国家网络安全宣传周
China Cybersecurity Week

2023 国家网络安全宣传周
CHINA CYBERSECURITY WEEK
网络安全为人民 网络安全靠人民

中国网络安全产业分析报告

（2023年）

中国网络安全产业联盟

2023.9.16

目录

1

2023年网络安全产业发展面临的新形势

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。

法律法规趋严趋细，合规要求更加全面深入

立法：《**网络安全法**》首次修订，增加从业禁止措施，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。
执法：《**网信部门行政执法程序规定**》发布，规范网信部门依法履行职责、实施行政执法。
合规监管：线上金融服务的合规监管日益严格，多家银行APP被点名通报。

政策标准密集发布，行业健康规范发展生态更加健全

细分领域：对网络安全保险、网安服务认证等方面提出要求，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安管理具体措施；
新兴产业：《生成式人工智能服务管理暂行办法》发布。
标准：**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；汽车信息安全、生成式人工智能数据安全、大型网络平台网络安全、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。

发展机遇

2.网络安全技术加快迭代升级，为产业发展注入更强动力

2022年以来，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。

零信任架构加快落地

- 2022.11 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。

生成式人工智能火爆全球

- 美国开放人工智能公司（OpenAI）推出聊天生成预训练转换器（ChatGPT）
- 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。

量子信息技术逐步落地应用

- 以量子计算、量子通信为代表的量子信息技术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、专利布局和标准转化，打造更强技术优势。

发展机遇

3.数字安全再提层级，数据安全产业将迎来爆发期

2022.12	2023.1	2023.2	2023.3	2023.5
数据二十条发布 ◆ 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》，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》印发** ◆ 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。	**《数字中国建设整体布局规划》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。	**国家数据局组建** ◆ 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。	**《中华人民共和国数字经济促进法（专家建议稿）》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。

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。

发展机遇

4.全球网络安全战略布局加快，对产业提出更高要求

美国

美国密集出台系列政策战略，强化网络安全保护和网络空间作战能力。

- 2022.09 美国网络安全和基础设施安全局（CISA）发布了**《2023—2025年战略计划》**：从**网络空间安全**、**基础设施安全**、业务协作和机构建设等方面提出四大目标和19个子目标；
- 2023.03 美国白宫发布近五年来**首份《国家网络安全战略》**；
- 2023.05 美国防部向国会提交**《2023年美国防部网络战略》**；
- 2023.05 拜登政府发布**《美国政府关键和新兴技术国家标准战略》（USGNSS）**，将**网络安全与隐私**列入关键和新兴技术（CET）范围。

欧洲

欧盟颁布系列指令、法律，力图持续通过强监管巩固网络安全管理和网络空间防御。

- 2022.09 欧盟委员会通过了**《网络弹性法案》**提案，试图将**所有具有数字元素产品的制造商**纳入网络安全规则管理规范中；
- 2023.01 欧盟委员会正式实施**《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）**；
- 2023.04 欧盟正式公布了《关于GDPR下的个人数据泄露通知的第9/2022号指南》；
- 2023.05 欧盟委员会发布了**《网络团结法案》**提案。

- **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，后续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”，给我们敲响警钟；**
- **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。**

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。
- 宏观经济表现不佳削弱了政府财力，压缩了企业盈利空间，政府和企业在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。
- 国内需求相对不足，**政府和企业在网络安全方面的预算和投入普遍降低或延后，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，网络空间成为现代战争和大国对抗的重要战场。
- 国家间**网络攻防、供应链攻击、数据泄露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。

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

- **AIGC、元宇宙、云原生、量子计算机等技术的迭代升级，也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。

