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。

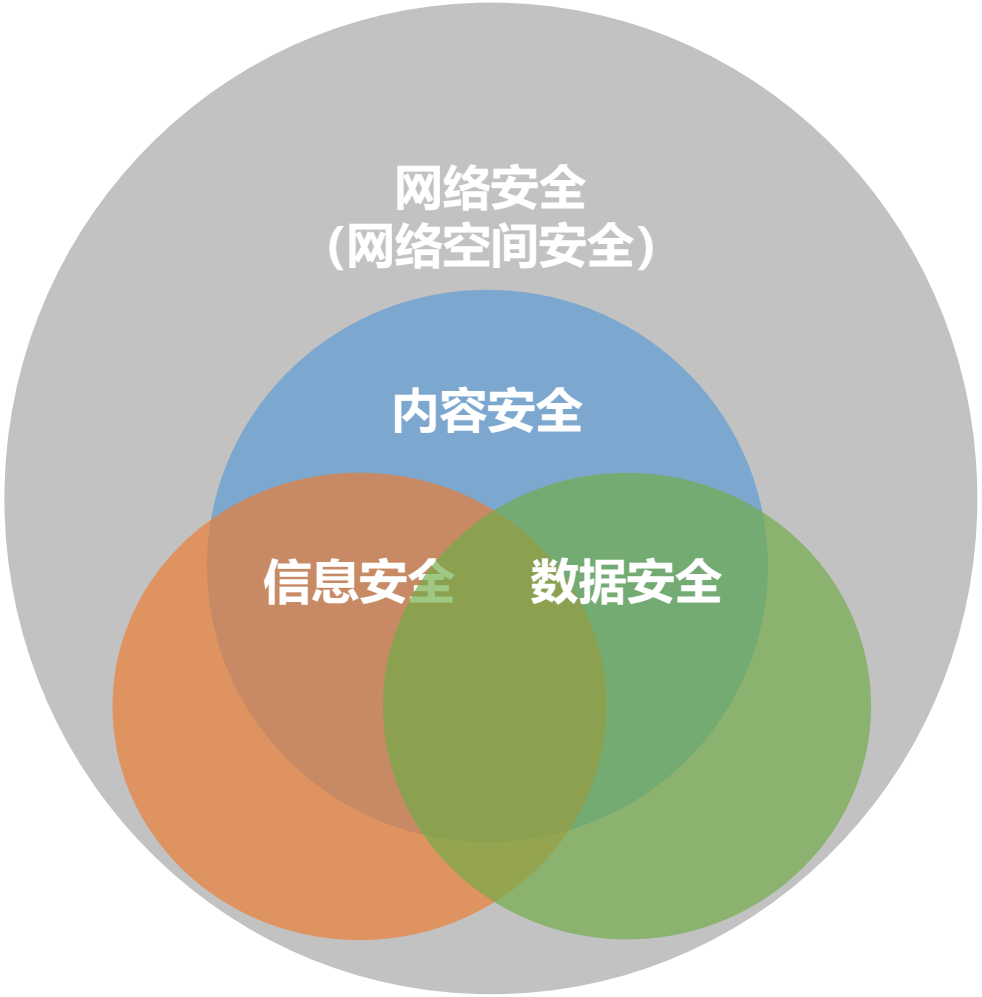
目录

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

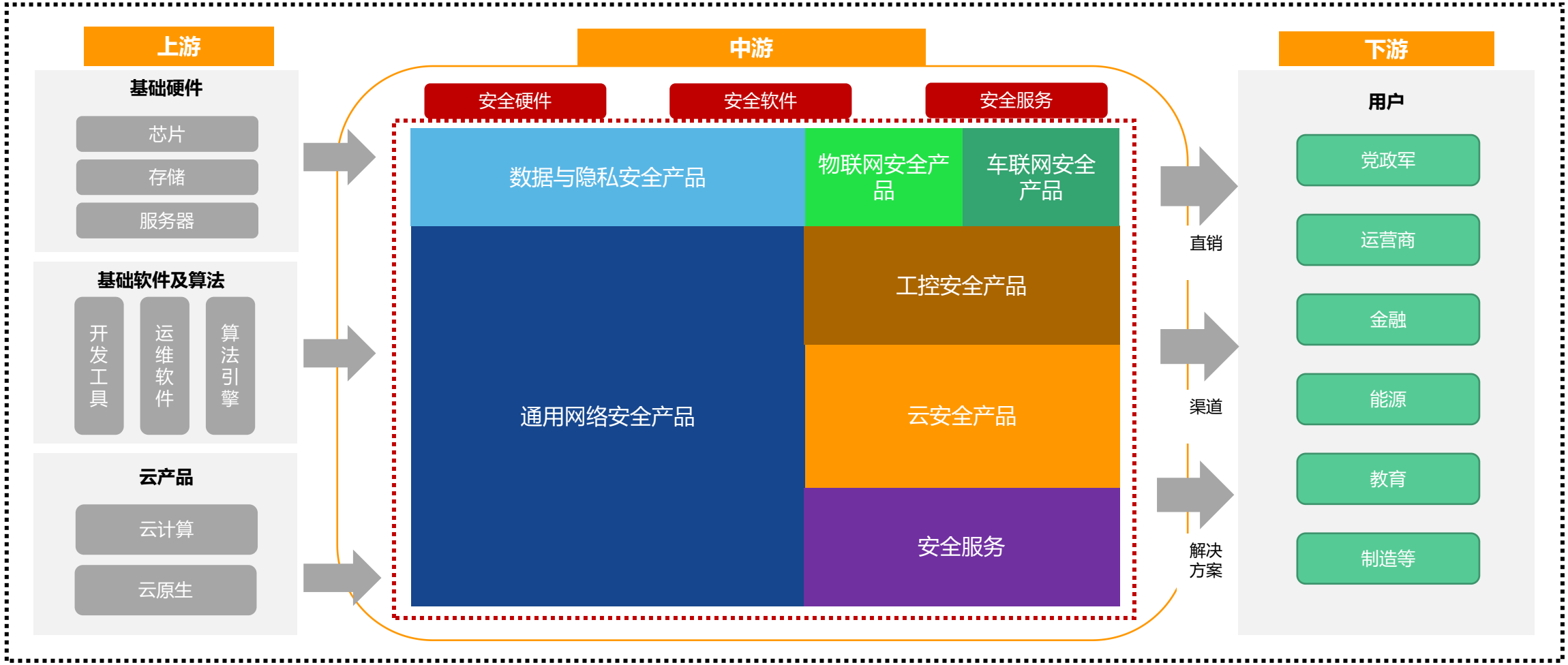
来源：《国家网络空间安全战略》



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	

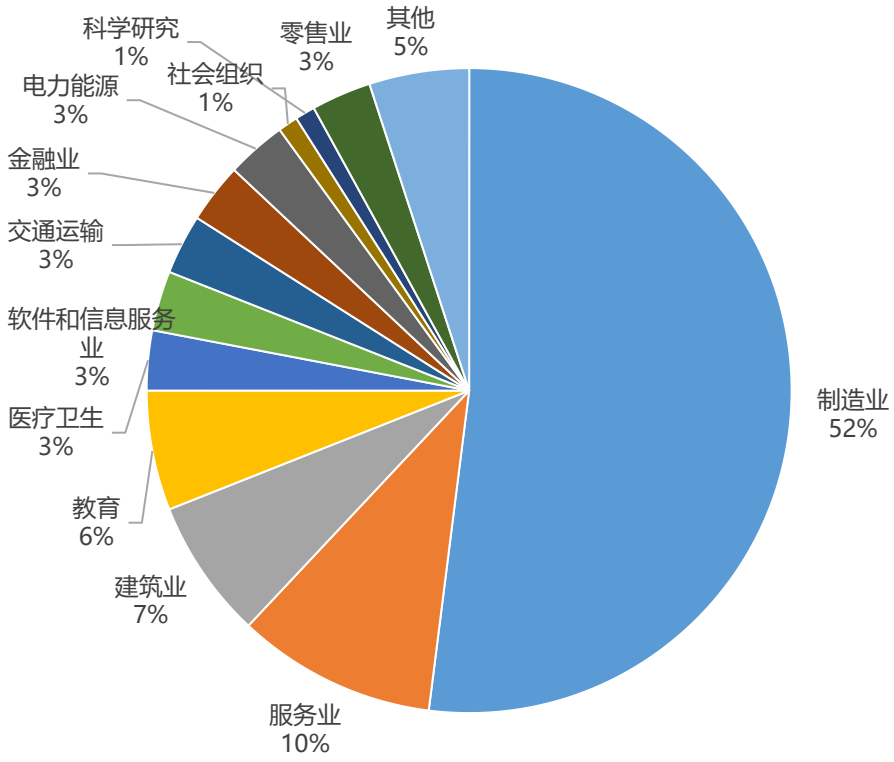
来源：安在新媒体整理

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

