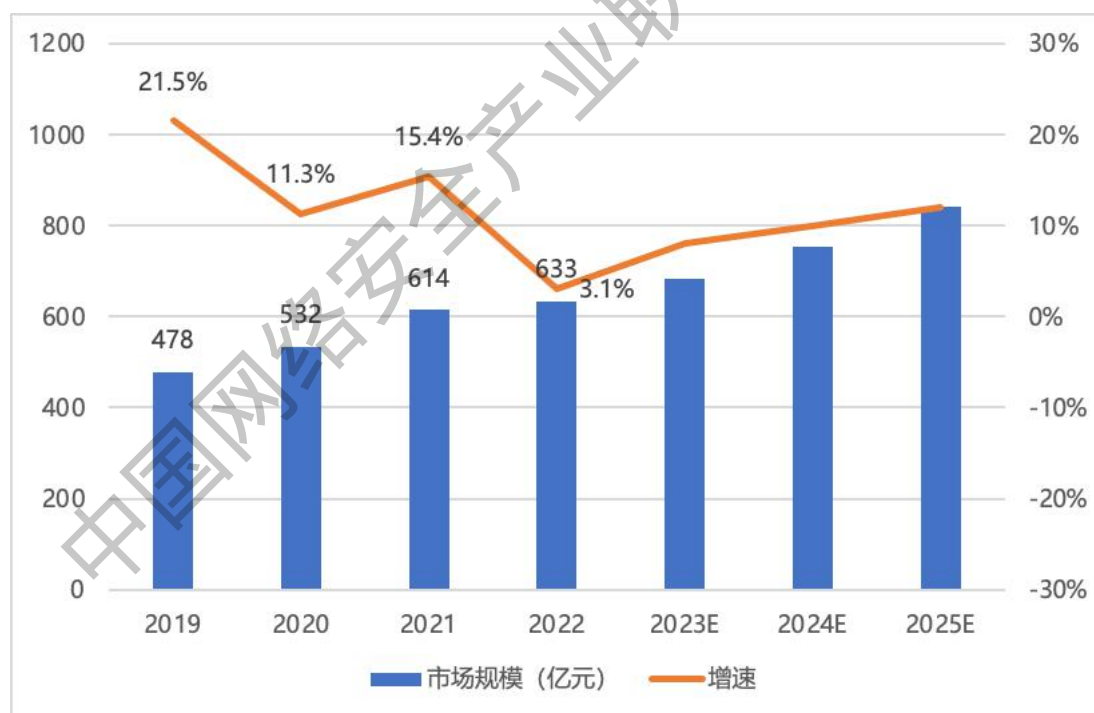


图 3 2022 年中国网络安全市场规模及增速

展望未来三年，网络安全产业发展顶层设计更加完善，促进行业发展的政策基础愈加稳固，数字经济加速发展等正

向激励将给网络安全产业注入新动力，产业结构调整逐步深化，更多网络安全板块将涌现出来，预计网络安全产业将保持 10%以上的增速，到 2025 年市场规模将超过 800 亿元。

## 2. 我国网络安全产业集中度分析

根据美国经济学家贝恩对产业集中度的划分标准，2022 年，我国网络安全市场集中度  $CR_n$ <sup>4</sup>具体表现为， $CR_1$  为 9.83%， $CR_4$  为 28.59%， $CR_8$  为 44.91%，网络安全市场集中度进一步提升（见图 4）。此外，2018-2022 年，领军企业的市场份额始终保持上升趋势，前四名企业的市场份额已经从 2018 年的 21.71% 升至 2022 年的 28.59%。领军企业以先发优势筑起更高的行业进入门槛，新晋企业需要找到创新和差异化的方式，在市场找到自身定位。

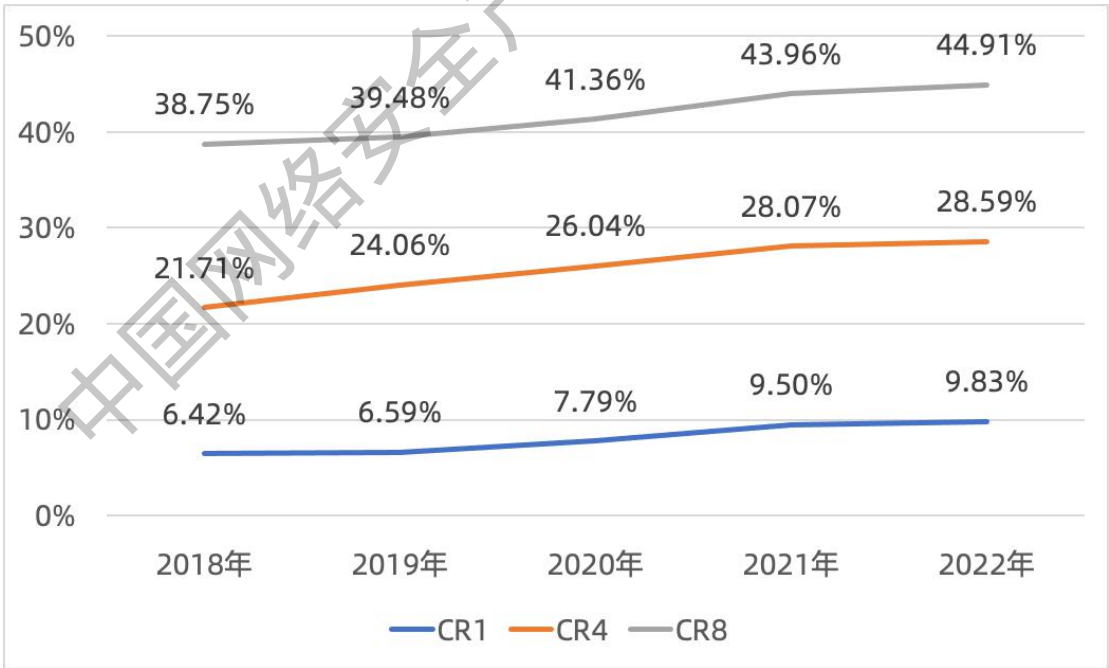


图 4 近五年中国网络安全行业集中度分析

<sup>4</sup> CR 是 Concentration Ratio 的缩写，中文含义为行业集中度（或行业集中率、市场集中度）。 $CR_n$ （如  $CR_1$ 、 $CR_4$ 、 $CR_8$ ）是指某行业内或相关市场内规模最大的前  $n$  家企业的收入占市场份额（营业收入）的总和。 $CR_n$  值越小则竞争越激烈，越大则越集中。



从主要企业市场占有率看，奇安信、启明星辰、深信服和天融信四家企业的市场占有率均超过了 5%（见图 5）。预计未来数年，领军企业市场占有率仍将保持小幅增长趋势。

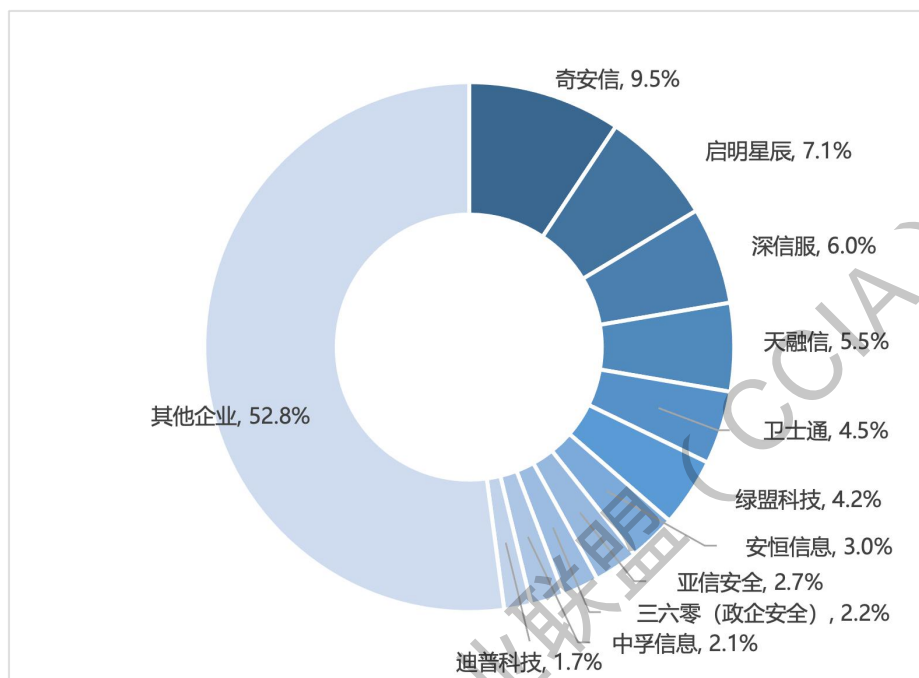


图 5 2022 年中国网络安全行业主要企业市占率情况

### （三）我国网络安全市场区域分布及增速分析

通过对国内网络安全企业调研数据和网络安全上市公司的公开数据进行综合分析，得出以下结论：

分区域来看，2022 年，华北、华东和华南等经济发达地区对网络安全的投入进一步加大，区域市场占比有所提升（见图 6）。同时，网络安全企业积极响应共建“一带一路”倡议，加快探索海外市场。深信服、奇安信和绿盟科技等领军企业海外业务发展良好，创新型企业积极尝试突破，2022 年取得一定成绩，海外市场占比小幅提升。预计未来海外市



场将成为中国网络安全企业新的业务增长点。

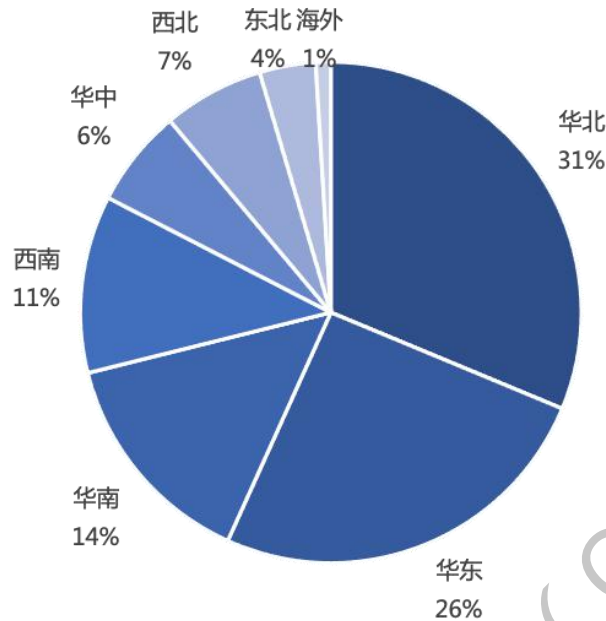


图 6 2022 年中国网络安全市场区域分布

分省市来看，2022 年，大部分省市的网络安全项目量增速保持正增长（见图 7），但受宏观经济形势影响，各省市增速分化较为明显，网络安全市场的区域分布呈现不均衡态势。