2

我国网络安全产业基本情况

（一）我国网络安全企业总体构成及分布

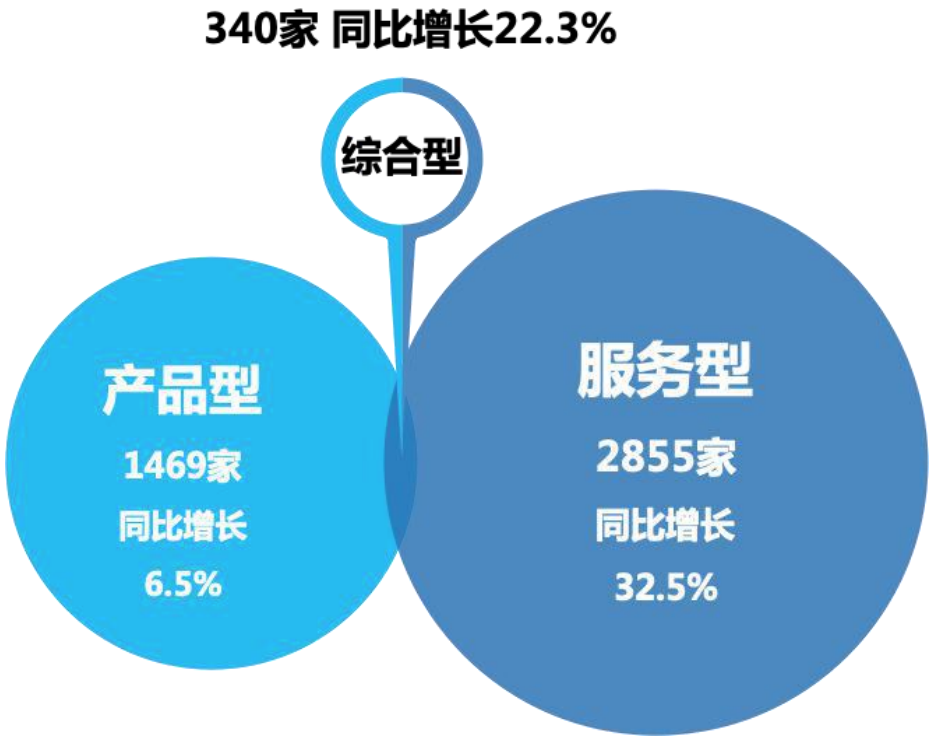


图 2023年我国网络安全企业的总体构成

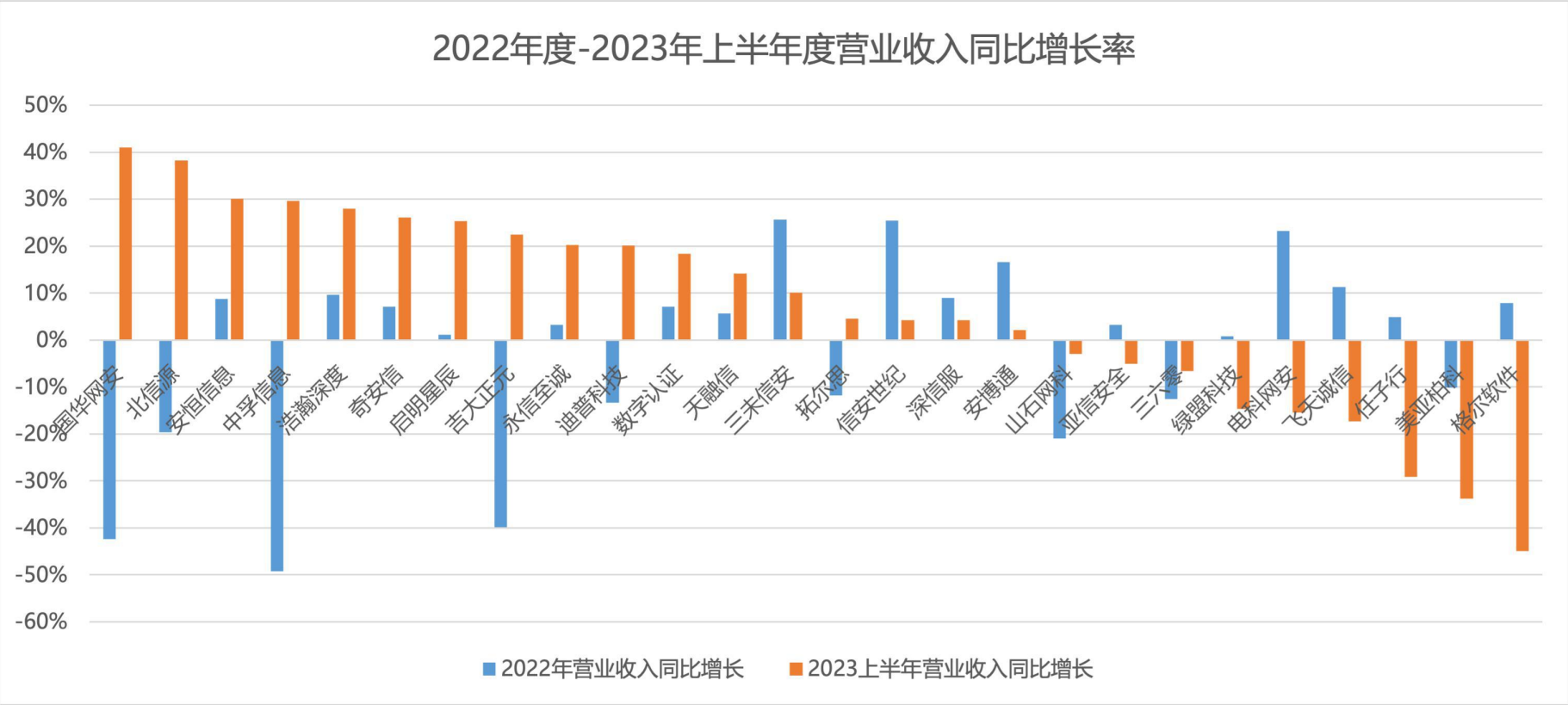
开展网络安全业务的企业总量

- 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%。

企业总体构成

- 2023年企业数量增长主要来源于服务型企业数量的上升，服务型企业数量达2855家，同比增长32.5%。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。

我国网络安全企业收入分析



我国网络安全企业收入分析

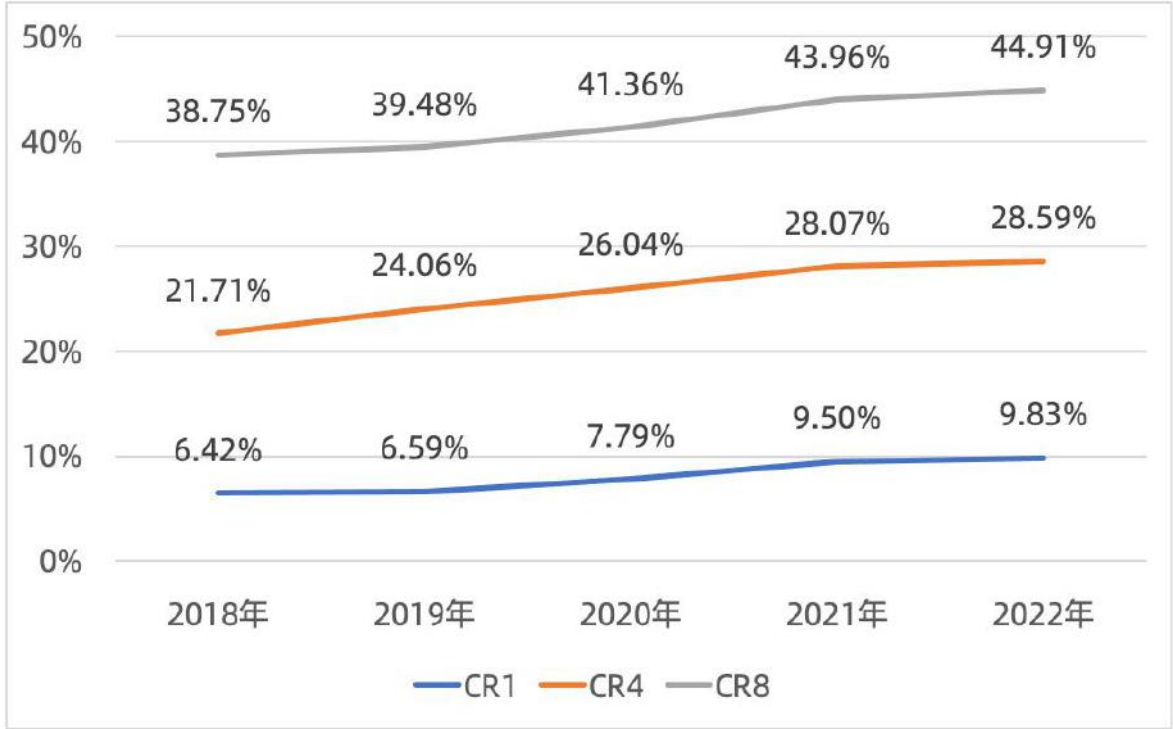
- **截至6月30日，我国已公开上市的网络安全企业共有26家，其中，2022年和2023年上半年营业收入都保持正增长的有11家。**
- 2023年，尽管国内经济逐步复苏，但下游市场需求恢复尚需时日。**上半年，26家安全上市公司营业收入总和达到200.3亿元，同比增长2.5%。其中，3家公司收入增速超过30%，7家公司收入增速在20%-30%之间，7家公司收入增速在0-20%之间，9家公司收入增速为负值。**