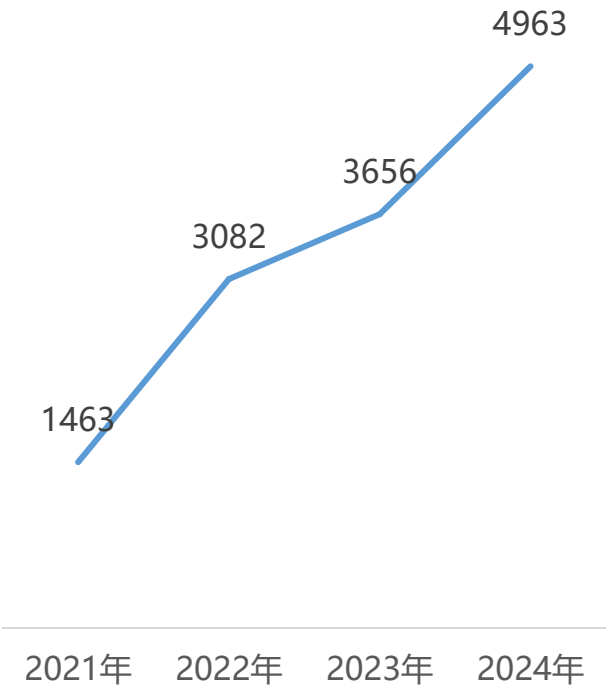
网络犯罪已经进入人工智能时代，勒索软件、APT 等高级威胁正在经历一次 “网络犯罪技术革命” 。人工智能技术降低了网络犯罪分子开发恶意软件的技术门槛，他们可以利用人工智能进行技术咨询、用于网络钓鱼的文本 / 媒体生成、情报收集与攻击侦察、保持匿名和躲避追踪、深度伪造 / 假冒等。随着 ChatGPT 的滥用增加和地下大语言模型工具的开发，复杂攻击的可能性已经升级。全球勒索病毒攻击事件数量呈现明显的持续增长态势。近一年来，全球范围内活跃的勒索病毒组织共计87个，其中活跃度排名前10位的勒索病毒组织发动的攻击活动占全部勒索病毒攻击活动的比例超过一半，呈现出较为集中的态势。近一年来我国受到攻击和勒索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

