安在·新榜
ANZER

2024年
中国网络安全产品市场
调查报告

关于本报告

本报告基于企业网络安全专家联盟（诸子云）甲方社群所实施的数据安全细分领域的产品用户调查，所形成的市场分析报告。

本报告通过对中国网络安全市场情况的调研和分析，力图展示一个真实的行业形象。

由于采集和分析的样本可能存在一定的局限性，因此如有勘误，敬请告知。

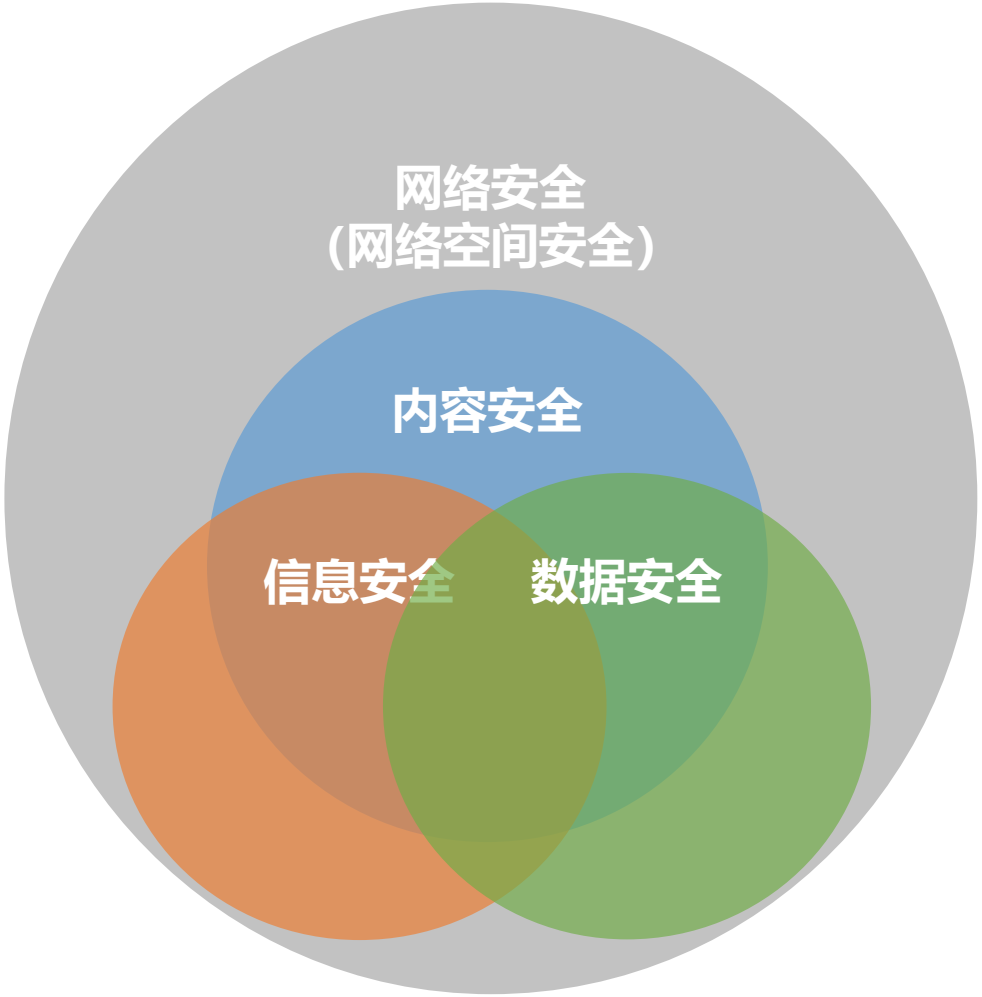
目录

中国网络安全范畴定义

网络空间安全（以下称网络安全）是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。根据《国家网络空间安全战略》，网络安全涵盖网络主权、政治安全、安全可信、安全制度、和平据止、企业尽责、关基保护、基础安全、人权保护等方面。

网络安全主要特性	
网络主权	我国对网络空间主权的看法是：网络空间具有国家主权，国家在网络空间的主权不容侵犯，各国有权选择网络管理模式，有权根据本国国情制定有关法律法规并依法管理本国信息系统和本国疆域上的网络活动。
政治安全	一个国家的政治稳定是其经济发展、人民幸福的基本前提，任何一个国家都不应该在网络空间中或利用网络空间渠道强行推行自己的价值观而不顾他国的社会政治稳定，要坚定反对通过网络颠覆我国国家政权、破坏我国国家主权的一切行为。
安全可信	提高产品和服务的安全性和可控性。我国在走向现代化进程中要秉持开放理念，吸收人类文明科技进步的一切成果为我所用，同时也需要力图保证所使用的（包括所引进的）技术、产品、服务没有安全隐患，安全风险控制到最低。
安全制度	要建立网络安全审查、等级保护、风险评估、漏洞发现等安全制度和机制。
和平拒止	网络空间要和平利用和开展国际合作。主张不在网络空间搞军备竞赛，不滥用信息技术来控制他国信息网络系统和窃取数据，不牺牲他国利益谋求自身的绝对安全，有效防范网络空间冲突。
企业尽责	鼓励网络安全企业做大做强，为保障国家网络安全夯实产业基础。相信在这种思想指导下，国家会继续加大相应措施和举措力度，促进网络安全企业的壮大发展，在国际上能对等竞争。
关基保护	国家关键信息基础设施的大行业领域，即公共通信、广播电视传输、能源、金融、交通、教育、科研、水利、工业制造、医疗卫生、社会保障、公共事业、国家机关、重要互联网应用（例如淘宝、微信、百度等），随着我国经济社会的进一步发展，属于国家关键信息基础设施的行业领域范围可能还会进一步细化和扩大。
基础安全	创造创新政策环境和优化市场环境，加强基础理论和重大问题研究，加强标准化和认证认可，完善监测预警应急处置机制，实施网络内容建设、中华优秀文化网络传播、网络安全人才3个工程，办好网络安全宣传周提高全民网络安全意识等。
人权保护	将“人权得到充分尊重”纳入发展目标，提出要保护知识产权、名誉权、财产权，提出要保护个人隐私、打击侵害公民个人信息行为，提出要提高青少年网络文明素养和加强未成年人上网保护，提出要弥合数字鸿沟，等等

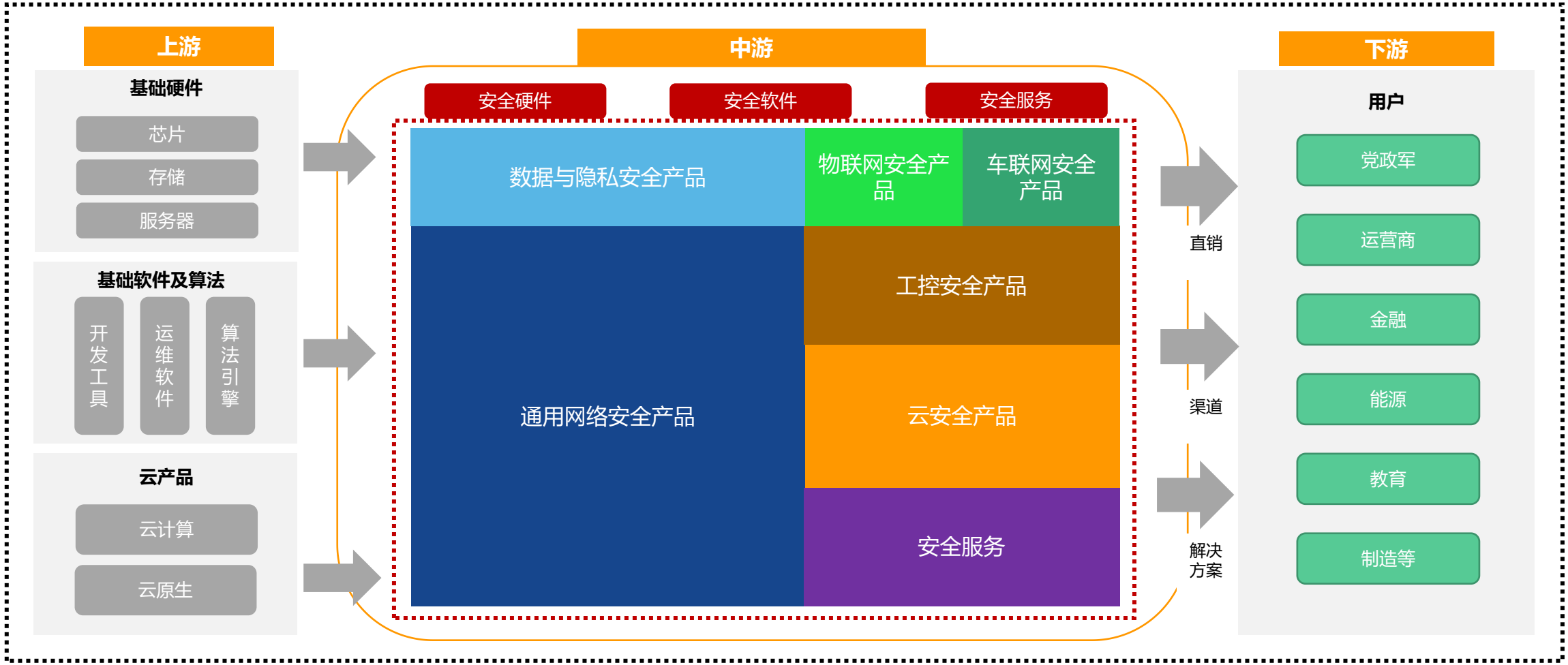
来源：《国家网络空间安全战略》



中国网络安全市场产业链

基于网络安全范畴的定义，网络安全产业链涵盖了从硬件设备、软件产品到服务提供等各个环节，形成了一个多元化、综合性的产业体系。其中中国网络安全市场是指网络安全产业链中游，涵盖了安全硬件、安全软件、安全服务在内的专业领域，鉴于网络安全产品边界的广泛性和模糊性，本报告所采用的整体框架，借鉴了业界公认的一些权威“全景图”，定义了本次报告所研究网络安全市场的边界为数据与隐私安全、通用网络安全、工控安全、物联网安全、车联网安全、云安全、安全服务等七大类产品。

网络安全产业链



来源：安在新媒体整理

市场研究框架：7大类160个子类构成网安市场范围

本次调查涉及的中国网络安全市场的产品和服务涉及数据与隐私安全、通用网络安全、工控安全、物联网安全、车联网安全、云安全、安全服务等7大类产品，160个子类。

2024年网络安全产品种类研究范围

数据与隐私安全

- 数据扫描与发现/分类分级
- 电子文档管理与加密
- 数据脱敏
- 存储备份与恢复
- 数据安全销毁
- 数据安全平台DSP
- 隐私计算
- 数据防泄露DLP
- 数据库安全
- 数据标签与水印
- 隐私管理工具
- 版权保护DRM
- 数据运营安全
- 数据安全交易平台

物联网安全

- 物联网设备安全
- 智能家居安全
- 视频专网安全

车联网安全

- 车载设备安全
- 路侧网络安全
- 车端网络安全
- 智能驾驶安全

通用网络安全

综合安全解决方案

- 零信任
- 数据安全治理DSG
- 威胁管理/XDR
- 安全运营MDR/MSS
- 安全访问服务边缘SASE
- 网络安全网格CSMA
- 用户实体行为分析（UEBA）
- 身份与权限管理IAM

AI安全

- 智能恶意代码/免杀分析
- 智能漏洞挖掘
- 智能应用风险识别
- 智能账号风险识别
- 智能网络风险识别
- 智能攻击识别
- 智能安全运营
- AIGC智能安全

业务安全

- 内容安全
- 支付安全
- 营销安全
- 反洗钱
- 注册/登录保护
- 流量反作弊
- 元宇宙安全
- 反诈骗

软件供应链安全

- 安全开发平台SDL
- 安全开发运维DevSecOps
- 静态应用安全测试SAST
- 交互式应用安全测试IAST
- 软件成分分析SCA
- 动态应用安全测试DAST
- 供应链安全

威胁管理

- 威胁情报
- 舆情监控
- 反爬虫
- 攻击面管理ASM
- 沙箱
- 自动化安全风险评估 ASRA

安全运营

- 安全管理平台/态势感知
- 漏洞扫描与漏洞管理
- 安全基线与配置管理CMDB
- 安全编排自动化（SOAR）
- 安全验证（BAS）
- 密码管理
- 安管/合规检查一体机
- 日志分析与审计
- 网络空间测绘
- 欺骗防御

应用安全

- Web应用防火墙
- Web扫描与监控
- DNS安全
- 自动化攻击防护
- 邮件安全
- 运行时应用自我保护RASP
- 网页防篡改
- API安全
- 安全浏览器

身份认证

- 硬件认证/数字证书
- 多因子认证（短信等）
- 单点登录/4A平台
- 生物认证（人脸纹等）
- 运维审计堡垒机
- 特权账号/权限管理

端点安全

- 终端检测和响应
- 主机/服务器加固
- 恶意软件防护
- 勒索病毒防护
- 终端安全管理

移动安全

- 移动终端安全
- 移动安全管理
- 移动应用安全

网络与基础设施安全

- 防火墙/UTM/下一代防火墙
- 上网行为管理
- 入侵检测与防御
- 网络隔离与单向导入
- 防病毒网关
- VPN/加密机
- 网络准入与控制
- 安全审计
- 抗拒绝服务攻击
- APT防护
- 应用交付/负载均衡
- SD-WAN
- 流量分析
- 5G安全
- 量子安全

物理安全

- 门禁系统
- 保密会议室
- 防窃听/防偷窥
- 视频监控
- IDC防火
- IDC供电保障
- IDC安防
- IDC运维管理
- IDC环境管理

工控安全

- 工控防火墙
- 工控安全管理/态势感知
- 工控主机安全
- 工控安全隔离与信息交换
- 工控检测审计
- 工控仿真/靶场
- 工控漏扫与漏洞管理

云安全

- 云安全资源池
- 微隔离
- 虚拟化安全
- 云安全托管
- 云原生应用保护平台（CNAPP）
- 容器安全
- 云工作负载保护
- 安全办公空间
- 云抗D
- 云WAF
- 云身份管理
- 云漏洞管理
- 云堡垒机
- 云下一代防火墙
- 云入侵检测
- 应用加速
- 云数据安全
- 云应用安全
- 云安全管理
- 云负载均衡