（二）我国网络安全产业规模及增速分析

我国网络安全产业规模与增速情况

- **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，但受宏观经济影响，网络安全行业增速持续放缓。**
- 展望未来三年，网络安全产业发展顶层设计更加完善，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，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。

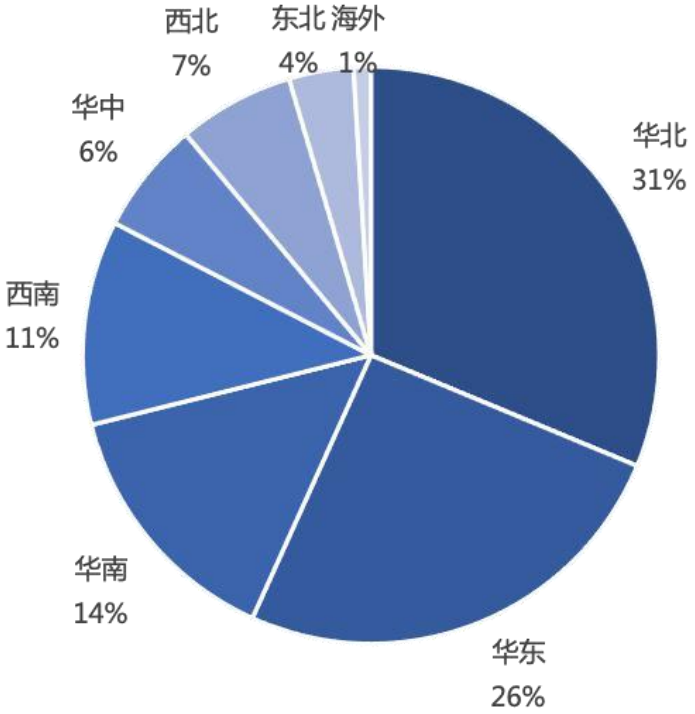
近五年我国网络安全产业集中度分析



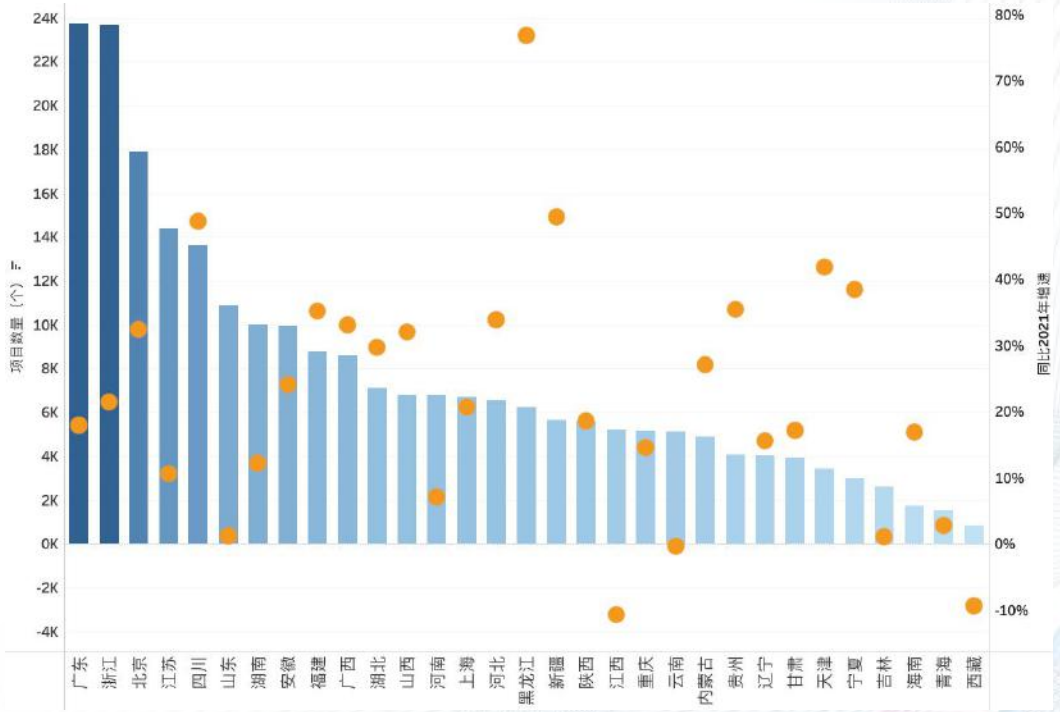
- **2022年我国网络安全市场集中度：CR_1为9.83%，CR_4为28.59%，CR_8为44.91%，网络安全市场集中度进一步提升。**
- **2018-2022年，领军企业的市场份额始终保持上升趋势，前四名企业的市场份额已经从2018年的21.71%升至2022年的28.59%。**

（三）我国网络安全市场区域分布及增速分析

- **全国区域分布看：2022年，华北、华东、华南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。
- **全国网络安全项目分布：2022年，大部分省市的网络安全项目量增速保持正增长，各省市增速分化较为明显，市场区域分布不均衡。**



2022年中国网络安全市场区域分布



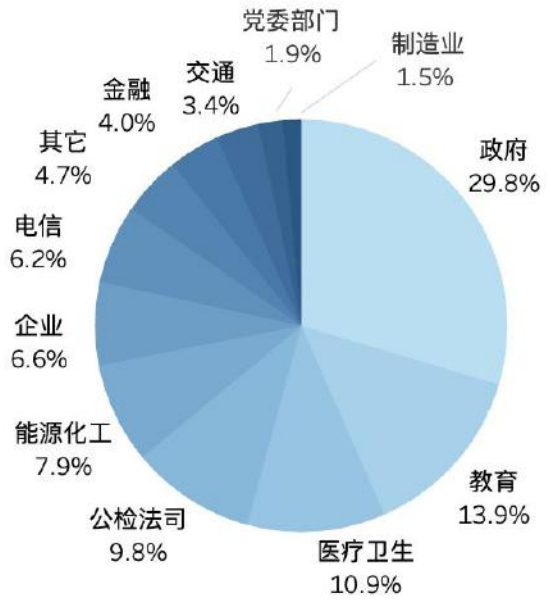
2022年中国网络安全项目数量省份分布及增速

（四）我国网络安全市场客户所属行业分布及增速分析

2022年中国网络安全客户地图

我国网络安全客户分布情况

- 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年涉及网安项目采购行为的客户有6.7万家。
- 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，川渝地区逐渐成为新的聚集区。
- 从行业分布看，政府部门对网络安全项目的需求较大，依然占据最大份额；教育、医疗卫生等国计民生相关领域紧随其后，也有较大占比。