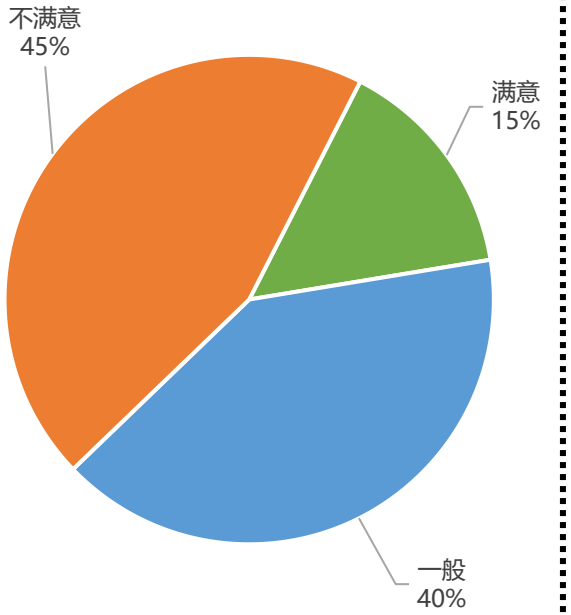


来源：国家计算机病毒应急处理中心、安在新媒体整理

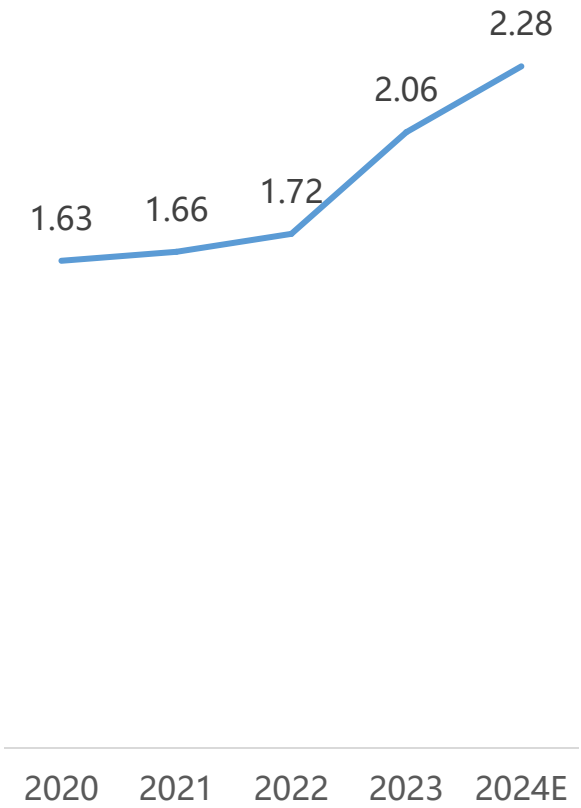
市场驱动力3：社会与民众诉求“安全感”触发企业社会责任建设

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

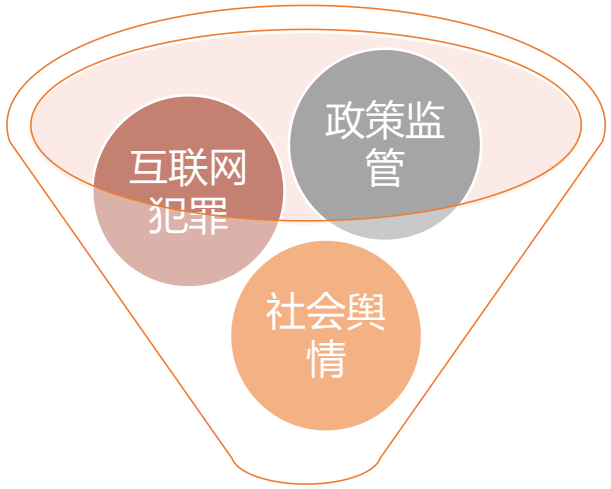
第1名	骚扰电话	未经接收者同意或请求，通过电话、短信等方式向其发送商业广告、推销产品或服务
第2名	手机木马盗资金	多种方式引诱用户在手机上安装木马，窃取支付账户或网上银行中的资金，同时利用用户信息进行盗刷购物或网络贷款。
第3名	违规精准推送	非法采集用户的兴趣、行为、地理位置等信息，向用户推送个性化的广告、内容或服务。
第4名	网络诈骗	利用互联网技术和平台，通过虚假信息、欺骗手段等方式骗取他人财物的行为。