安全服务

- 咨询规划
- 安全集成
- 安全运营/运维
- 反技术窃密TSCM
- 安全培训
- 风险评估
- 渗透测试/红蓝对抗
- 数据跨境合规
- 应急响应
- 攻防靶场实训
- 代码审计
- 数据恢复
- 安全意识教育
- 安全众测
- 重保服务
- 互联网保险
- 样本分析/逆向
- 攻击链分析/互联网调查

来源：安在新媒体整理

市场发展史：五阶段发展进入智能信创时代

中国网络安全市场的发展历史可以概括为以下几个阶段：1.网络安全时代：随着企业办公自动化，网络安全问题开受到关注，防火墙、入侵检测系统、杀毒软件等安全产品进入企业；2.信息安全时代：随着企业内网系统越建越多，纵深防御、信息安全体系的思想开始深入人心；3.互联网安全时代：国家发起“互联网+”行动，互联网、移动互联网应用开始大量进入企业，对抗攻击的安全防御思路逐步呈现；4.网络空间安全时代：《网络安全法》正式颁布，标志着网络安全已经成为国家安全的重要组成部分，网络安全的企业义务得到明确；5.数据安全时代：数据成为新的生产要素，数字化转型席卷全国，保护数据安全就是保护企业发展权；6.智能信创时代：ChatGPT的发布，以及黎巴嫩BP机爆炸事件，使中国发展自主可控的智能网络安全保护体系成为迫在眉睫的任务。

1990年

网络安全时代

- 1994年：《计算机信息系统安全保护条例》发布，这是中国早期关于计算机信息系统安全的法规之一。以企业内网为核心的网络安全时代到来。

2005年

信息安全时代

- 2005 年国际标准化组织（ISO）和国际电工委员会（IEC）联合发布了ISO/IEC 27001国际标准，全球兴起了信息安全管理体系建设的热潮。

2010年

互联网安全时代

- 随着智能手机和移动设备的普及，以及物联网（IoT）技术的发展，电子商务、O2O、的使用变得更加广泛，互联网安全成为一个关键的考虑因素。

2017年

网络空间安全时代（简称网络安全）

- 2017年6月1日《中华人民共和国网络安全法》正式施行，这是中国网络安全领域的基础性法律，为网络安全工作提供了法律依据。也定义了我国网络安全的范畴，也标志着网络空间安全时代的到来。

2020年

数据安全时代

- 2020年4月9日：中共中央、国务院发布《关于构建更加完善的要素市场化配置体制机制的意见》，在这份文件中明确提出将数据作为生产要素，并强调了加快培育数据要素市场的重要性。同时，也标志着正式进入数据安全时代

2023年

智能信创时代

- 2022 年 11 月美国 OpenAI 公司推出的聊天机器人产品ChatGPT，2023 年 8 月 15 日国家互联网信息办公室发布施行《生成式人工智能服务管理暂行办法》。标志着智能安全时代的到来。
- 2024年9月18日，以色列远程操控黎巴嫩BP机爆炸近3000人受伤，全球开始关注信息系统信创安全。

来源：安在新媒体整理

市场驱动力1：法律法规与监管处罚驱动企业安全建设

自2017年《网络安全法》颁布以来，网络安全监管政策不断完善，在等级保护、关键信息基础设施保护、个人信息保护、数据安全、密码管理、反电信诈骗、人工智能安全等领域已出台一批法律法规，形成了我国基本的网络治理机制，同时通过约谈、检查、评测、执法等行动，网信办及公安机关在等保2.0、电信诈骗、APP安全、个人信息保护、内容安全、数据安全法等领域开展持续的监管和处罚工作。这样的态势使企业面临较大的网络安全合规压力，尤其是政企用户、上市公司、外资企业等。在强监管下，网络安全市场形成了持续发展的驱动力。

网络安全相关法律法规要求

类别	法律法规名称
网络安全法	2017年6月1日起实施，是我国第一部全面规范网络空间安全管理方面问题的基础性法律。
关键信息基础设施保护条例	2021年9月1日起施行，是我国首部专门针对信息基础设施安全保护工作的行政法规
数据安全法	2021年9月1日起施行，是我国数据领域的基础性法律，也是国家安全领域的一部重要法律
汽车数据安全管理若干规定	2021年10月1日起施行，用于规范汽车数据处理活动，保护个人、组织的合法权益，维护国家安全和社会公共 利益，促进汽车数据合理开发利用
个人信息保护法	2021年11月1日起施行，是为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用而制定的法律
网络安全审查办法	2022年2月15日起施行，是为了进一步保障网络安全和数据安全，维护国家安全而制定的部门规章
反电信网络诈骗法	2022年12月1日起施行，是为了预防、遏制和惩治电信网络诈骗活动，加强反电信网络诈骗工作，保护公民和组织的合法权益，维护社会稳定和国家安全，根据宪法，制定的法规。
生成式人工智能服务管理暂行办法	2023年8月15日起施行，是我国首歌针对生成式人工智能服务的规范性政策
网络暴力信息治理规定	2024年8月1日起施行，明确网络信息内容管理主体责任、建立健全预防预警机制、规范网络暴力信息和账号处置、强化用户权益保护、加强监督管理、明确法律责任等方面，为加强网络暴力信息治理提供有力支撑

近年来安全监管与处罚

主体	罚金	原因
厦门银行	764.6万元	违反个人金融信息保护规定等23项违法行为
北京某模塑科技有限公司	罚100万元	泄露了小米汽车前后保险杠的早期设计稿
江西某公司	罚50万元	早黑客组织攻击并植入木马病毒，主机存在受控的风险
衡南县某医院	6.2万元罚单	未履行数据安全保护义务，造成部分数据泄露
浙江某科技公司	100万元	未经客户同意，将敏感业务数据擅自上传至公有云服务器上，造成严重数据泄露
赣州某信息技术公司	15万元	业务系统疑似遭受黑客攻击，存在数据泄露风险
平安银行	3492.5万元	违反信用信息采集、提供、查询及相关管理规定，未按规定履行客户身份识别义务，未按规定保存客户身份资料和交易记录，未按规定报送大额交易报告
邮储银行	3186万元	
人保财险	464万元	
南昌某高校	80万元	教职工信息、学生信息、交费信息等3000余万条信息的数据库被黑客非法入侵
知网	5000万元	违法处理个人信息行为的性质、后果、持续时间，特别是网络安全审查情况等因素
重庆某科技公司	10万元	因业务开展，收集、存储、处理网络数据量较大，但未按法律要求建设等保
中行嘉兴分行	210万元	违规泄露客户信息
百行征信	51.5万元	违反征信机构规定采集、提供、查询用户个人信息
腾讯QQ平台	100万元	小世界板块存在大量色情等违法信息，危害未成年人身心健康
上海某政府信息系统承包商	行政处罚	违规将政务数据置于互联网进行测试期间，相关存储端存在高危漏洞，导致大量公民数据泄露，以致成为境外不法分子窃取政务数据的供应链入口
浙江嘉善农商银行	121万元	存在多项数据违法行为
河南光山农商银行	84.2万元	存在8项违法行为
夸克	50万元	破坏网络生态问题
华美银行	60万元	生产环境安全管控不足和生产数据安全管控不足
浙江某大药房	110万元	违反数据安全法
中国银行	430万元	部分重要信息系统识别不全面，灾备建设和灾难恢复能力不符合监管要求，信息系统运行风险识别不到位、处置不及时，引发重要信息系统重大突发事件；
中信银行	400万元	

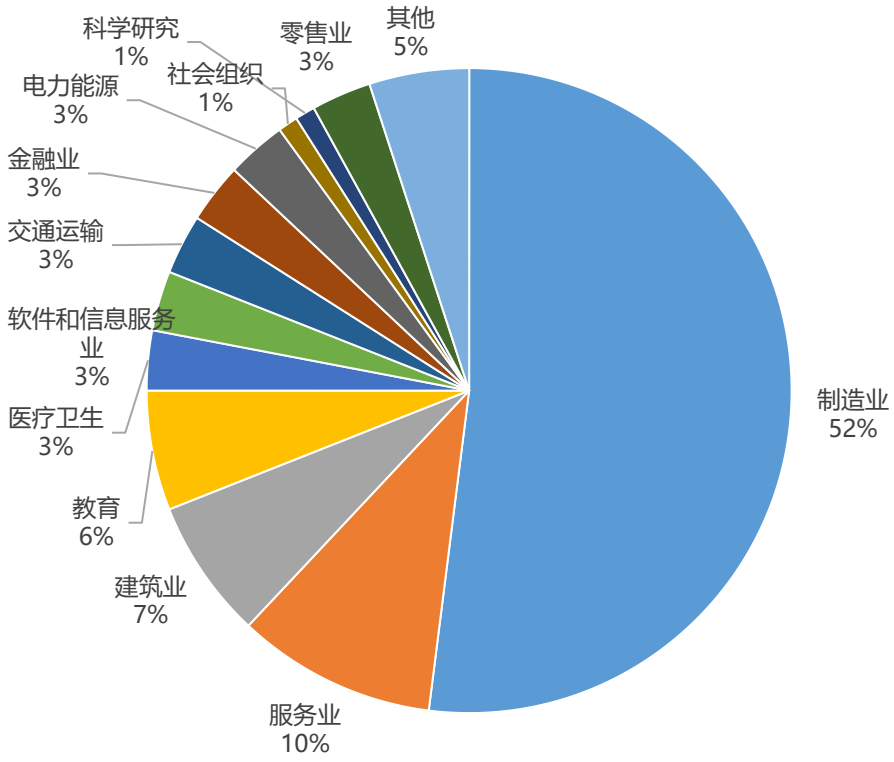
来源：安在新媒体整理

市场驱动力2：网络犯罪与攻击事件促进企业加强防护能力

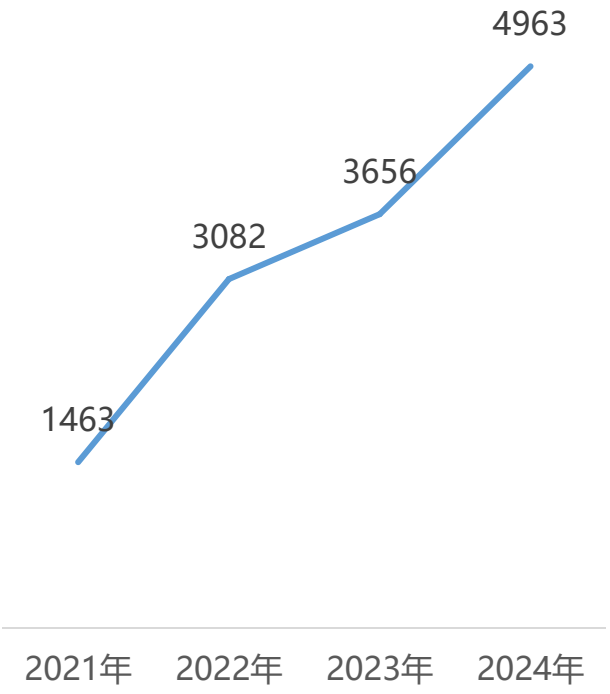
网络犯罪已经进入人工智能时代，勒索软件、APT 等高级威胁正在经历一次 “网络犯罪技术革命” 。人工智能技术降低了网络犯罪分子开发恶意软件的技术门槛，他们可以利用人工智能进行技术咨询、用于网络钓鱼的文本 / 媒体生成、情报收集与攻击侦察、保持匿名和躲避追踪、深度伪造 / 假冒等。随着 ChatGPT 的滥用增加和地下大语言模型工具的开发，复杂攻击的可能性已经升级。全球勒索病毒攻击事件数量呈现明显的持续增长态势。近一年来，全球范围内活跃的勒索病毒组织共计87个，其中活跃度排名前10位的勒索病毒组织发动的攻击活动占全部勒索病毒攻击活动的比例超过一半，呈现出较为集中的态势。近一年来我国受到攻击和勒索的71个机构涉及14个国民经济行业，其中制造业受害情况最为严重。网络犯罪的现实风险驱动企业必须加强网络安全防护能力。

2024年度网络攻击热词

2024年度我国遭受勒索病毒组织攻击行业情况



2024年全球勒索病毒攻击事件数量（单位：起）

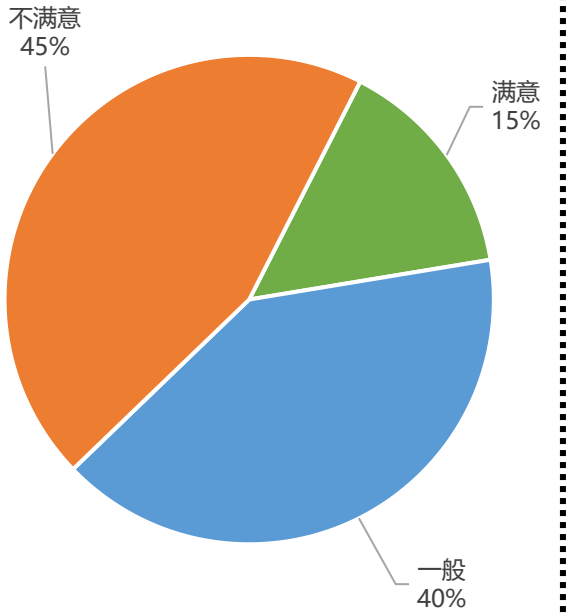


来源：国家计算机病毒应急处理中心、安在新媒体整理

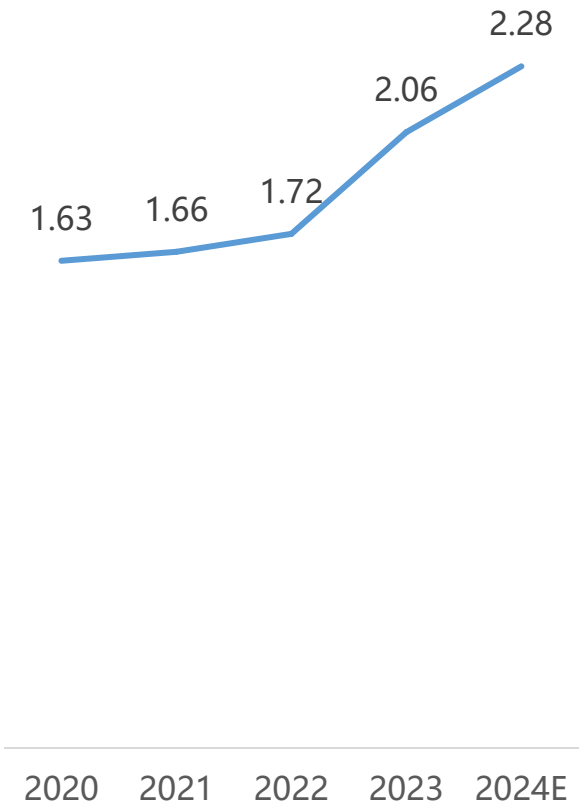
市场驱动力3：社会与民众诉求“安全感”触发企业社会责任建设

随着信息技术的快速发展，民众对隐私保护的意识正在逐步觉醒。在对网民满意度的调查中显示，45%的网民对当前企业的隐私保护现状不满意，仅15%的表示满意。在大数据时代，个人信息的收集和处理变得无处不在，人们开始更加关注个人隐私的保护。2024年，预计网民发起网络侵害事件的举报讲达到2.28亿次。网民呼吁网络“安全感”，这是对企业网络安全保护建设的要求，加强隐私保护建设，就是保护企业客户的权益。继“质量”之后，“安全”成为民众和用户对企业的新诉求，驱动着企业必须加大安全建设的投入，以在新时代下争夺用户的心智。