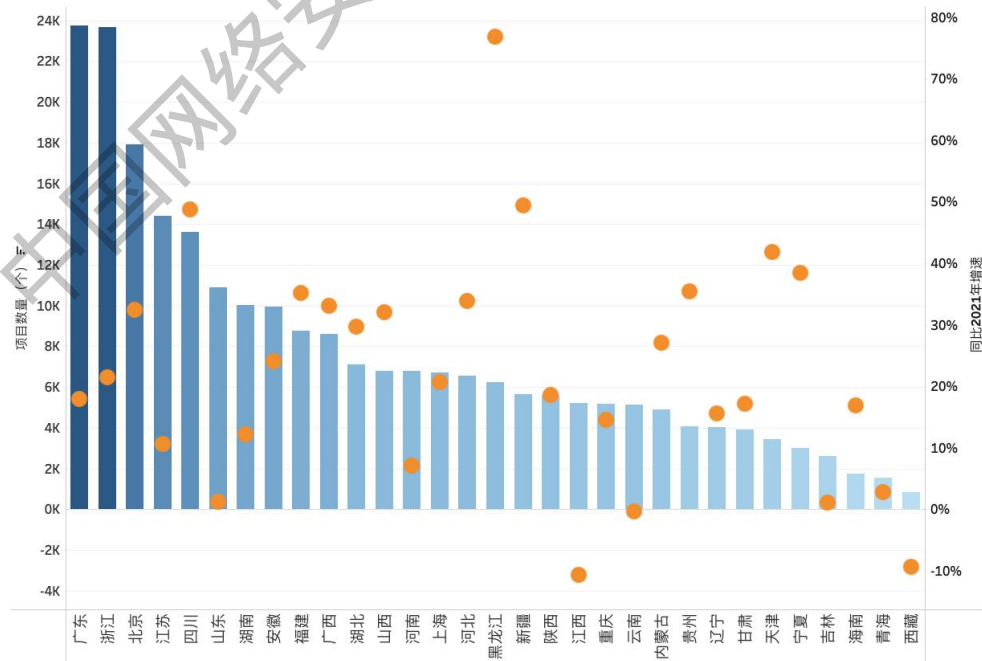


图 7 2022 年中国网络安全项目数量省市分布及增速

#### （四）我国网络安全客户所属行业分布及增速分析

数说安全分析数据显示，2018 年至今，中国网络安全客户总量超过 15.8 万家，2022 年发生网安项目采购行为的客户有 67183 家，过去三年持续在网络安全投入的客户超过 2 万家。

从区域分布来看，网络安全客户主要分布在京津冀、长三角和珠三角地区，川渝地区客户数量增长显著，逐渐成为新的聚集区（见图 8）。



图 8 中国网络安全客户地图

从行业分布来看，政府部门因政策监管严格，其信息系统涉及国计民生和国家安全等重要业务，对网络安全项目的需求较大，依然占据最大份额；教育、医疗卫生、公检法司、能源化工等与国计民生紧密相关的领域紧随其后，也有较大占比（见图 9）。

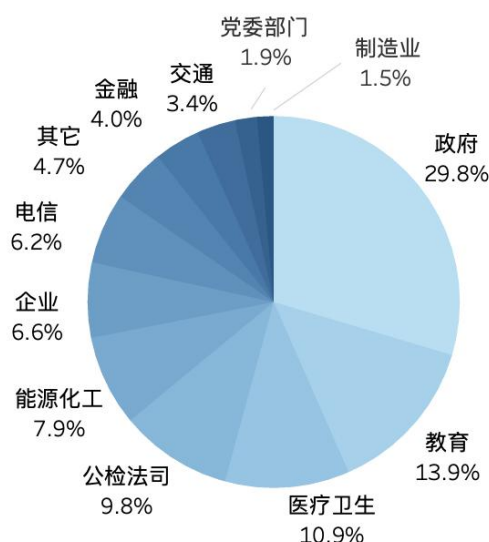


图 9 2022 年中国网络安全项目数量行业分布

### （五）我国网络安全客户产品需求热度分析

2022 年，我国网络安全产品需求呈现等保合规类产品为主流（见图 10），新产品和新应用不断孕育，部分传统安全产品需求降低的态势。具体来看：首先，网络安全市场需求受国家相关热点法规政策影响仍然显著，等保合规类产品需求依旧旺盛，市场占有率较高；但因用户基础网络安全建设逐渐趋于完备，市场增长率相对较低。其次，由新技术和新场景孕育而出的一系列新产品和新应用（见图 10 左上角）尚处于探索推广阶段，市场规模较小，增速较快。预计未来受政策要求、安全事件等因素影响，市场需求将持续释放。再次，负载均衡、数据库防火墙等部分传统安全产品采购热度降低，增速为负。可以预见，一些功能较为单一的传统安全产品未来将逐渐作为某些功能特性，被整合进通用型的安全产品，亦或者被更先进的技术产品所取代。



图 10 2022 年中国网络安全产品采购趋势

## （六）我国网络安全市场分类及全景图

受到更加复杂多变的网络安全事件和快速迭代创新的网络安全技术刺激，传统的单点防御加速向点线面一体化的综合防御进化，并已形成了一定的市场规模。基于对各细分市场市场发展状况、市场成熟度、品牌渗透率、技术发展趋势的综合研判，形成 2023 年中国网络安全市场分类架构图（见图 11），涵盖七大基础安全领域（网络与基础架构安全、端点安全、身份与访问管理、应用安全、数据安全、开发安全、安全管理）、六大安全解决方案（零信任、数据安全治理、威胁管理/XDR、攻击面管理、安全运营/MDR/MSS、安全访问服务边缘）、四大应用场景（云安全、移动安全、物联网安全、工业互联网安全），以及九大安全服务（安全方案与集成、安全运维、风险评估、渗透测试&红蓝对抗、应急响应、攻防实训/靶场、培训认证、安全意识教育、安全众测），

涉及产品、解决方案、应用场景、服务四个维度，覆盖了目前我国网络安全行业所有成熟的细分市场。



图 11 中国网络安全市场分类架构示意图

基于网络安全市场分类架构图，报告系统梳理了我国网络安全企业构成，形成了 2023 年中国网络安全市场全景图（见图 12）。受外部环境变化、国家政策驱动、应用场景变迁、资本市场助力、全民安全意识提升等多方面因素影响，我国网络安全产业进入群雄逐鹿、百花齐放的阶段，国内企业积极探索、勇于创新，新技术、新产品不断涌现，在一些技术领域我国网络安全产品和服务水平已接近或达到国际一流水准。同时，从中短期来看，尽管网络安全产业集中度不断提高，但中小型企业数量仍然很多，市场碎片化特征依

旧会延续，这有利于产业的进步和发展，但对于网络安全企业来说，市场竞争将更加激烈，更多企业需要直面淘汰出局的风险。

中国网络安全产业联盟 (CCIA)





图 12 2023 年中国网络安全市场全景图

### 三、我国网络安全企业竞争力与产业格局

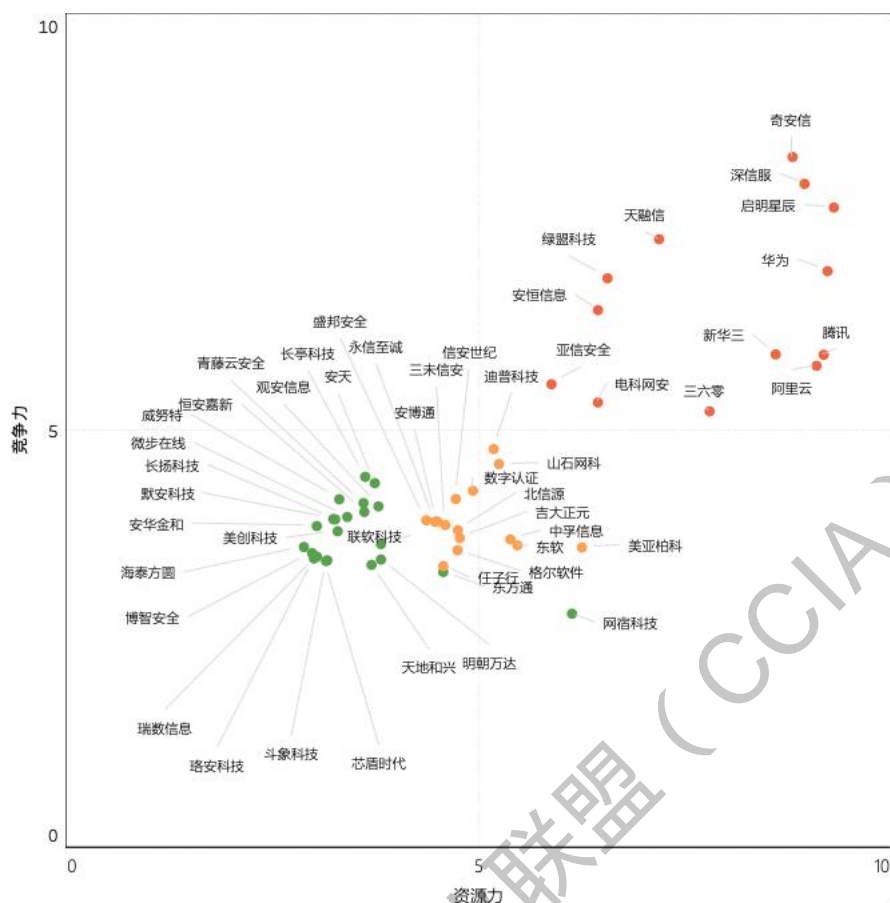
#### （一）我国网络安全企业竞争力评估

根据公司生命周期理论，网络安全企业的发展可分为初创期、成长期、成熟期、衰退期四个阶段。鉴于网络安全产业仍处于增长阶段，本报告重点针对初创期、成长期和成熟期的网络安全企业进行竞争力评估分析（评估标准和分析方法见附件二），并评选出代表成熟期企业的“CCIA 50 强”、代表成长期企业的 20 家“CCIA 成长之星”以及代表初创期企业的 30 家“CCIA 潜力之星”。通过对以上 100 家企业样本进行分析，得出以下结论：

##### 1. 网络安全成熟期企业竞争力分析

成熟期企业主要覆盖了中等规模以上的网络安全企业，其安全业务年收入普遍在 1 亿元以上，安全业务毛利达到 1 亿元左右。成熟期企业分布如图 13 所示，右上角领军企业都已成为上市公司，资源力和竞争力表现均十分突出。领军企业之间的竞争较为激烈，其发展也呈现分化趋势，未来一段时间将会延续这种竞争态势。