第5名	大数据杀熟	企业利用大数据技术，根据用户的消费习惯、行为模式、地理位置等信息，对不同用户实行不同的价格策略。
第6名	个人信息泄露	个人信息泄露是指个人的姓名、身份证号、电话号码、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

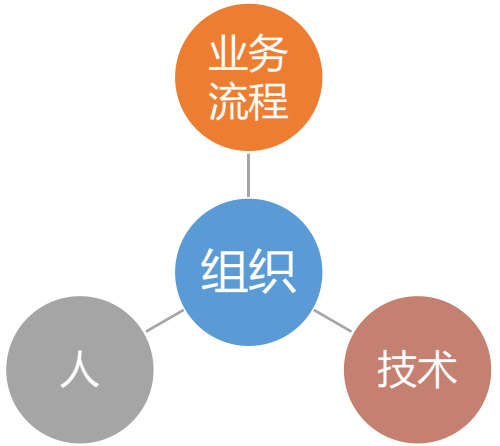
2024年，受外部环境威胁变化和内部降本增效，以及安全投资收紧的影响，预判中国市场企业当前的风险水平为8级安全风险“易受骚扰”级，意味着企业日常在内部经常会发现犯罪分子从外部尝试入侵的痕迹。对于防范能力较弱的企业来说，则有可能面临突发重大安全事件的影响。因此，企业当前的安全建设多会围绕容灾、备份、应急、风险发现能力、运营能力等方面。

企业网络安全风险预测



网络安全外部威胁

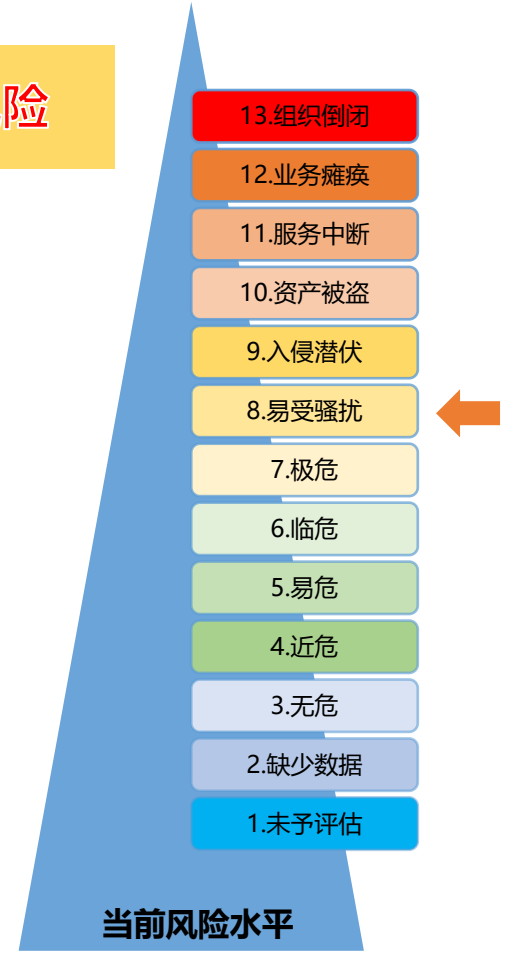
1	政策监管执法力度加大
2	互联网犯罪花样层出不穷
3	社会对隐私保护和网络安全关注度与日俱增