网民对企业保护隐私现状满意度



全国受理网络事件举报数量（单位：亿件）



2024网民最关注的网络安全10大问题

2024网民最关心的网络安全问题TOP10

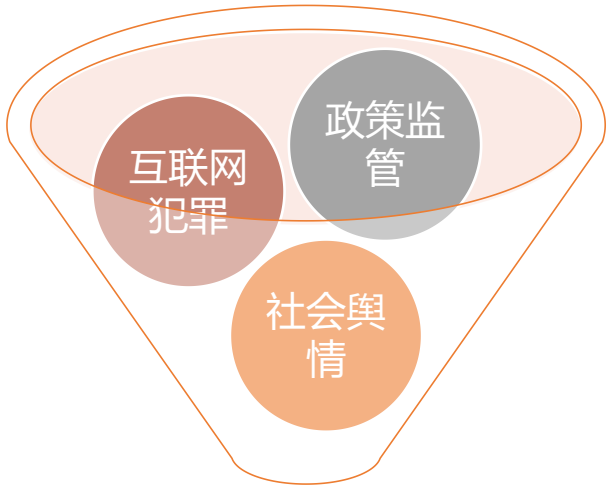
第1名	骚扰电话	未经接收者同意或请求，通过电话、短信等方式向其发送商业广告、推销产品或服务
第2名	手机木马盗资金	多种方式引诱用户在手机上安装木马，窃取支付账户或网上银行中的资金，同时利用用户信息进行盗刷购物或网络贷款。
第3名	违规精准推送	非法采集用户的兴趣、行为、地理位置等信息，向用户推送个性化的广告、内容或服务。
第4名	网络诈骗	利用互联网技术和平台，通过虚假信息、欺骗手段等方式骗取他人财物的行为。
第5名	大数据杀熟	企业利用大数据技术，根据用户的消费习惯、行为模式、地理位置等信息，对不同用户实行不同的价格策略。
第6名	个人信息泄露	个人信息泄露是指个人的姓名、身份证号、电话号码、银行账户信息、家庭住址等敏感信息被非法获取、披露或使用的行为。
第7名	勒索病毒	勒索病毒的攻击不仅会导致用户的数据丢失和业务中断，还可能会对用户的声誉和经济利益造成严重影响。
第8名	网络虚假信息	互联网上传播虚假新闻、谣言、虚假广告、虚假评论等。
第9名	恶意弹窗	在用户浏览网页、使用软件等过程中，突然弹出的广告、推广信息等窗口。
第10名	人脸伪造	又叫“深度伪造”，指利用人工智能技术和软件，对人脸图像进行修改、合成或伪造的行为用于诈骗、虚假宣传、恶意攻击等不良目的。

来源：安在新媒体整理

市场环境：内外压力造成安全风险高企，安全事件多发

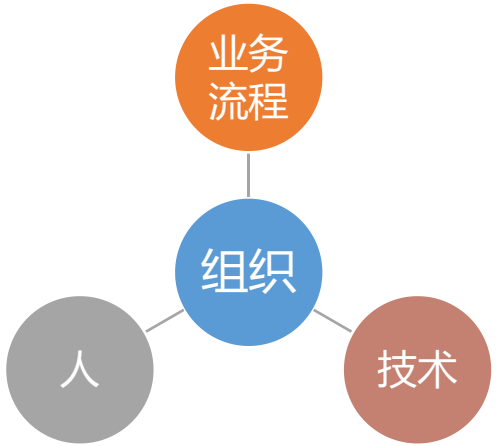
2024年，受外部环境威胁变化和内部降本增效，以及安全投资收紧的影响，预判中国市场企业当前的风险水平为8级安全风险“易受骚扰”级，意味着企业日常在内部经常会发现犯罪分子从外部尝试入侵的痕迹。对于防范能力较弱的企业来说，则有可能面临突发重大安全事件的影响。因此，企业当前的安全建设多会围绕容灾、备份、应急、风险发现能力、运营能力等方面。

企业网络安全风险预测



网络安全外部威胁

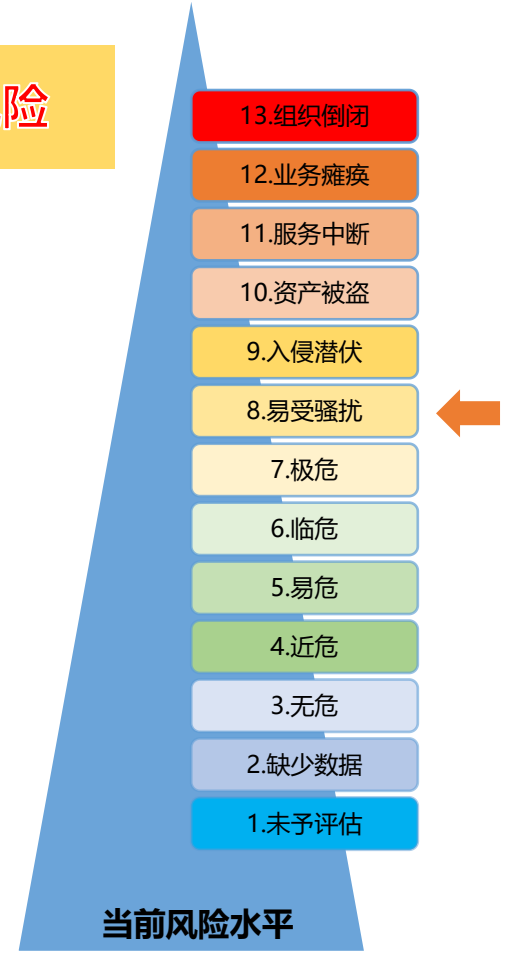
1	政策监管执法力度加大
2	互联网犯罪花样层出不穷
3	社会对隐私保护和网络安全关注度与日俱增



企业组织内部隐患

1	业务流程面临转型，安全预算收紧
2	技术需要引入AI化并迭代
3	员工面临裁撤或低数量水平运转

8级安全风险

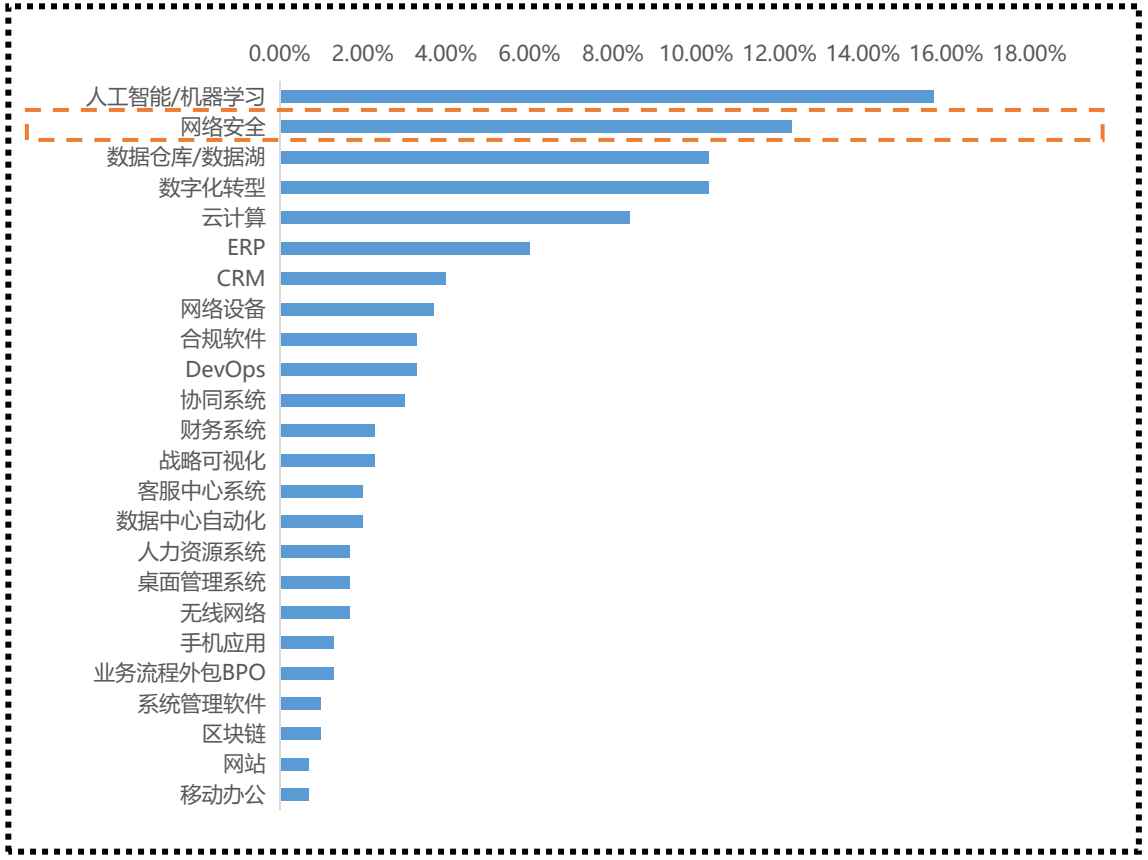


来源：安在新榜整理

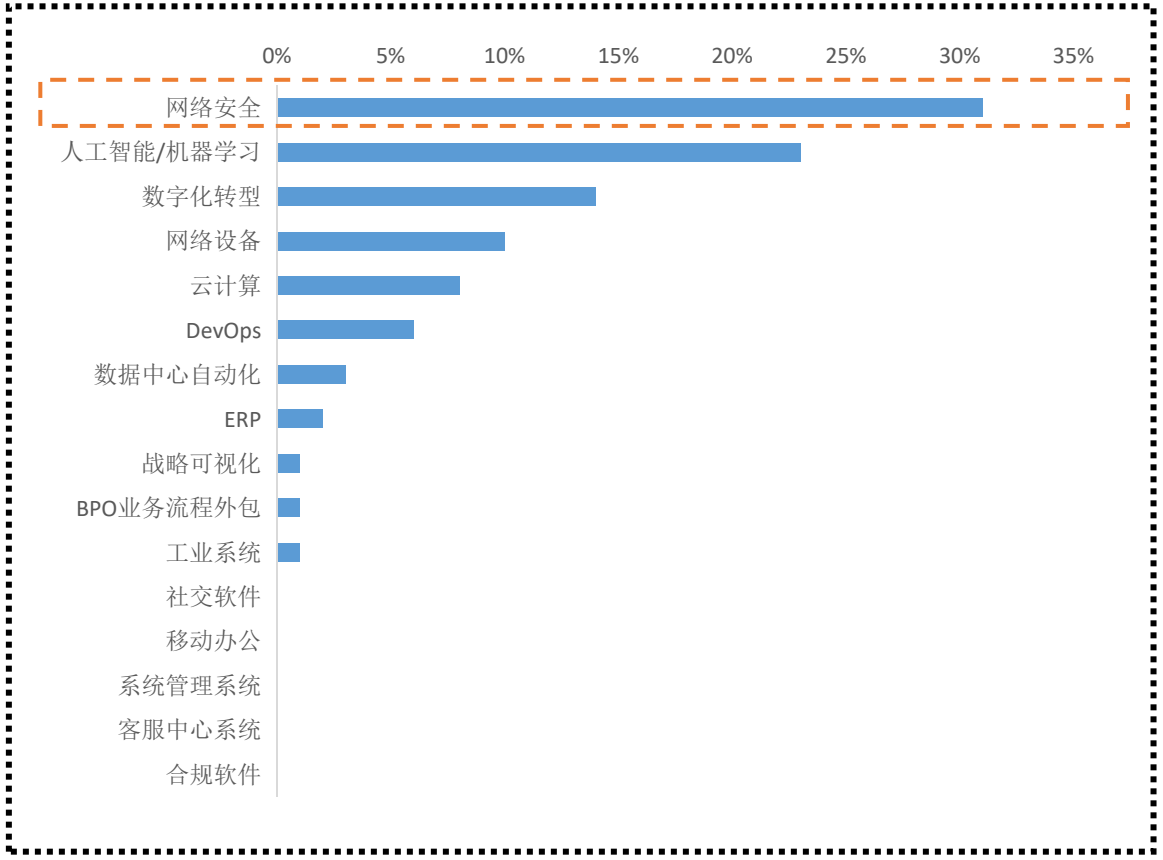
建设意愿：网络安全市场有着必然增长的动能，和持续增长的动力

调查显示，在CIO眼中，2024年，除了AI以外，网络安全方面的开支是最值得公司花钱的地方，也是最不可能削减预算的地方。这显示出网络安全已经成为企业IT支出中不可或缺的一部分，其重要性随着数字化转型的深入而日益凸显。企业必须持续投资于网络安全，以确保数据安全、保护企业资产、维护客户信任，并满足法律法规的要求。因此，当前的网络安全投资疲软，只是短期市场调整。从长期来看，网络安全市场有着较强的必然增长动能，和持续增长的动力。