## 2. 网络安全成长期企业和初创期企业竞争力分析

虽然成长期企业已经具备一定的规模 and 市场份额，但是他们和成熟期企业的差距正在扩大。部分成长期企业在经历了早期快速增长后，业务开始放缓或遭遇瓶颈，需要寻找新的增长点，否则较难向成熟期企业过渡，当前所处市场地位也可能受到威胁。

初创期企业在网络安全细分领域具有独特的创新优势，尽管在技术成熟度和市场营销能力上还有待提高，但其创新能力和发展潜力受到了投资界的关注。

## （二）我国网络安全产业竞争格局

从产业竞争格局的角度来看，我国网络安全企业可以划分为领导者、战略布局者、成长者和创新者（见图 14）。

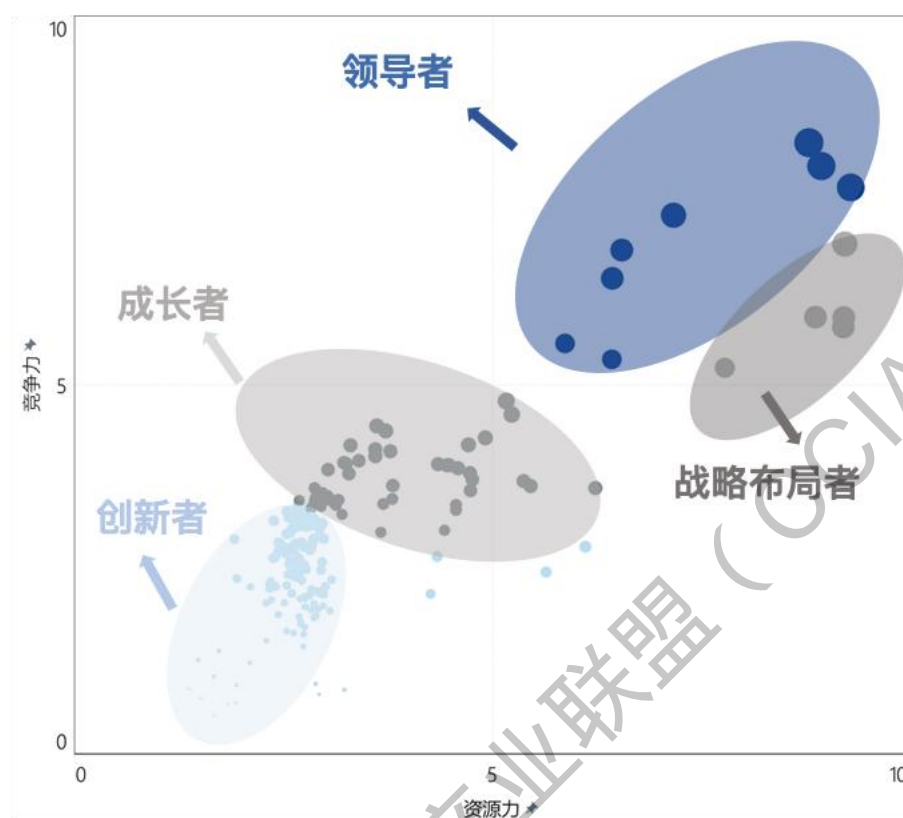


图 14 2022 年中国网络安全产业竞争格局

1. **领导者：**产业领导者均为上市公司，资源力和竞争力均十分突出，大多处于发展成熟期。领导者之间的竞争较为激烈，并呈现出“强者愈强”的分化趋势，未来一段时间这种竞争态势将会延续。

2. **战略布局者：**战略布局者多为 IT 龙头企业、大型互联网企业以及国有企业等，尤其是国有企业正在逐渐成为网络安全产业的重要参与者。

3. **成长者：**成长者一般具有一定规模，形成了较为成熟的商业模式，业务方向相对聚焦，部分企业已上市或接近上市标准。总体来看，成长者与领导者的资源和竞争力差距

正在扩大，部分成长者收入第二增长曲线放缓，市场地位受到威胁。

4. **创新者：**大部分创新者成立时间较短，商业模式尚不够成熟。尽管在技术成熟度和市场营销能力上还有待提高，但因其创新属性强和发展势能足等特征备受投资界关注。

综上所述，网络安全产业领导者与其他企业的差距仍在扩大；以大型国有企业和三大电信运营商为代表的战略布局者持续加大网络安全业务投入，将对产业竞争格局产生重大影响，带来新的变化；创新者和成长者也将因此面临更大的挑战，需要规划新的发展战略，寻找新的发展路径和业务增长点。

## 四、我国网络安全资本市场分析

### （一）我国主要网络安全企业经营情况分析

我国网络安全资本市场分为一级市场和二级市场。报告选取 2022 年已上市的 26 家网络安全企业中的 20 家作为分析样本，通过对其经营数据进行分析，以了解我国网络安全的总体经营情况，原因如下：一是部分企业为混业经营，上市主体中包含非安全业务且占比较高，因此未列入本次数据选取范围（见表 2）；二是与一级市场的网络安全企业数据相对不透明不同，二级市场的企业经营数据定期公开，数据

可获得性高；三是样本企业在 2022 年的收入占国内网络安全市场份额超过 60%，在一定程度上可反映网络安全企业总体经营状况<sup>5</sup>。

表 2 公开上市的网络安全企业 2022 年经营情况

交易所	板块	证券代码	公司	营业收入 (亿元)	扣非净利润 (亿元)	是否选为样 本企业
上海	科创板	688561.SH	奇安信	62.2	-3.1	是
上海	科创板	688489.SH	三未信安	3.4	1.0	是
上海	科创板	688292.SH	浩瀚深度	4.5	0.5	是
上海	科创板	688244.SH	永信至诚	3.3	0.4	是
上海	科创板	688225.SH	亚信安全	17.2	0.1	是
上海	科创板	688201.SH	信安世纪	6.6	1.6	是
上海	科创板	688168.SH	安博通	4.6	-0.2	是
上海	科创板	688030.SH	山石网科	8.1	-2.1	是
上海	科创板	688023.SH	安恒信息	19.8	-3.0	是
上海	主板	603232.SH	格尔软件	6.6	-0.5	是
上海	科创板	601360.SH	三六零	95.2	-18.6	否
深圳	创业板	300768.SZ	迪普科技	8.9	1.4	是
深圳	创业板	300579.SZ	数字认证	11.0	1.0	是
深圳	创业板	300454.SZ	深信服	74.1	1.0	是
深圳	创业板	300386.SZ	飞天诚信	8.7	-1.2	否
深圳	创业板	300369.SZ	绿盟科技	26.3	0.1	是
深圳	创业板	300352.SZ	北信源	5.4	-1.9	是
深圳	创业板	300311.SZ	任子行	7.3	-0.2	否
深圳	创业板	300229.SZ	拓尔思	9.1	0.8	否
深圳	创业板	300188.SZ	美亚柏科	22.8	0.9	否
深圳	中小板	003029.SZ	吉大正元	4.9	-0.4	是
深圳	中小板	002439.SZ	启明星辰	44.4	5.2	是
深圳	中小板	002268.SZ	电科网安	34.4	2.6	是
深圳	中小板	002212.SZ	天融信	35.4	1.5	是
深圳	中小板	000004.SZ	国华网安	1.7	-5.9	否
深圳	创业板	300659.SZ	中孚信息	6.4	-4.7	是

从营业收入来看，2022 年，样本企业安全业务营业收入

<sup>5</sup> 网络安全市场和企业收入呈现较为突出的季节性分布特征，下半年收入占全年比例较高，因此，为更加科学准确地分析企业经营情况，报告选取 2022 年全年企业经营数据进行分析。

合计 387.6 亿元，同比增长 3.1%。其中，安全业务收入超过 10 亿元的有 9 家；超过 20 亿元的有 6 家，分别是深信服、奇安信、启明星辰、天融信、电科网安和绿盟科技（见图 15）。

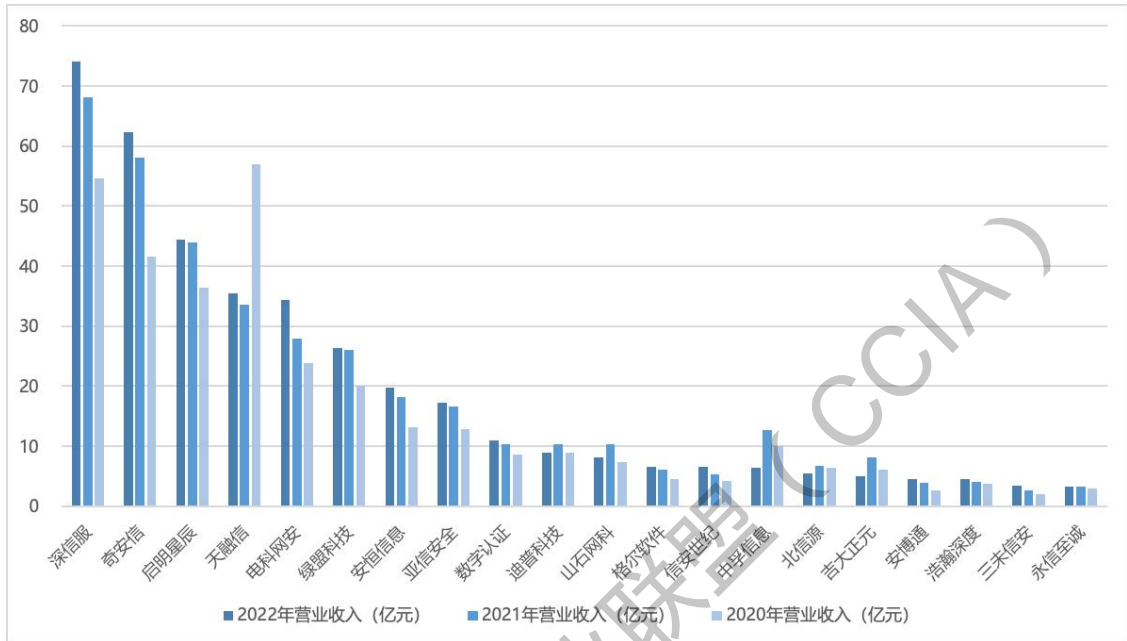


图 15 2020-2022 年样本网络安全企业安全业务营业收入

从营收增长情况来看，2022 年，样本企业中，4 家收入同比增长超过 10%，5 家收入出现负增长。16 家收入增速为正，收入增速最高的三家企业为三未信安、信安世纪和电科网安（见图 16）。