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

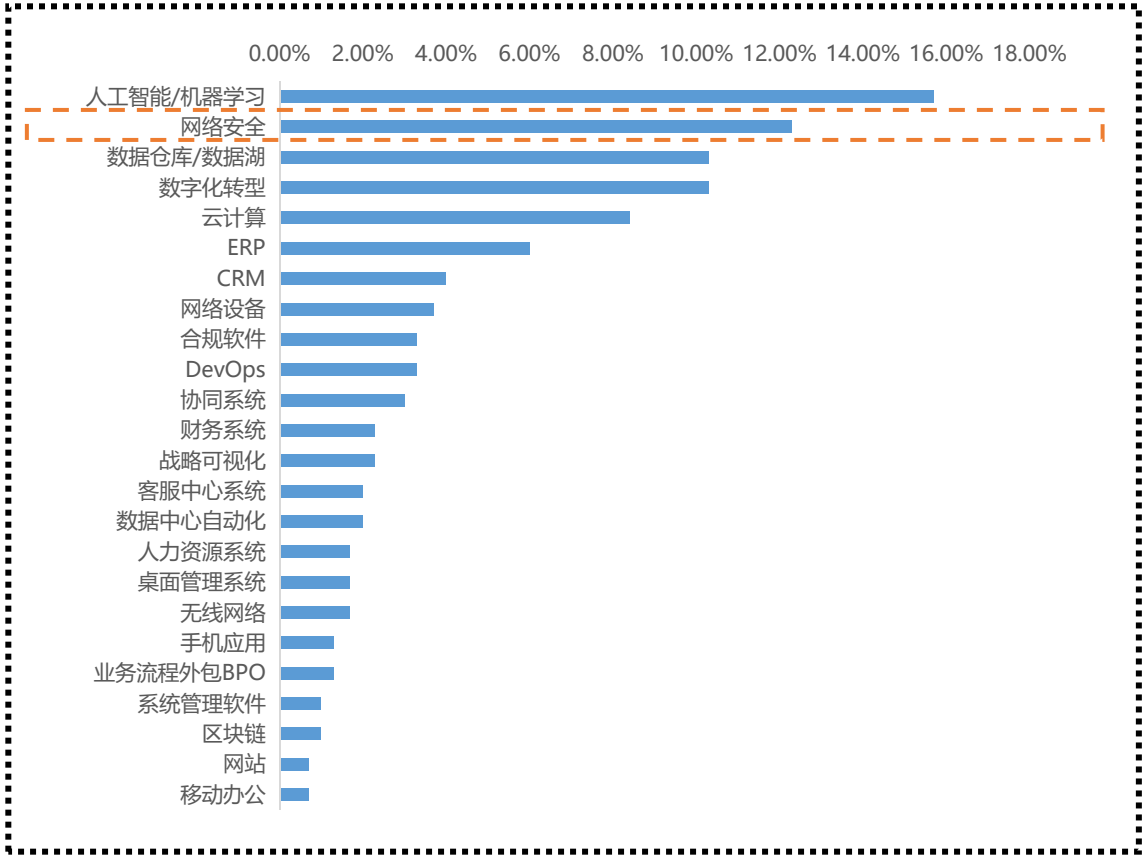


来源：安在新榜整理

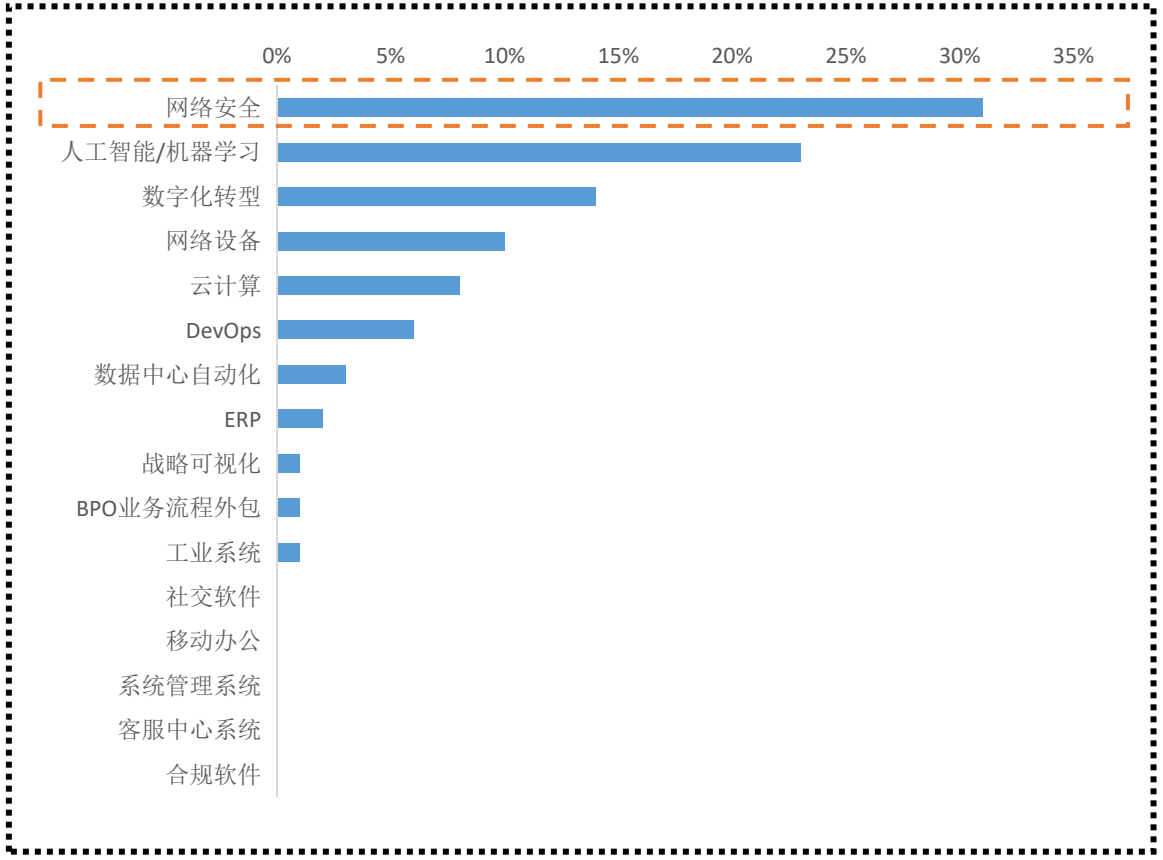
建设意愿：网络安全市场有着必然增长的动能，和持续增长的动力

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