2024支出增幅最大的项目



2024最不可能被削减的IT项目



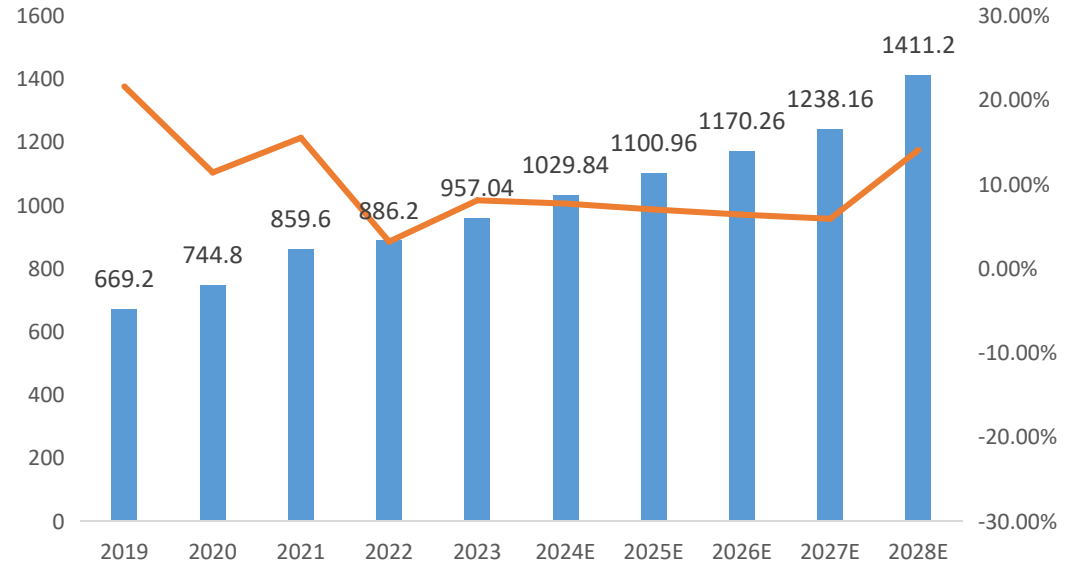
来源：安在新媒体整理

目录

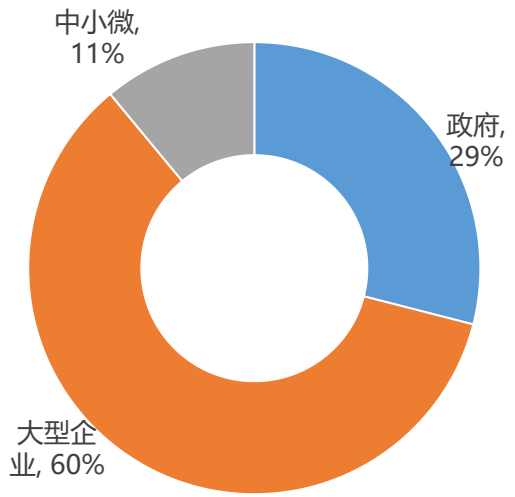
市场概况：当前中国网络安全市场预计1029.84亿元

2023年我国网络安全市场规模为957.04亿元，2024年市场规模将达到1029.84亿元，预计到2028年突破1400亿元。我国网络安全市场的用户主体超过60% 的是大型企业，政府占比29%，其次为中小微企业，占比为11%。

中国网络安全市场规模（亿元）



用户类型构成

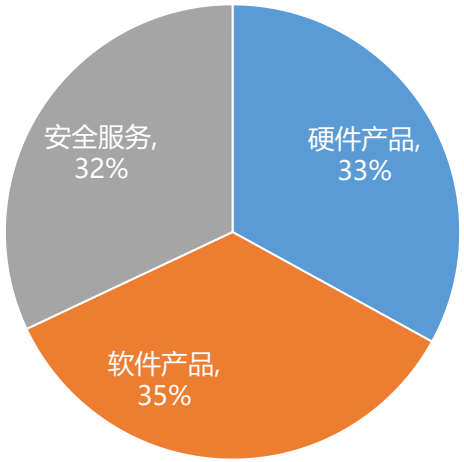


来源：安在新媒体整理

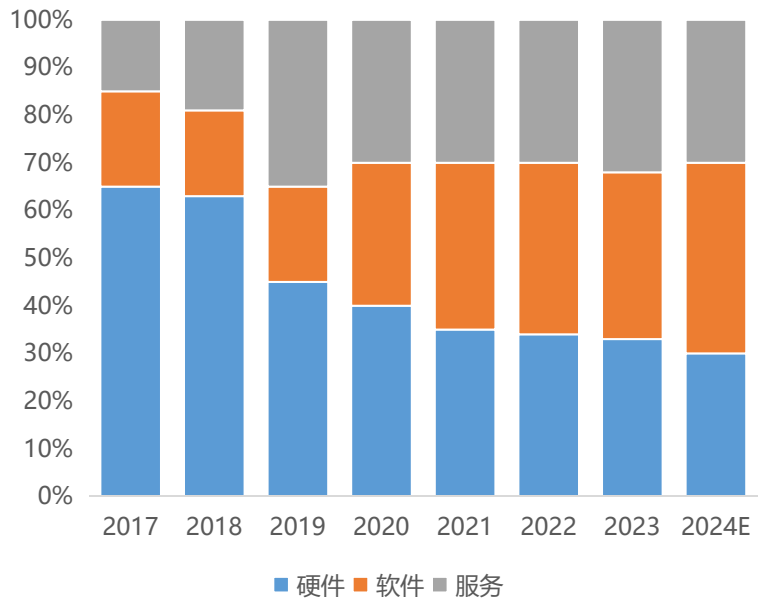
细分格局：安全软件市场规模逐年扩大，蚕食安全硬件市场

我国网络安全市场中软件产品市场规模最大，市场规模334.96亿元，占比为35%，其次是硬件产品，市场规模为315.82亿元，占比33%，安全服务市场规模为306.25亿元，占比为32%。从发展历程来看，安全硬件市场不断被安全软件蚕食，到如今，网络安全市场呈“三足鼎立”态势。从地理格局来看，华北、华东、华南是网络安全的主要市场。

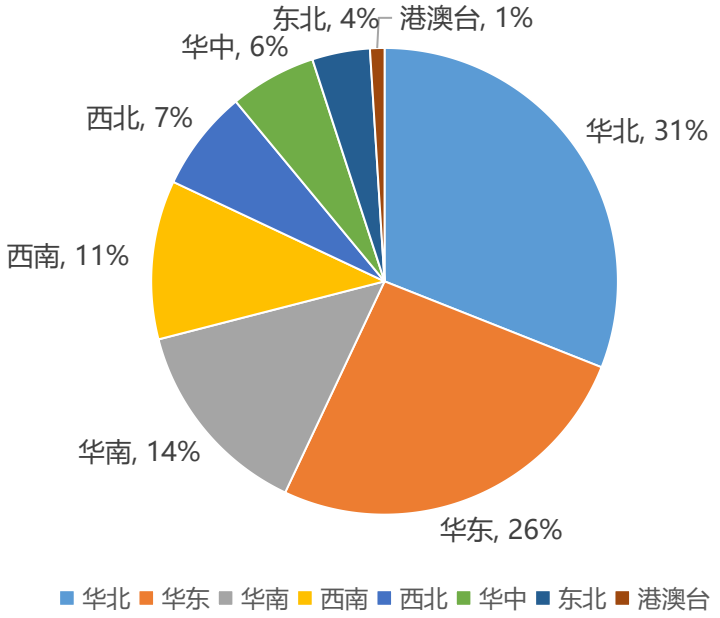
市场分类



细分市场结构变化



地域格局

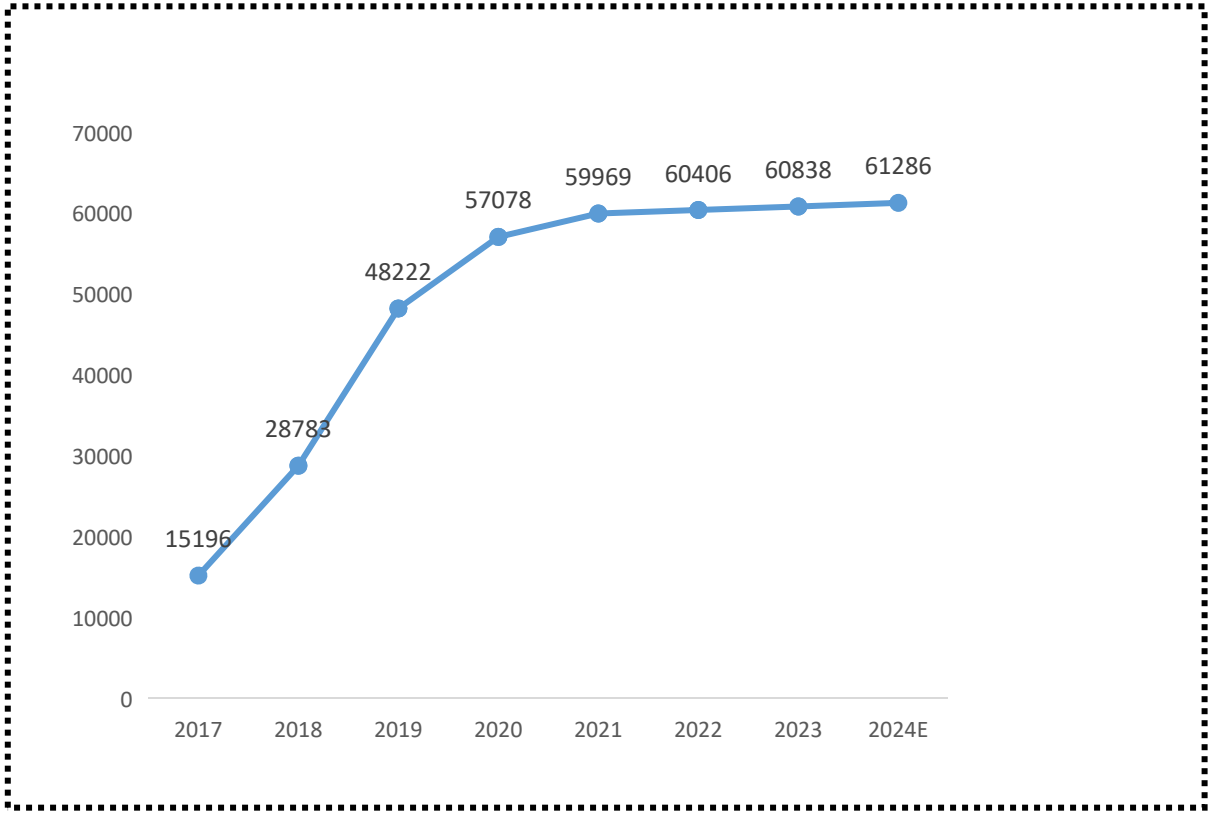


来源：安在新媒体整理

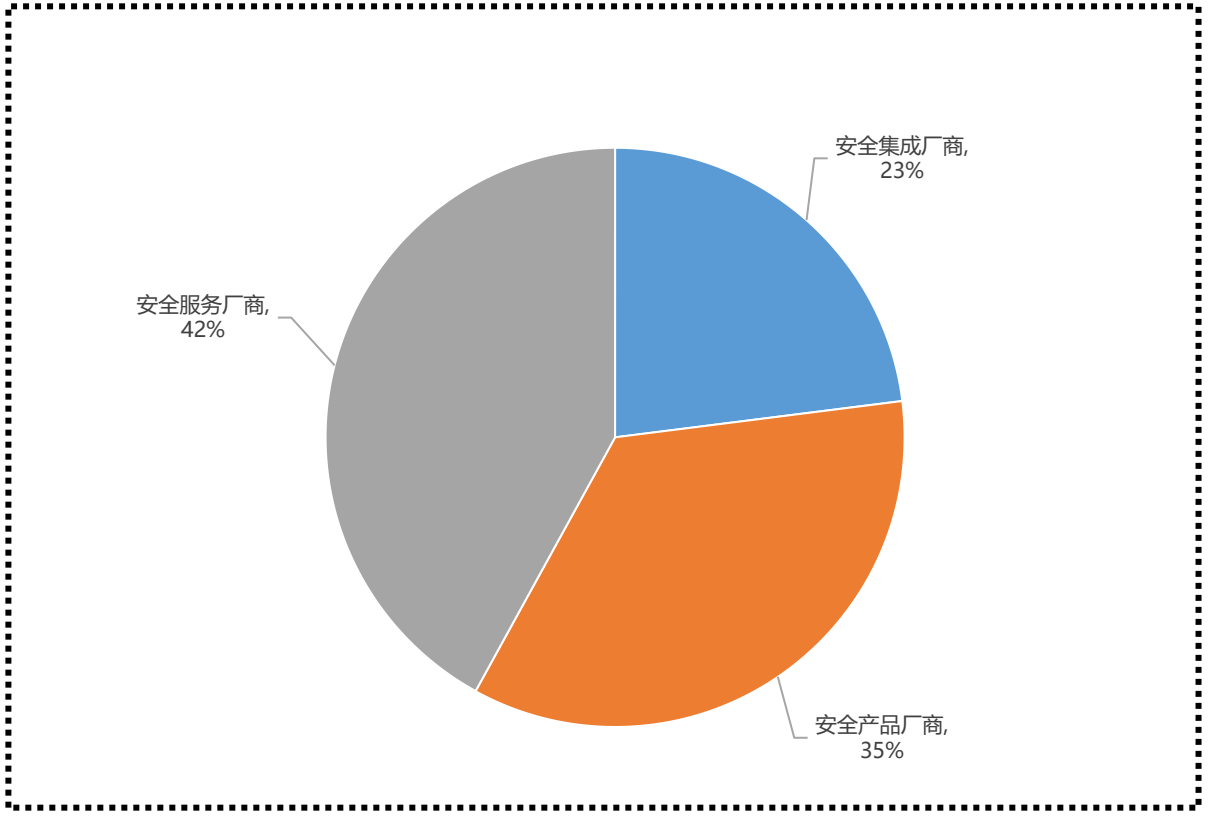
安全厂商：企业数量增长减弱，标志市场达到阶段性饱和状态

2024年中国网络安全企业预计达到61286家，相较前几年，已度过了快速增长期，标志着现有企业能够满足市场需求，导致新企业进入市场的动力减弱。也说明在没有新技术、新场景出现前，网络安全市场达到了阶段性饱和状态。另外，所有厂商中，42%是安全服务厂商，35%是安全产品厂商，23%是安全集成厂商。这之中，安全集成厂商有所增加，一方面可能是传统IT集成厂商杀入了安全集成领域，另一方面也可能是市场竞争加剧，推动厂商向更多元化的方向发展的结果。无论如何，网络安全企业数量连续多年低速增长反映出行业的成熟、市场竞争的加剧、外部经济环境的影响等多种因素。这种状态可能促使现有企业更加注重创新和提升服务质量，以维持竞争力。