2022年中国网络安全项目数量行业分布及增速

（五）我国网络安全客户产品需求热度分析

- **2022年，从网络安全产品需求看，等保合规类产品仍为主流、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。**

- 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（位于图9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。**

2022年中国网络安全产品采购趋势

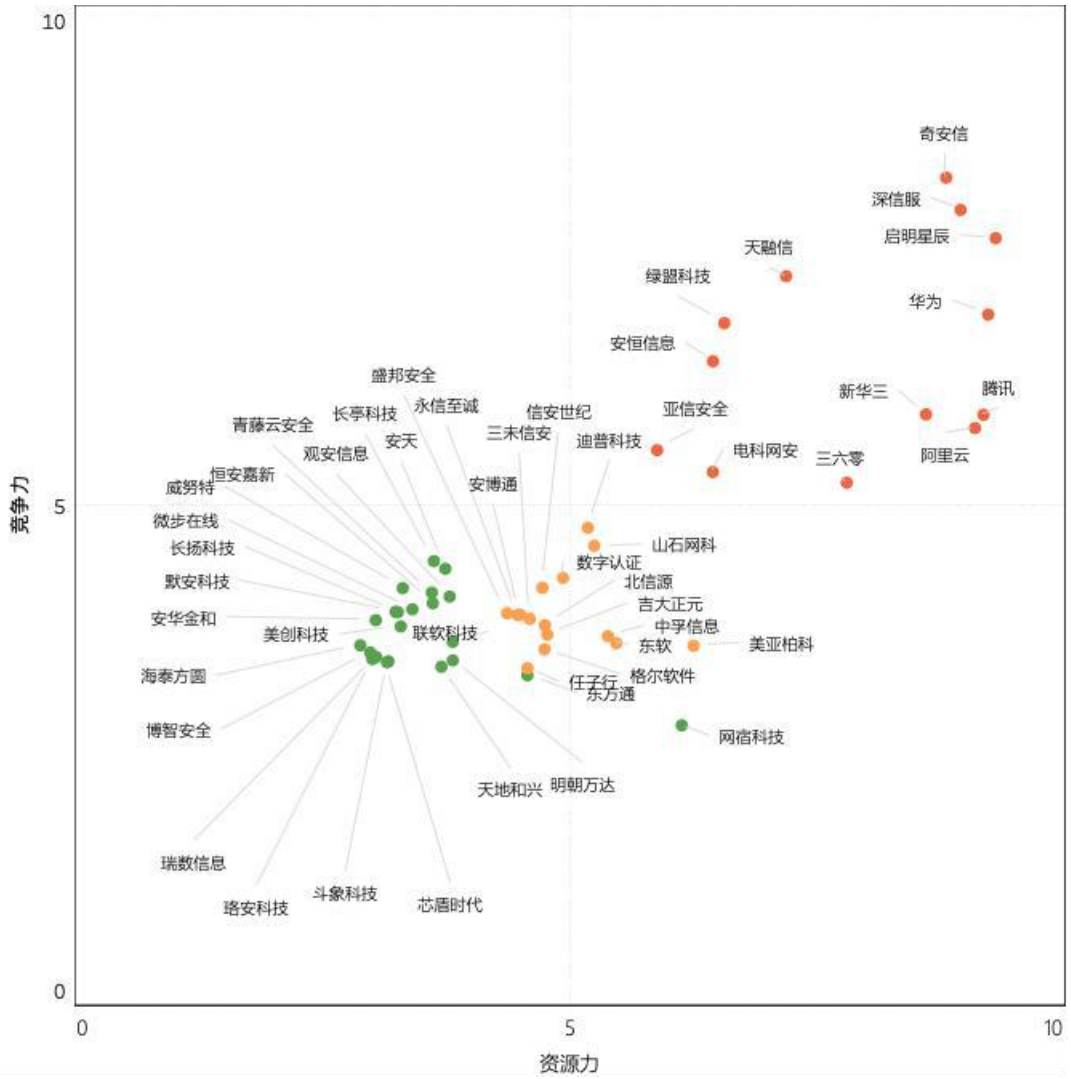
（六）我国网络安全市场分类

- **2023年中国网络安全市场分类架构图涵盖七个基础安全领域、六个安全解决方案、四个应用场景、九个安全服务。**
- 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，我国网络安全行业进入群雄逐鹿、百花齐放的时代，国内企业积极探索和创新，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，市场竞争将更加充分并富有挑战，更多企业需要直面淘汰出局的风险。

3

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



CCIA 50强企业画像

- **报告重点针对初创期、成长期、成熟期的网络安全企业进行竞争力评估分析。**
- **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，居于右上角位置，其资源力和竞争力表现较为突出。**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。
- **成长期企业：已经具备一定的规模和市场份额，部分成长期企业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，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创新优势，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