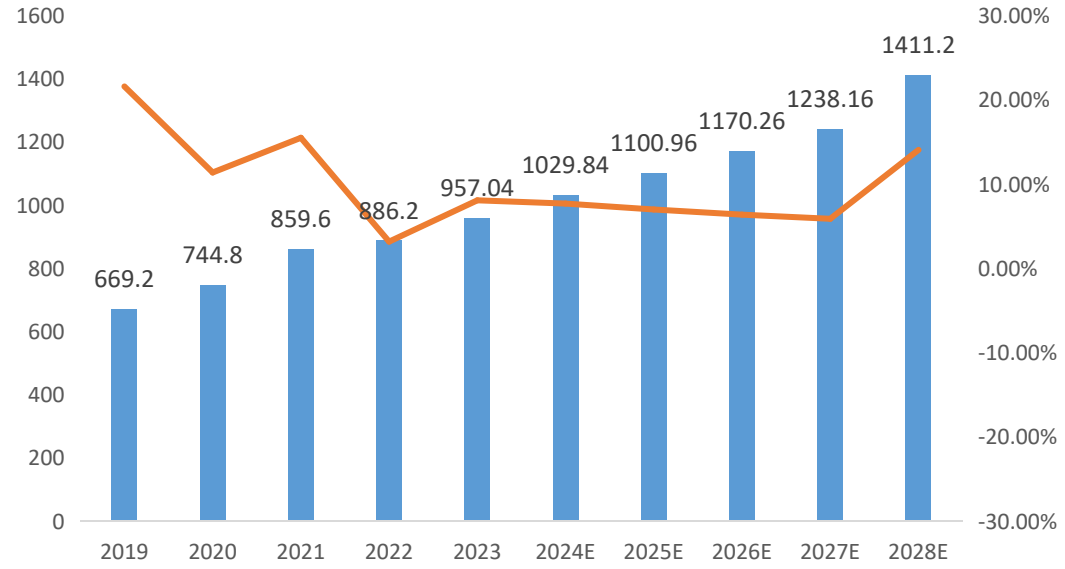
来源：安在新媒体整理

目录

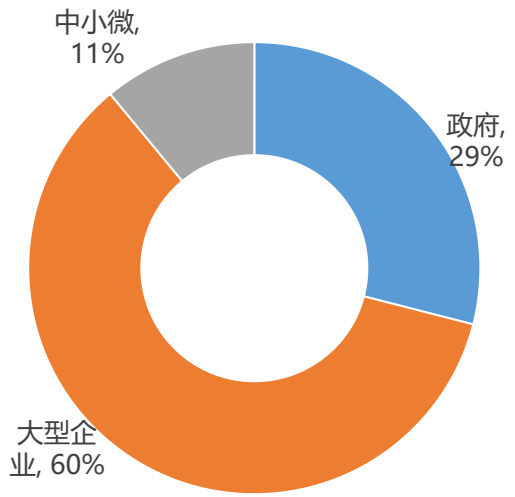
市场概况：当前中国网络安全市场预计1029.84亿元

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