2024中国网络安全企业数量



中国市场厂商类型



来源：安在新媒体整理

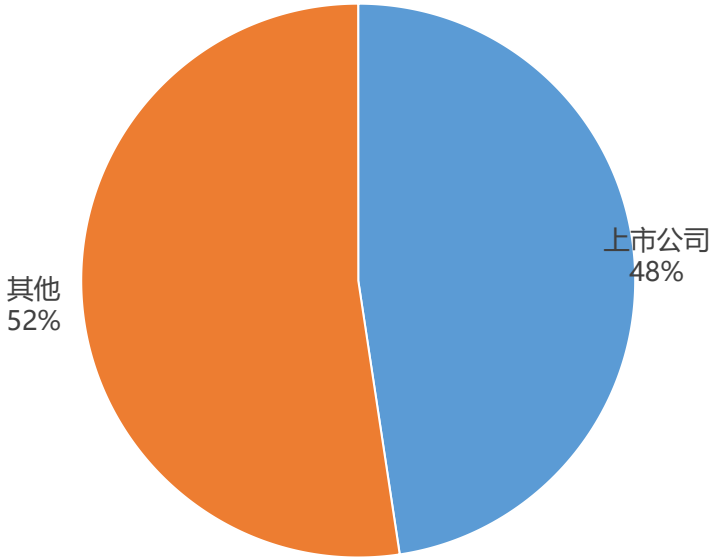
竞争格局：六霸五超多强格局即成，上市公司仍是市场主力

在本次调查涉及的160种安全产品及服务品类中，每个品类的产品和服务都涉及到20家以上的厂商在竞争，而对所有品类产品的前十强进行统计后，我们发现，在充分竞争的网络安全市场中，在企业用户心目中网络安全市场已形成“六霸五超多强”的格局。而且这一局面多年来趋于稳定。另外，2023年度，29家网络安全类上市公司营收总和占中国网络安全市场67%的份额，仍然是该厂商的主力。

中国市场主要厂商分级

级别	类别	说明	代表厂商（不分先后顺序）
六霸	综合性厂商	在多个安全领域有独到的安全产品，可以称霸一方，同时有兼具广泛地安全能力覆盖面，每家厂商都覆盖了超过一半以上的网络安全细分赛道。是整合整个网络安全市场的超级玩家级企业；	奇安信、360数字安全、SANGFOR深信服科技、启明星辰、NSFOCUS、HUAWEI
五超	扩张性厂商	企业安全能力和口碑，都远超其他安全厂商，覆盖了超过1/3以上的网络安全细分赛道，并在多个赛道上有制霸的产品。这是正试图向上一级“六霸”传统优势领域发起挑战的企业；	腾讯安全、阿里安全、安恒信息、H3C、AsiaInfo、亚信安全
多强	成长性厂商	企业已经在某一领域取得优势地位，并开始在多个领域开展技术布局，谋求扩张，但这类企业面临最多的竞争，一方面需要稳住自己的优势领域，另一方面又面临多个方面同时需要开拓和突破的挑战。	天融信、卡亭科技、斗象科技、观安、联软科技、DP tech
其他	专业性厂商	企业在细分领域具备技术优势，或者在特定地域获得本地化优势，并寻求扩大品牌壁垒的厂商。	美亚柏科、天空卫士、齐治科技

上市安全厂商营收权重

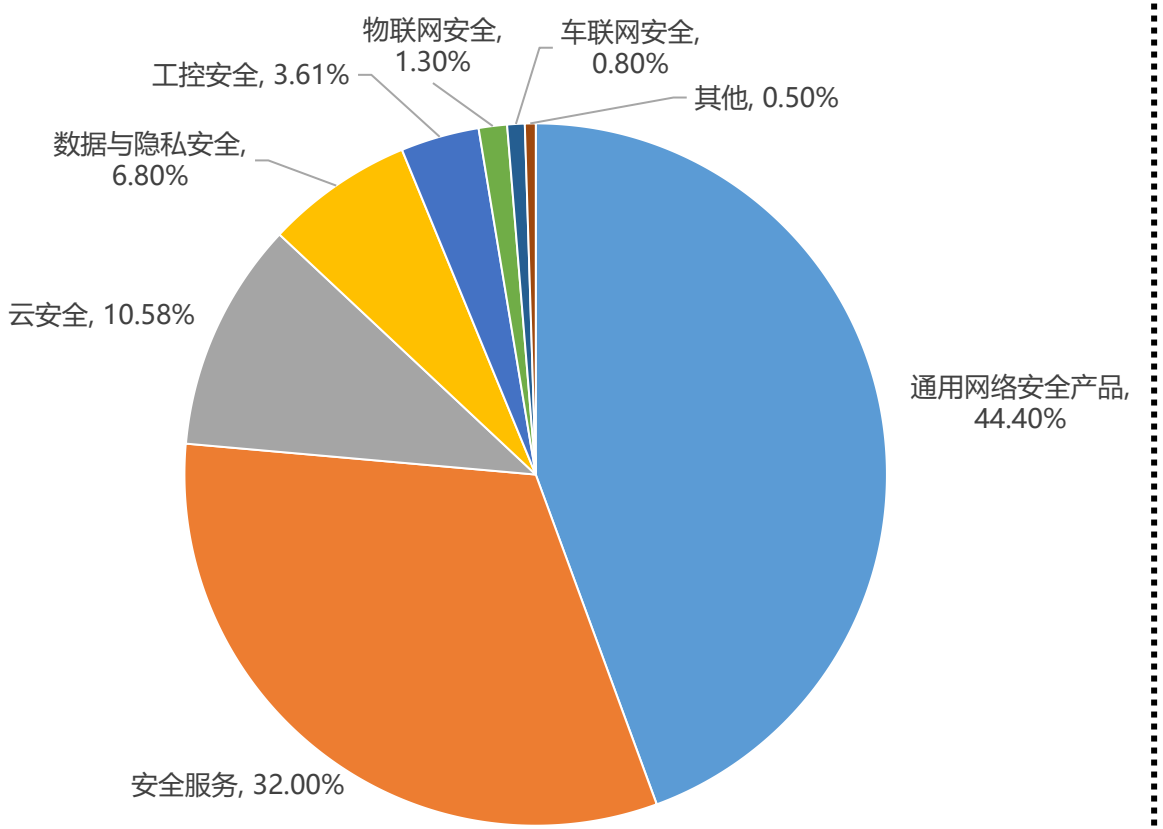


来源：安在新媒体整理

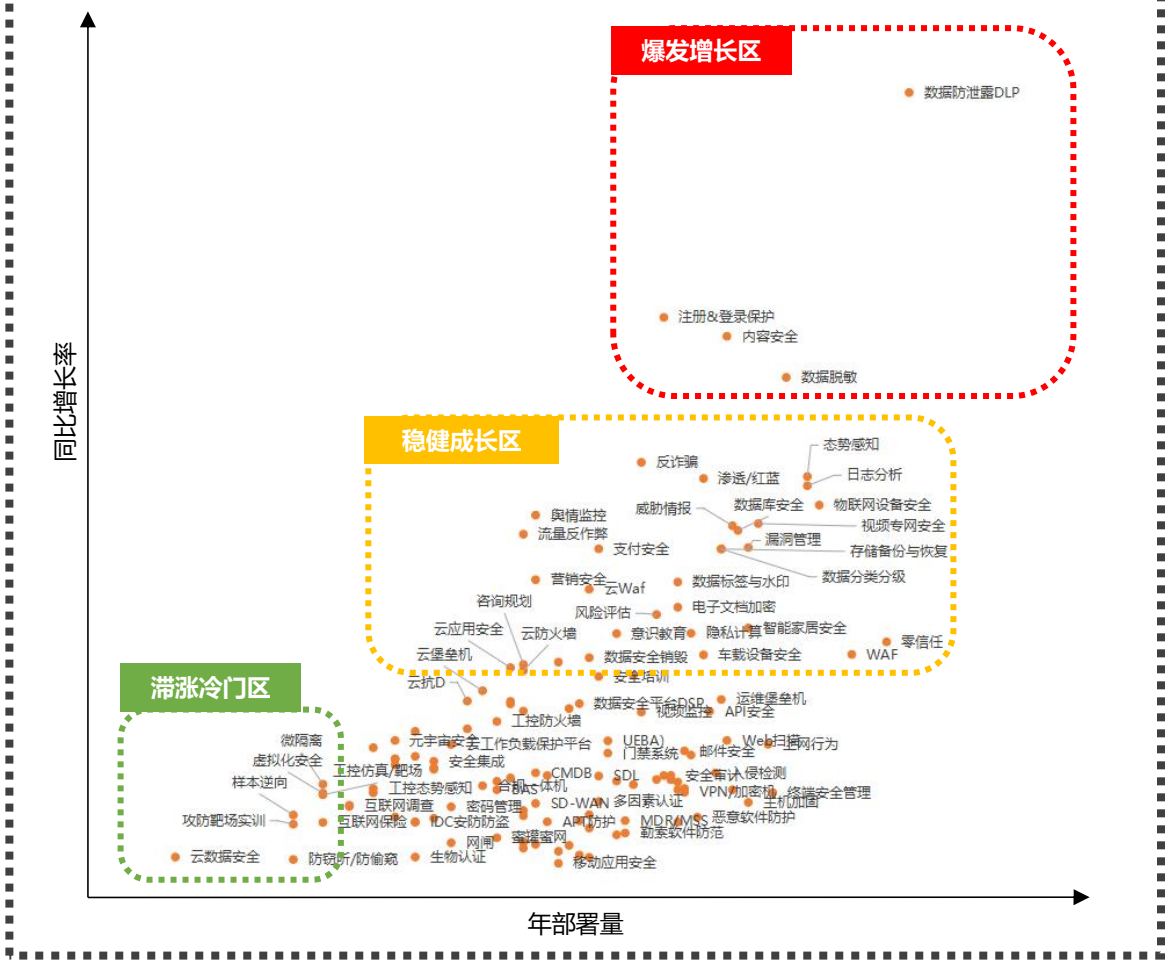
分类市场：云安全、数据与隐私安全、工控安全市场不断扩大

按产品类型分，我国网络安全市场中通用网络安全产品占比最高达到44.4%，安全服务占比32%，云安全产品占比10.58%，数据与隐私安全产品占比6.8%，工控安全产品占比3.61%，物联网安全产品占比1.3%，车联网安全产品占比0.8%。其中得益于监管政策的推动，数据与隐私安全市场增长最快，其次为云安全市场，在疫情后居家办公推动的上云趋势，让云安全成为市场创新迭代速度加快，而随着制造企业日益重视网络安全，工控安全市场也开始稳步增长。物联网安全、车联网安全市场尚属于萌芽期。

中国网络安全产品分类市场



年度增长最快产品



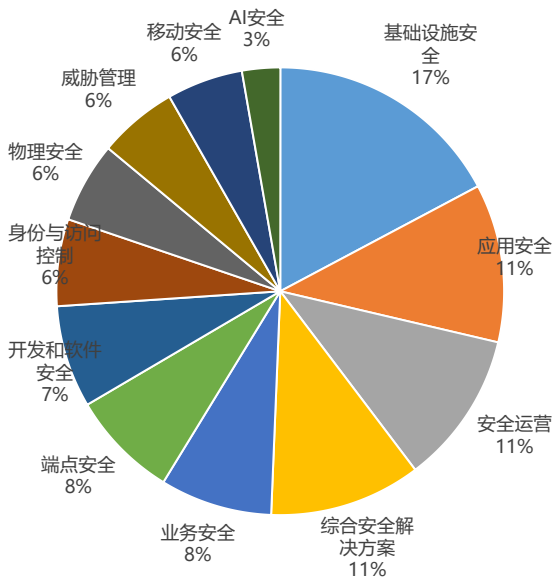
来源：安在新媒体整理

通用网络安全：产品种类碎片化，市场集中度低，AI安全成新热点

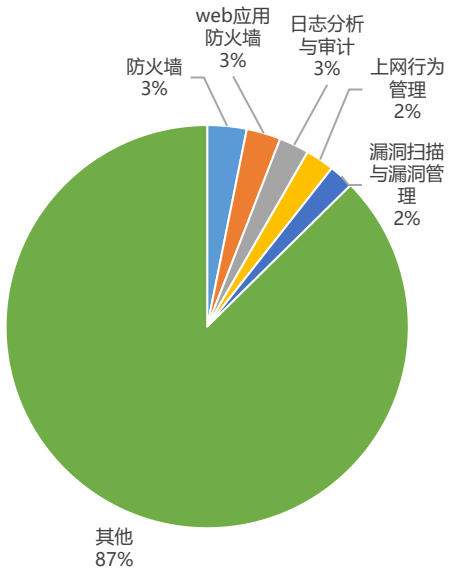
2023年我国通用网络安全市场规模424.96亿元，其中基础设施安全产品占比17%，应用安全占比11%，安全运营占比11%，综合安全解决方案占比11%，业务安全占比8%，端点安全占比8%，开发和软件供应链安全占比7%，身份与访问控制占比6%，物理安全占比6%，威胁管理占比6%，移动安全占比6%，AI安全占比3%。随着生成式人工智能的普及，AI安全成为新热点。