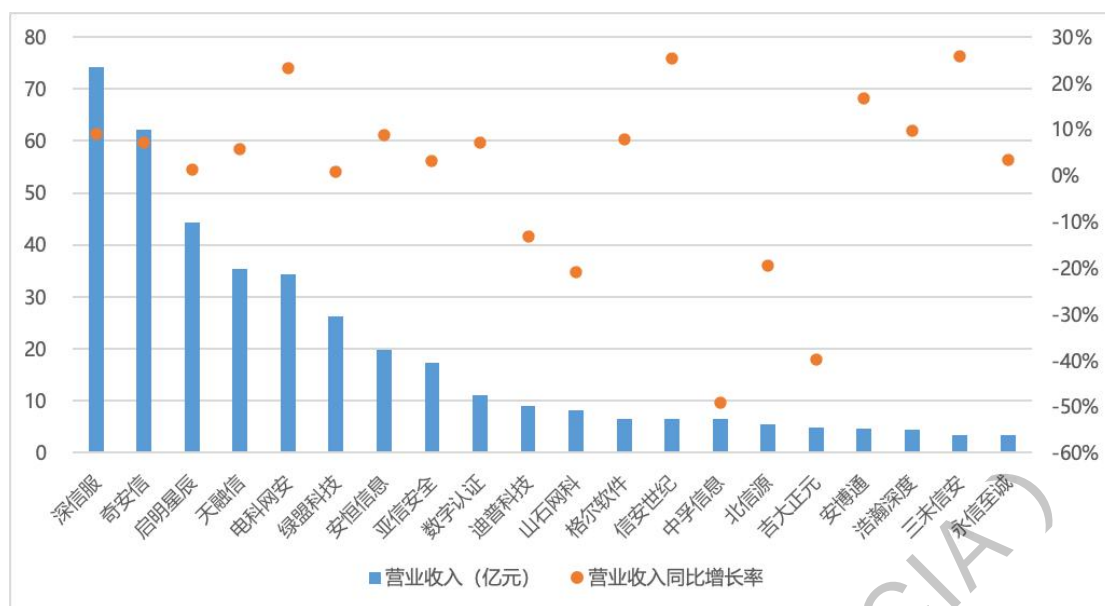


图 16 2022 年样本企业安全业务营业收入及营收增长情况

从盈利能力来看，2022 年，样本企业盈利能力持续下滑，26 家企业中有 12 家盈利，6 家亏损（见图 17），扣非净利润不足 1 亿。

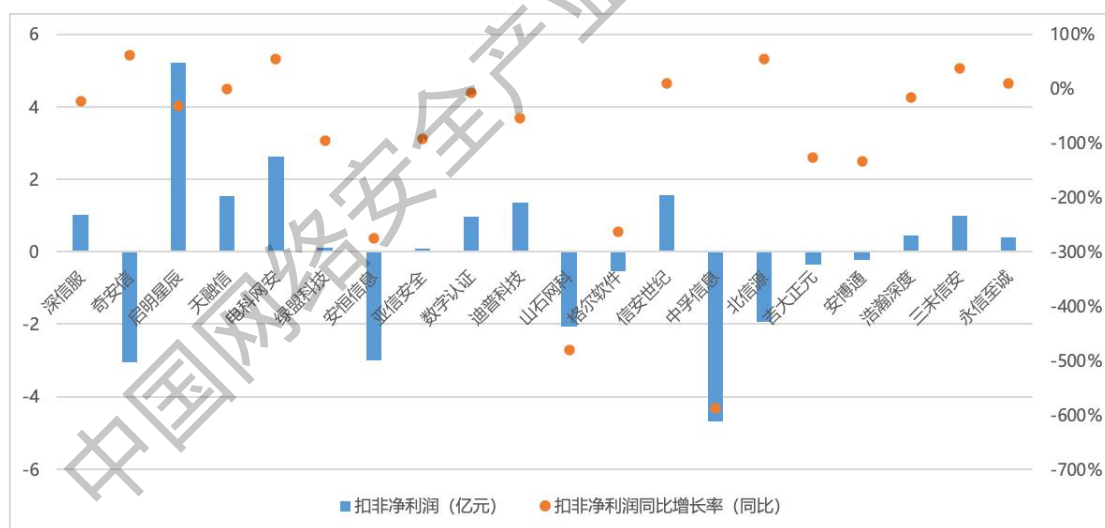


图 17 2022 年样本网络安全企业安全业务盈亏状况

2022 年，我国网络安全企业继续加大研发和销售投入，样本企业研发和销售费用合计达到 203 亿元，占企业营业收入的 54.0%。其中，销售费用为 106.7 亿元，同比增长 10.4%，研发费用达到 96.3 亿元，同比增长 9.5%。此外，有 8 家企

业的四项费用率（销售费用率+研发费用率+管理费用率+财务费用率）超过 60%（见图 18），相较于 2021 年的 4 家，有大幅上升，显示出越来越多的企业盈利空间受到压缩。

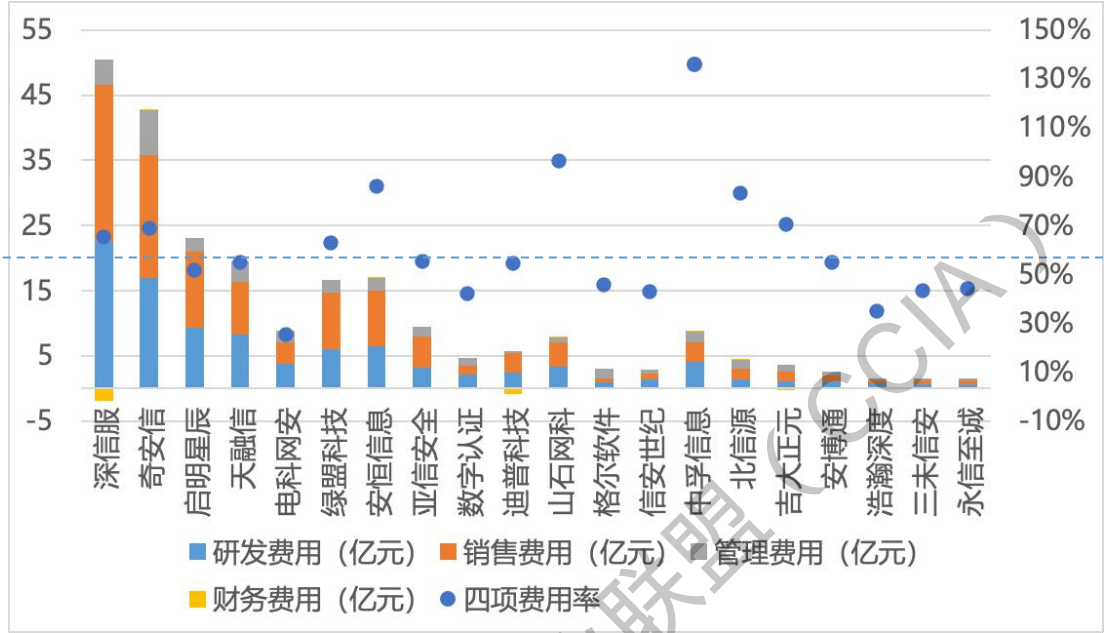


图 18 2022 年样本企业费用以及四项费用率构成

从企业现金流量来看，如图 19 所示，2022 年，样本企业的经营性现金流净额合计为-17.24 亿元，相较于 2021 年同期的 24.89 亿元，下滑显著。更加需要引起重视的是，2022 年行业整体经营性现金流净额首次出现转负的情形。此外，投资活动产生的现金流净额合计为-17.78 亿元，筹资活动产生的现金流净额合计为 44.89 亿元。



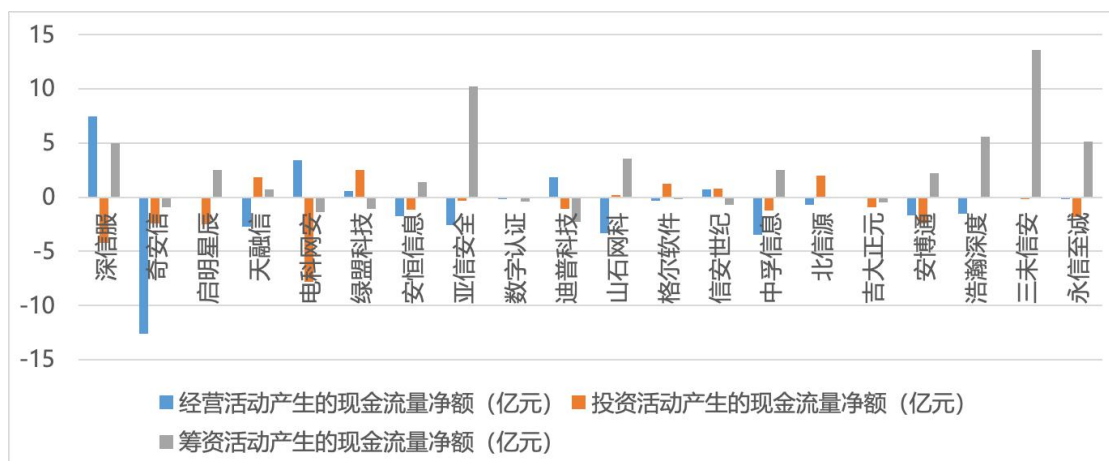


图 19 2022 年样本企业现金流净额

综上所述，2022 年，受宏观经济不振和行业竞争加剧等因素影响，我国网络安全企业经营状况普遍挑战增大，收入增速放缓，盈利能力和现金造血能力进一步下滑。

## （二）我国网络安全产业资本市场表现

我国网络安全上市企业总市值规模从 2018 年底开始急剧增长，2021 年创历史新高，总市值接近 4000 亿，2022 年 5 月回落至近 2000 亿，2023 年 4 月总市值再次攀升至 3400 亿，较 2022 年最低点上涨约 90%（见图 20）。