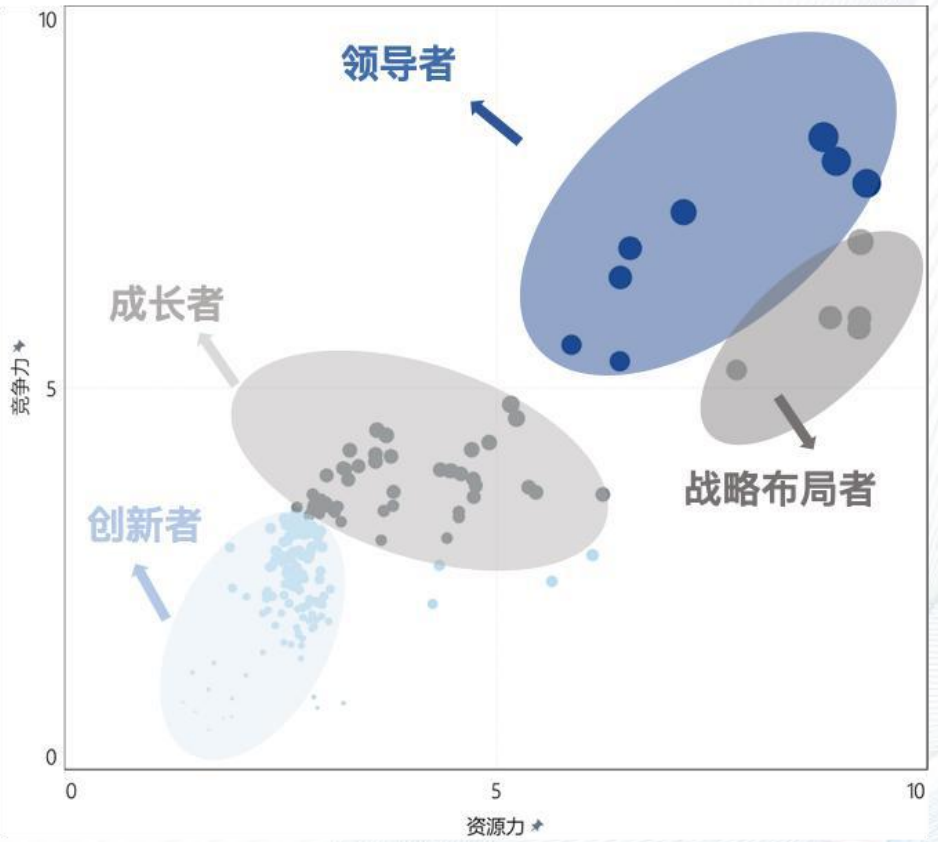
【领导者】：产业领导者均为上市公司，资源力和竞争力均十分突出，大多处于发展成熟期。领导者之间的竞争较为激烈，并呈现出“强者愈强”的分化趋势，未来一段时间这种竞争态势将会延续。

【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。

【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。

【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。

从产业竞争格局的角度来看，可以划分为领导者、战略布局者、成长者、创新者。分析显示，网络安全产业领导者资源力、竞争力突出，强者恒强特征明显；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，对产业竞争格局产生重大影响；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。