在所有子类产品中，市场份额排名前五的分别是防火墙3%、Web应用防火墙3%、日志分析与审计3%、上网行为管理2%、漏洞扫描与漏洞管理2%，前五名总份额仅占10%，市场集中度低。但是该领域厂商集中度一般，排名前五的厂商奇安信、启明星辰、深信服、绿盟科技、华为（排名不分先后）市场规模总额占比达27.5%。

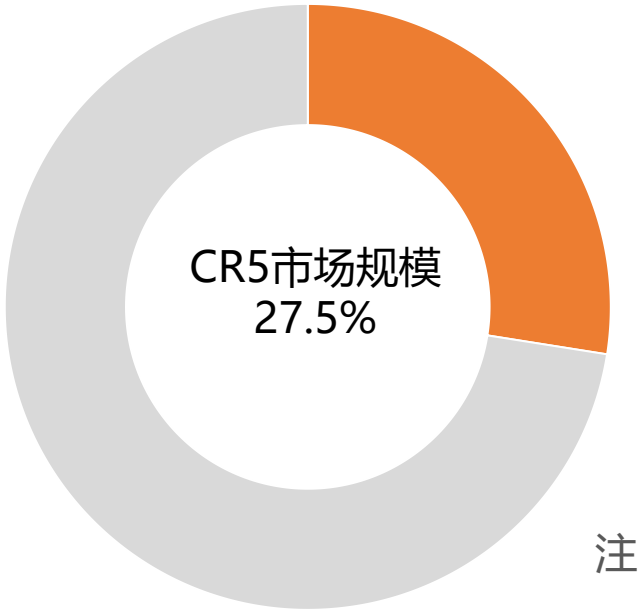
通用网络安全产品市场



市场集中度



通用网络安全产品CR5厂商市场规模占比



奇安信 启明星辰 SANGFOR 深信服科技 NSFOCUS HUAWEI

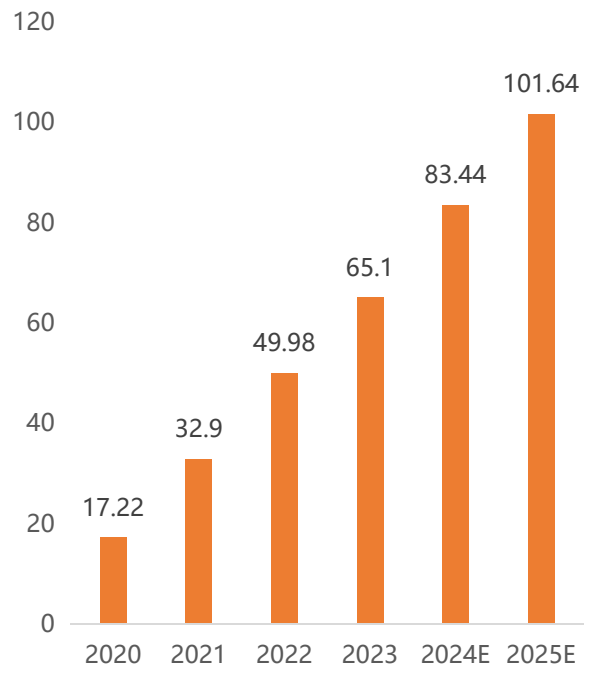
注：CR5排名不分先后

来源：安在新媒体整理

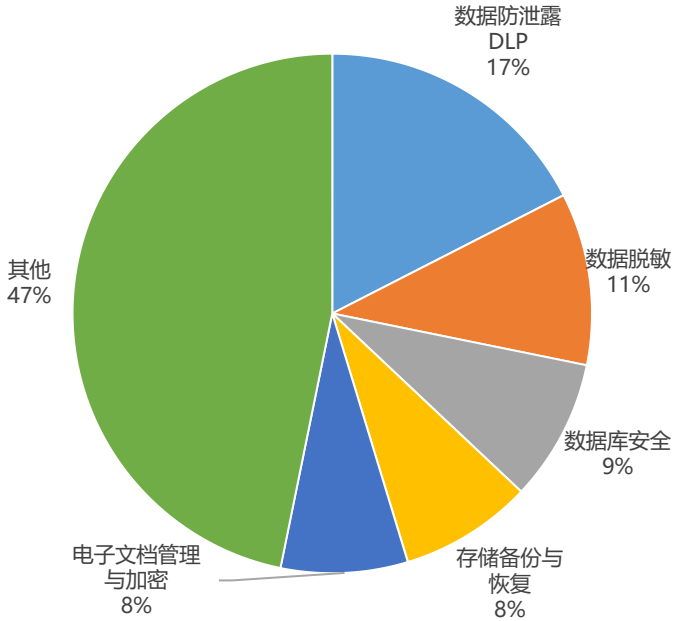
数据与隐私安全：进入快速增长阶段，市场集中度高，DLP产品成最热

我国2023年数据与隐私安全市场规模65.1亿元，预计2024年达到83.44亿元，2025年将达到101.64亿元，该领域正进入快速增长期。
在所有子类产品中，市场份额排名前五的分别是数据防泄露17%、数据脱敏11%、数据库安全9%、存储备份与恢复8%、电子文档管理与加密8%，前五名总份额占53%，市场集中度高。同时，该领域厂商集中度一般，排名前五的厂商深信服、奇安信、天空卫士、美创、观安（排名不分先后）市场规模总额占比达37.43%。

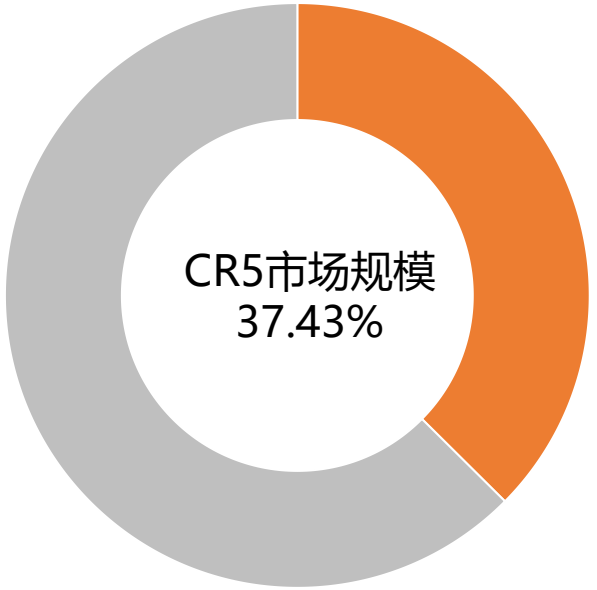
中国数据与隐私安全市场规模（亿元）



市场集中度



数据和隐私安全产品CR5厂商市场规模占比



SANGFOR 深信服科技
奇安信
天空卫士 SkyGuard
美创 MEICHUANG
观安

注：CR5排名不分先后

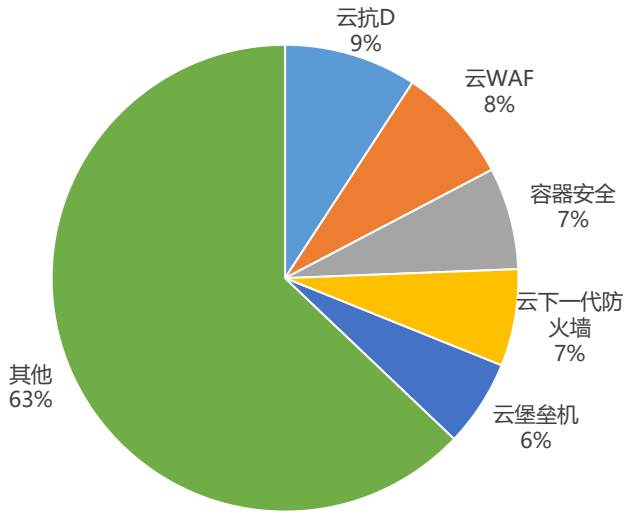
来源：安在新媒体整理

云安全：市场稳步增长，云安全厂商崛起

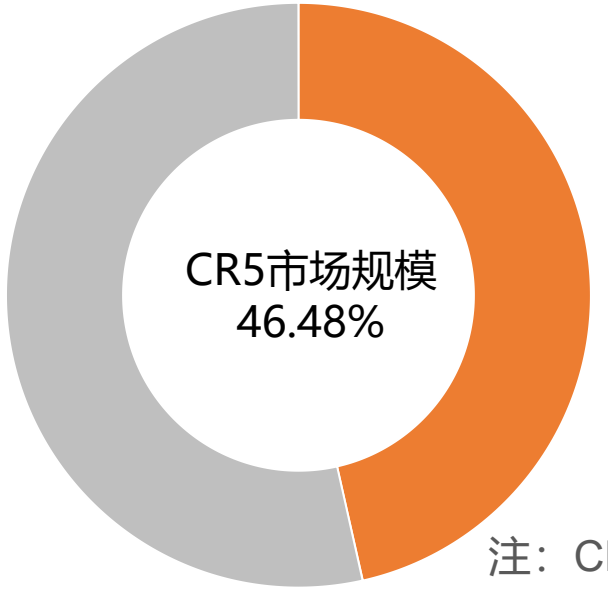
我国2023年云安全市场规模101.22亿元，预计2024年达到120.96亿元，2025年将达到140.42亿元，该领域正进入稳定增长期。
在所有子类产品中，市场份额排名前五的分别是云抗D9%、云WAF8%、容器安全7%、云下一代防火墙7%、云堡垒机8%，前五名总份额占37%，市场集中度较高。同时，前五名也显示出当前云安全产品还是围绕企业上云替换为主的趋势。
在厂商方面，该领域厂商集中度较高，排名前五的厂商奇安信、阿里安全、腾讯安全、360数字安全、深信服（排名不分先后）市场规模总额占比达46.48%。其中，阿里安全、腾讯安全等云计算企业逐步下场角逐网络安全传统厂商市场份额成为趋势。

中国数据安全市场规模（亿元）

市场集中度



云安全产品CR5厂商市场规模占比



奇安信
阿里安全 ALIBABA SECURITY
腾讯安全 Tencent Security
360数字安全
SANGFOR 深信服科技

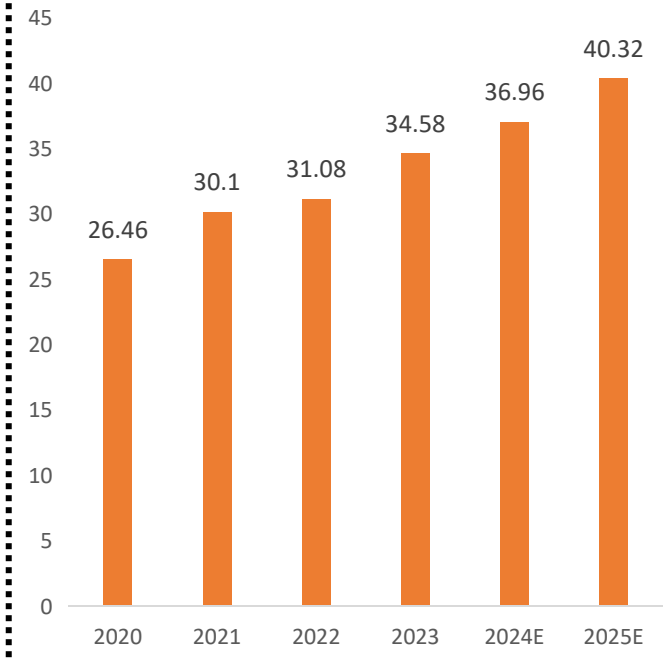
注：CR5排名不分先后

来源：安在新媒体整理

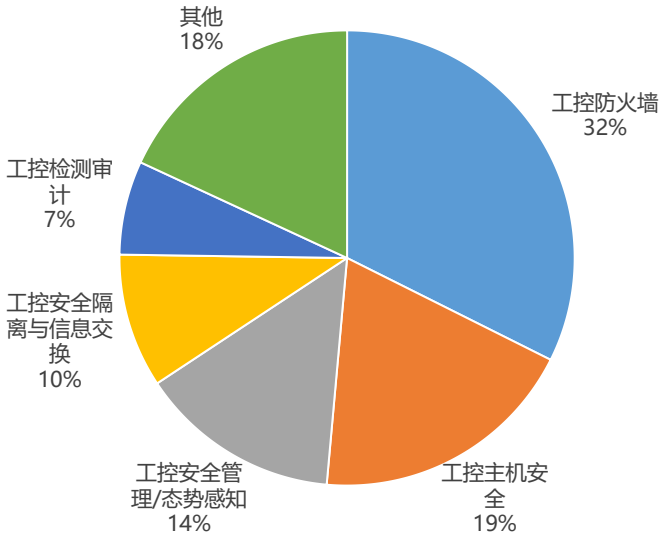
工控安全：市场稳定增长，产品集中度高，技术创新不足

我国2023年工控安全市场规模34.58亿元，预计2024年达到36.96亿元，2025年将达到40.32亿元，该领域正进入稳定增长期。
在所有子类产品中，市场份额排名前五的分别是工控防火墙32%、工控主机安全19%、工控态势感知14%、工控安全隔离与信息交换10%、工控检测审计7%，前五名总份额占82%，市场集中度极高，也表明该领域技术创新不足。同时，该领域厂商集中度也比较高，排名前五的厂商迪普、威努特、六方云、奇安信、长扬科技（排名不分先后）市场规模总额占比达53.26%。