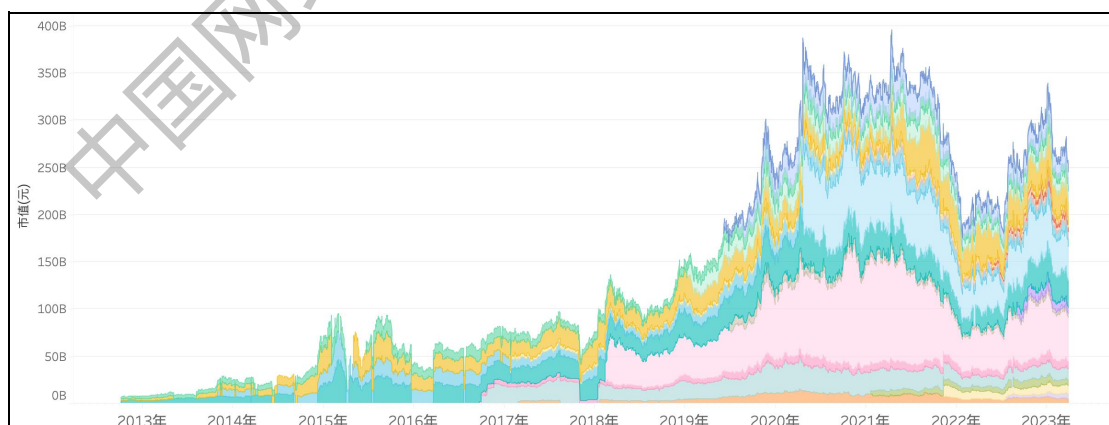


图 20 2013-2023 年中国上市网络安全企业市值动态

截至 2023 年 6 月 30 日，国内网络安全上市企业 PS-TTM



中位数<sup>6</sup>为 6.6，PE-TTM（扣非）中位数<sup>7</sup>为 19.4（见图 21），上市企业整体估值有所回升，但仍处于底部。

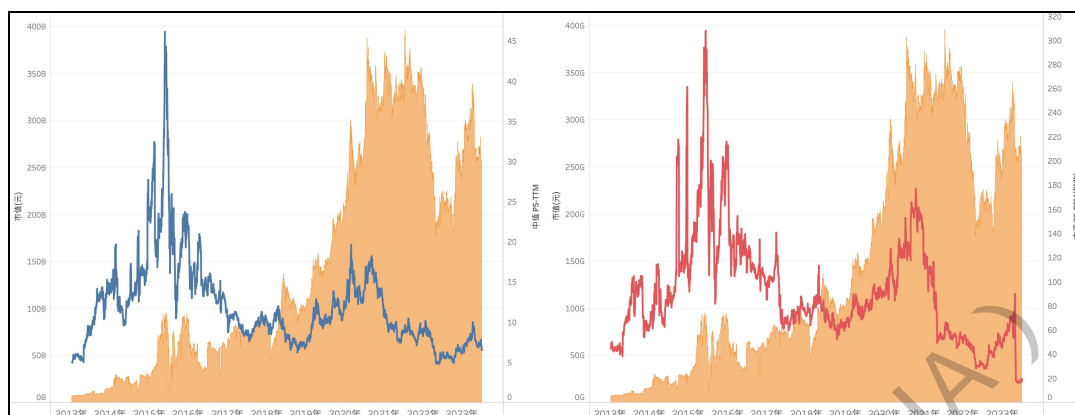


图 21 2013-2023 年中国上市网络安全企业估值动态

“十四五”期间，网络安全重要性越发凸显，网络安全产业的发展壮大具有较强的确定性。在成长性确定和低估值的双因素推动下，网络安全产业有望再次吸引资本的关注和投入。

### （三）我国网络安全企业 IPO 动态

2022 年，亚信安全、三未信安、浩瀚深度和永信至诚成功登陆科创板；2023 年，盛邦安全成功登陆科创板。同时，网络安全企业在科创板的 IPO 申报节奏正在回归常态，明朝万达和渔翁信息 2 家网络安全企业处于申报进程中。

<sup>6</sup> PS-TTM 计算公式为：市值/[期末营业总收入+(期初全年营业总收入-期初营业总收入)]。文中的 PS-TTM 中位值指的是过去 10 年网络安全行业的 PS-TTM 中值，代表市场的近 10 年的平均水平。

<sup>7</sup> PE-TTM（扣非）计算公式为：市值/[期末归属于母公司普通股股东的扣非净利润+(期初全年归属于母公司普通股股东的扣非净利润-期初归属于母公司普通股股东的扣非净利润)]。文中的 PE-TTM（扣非）中位值指的是过去 10 年网络安全行业的 PE-TTM（扣非）中值，代表市场的近 10 年的平均水平。

表 3 2020-2023 年网络安全企业上市进程情况

序号	企业名称	当前状态	板块	受理时间	更新时间	上市时间	上市历经天数	发行市值（亿元）	最新市值（亿元）
1	奇安信	上市	科创板	2020/5/11	2020/7/7	2020/7/22	72	381	347
2	信安世纪	上市	科创板	2020/6/29	2021/3/25	2021/4/21	296	25	56
3	亚信安全	上市	科创板	2021/3/12	2022/1/10	2022/2/9	334	122	78
4	浩瀚深度	上市	科创板	2021/6/21	2022/4/29	2022/8/18	423	26	40
5	永信至诚	上市	科创板	2021/6/30	2022/3/1	2022/10/19	476	23	49
6	三未信安	上市	科创板	2021/12/21	2022/6/6	2022/12/2	346	15	63
7	盛邦安全	上市	科创板	2022/6/28	2023/5/17	2023/7/26	393	30	38
8	明朝万达	已问询	科创板	2022/12/30	2023/6/28	n/a	n/a	n/a	n/a
9	渔翁信息	已问询	科创板	2022/12/29	2023/4/26	n/a	n/a	n/a	n/a
10	联软科技	终止	科创板	2021/6/23	2022/1/1	n/a	n/a	n/a	n/a
11	齐治科技	终止	科创板	2020/11/5	2021/3/1	n/a	n/a	n/a	n/a
12	溢信科技	终止	科创板	2020/6/23	2020/10/28	n/a	n/a	n/a	n/a

#### （四）我国网络安全产业投融资情况

2022 年，受宏观环境影响，网络安全一级市场投资热度下滑较多，网络安全产业融资事件共有 124 起，同比下降 32.6%；融资额为 67.8 亿元，同比下降 49.9%（见图 22）。

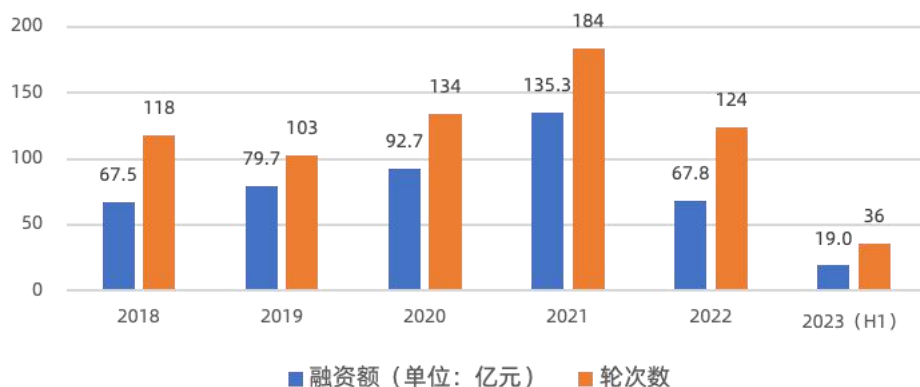


图 22 2018-2022 年中国网络安全领域融资事件数量金额比较

2022 年，单笔融资额达到亿元以上的融资有 13 起，千万级的有 47 起，千万级以上融资事件数量占全年融资数量为 48.4%。与 2021 年相比，千万级以上融资事件占比降幅较大。

2022 年，投资机构对于网络安全项目的投资变得更加谨慎，尤其是成长期和中后期项目受影响较大。早期项目获投数量增长较快。随着注册制改革加速及北交所开市，网络安全投资退出通道进一步丰富，将对网络安全投资产生正向激励。

表 4 2022 年-2023 年网络安全企业（一级市场）融资（亿元级）情况

时间	公司简称	轮次	交易金额	投资方
2022/2/24	未来智安	A 轮	亿元级别	君联资本、泰岳梧桐资本
2022/2/25	青藤云	F 轮	未披露	博裕资本、丰厚资本、大湾区共同家园发展基金
2022/3/22	悬镜	B 轮	数亿元	源码资本、GGV 纪源资本、红杉中国，腾讯投资
2022/3/28	微步在线	E+轮	超 3 亿元	鼎晖投资、星路资本

时间	公司简称	轮次	交易金额	投资方
2022/3/29	亿格云	Pre-A 轮	近亿元	红杉中国种子基金
2022/3/30	默安科技	D 轮	3 亿	博裕资本、中金资本
2022/4/14	芯盾时代	D 轮	数亿元	启宸资本、光远资本、临港科创投、朗玛峰创投
2022/4/20	华顺信安	C 轮	数亿元	招银国际资本、高榕资本、首建投、招商局中国基金、红树成长
2022/5/30	天地和兴	D 轮	数亿元	复星创富、国家电投、电科投资、松禾资本、国科嘉和、苏州国发创投，国网产业基金、银杏谷资本、中叶资本、南钢股份、尚硕资本
2022/6/6	威努特	pre-IPO 轮	数亿元	广州工控资本管理有限公司领投、国开制造、上海国和投资、深投控与农银国际合作基金跟投
2022/7/18	珞安科技	C 轮	超 5 亿	中金资本、联通、上汽恒旭、国铁建信、容腾 5G 产业基金
2022/11/1	六方云	C+轮	数亿元	北京创新产业投资有限公司、德厚投资
2022/12/29	长扬科技	F 轮	近 3 亿元	曦域资本、景泰投资
2023/1/15	云天安全	A 轮	1.22 亿元	山东发展投资集团、泰山创投、乐知基金、高华投资
2023/1/17	烽台科技	B 轮	2.5 亿元	中网投、毅达资本、贵州创新赋能大数据投资基金、元起资本、中信建设资本、火山石资本、贵阳创投
2023/2/3	观安信息	E 轮	近 3 亿元	国鑫创投、国家制造业转型基金、卓戴资本
2023/5/23	领信数科	B 轮	超亿元	晨壹并购基金
2023/6/6	烽台科技	B+轮	1.2 亿元	中化基金、中移北京基金

## 五、我国网络安全产业发展热点分析

基于对行业领军企业、研究机构，以及权威的网络安全领域专家进行问卷调查和深度访谈，结合对国内外网络安全

技术发展趋势的综合研判，从网络安全技术、服务和治理三个维度，提出 10 项网络安全产业发展热点：

### （一）生成式人工智能

随着 OpenAI 推出 ChatGPT，生成式人工智能（AIGC）和大语言模型技术在全球范围内掀起浪潮。生成式人工智能技术更被 Gartner 公司评为 2022 年十二大战略性技术趋势第一位<sup>8</sup>，多个科技巨头重点布局并持续加大投入。其中，谷歌推出生成式人工智能聊天机器人 Bard 和大型视觉语言模型 PaLM 2，微软更新升级搜索引擎必应（Bing）应用了生成式预训练大模型 4 技术（GPT-4），META 公司发布人工智能大型语言模型 LLaMA 等。国内方面，百度“文心一言”、阿里“通义千问”、科大讯飞“星火认知”、腾讯“混元助手”、华为“盘古”等相继推出，生成式人工智能大规模兴起。

生成式人工智能技术是指具有文本、图片、音频、视频等内容生成能力的模型及相关技术<sup>9</sup>。基于大模型高算力训练基础，生成式人工智能具备自动化内容创作、大规模数据分析等功能优势，广泛应用于对话聊天、图像生成、自然语言处理、游戏开发、金融分析等领域，但也带来一定法规风险和伦理挑战，如数据源违规收集、算法失控、内容真实性可

<sup>8</sup> Gartner. Gartner identifies the top strategic technology trends for 2022. <https://www.gartner.com/en/newsroom/press-releases/2021-10-18-gartner-identifies-the-top-strategic-technology-trends-for-2022>.