2022年中国网络安全市场格局

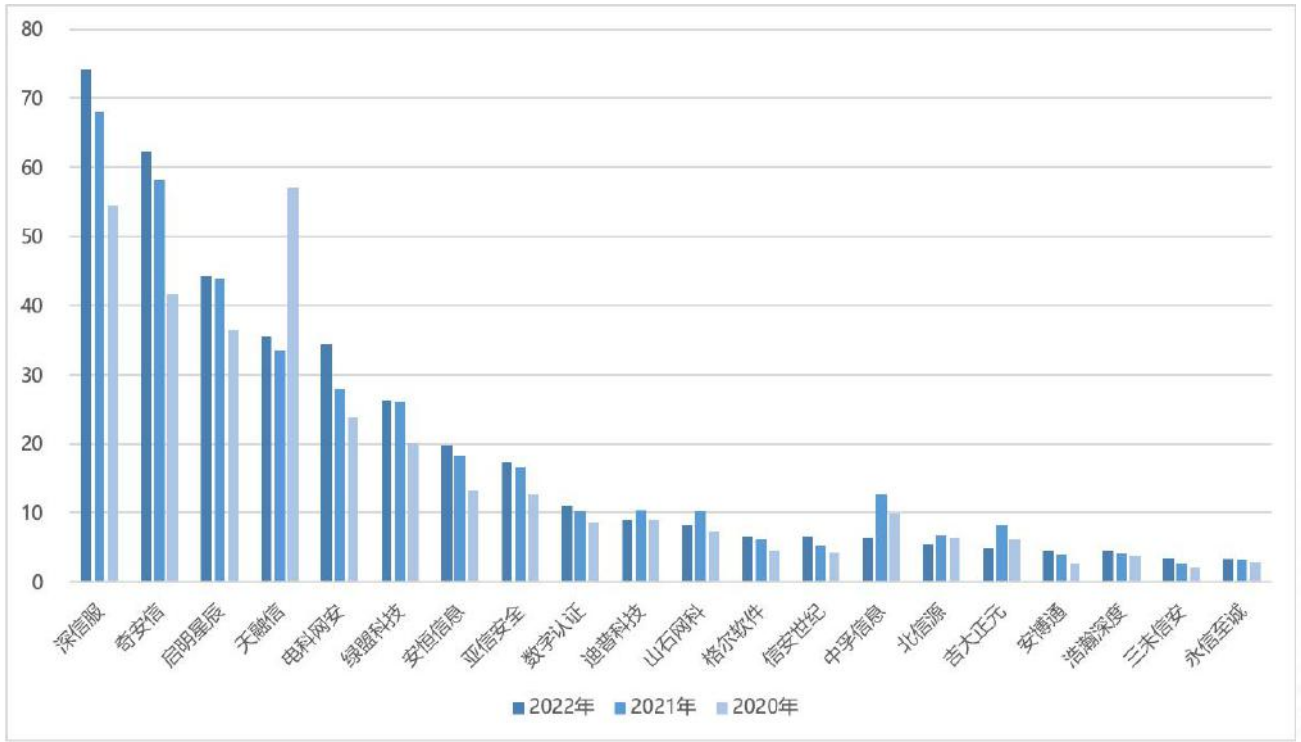
4

我国网络安全资本市场分析

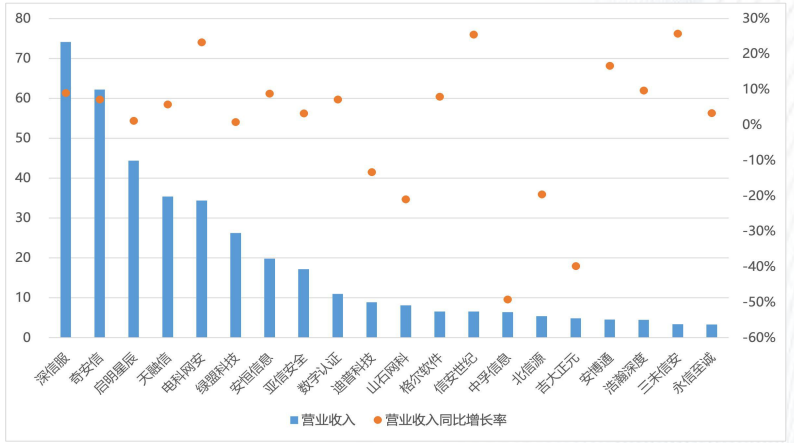
企业经营情况

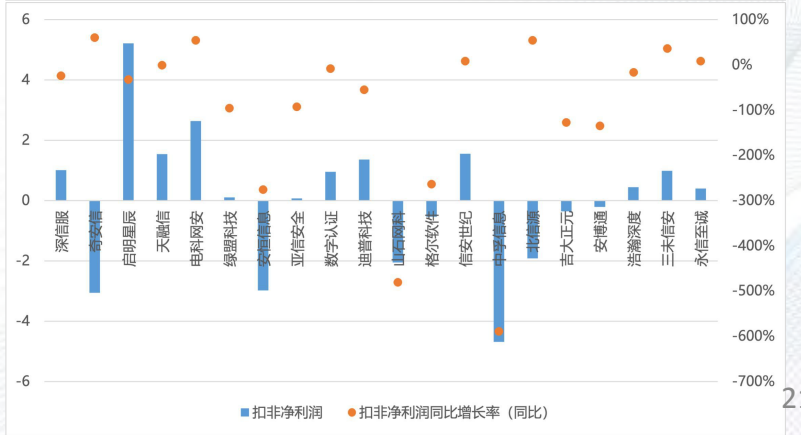
Enterprise

- **选取26家网络安全上市企业中的20家作为分析样本。**样本企业在2022年的收入占国内网络安全市场份额达到65%，在一定程度上可反映网络安全企业总体经营状况。
- **从营业收入来看，2022年，样本企业安全业务营业收入合计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。
- **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。
- **从盈利能力来看，2022年样本企业盈利能力持续下滑，12家盈利，6家亏损。**

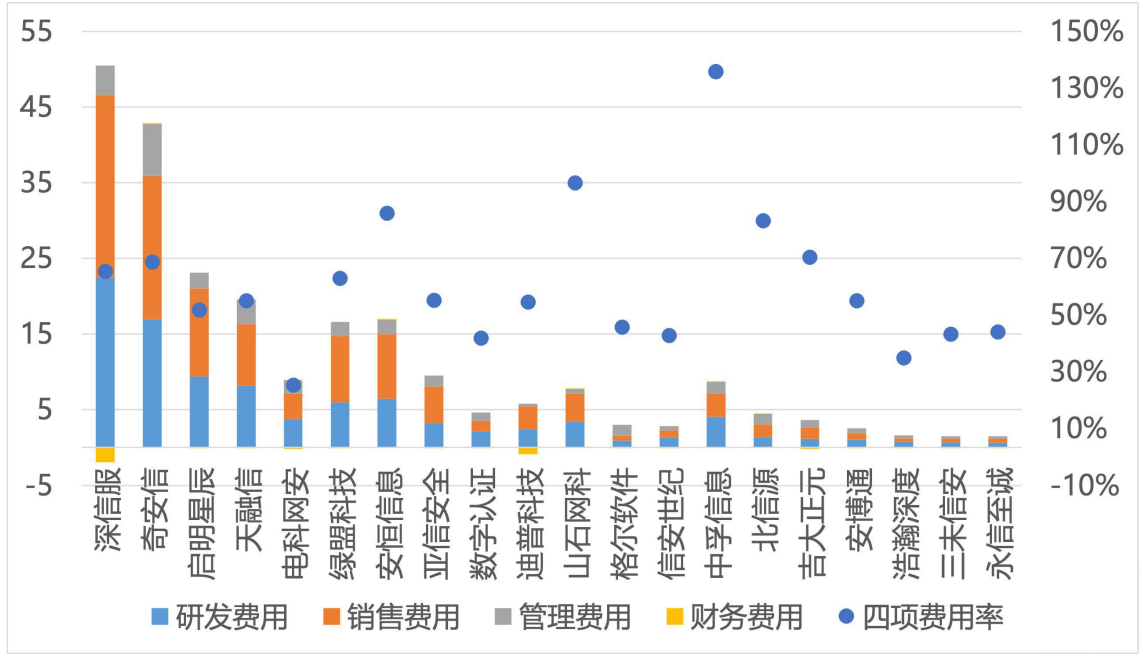


2020-2022年样本网络安全企业安全业务营业收入统计

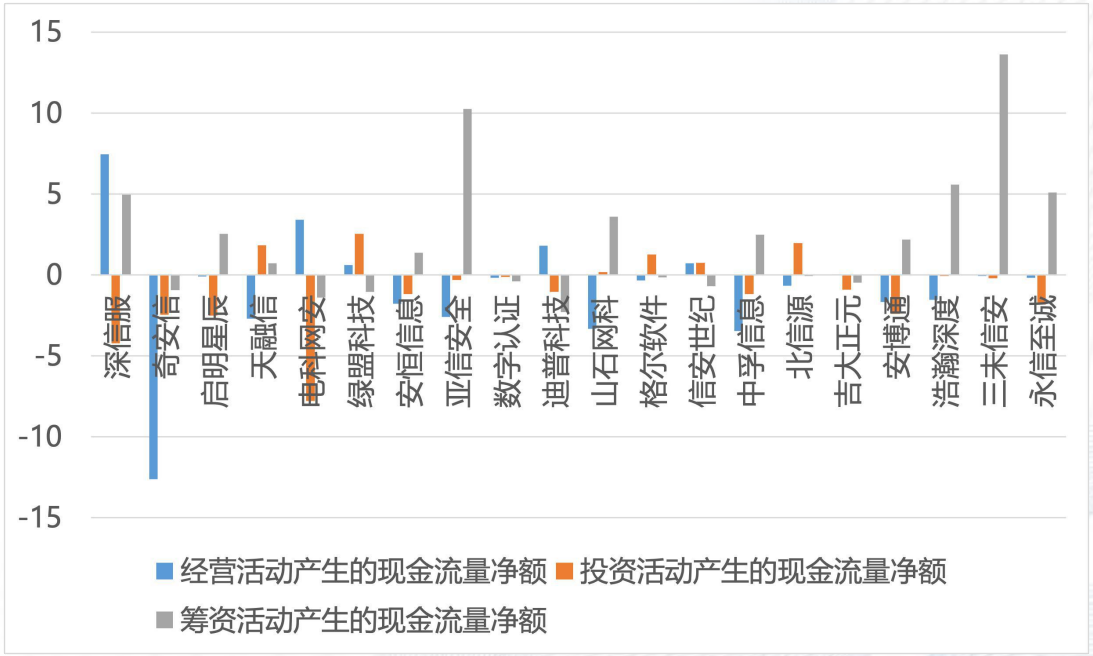




- 2022年我国网络安全企业继续加大了研发和销售的投入，**2022年样本企业销售费用和研发费用达到203亿元，占样本企业营业收入的54.0%。**
- **从企业现金流量来看，2022年样本企业的经营性现金流净额合计为-17.24亿元，相较2021年同期的24.89亿元，下滑明显。**更加需要引起重视的是，2022年行业整体经营性现金流净额首次出现转负的情形。