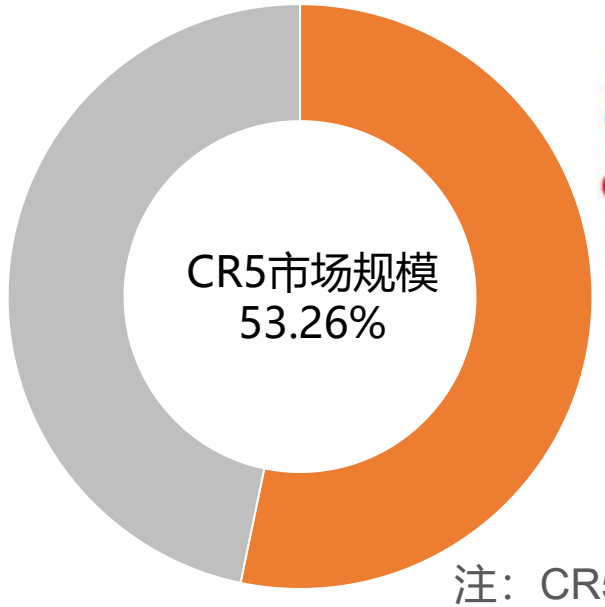
中国工控安全市场规模（亿元）



市场集中度



工控安全CR5厂商市场规模占比



DP tech 威努特 WINICSSEC 6cloud 六方云 奇安信 长扬科技 CHANGYANG TECH

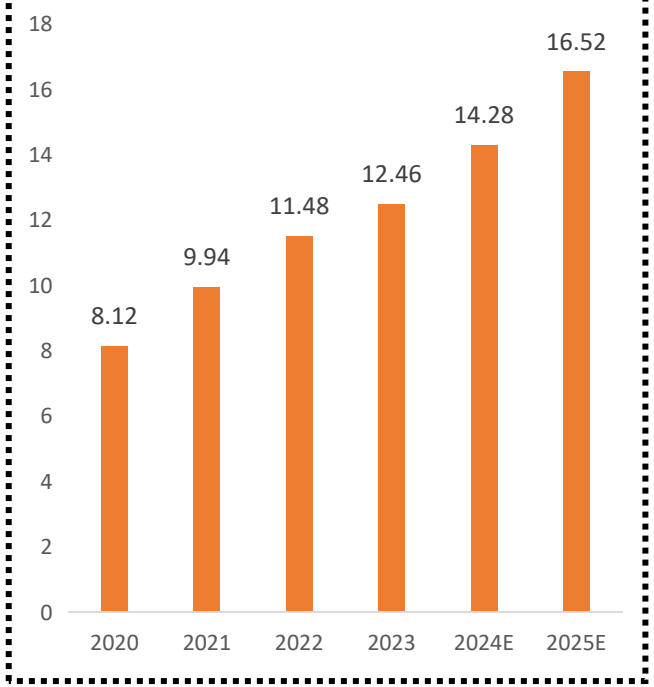
注：CR5排名不分先后

来源：安在新媒体整理

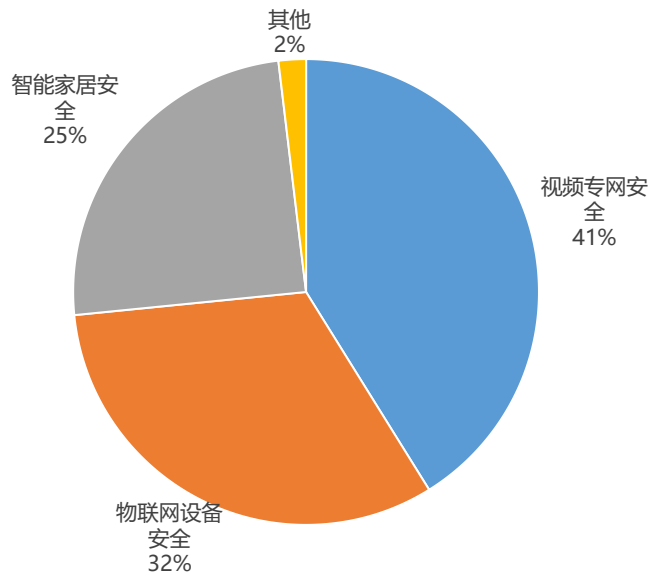
物联网安全：各类专网安全将成为下一阶段的市场增长点

我国2023年物联网安全市场规模12.46亿元，预计2024年达到14.28亿元，2025年将达到16.52亿元，该领域市场规模正逐步扩大。
在所有三类子类产品中，视频专网安全41%、物联网设备安全32%、智能家居安全25%，其他产品2%。视频专网安全产品占比最大，随着物联网设备的普及，各类专网安全将成为下一阶段的市场增长点。
同时，该领域厂商集中度较低，排名前五的厂商华为、小米、天懋信息、绿盟科技、奇安信（排名不分先后）市场规模总额占比达25.16%。

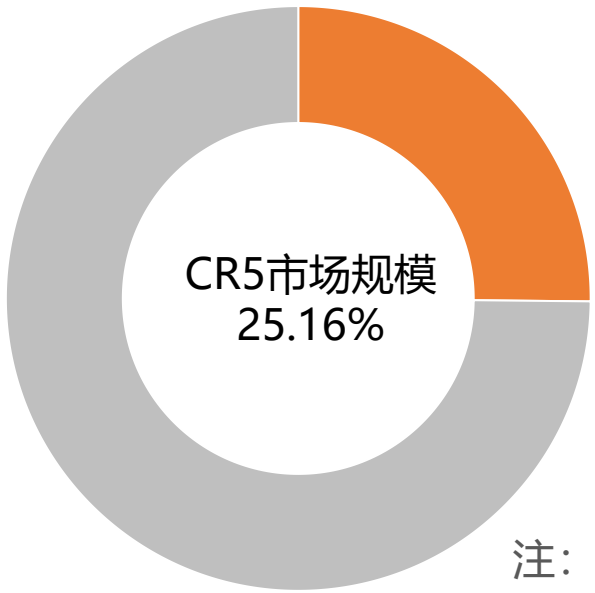
中国物联网安全市场规模（亿元）



市场集中度



物联网安全CR5厂商市场规模占比



HUAWEI
小米 xiaomi.com
天懋信息 TRUSTMO INFO
NSFOCUS
奇安信

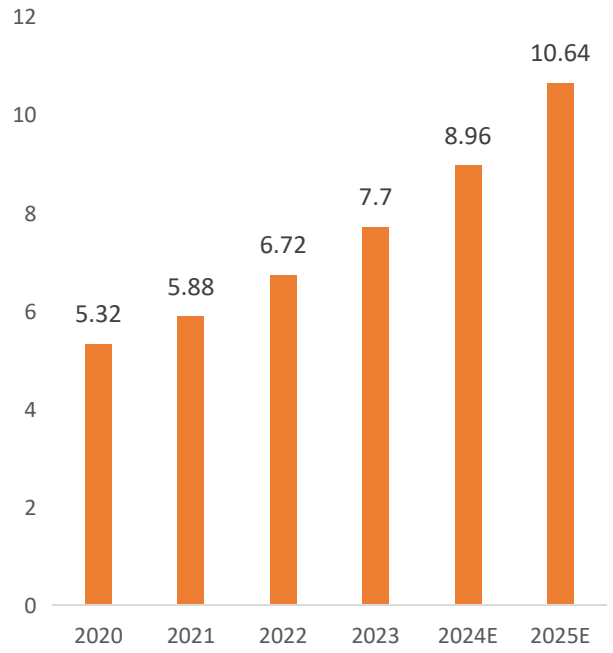
注：CR5排名不分先后

来源：安在新媒体整理

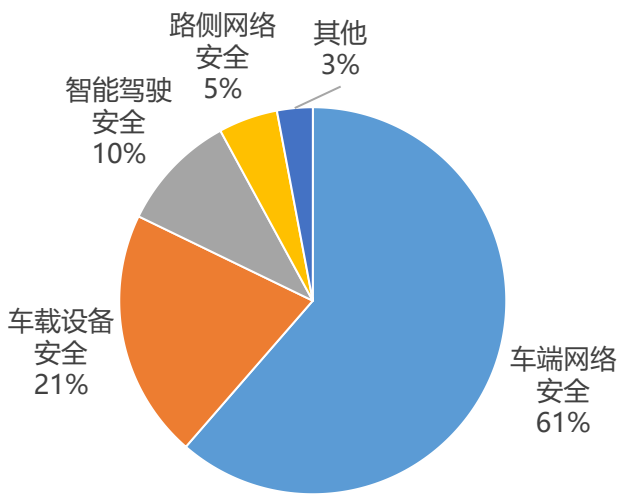
车联网安全：想象空间巨大，技术能力不足，亟待研发新产品

我国2023年车联网安全市场规模7.7亿元，预计2024年达到8.96亿元，2025年将达到10.64亿元，该领域市场规模正逐步扩大。
在所有四类子类产品中，车端网络安全61%，车载设备安全21%，智能驾驶安全10%，路侧网络安全5%，其他占比3%。该领域安全市场想象空间巨大，但受限于技术能力，该领域网络安全解决方案仍显不足，亟待研发。
该领域厂商集中度一般，排名前五的厂商华为、360数字安全、奇安信、绿盟科技、安恒信息（排名不分先后）市场规模总额占比达32.62%。

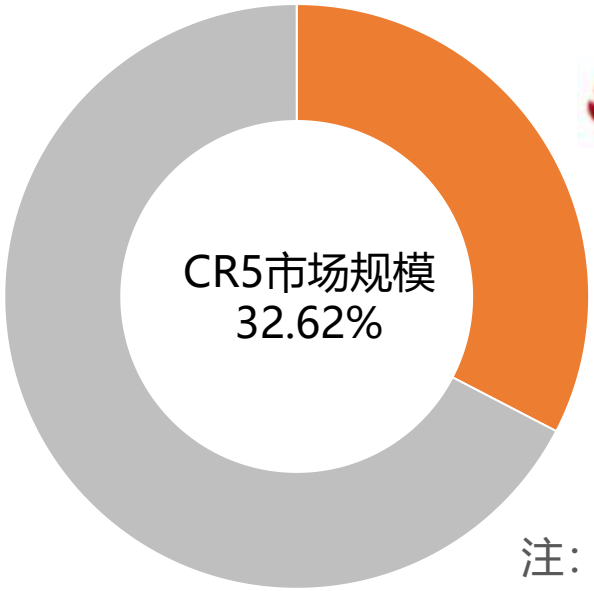
中国车联网安全市场规模（亿元）



市场集中度



车联网安全CR5厂商市场规模占比



HUAWEI
360数字安全
奇安信
NSFOCUS
安恒信息

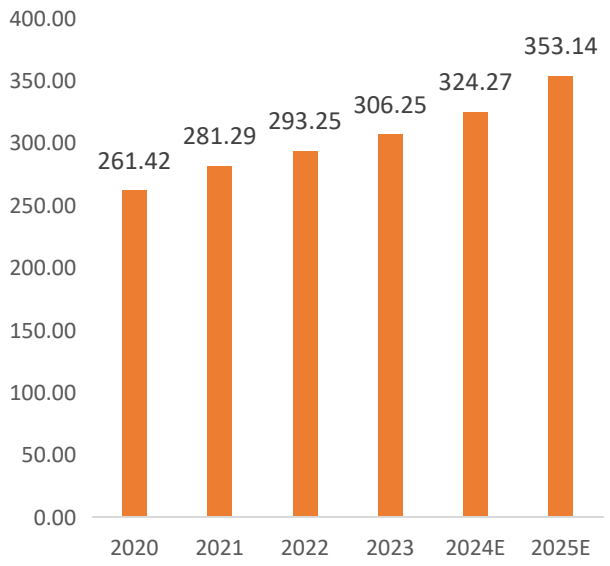
注：CR5排名不分先后

来源：安在新媒体整理

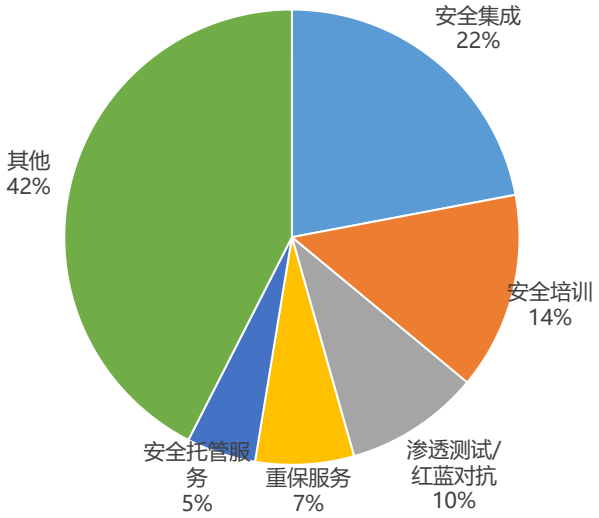
安全服务：安全托管服务日益兴起，成为安全服务新趋势

我国2023年安全服务市场规模306.25亿元，预计2024年达到324.27亿元，2025年将达到353.14亿元，该领域发展稳定。
在所有子类服务中，市场份额排名前五的分别是安全集成22%、安全培训14%、渗透测试/红蓝对抗10%、重保服务7%、安全托管服务5%，前五名总份额占58%，市场集中度较高。安全托管服务日益兴起，成为安全服务新趋势。
在厂商方面，该领域厂商集中度也一般，排名前五的厂商启明星辰、奇安信、绿盟科技、深信服、天融信（排名不分先后）市场规模总额占比达29.24%。

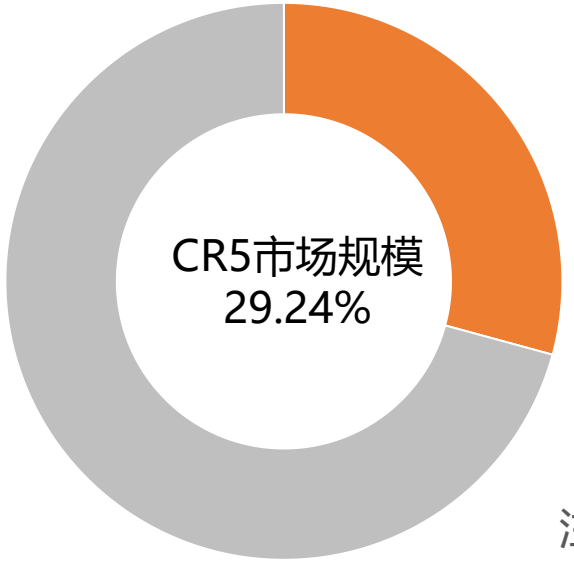
中国安全服务市场规模（亿元）



市场集中度



安全服务CR5厂商市场规模占比



启明星辰 奇安信 NSFOCUS SANGFOR 深信服科技 天融信 TOPSEC

注：CR5排名不分先后

来源：安在新媒体整理

目录

趋势一：中国网络安全市场热门趋势预测

中国网络安全市场在当前地缘紧张局势和经济下行压力下，进入产业调整期，预计在2025年下半年企稳，同时在新一轮外部威胁下，重新进入快速增长通道，将在服务化转型、行业应用深化、供应链安全重视、云安全和边缘计算挑战、隐私增强技术采用、网络安全保险增长、国际合作与数据跨境、政策驱动和需求拉动以及产业自主可控等多方面形成新的发展动能。