<sup>9</sup> 《生成式人工智能服务管理暂行办法》（国家互联网信息办公室 中华人民共和国国家发展和改革委员会 中华人民共和国教育部 中华人民共和国科学技术部 中华人民共和国工业和信息化部 中华人民共和国公安部 国家广播电视总局令第 15 号）2023-07

靠性存疑、隐私保护确认、知识产权侵害以及不正当竞争等问题<sup>10</sup>。从攻击角度看，大语言模型的代码自动化等功能将会降低网络攻击门槛，如生成更加逼真的虚假图像或钓鱼邮件，甚至自动生成恶意软件代码等，此外，针对 AI 算法的攻击，如数据投毒、对抗样本、成员推断、模型萃取等攻击方式，为生成式人工智能的广泛应用带来严重威胁，也使得网络安全监管难度进一步提升。

未来，随着大语言模型技术与多模态技术加速融合，生成式人工智能将应用于更多场景，特别是在网络安全领域具备不可估量的发展潜力，如智能化威胁检测和响应、自动化安全防护和修复、实时威胁情报和预测、自适应安全策略和防御、人机协同防御等。因此，政府和业界应在鼓励其技术发展和行业应用的同时，直面风险挑战，建立统筹发展与安全、符合客观规律和发展阶段的赋能型监管理念。

## （二）人工智能对抗攻防技术

近年来随着数据量的爆发式增长、深度学习算法优化改进、计算能力大幅提升，AI 技术呈现跨越式发展趋势，在计算机视觉、自然语言处理、自动驾驶等领域取得了突破性进展。与此同时，AI 安全性和鲁棒性问题引起了业内高度关注，对抗样本攻击与防御技术是其中受到关注度最高的研究方向之一，学术界和产业界提出了多种典型的攻击和防御方

---

<sup>10</sup> 马永强.生成式人工智能的风险挑战与监管框架.中国信息安全,2023-04.

法，两者之间的对抗也在不断进化演绎。

AI 对抗攻防技术是人工智能对抗样本攻击与防御技术的简称，其中，对抗样本指的是对原始样本添加微小扰动的样本，以欺骗 AI 算法，使其产生错误输出结果。因此，AI 对抗样本攻击与防御技术是指围绕人工智能算法和应用，设计对抗样本进行攻击或开展针对性防御的技术。近年来，AI 对抗攻防技术广泛应用于自动驾驶、医疗卫生、金融应用等领域。AI 智能系统的非正常运行将直接危害人身安全和财产安全，AI 对抗攻防技术作为挖掘模型对抗安全风险并进行防御的关键手段，其发展面临以下难点<sup>11</sup>：一是深度网络模型存在技术脆弱性，由于 AI 技术中广泛使用的深度学习模型参数规模大、体系结构复杂，预训练需要海量的数据，将导致攻防技术主要聚焦在单点上，对抗样本的影响难以真正消除；二是现有防御能力不足，面对不断演进的对抗样本攻击，主流的防御方式鲁棒性泛化能力弱，防御方法跟进滞后，针对某种对抗攻击的防御方法通常难以适用于其它攻击方法。

当前，AI 对抗攻防技术正处于由学术研究转化为商业应用的探索期，大量科技企业、科研院所和高校纷纷入场，在 AI 安全工具、工业互联网、模型鲁棒性基准测试等场景开展实践探索，并开辟出一些应用场景，例如，目前已经出现 Cleverhans、Foolbox、ART、Advbox 等支持学术研究的开源

---

<sup>11</sup> 北京百度网讯科技有限公司.《AI 对抗攻防技术发展研究报告》.2022-11

工具，以及利用对抗样本攻击评测计算机视觉模型安全性的商用平台 RealSafe。阿里巴巴、腾讯、百度等科技企业通过举办人工智能对抗攻防大赛，积极发现针对人脸识别、图像分类、文本分析、目标检测等人工智能典型应用的有效对抗样本攻击和防御方法，并在关乎人身安全、财产安全以及国家社会安全的重要领域，探索人工智能应用安全防护工作。在可预见的未来，AI 对抗攻防技术将在人工智能技术生态重扮演越来越重要的角色，通过提高模型的鲁棒性、增强系统的安全性以及加强用户隐私保护，AI 对抗攻防技术将使人工智能系统更加可靠可信。

### （三）量子安全技术

量子计算机的崛起可能会破解加密算法，威胁到传统加密的安全。为应对这一挑战，量子安全技术应运而生，并从量子计算和量子通信的快速发展中受益匪浅。它是一种基于量子力学原理的加密解决方案，旨在抵御未来量子计算机对传统加密算法的破解威胁。该技术主要包括以下内容：一是量子密钥分发（Quantum Key Distribution, QKD），利用量子纠缠和不可克隆性原理，实现安全的密钥分发过程。QKD 确保密钥的安全传输，因为任何对密钥的窃听或干扰都会破坏量子态，从而被发现。二是量子随机数生成（Quantum Random Number Generation, QRNG），利用量子物理过程生成真正的随机数，这些随机数在加密中起到重要作用，用于



生成密钥、初始化向量等。三是量子认证（Quantum Authentication, QA），利用量子力学特性实现身份验证过程。通过量子随机数生成和量子态测量，能够确保通信双方的身份真实性和通信内容的完整性。四是量子安全协议，基于量子密钥分发和量子认证等机制设计和实施安全协议，用于实现保密通信、数据完整性验证和身份认证等功能。

量子安全技术的目标是提供一种能够抵御量子计算攻击的加密解决方案，利用量子力学的不可破坏性和测量干扰原理，提供了更高级别的加密保护，为未来量子计算机时代的安全通信打下基础。一方面，基于量子力学原理，量子安全技术物理层面上不可破解，为信息理论安全提供保证；另一方面，量子密钥分发和量子认证等技术可实时检测窃听和干扰行为，从而确保通信的机密性和完整性；此外，量子安全技术提供了更高级别的密钥管理机制，包括不可克隆性和完美保密性，增强了密钥的安全性。

尽管目前量子安全技术仍存在技术高成本和复杂性、标准化和统一规范尚不成熟、易遭受侧信道攻击等问题，商业应用还处于早期阶段，距广泛应用落地尚需时间，但其在特定领域中的实际应用展现出了巨大的发展潜力，电信、金融、监管等对安全性要求高的部门已开始部署 QKD 系统来确保通信的保密性。在可预见的未来，量子安全技术将广泛应用于金融、电信、军事等涉及国家安全、经济安全、国防安全、

产业安全和民生安全的重点领域，政府、学术机构和企业将继续加大研发投入，加深合作力度，加速量子安全技术创新和应用落地，助力信息安全步入量子计算时代。

#### **（四）云原生安全**

近年来，伴随云计算和容器化技术的广泛应用，企业将应用和数据逐步迁移到云平台，安全威胁也随之增加。传统的安全解决方案难以充分适应云原生架构的特点和需求，云原生安全技术和服务应运而生。云原生安全技术和服务针对云环境中的安全需求，提供一系列技术、工具和服务以保护云上应用和数据的安全，具体包括：云环境的实时监测和审计、漏洞扫描和风险评估、访问控制和身份验证、日志管理和分析，以及威胁情报和事件响应等。云原生安全工具和技术能够检测和预防云环境中的恶意活动、数据泄露、网络入侵等安全威胁，并进行实时监控和警报，帮助企业及时发现和应对潜在的网络安全漏洞和攻击。通过云原生安全技术服务，企业可以提高云环境的安全性和可信度，保护敏感数据和业务运行的连续性。

与传统的安全技术相比，云原生安全技术更能适应云原生架构，可提供实时监测和防护，自动化和智能化水平更高，可扩展性更强。但目前，云原生安全服务仍存在复杂云环境的高技术资源投入要求、与传统安全解决方案的集成困难、安全服务效果对云平台的安全性能和配置依赖程度高等不

足，需要综合考虑多方面因素来实现全面的云安全保护。目前，云原生安全主要应用于企业级云平台、云原生应用开发和部署、容器化环境以及云原生数据库等场景。未来，随着企业对云环境的依赖程度不断加深，云原生安全技术需求将不断增长，并在云环境安全性增强、实时威胁检测和响应、多云环境的集中管理、合规性和监管要求、可视化的安全分析和报告等领域得到更为广泛且深入的应用。当前，国内诸多企业在云原生安全相关领域已有相对成熟的技术和较大的投入，并已有产品落地应用，市场前景将十分广阔。

### **（五）网络安全保险服务**

当前，我国数字经济快速发展，网络安全基础性、保障性作用逐步增强。网络安全保险作为具有网络安全风险管理和经济补偿功能的新型网络安全服务<sup>12</sup>，对于提升企业网络安全风险应对能力，促进中小企业数字化转型发展，推进构建网络安全社会化服务体系具有重要意义。2023年7月，工业和信息化部、国家金融监督管理总局联合印发《关于促进网络安全保险规范健康发展的意见》，提出促进网络安全保险规范健康发展。

网络安全保险服务旨在通过制定保险政策、开展风险评估和管理、提供应急响应服务和技术支持培训等服务帮助企业管理和降低网络安全风险，在网络安全事件发生时，网络

---

<sup>12</sup> 光明网.网络安全保险保障数字经济高质量发展.2023-07.