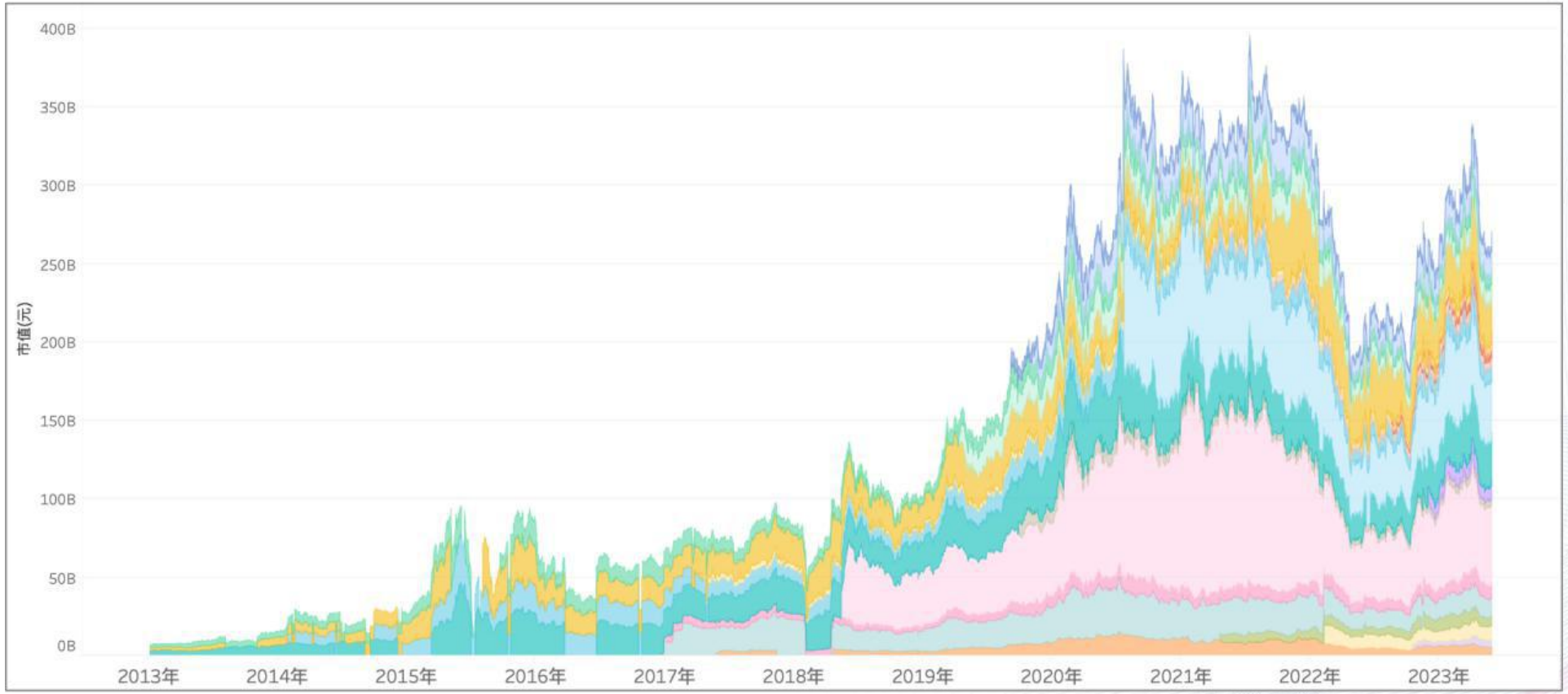


2022年样本企业费用以及四项费用率构成



2022年样本企业现金流净额

- **我国网络安全上市企业总市值从2018年底开始急剧增长，2021年创历史新高，总市值接近4000亿元，2022年5月回落至近2000亿元，2023年4月总市值再次攀升至3400亿元，较2022年最低点上涨约90%。**
- “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。

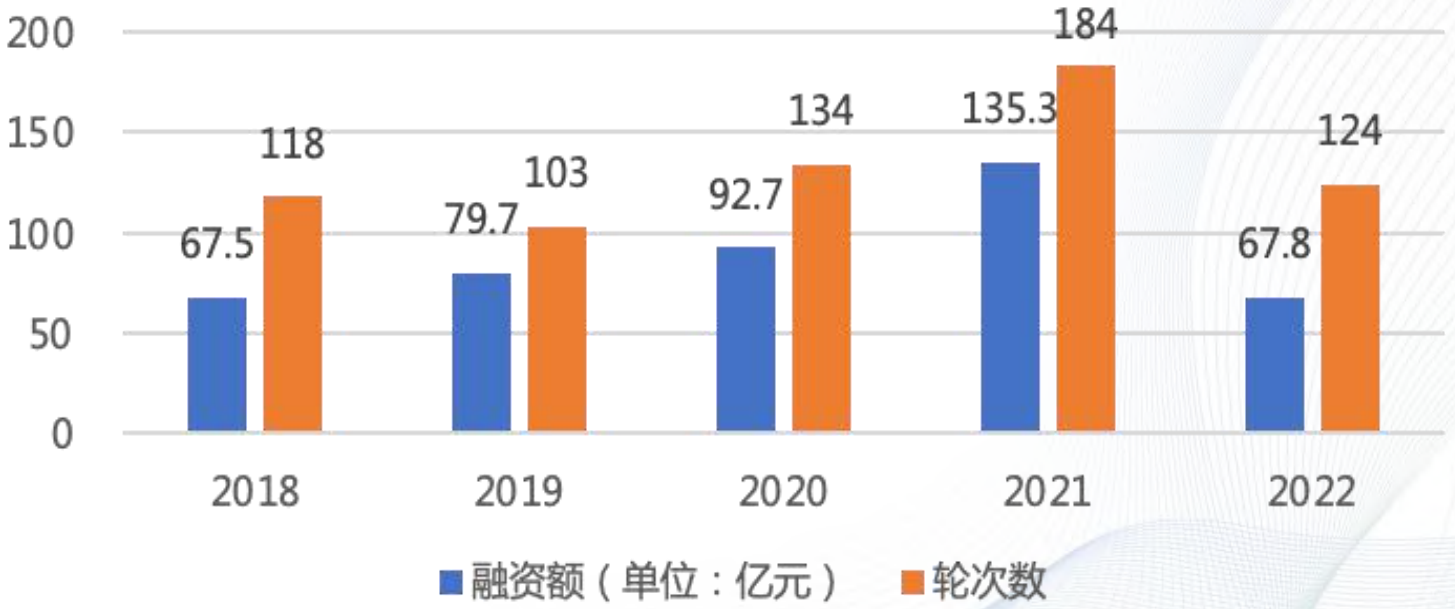


2013-2023年中国上市网络安全企业市值动态

企业IPO及投融并情况

Enterprise

- **2022年，成功登陆科创板的企业有亚信安全、三未信安、浩瀚深度、永信至诚。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。
- **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，网络安全产业融资共有124项，同比下降32.6%；融资额为67.8亿元，同比下降49.9%。**
- 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。