中国网络安全市场预测

威胁态势	虚假信息	供应链&信创	密码算法
21%	50%	30%	8%
由于勒索病毒攻击中招后就很难恢复的特点，利用暴露数据管理来预防威胁将同比增长21%	对抗虚假信息的开支将同比增加50%	30%的大型企业将坚决发展反脆弱供应链或信创替代，以实现在中断和不确定性的开源组件情况下实现企业业务目标	经典加密算法面临来自AI和量子计算机的挑战，8%的组织将开始迁移到量子加密系统上保护数据
2025	2025	2026	2028

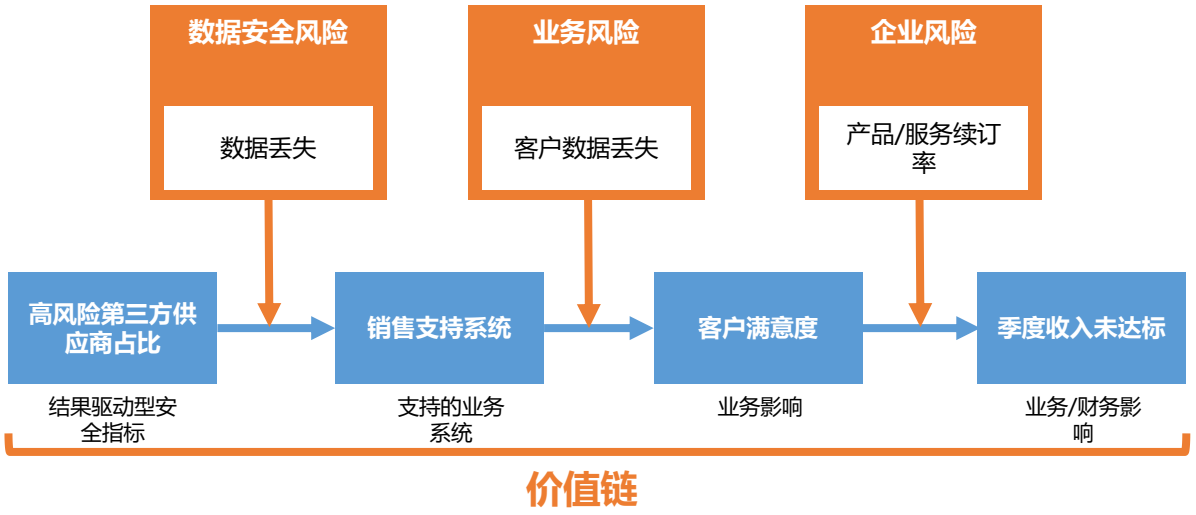
董事会治理	隐私	人的因素	混合工作安全
60%	53%	80%	36%
60%企业董事会成员中包含一名具有网络安全经验的成员	53%的企业将提供集中式的隐私用户体验，如通过自助服务管理用户隐私偏好和同意，以提高用户满意度和合规性。	80%人为风险将通过AI赋能的方式加以控制，如弱口令、网络钓鱼、误操作、欺诈、舞弊、社交攻击等。	远程和混合工作模式将普及，个人数据的追踪和监测活动将变得更加频繁，36%的企业需要成熟的零信任或SASE架构规划
2028	2028	2030	2030

来源：安在新媒体整理

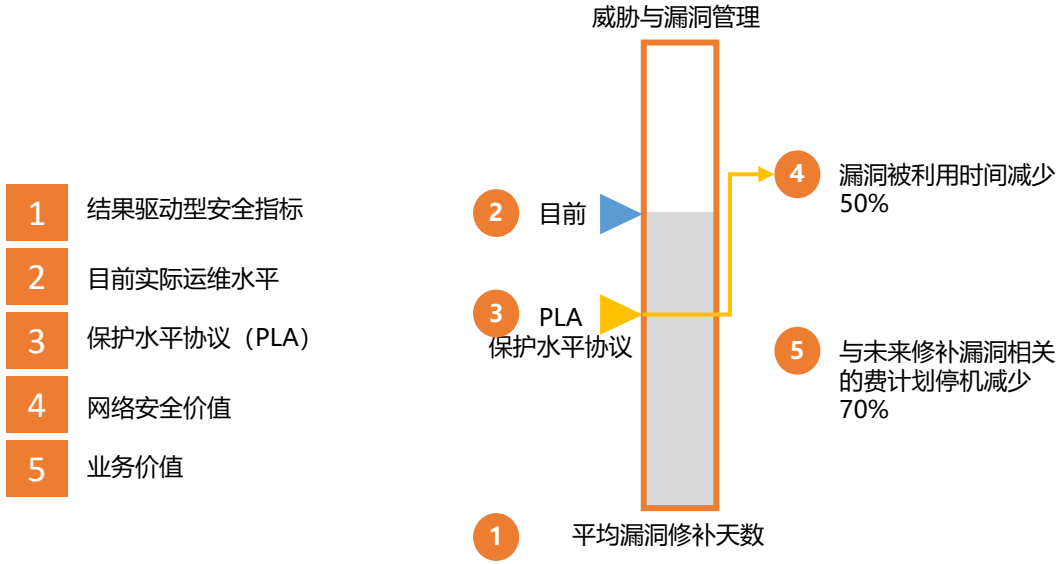
趋势二：以业务成果为中心进行安全投资，形成保护水平协议（PLA）

随着网络安全市场进入调整期，企业安全投资面临降本增效的考验，以业务成果为导向的安全建设将成为趋势，在组织业务价值链中搜集测量数据，推动业务部门领导者等利益相关者共同参与安全治理，与安全部门协商确定业务部门所需的网络安全保护水平。并基于可衡量的网络安全保护水平和财务投资挂钩，使保护水平符合企业预期业务成果。类似于IT服务管理中的服务等级协议（SLA），未来保护水平协议（PLA）将成为安全部门服务业务部门的价值表现，同时也是安全预算或投资的参考指标来源。

建立安全指标与业务成果之间的关系



保护水平协议（PLA）



来源：安在新媒体整理

趋势三：大型企业用户寻求安全产品/服务供应商的整合

大型企业在多年的网络安全建设后，发现历年购买堆砌的网络安全产品之间或多或少存在功能重叠、系统不兼容、数据难打通、基线难维护、供应链依赖等一系列的问题，在当下数字化转型的背景下，越来越多的大型企业希望寻求基于企业网络安全架构的安全产品/服务的能力整合。安全产品/服务供应商的整合是网络安全领域的一个重要趋势，它涉及到将不同的安全技术和工具集成到一个统一的平台上，以便更好地管理和防御网络安全威胁。这种整合不仅有助于提高安全运营的效率，还能够通过减少安全工具的重复和提高自动化水平来降低成本。

安全产品整合示意图

来源：安在新媒体整理

趋势四：从安全意识宣贯到量化安全行为绩效

鉴于网络钓鱼、社交攻击等针对人的弱点的攻击方式，在现实网络攻击中比重的增大，人员的网络安全意识教育工作将向人员的安全行为约束方向转变。员工在长期的网络安全意识教育中学习到的网络安全知识，和现实中个人的网络行为习惯存在着矛盾，这也是员工在安全意识考试的高分和频频在模拟钓鱼测试中中招表现背后的原因。随着零信任、IAM、UEBA、AI安全助理等工具在企业中的应用，量化员工安全行为作为绩效将成为趋势，尤其是业务流程中关键节点会优先开始使用，如离职、在职背景调查、第三方审计等活动中。

安全行为绩效评价体系

员工安全行为计分卡

项目	结果		正常值
口令平均长度	9.4		8~15位/系统
口令更新频度	4		3~6/年/系统
核心数据库访问频率	42	↑	10~24/周
模拟钓鱼邮件	2	↑	0/年
上网外发文件	3次	↑	0/月
门禁			

外包人员行为计分卡

项目	结果	正常值
口令平均长度	10.6	8~15位/系统
口令		

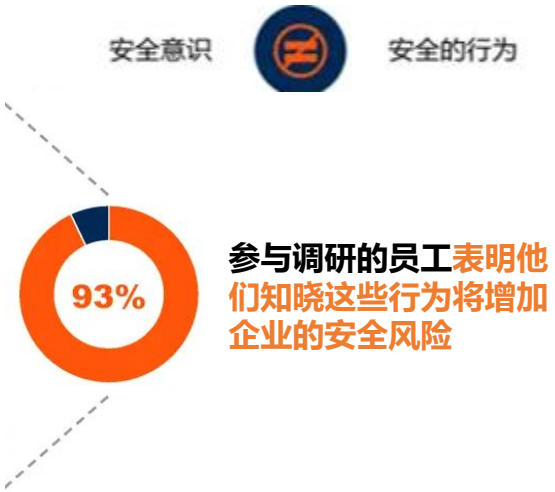
供应商行为计分卡

项目	结果		正常值
合同中安全条款	缺项	↑	考虑泄密和中断风险
数据保护能力	未测评	↑	等保二级

……

部门安全行为计分卡

69% 的员工在过去12个月里，有意识的越过安全规范	⊘
65% 的员工有时或更频繁地在公司设备上打开未知来源的邮件/链接/附件	⊘
63% 的员工使用工作设备或帐号处理个人事物（如登录个人邮箱）	⊘
5% 的员工在没有获得公司审批的情况下，有时或更频繁的将他们的工作密码直接存储在公网浏览器中	○



参与调研的员工表明他们知晓这些行为将增加企业的安全风险

来源：安在新媒体整理

趋势五：十大产品领域或将成2025年市场追捧热点

随着人工智能、量子计算、区块链等技术的快速发展，安全产品能够提供更高级的威胁检测、自动化响应和数据保护功能，满足市场对于高效、智能化安全解决方案的需求。在网络攻击日益复杂，安全合规要求越来越严格的背景下，以下十大产品将成为市场追捧的热点。

2025年中国市场十大热门安全产品

1.AI安全助手

AI安全助手是网络安全领域的一个新兴技术，它结合了人工智能技术，尤其是生成式AI，以提高安全运营的效率和效果。

2.软件供应链安全

软件供应链安全产品是一套解决方案，旨在保护软件从开发到部署的整个生命周期，确保软件组件、代码和交付过程的安全性，以及防范和减轻潜在的安全威胁。

3.威胁狩猎

威胁狩猎产品通过主动搜索、分析和响应潜在的网络安全威胁，旨在提前发现并应对复杂威胁，减少安全风险。

4.安全验证平台BAS

BAS通过模拟真实的攻击手段和场景来测试组织的网络安全防御体系。BAS技术的核心价值在于它能够持续地验证安全控制措施的有效性，帮助企业及时发现并修复潜在的安全漏洞，从而提高应对网络攻击的能力。

5.攻击面管理

攻击面管理产品通过自动化资产发现、漏洞评估、威胁情报集成、风险优先级排序、实时监控和响应、以及可视化管理，为组织提供全面、主动、智能化的网络安全防护，以降低潜在的安全风险。

6.数据安全治理平台DSG

数据安全治理平台（DSG）产品的特点在于提供全面的解决方案，用于管理和保护组织内的数据资产。这些产品通常包括数据资产梳理、数据分类分级、风险评估与收敛、数据安全合规、综合报表分析以及安全能力协同等关键功能。

7.态势感知管理平台

态势感知管理平台通过实时监控和自动收集安全数据、利用大数据和AI技术进行高级分析、整合威胁情报以提高威胁识别能力、支持安全事件的自动化响应和处置。

8.安全编排自动化SOAR

SOAR产品的核心特点在于将不同的安全工具和流程通过自动化和编排技术整合在一起，以提高安全事件的响应速度和效率。它通过预定义的剧本和工作流引擎自动化执行安全操作，实现对安全事件的快速响应和处置。

9.增强身份管理IAM

增强身份管理（IAM）产品的特点在于提供一个全面的框架，用于管理用户的身份验证、授权、访问控制以及身份的全生命周期。

10.API安全

提供全面的API资产发现和管理，通过集成多种安全技术，如身份验证、授权、输入验证、速率限制、配额管理、API网关、审计记录、错误处理、监控和补丁管理等，来确保API的安全性和稳定性。

来源：安在新媒体整理

安在·新榜业务简介（广告）

- 安在·新榜是安在新媒体依托诸子云（一个由安在新媒体发起并运营的，全国分布，各行各业，实名注册的完全由甲方网络安全业者构成的共享互助社群）而进行，有近3000人（家）企业一线安全业者提供了真实的数据反馈；
- 由各典型行业标杆企业的安全负责人或大咖专家提供全程指导，进行过程监督，并对结果做必要审核；
- 策划、组织、实施、编辑、报告，项目全程，基于信息安全专业咨询方法论的积累和行业经验；
- 不带有任何导向性，杜绝任何厂商或非用户端的影响和干扰，问题采自用户，数据源自用户，报告用之用户。

安在新榜报告业务

用户年度调查报告	针对用户网络安全需求、解决方案、产品部署、使用体验、发展趋势、预算投入等的年度全面调查报告
细分领域行业报告	在特定网络安全产品或服务领域开展的外部威胁、用户痛点、解决方案、产品选择、服务体验等的针对报告
企业市场分析报告	结合各类调查数据，针对特定网络安全厂商出具的全面市场情况的分析报告，涉及真实的用户选择、反馈和体验

▼合作咨询

徐 倩
Tel：15101590512
Email：xuq@anzerclub.com

安在·新榜
ANZER

横向分析，行业深度，展现价值

欢迎合作！