安全保险服务能够为企业相应提供补偿，以减轻企业在财务和名誉方面的损失。目前，我国网络安全保险服务模式主要有两种：一是面向企业网络安全风险管理需求的“保险服务+安全风控”模式，保险公司发挥主导作用，借助网络安全企业、专业网络安全测评机构的网络安全技术能力、场景化评估分析能力和数据整合分析能力，开展产品开发、核保定价、防灾减损等保险服务，为企业提供网络安全财产损失险、责任险、综合险等保险产品。二是面向网络安全产品残余风险转移需求的“安全防护+保险保障”模式，由网络安全企业主导，为客户提供网络安全防护类产品的同时，附加网络安全专门保险，如在招标文件中明确网络安全服务中包含为服务责任兜底的网络安全保险产品。

据全球知名研究机构 CyberVentures 估计，到 2025 年，全球网络犯罪将造成 10.5 万亿美元的损失，这会对企业、公众、政府都产生巨大负担，网络安全保险在防范、转移和分担该损失中将发挥越来越巨大的积极作用。目前国内网络安全企业纷纷试水网络安全保险业务，未来几年是网络安全保险快速发展的重要机遇期，将迎来更多网络安全保险新产品、新服务、新模式的创新和落地。

## **（六）安全审计和合规性服务**

网络安全审计和合规性是保护企业数据安全的重要环节，是加强关键业务信息和客户数据安全保护的重要手段，

也是满足日益丰富和细化的网络安全法律法规和政策标准合规性要求的重要途径。通过评估和改进网络安全措施，确保符合相关的合规性标准，不仅可以帮助企业进一步夯实网络安全基础，提升潜在网络安全威胁和风险防范能力，也可以帮助企业满足相关政策法规要求，避免承担网络安全相关法律责任和声誉损失，真正实现业务不宕机、合规不踩线。

安全审计和合规性服务是指对组织的信息系统进行安全审计，以确保它们符合相关法规和标准。该服务旨在发现潜在的安全漏洞，评估安全控制的有效性，并确定是否存在任何违规行为。安全审计服务包含安全控制评估、安全漏洞扫描、安全策略审查、安全事件响应评估等；合规性服务包含法规合规性评估、标准合规性评估、行业合规性评估等。通过开展安全审计和合规性服务，可以评估和改进网络安全控制措施、策略和流程，提高企业整体的安全水平。但是，安全审计和合规性服务也存在资金成本较高、服务范围和深度有限、难以及时跟进最新技术变化和政策要求等不足。当前，安全审计和合规性服务已广泛应用于金融、医疗健康、零售和电子商务、能源和公用事业等领域，部分企业已面向各类客户提供安全控制评估、安全漏洞扫描、安全策略审查、安全事件响应评估等安全审计服务，以及法规合规性评估、标准合规性评估、行业合规性评估等合规性服务。未来在多领域技术带动下，安全审计和合规性服务将朝着自动化、智能

化和融合化发展，拓展衍生云安全审计、物联网安全审计、区块链合规性审计等多领域网络安全审计和合规性服务，从而降低服务成本、提高服务时效性和有效性。

### **（七）网络安全防护有效性验证服务**

据 Gartner 的调查显示，97% 的网络入侵行为发生在已经部署网络安全防护系统的公司，99% 的网络攻击行为是使用已知并且存在多年的攻击方式或者漏洞，95% 的绕过安全防护设备的入侵攻击行为是由错误配置造成的。由此可见，即使各类安全防护设备已做好部署，如果没有持续升级或正确配置网络安全防护策略，这些安全防护设备仍然无法发挥最大效果，难以有效防范网络安全入侵。因此，网络安全防护有效性验证服务的重要性日益凸显，网络安全验证成为 Gartner 发布的 2023 年 9 大主要网络安全趋势之一，指汇集多项技术、流程和工具，对潜在攻击者利用已知威胁暴露面的方式进行验证。网络安全防护有效性验证服务能够提供模拟攻击验证的方法，检验各类设备的防护策略是否有效，全面评估防御的有效性并测试出防护短板，帮助企业了解其网络系统的安全状况，识别潜在的安全风险，并提出相应的解决措施。当前，国内一些网络安全企业通过漏洞扫描、渗透测试、入侵与模拟攻击、安全配置审核和风险评估等网络安全测试，验证客户网络安全防护的有效性。综上所述，网络安全防护有效性验证服务是网络安全运营体系的补充，将成

为企业增强网络安全性、保障网络稳定运行的重要抓手。

## （八）云密码服务

大数据、人工智能、移动互联网、物联网等技术的蓬勃发展离不开云计算的支撑，传统的信息技术和产品需要从产品形态、部署方式、商业模式等各层面适应云计算中的服务化需求。当前，在云计算迅猛的发展势头中，安全成为掣肘云计算发展的最关键问题，作为网络安全核心技术和基础支撑的密码技术在云计算中的作用变得更为重要。我国高度重视网络安全保障中的密码技术，将密码作为国家的重要战略资源，在金融、国防、电信等重要应用领域全面推广应用国产密码算法。《网络安全法》、网络安全等级保护制度 2.0 和《密码法》中，对云计算环境的安全建设提出要求，明确三级及以上的系统需要进行密码应用安全性测评。

云密码服务是一种全新的密码功能交付模式，是云计算技术与身份认证、授权访问、传输加密、存储加密等密码技术的深度融合。密码服务提供商按照云计算技术架构的要求整合密码产品、密码使用策略、密码服务接口和服务流程，将密码系统设计、部署、运维、管理、计费等组合成一种服务，来解决用户的密码应用需求。根据云计算中的密码应用需求，云密码服务可以分为三类：云密码资源服务（Cryptography Resource as a Service, CRaaS）、云密码功能服务（Cryptography Function as a Service, CFaaS）、云密码

业务服务（Cryptography Business as a Service，CBaaS）。CRaaS、CFaaS、CBaaS 构成了从低到高的层级关系，低层可为高层提供密码服务支撑，并且每一类也可直接为用户提供服务，用户可通过自身信息系统部署环境，以及自建的信息系统的边界选择相应的服务类型。

在云、移动端、物联网等新场景需求带动下，云密码服务将在工控、车联网、数字安防等领域逐步实现大规模应用。当前，网络安全企业正在将密码服务与云计算平台进行结合，通过调度加密机集群动态扩充密码运算能力，使密码运算速度显著提高，增强了系统稳定性，为用户提供集中化、虚拟化、透明化的密码运算服务。在政策合规和云计算技术发展的双重驱动下，云密码服务或将成为网络安全细分领域的一片新蓝海。

### （九）数据安全治理

数据安全是网络空间安全的关键所在，也是国家安全的重要组成部分。随着数据安全产业迅猛发展，数据安全单点产品数量逐步增加，但是，数据安全工具的碎片化影响了实际产品效能，急需构建全面、系统的数据安全治理体系，实现对数据安全风险的主动防御和综合防御，确保数据的安全高效利用。

早在 2017 年，Gartner 便在其召开的安全与风险管理峰会上提出了数据安全治理理念，认为数据安全治理不仅是一



套用工具组合而成的产品级解决方案，更是从决策层到技术层，从管理制度到工具支撑，自上而下贯穿整个组织架构的完整链条。国内网络安全企业经过数年的探索推广，形成一系列保护和管理客户数据安全的工具和服务，涵盖数据安全的策略制定、规范制定、风险评估、监控和培训等方面。数据安全治理服务的核心在于确保数据得到适当保护，防止数据泄露、滥用或未经授权的访问。通过有效的数据安全治理服务，企业可以建立较为完备的数据安全管理体系，进而降低数据安全风险。

未来，数据安全治理将在个人信息保护、数据共享与合作、云计算和大数据安全、边缘计算和物联网安全、数据伦理和隐私保护以及 AI 与数据安全等领域发挥越来越突出的作用。但也应注意，数据安全治理服务在自动化程度、安全与隐私平衡、新兴技术应用风险以及用户安全意识等方面仍存在较大挑战。随着技术发展和理论体系逐步完善，数据安全治理将不断创新和演进，以上问题有望得到解决和改进，从而增强对数据安全风险的主动性、体系化防御能力。

## **（十）软件供应链安全治理**

2023 年，软件供应链的安全威胁和风险继续攀升，据 Gartner 分析，到 2025 年，全球 45% 的组织 and 企业的软件供应链将遭受攻击。软件供应链攻击是指针对软件供应链所发动的网络攻击，攻击者会先攻击软件供应链中安全防护相对

薄弱的部分，然后再利用软件供应链之间的相互连接（如软件供应、开源应用）等，将风险扩大至上下游企业，对大量供应商和最终用户带来巨大影响。与其它攻击形式相比，软件供应链攻击往往会产生“牵一发而动全身”的效果。在软件供应链中，各个环节均可能存在安全风险，例如开发过程中的代码漏洞、分发过程中的恶意软件、配置和使用过程中的错误等，这些风险不仅会对企业造成经济损失，还会对用户的个人信息安全造成威胁。

软件供应链安全治理是指采取针对性防范措施，对软件开发、分发、安装、配置、使用、维护以及报废等全生命周期过程中所涉及的各类资源进行管理和控制，以保障软件供应链中的各个环节和组织进行业务活动和信息交换的安全性，有效应对软件供应链中各个环节中可能存在的多种安全威胁。软件供应链安全治理主要包括：供应商管理、采购管理、开发管理、测试管理、发布管理、运维管理、报废管理等。通过这些措施，可以确保软件供应链的透明度、可追溯性和安全可控性。近年来，国内企业越来越关注软件供应链安全风险治理，多个企业在软件供应链安全治理新模式方面开展了有益探索，可以看到，全面、高效地保障软件供应链的安全对于加快数字化进程、推动软件产业高质量发展、切实保障网络空间安全具有重要意义。

## 六、我国网络安全产业发展展望

基于多年来对网络安全产业发展动向和趋势的深入分析研究，对我国网络安全产业未来几年的发展态势作出如下展望：

### （一）政策驱动、需求拉动的发展趋势将更加明显

2023 年，中央和地方相继推出多项网络安全法律法规、规划政策。如前所述，网信办、发改委、工信部、市场监管总局等部门出台数据安全、商用密码、网络安全保险、网安服务认证、政务大数据等政策新规。河北、山东、上海、深圳、云南、西藏等地相继推出数据安全、关键信息基础设施、数字政府等新政策。网络安全治理体系将进一步沿着行业、领域、地域、场景等脉络进行切分和细化，相关规制更加明确具体。在守法合规的基础上探索发展路径仍是网络安全产业发展的主要驱动因素，政策导向仍将在很大程度上影响国家网络安全产业布局和企业重点发力和资源投入方向。数字经济发展进入快车道开辟了更多网络安全产业“新赛道”，数据安全、云原生安全、工业互联网安全、物联网安全、车联网安全等应用场景安全需求，智慧城市建设中交通、能源、医疗等新基建安全需求，5G、人工智能、量子信息、元宇宙等新技术安全需求，均将成为支撑网络安全市场规模扩容并高速增长的新板块，网络安全产业发展逐步向“政策+需求”