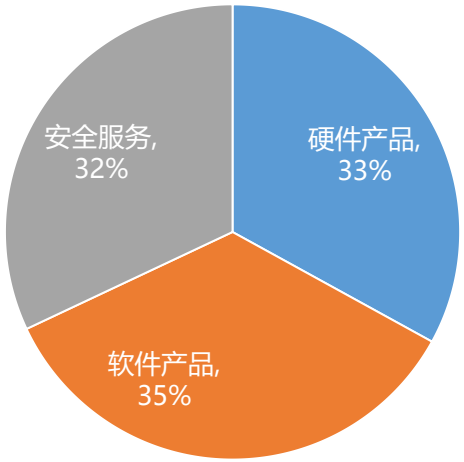


来源：安在新媒体整理

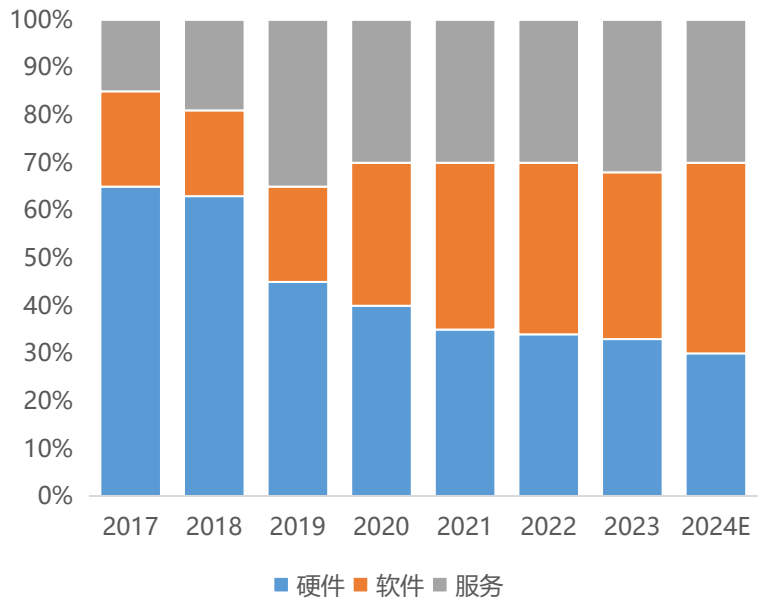
细分格局：安全软件市场规模逐年扩大，蚕食安全硬件市场

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。

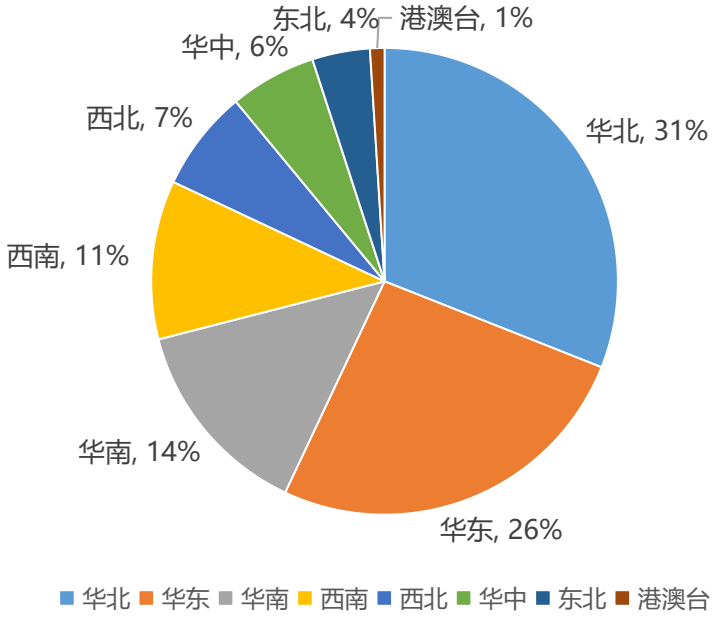