2018-2022年中国网络安全领域融资事件数量金额比较

5

我国网络安全产业技术热点分析

（一）生成式人工智能

随着OpenAI推出了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被Gartner公司评为2022年十二大战略性技术趋势第一位，多个科技巨头重点布局并持续加大投入。

Google Bard

OpenAI ChatGPT

Microsoft Bing GPT-4

Meta LLaMA

百度 文心一言

科大讯飞 星火认知

阿里 通义千问

腾讯 混元助手

华为 盘古

商汤 日日新

中国电信 星河

中国移动 九天

浪潮 源

定义

- 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。

应用与挑战

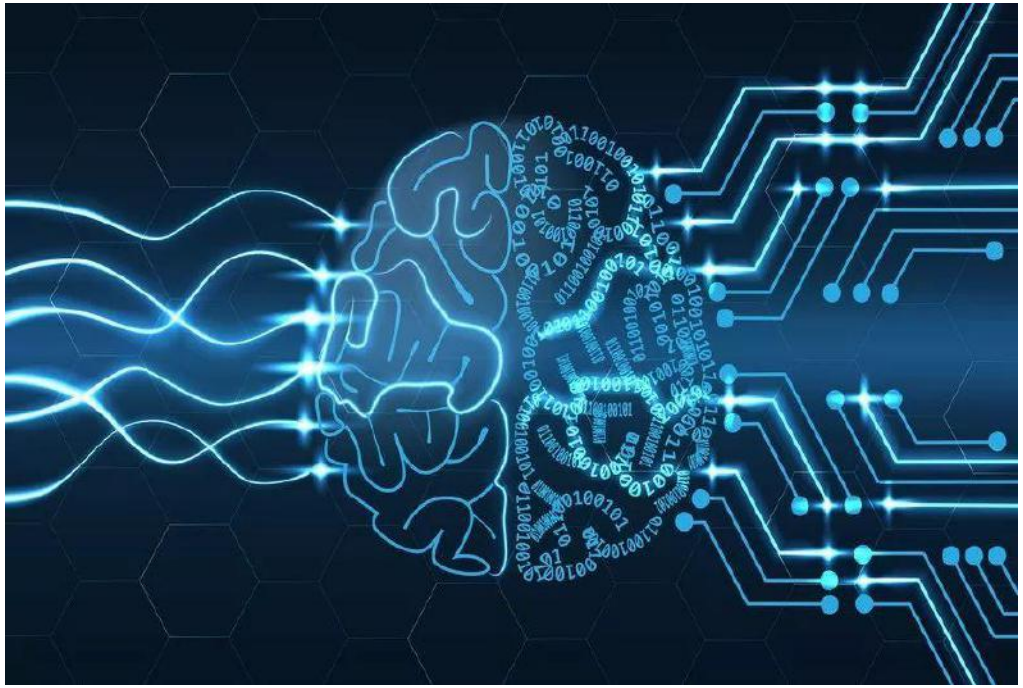
- 基于大模型高算力训练基础，AIGC具备自动化内容创作、大规模数据分析等功能优势，广泛应用于对话聊天、图像生成、自然语言处理、游戏开发、金融分析等领域。
- 面临数据源违规收集、算法失控、内容真实性可靠性存疑、隐私保护确认、知识产权侵害以及不正当竞争等问题。

发展前景

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。

（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，人工智能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，人工智能安全性和鲁棒性问题引起了人们的极大关注，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。



定义

- 人工智能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。

应用与挑战

- 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，作为挖掘模型对抗安全风险并进行防御的关键手段。
- 深度网络模型存在技术脆弱性，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；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。

发展前景

- 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获益匪浅。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。

- 量子密钥分发
- 量子认证
- 量子随机数生成
- 量子安全协议

应用与挑战

- 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。**
- 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。

发展前景

- 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。

- 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
- 威胁情报和事件响应

提高云环境的安全性和可信度

- 云原生安全技术和服务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，云原生安全技术服务需求将不断增长，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。

（五）网络安全保险服务

网络安全保险服务模式

面向企业：“保险服务+安全风控”模式

面向产品：“安全防护+保险保障”模式

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**，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。

发展前景

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、新模式的落地。

（六）安全审计和合规性服务

网络安全审计和合规性服务

重要性

加强关键业务信息和客户数据安全保护

提升潜在网络安全威胁和风险防范能力

帮助企业满足相关政策法规要求

内容

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。

旨在发现潜在的安全漏洞，评估安全控制的有效性，检查是否有违规行为。

应用前景

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。

未来将朝着自动化、智能化和融合化发展。

（七）网络安全防护有效性验证服务

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。

应用情况

- 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。

发展前景

- 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

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。

- 云密码资源服务
- 云密码功能服务
- 云密码业务服务

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

需求背景

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。

应用展望

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。

具体内容

经过业界数年的探索推广，数据安全治理服务是指为了保护和管理数据安全而提供的一系列服务，**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。

（十）软件供应链安全治理

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。

6

我国网络安全产业发展展望

产业环境因素

政策驱动、需求拉动的发展趋势将更加明显

- 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**，以及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”，**应用场景安全需求、新基建安全需求、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，网络安全产业发展由单一的政策驱动逐步向“政策+需求”双轮驱动进阶。

产业内核驱动

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。**
- “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。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。
- **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。

发展展望

市场发展方向

“产品+服务”双轮驱动的发展趋势将更加明显

- **“单一化、碎片化、片面化”的网络安全产品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。
- 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。**

企业竞争格局

领军企业带动、产业链协同的发展趋势将更加明显

- 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。**
- 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。

技术服务动向

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、深度更广，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。
- 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。

国家网络安全宣传周
China Cybersecurity Week

感 谢 ！