双轮驱动进阶。

## （二）产业自主可控的发展趋势将更加明显

近年来，工信部、国资委等部门出台多项政策推进产业自主可控发展，维护关键基础设施安全，信息技术应用创新（以下简称信创）产业已走过“试点实践期”，并逐步迈向“规模化推广期”的关键阶段。随着“数字中国”建设规划的逐步推进，信创产业需求不断释放，从党政信创到行业信创，从金融、通信到教育、医疗等领域，国产软硬件渗透率快速提升。2022年9月，国资委发布的79号文件要求国企央企落实信息化系统的国产化改造，明确要求到2027年所有中央企业的信息化系统完成信创替代，范围涵盖芯片、基础软件、操作系统、中间件等领域，这无疑对信创产业发展产生重大激励作用。根据《2022 中国信创生态市场研究和选型评估报告》<sup>13</sup>数据，2022 年我国信创产业规模达到 9220.2 亿元，近 5 年复合增长率为 35.7%，预计 2025 年将突破 2 万亿元。信创产业和网络安全产业息息相关，信创产业的爆发也为网络安全产业带来重大发展机遇。另外值得关注的是，国产密码技术取得较大突破，将在基础信息网络、重要信息系统、工业控制系统等领域得到更加广泛的应用，有力保障我国多领域科研成果和产业应用的信息安全，为网络安全产业自主可控发展保驾护航。

---

<sup>13</sup> 海比研究院联合中国软件行业协会、中国软件网联合发布。

### **（三）“产品+服务”双轮驱动的发展趋势将更加明显**

持续不断的灾难性网络攻击事件多次印证网络安全风险关乎企业存亡、产业重构乃至国家安全。面对安全事件层出不穷、网络威胁不断升级、网络攻击持续演进的趋势，“单一化、碎片化、片面化”的网络安全产品已经难以应对多重复杂且持续变化的网络安全风险，越来越多的网络安全企业正在建立以产品技术为核心，以多元化、系统性服务为竞争抓手的网络安全业务发展理念，网络安全市场向服务化转型的趋势愈发明显。数说安全近年的分析数据显示，2018年至2022年以来，网络安全服务项目数量持续增长，在整体网安项目中的占比逐年提高，2023年上半年，服务型企业数量同比增长32.5%，成为网络安全市场扩容的主要力量。奇安信、启明星辰、深信服、天融信等行业头部企业也在向“产品+服务”综合解决方案的提供商转变。同时，越来越多的用户企业将网络安全挑战视为重要的商业风险，愈发看重网络安全服务的有效性、持续性和体系化，网络安全市场将从技术产品的“单打独斗”向产品和服务相辅相成的方向转型。此外，伴随虚拟化及云服务理念逐渐深入，网络安全产品正在由以硬件交付安全产品，人工交付安全服务的形式，逐步向云化、SaaS化方式交付技术和服务等形式转变<sup>14</sup>。

### **（四）领军企业带动、产业链协同的发展趋势将更加明显**

---

<sup>14</sup> 数说安全研究院.2023 中国网络安全产业八大趋势.

国内网络安全企业数量众多，业务重点和发展模式各有所长、各占胜场，各自为战的分散型竞争模式长久存在。随着网络安全技术持续升级，网络环境和安全需求日益复杂，对网络安全产品研发、人才资源等方面提出了更高要求，网络安全市场份额进一步向具有一定技术实力和品牌知名度的企业集聚。如前所述，头部企业的市场份额呈现逐年上升趋势，前四名企业的市场份额已经从 2018 年的 21.71% 提升到 2022 年的 28.59%。头部企业对市场的把握和牵引能力更强，领先优势将进一步扩大。此外，产业链上下游和生态圈伙伴企业间在技术、市场等方面逐渐呈现协同发展态势。例如，南水北调集团与奇安信签署战略合作协议以强化国家水网安全运营，华为、太保产险等企业开展网络安全保险创新合作，企业间的合作更加频繁。未来，随着新技术、新产品、新模式加速融合，协同发展、优势互补的网络安全产业生态将逐步形成。

#### **（五）技术服务“智能化+主动化”的发展趋势将更加明显**

近年来，网络攻击手段更加多元、频次更快、影响更大，政府、企业、组织已经不能满足于对网络安全威胁采取低智能化的静态防御、被动防御和刚性防御。随着攻击面管理、威胁狩猎、量子安全技术、隐私计算、数据安全治理、网络安全防护有效性验证等技术和服务在更多产业和领域更为

广泛的应用，政府、企业和组织的主动防御能力不断提升，攻防一体的网络安全治理机制逐渐建立。此外，面对日趋复杂的网络攻防态势演变，网络安全技术正在朝着智能化、多元化、个性化的方向发展，尤其在人工智能技术创新的持续推动下，网络安全技术将实现对安全威胁的快速感知、主动捕获、动态对抗、关联预测，还将支持场景定制化、全局网络安全联动部署，智能主动安全类产品将迎来规模化应用，在网络攻防对抗与网络安全防护等方面凸显重要价值。

中国网络安全产业联盟(CCA)

## 附件一 2022.9-2023.9 网络安全相关法律法规和政策列表

文件名称	发布部门	发布时间
《中华人民共和国反电信网络诈骗法》	全国人民代表大会常务委员会	2022 年 9 月 2 日
《5G 全连接工厂建设指南》（工信厅信管〔2022〕23 号）	工信部	2022 年 9 月 6 日
《互联网弹窗信息推送服务管理规定》	网信办、工信部、市场监管总局	2022 年 9 月 9 日
《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》	网信办	2022 年 9 月 14 日
《国家车联网产业标准体系建设指南(智能网联汽车)（2022 年版）》	工信部	2022 年 9 月 16 日
《气象数据开放共享实施细则（试行）》	气象局	2022 年 9 月 19 日
《民政部贯彻落实〈国务院关于加强数字政府建设的指导意见〉的实施方案》（民办便函〔2022〕856 号）	民政部	2022 年 9 月 28 日
《关于民航大数据建设发展的指导意见》（民航发〔2022〕53 号）	民航局	2022 年 10 月 13 日
《全国一体化政务大数据体系建设指南》（国办函〔2022〕102 号）	国务院办公厅	2022 年 10 月 28 日
《电力行业网络安全等级保护管理办法》（国能发安全规〔2022〕101 号）	能源局	2022 年 11 月 16 日
《互联网信息服务深度合成管理规定》（国家互联网信息办公室 中华人民共和国工业和信息化部 中华人民共和国公安部令 第 12 号）	网信办	2022 年 11 月 25 日
《工业和信息化领域数据安全管理办法》（工信部网安〔2022〕166 号）	工信部	2022 年 12 月 13 日
《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》	中共中央、国务院	2022 年 12 月 19 日
《工业和信息化部等十六部门关于促进数据安全技术产业发展的指导意见》（工信部联网安〔2022〕182 号）	工信部、网信办、发改委、公安部等十六部门	2023 年 1 月 3 日
《个人信息出境标准合同办法》（国家互联网信息办公室令 第 13 号）	网信办	2023 年 2 月 22 日
《数字中国建设整体布局规划》	中共中央、国务院	2023 年 2 月 27 日
《证券期货业网络和信息安全管理办法》（中国证券监督管理委员会令第 218 号）	证监会	2023 年 2 月 27 日
《关于开展网络安全服务认证工作的实施意见》（国市监认证规〔2023〕3 号）	市场监管总局、网信办、工信部、公安部	2023 年 3 月 15 日
《新时代的中国网络法治建设》白皮书	国务院新闻办	2023 年 3 月 16 日



文件名称	发布部门	发布时间
《中华人民共和国数字经济促进法》（专家建议稿）	《数字经济促进法（专家建议稿）》学术研讨会	2023 年 4 月 15 日
《商用密码管理条例》（国务院令第 760 号修订）	国务院	2023 年 4 月 27 日
《公路水路关键信息基础设施安全保护管理办法》（交通运输部令 2023 年第 4 号）	交通运输部	2023 年 5 月 6 日
《个人信息出境标准合同备案指南（第一版）》	网信办	2023 年 5 月 30 日
《近距离自组网信息服务管理规定（征求意见稿）》	网信办	2023 年 6 月 6 日
《商用密码检测机构管理办法（征求意见稿）》	国家密码管理局	2023 年 6 月 9 日
《商用密码应用安全性评估管理办法（征求意见稿）》	国家密码管理局	2023 年 6 月 9 日
《生成式人工智能服务管理暂行办法》（国家互联网信息办公室 中华人民共和国国家发展和改革委员会 中华人民共和国教育部 中华人民共和国科学技术部 中华人民共和国工业和信息化部 中华人民共和国公安部 国家广播电视总局令第 15 号）	网信办、国家发改委、教育部、科技部、工信部等 7 部门	2023 年 7 月 10 日

## 附件二 网络安全企业竞争力评估指标和分析方法

本报告主要通过“资源力”和“竞争力”两个维度来对网络安全企业进行评估。其中，“资源力”指企业所拥有的资本、技术、人力等相关资源的多寡程度，资源的多寡会对企业的经营表现有直接而重要影响。主要参考指标包括是否为上市公司、公司收入规模、市值与估值、人员规模与人才质量、安全业务营收占比。

“竞争力”是指企业在当前商业模式下呈现出的总体能力，是企业所拥有的资源到经营成果的转化。竞争力强的企业，通常能高效地调动和运用相关资源，形成较高的竞争壁垒，在市场中不断获得可观的经营回报。从我国网络安全企业的运营特点来看，对企业竞争力的量化评估从品牌、营销、产品、研发、服务和经营这六个维度展开。主要评估指标包括公众号影响力、官网影响力、百度品牌指数、安全业务营收和毛利、安全业务增长率、净利润率、收入构成情况、员工构成分布、服务资质、应急响应单位级别、销售许可证数量与级别、研发投入情况、专利情况、客户数量等。

1. 针对成熟期企业，企业的经营数据能基本反映出企业运营情况，以及在市场中竞争力的强弱和发展潜力。因此在分析方法上，本报告采取了定量分析的原则，主要基于企业公开数据，或者在调研过程中获得的企业经营数据进行评

选。成熟期企业具体评价指标主要依据“资源力”和“竞争力”两个维度定量分析。

2. 针对成长期企业，在数据基础上对企业竞争力和成长性 2 个维度对企业综合能力进行画像。其中，竞争力：同 50 强评价体系一致。成长性：关注企业成长周期、人员规模、业务规模、业务增长等情况。在今年评选中，将成长之星企业的人员规模最大不超过 600 人上调至最大不超过 800 人，这与当下我国网安产业的发展速度更加匹配。同时，更加看重企业的成长速度，企业成立时间越短，得分越高。

3. 针对初创企业，在数据基础上对企业竞争力、成长性和资本热度 3 个维度对企业综合能力进行画像。其中，竞争力：同 50 强评价体系一致。成长性：关注企业成长周期和成长质量，2023 年潜力之星评价中，将企业营收同比增长调整为 2 年以上复合增长，这样调整一是剔除疫情对初创企业的影响，另外更加关注初创企业可持续性发展的能力，而不会出现昙花一现的情况。资本热度：从融资金额、融资次数、融资轮次、企业最新估值情况等多个方面来考量企业的资本能力。