市场分类



细分市场结构变化



地域格局

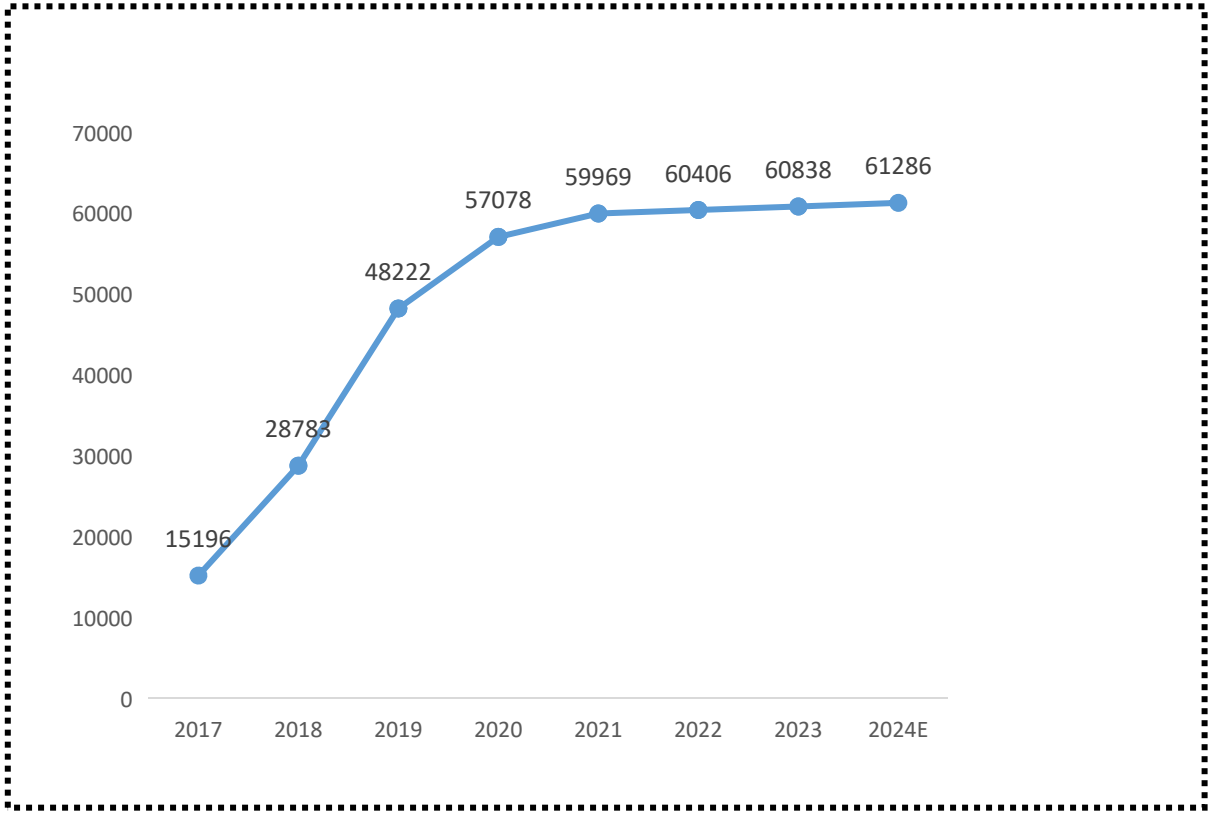


来源：安在新媒体整理

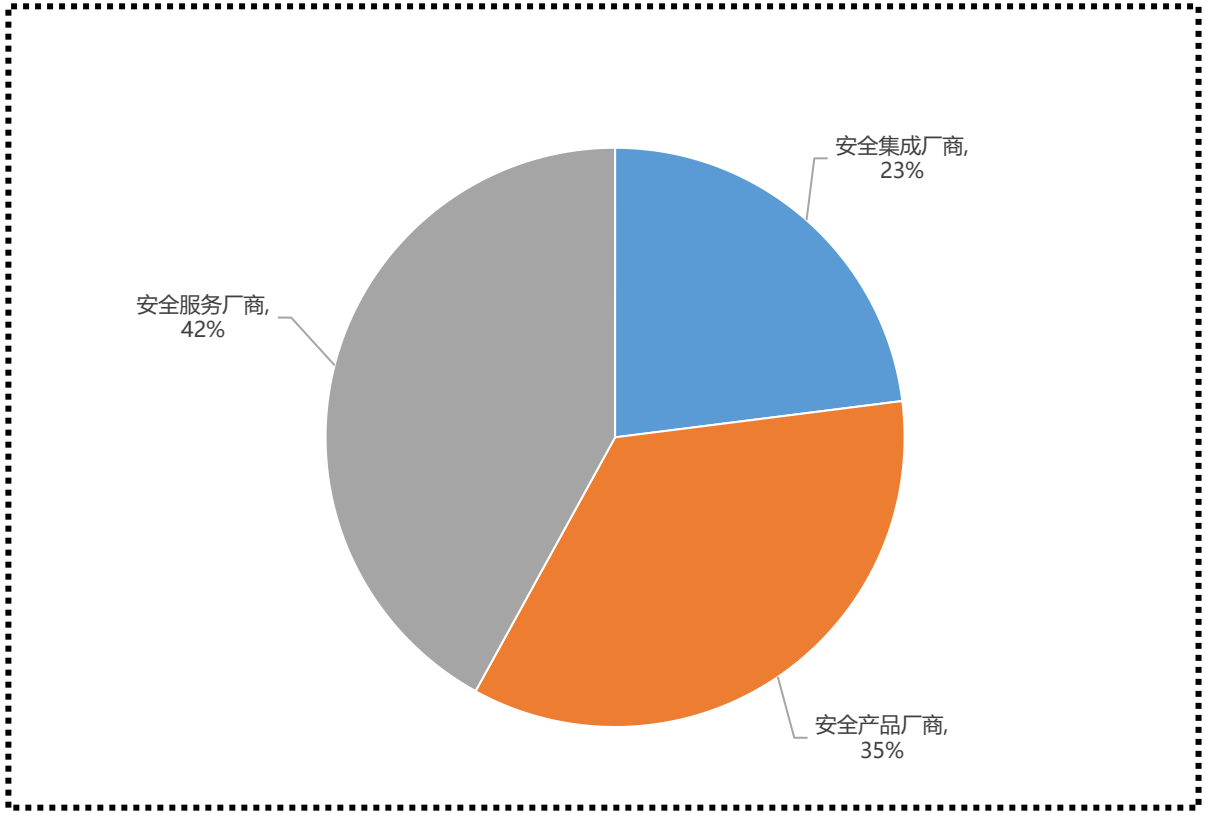
安全厂商：企业数量增长减弱，标志市场达到阶段性饱和状态

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