赛迪网
CCIDNET

2022-2023

中国网络安全行业发展年度报告

赛迪网
2024年1月

郑重声明

本报告的著作权归赛迪所有。本报告是赛迪的研究与统计成果，其性质是供客户内部参考的业务资料，其数据和结论仅代表本公司的观点。本报告有偿提供给购买本报告的客户使用，并仅限于该客户内部使用。购买本报告的客户如果希望公开引用本报告的数据和观点，在事先向赛迪提出书面要求后，必须经过赛迪的审核、确认，并得到赛迪的书面授权。未经赛迪的审核、确认及书面授权，购买本报告的客户不得以任何方式在任何媒体上（包括互联网）公开引用本报告的数据和观点，不得以任何方式将本报告的内容提供给其他单位或个人。否则引起的一切法律后果由该客户自行承担，同时赛迪亦认为其行为侵犯了赛迪的著作权，赛迪有权依法追究其法律责任。

目录

目录.....1

图表目录.....6

第一章 网络安全发展环境及背景.....1

第一节 网络安全内涵.....1

第二节 网络安全发展背景.....2

一、全球背景.....2

二、中国背景.....3

第三节 网络安全相关政策解读.....5

一、网络安全规划.....5

二、网络安全相关政策.....8

第四节 网络安全相关技术发展情况.....13

第二章 中国网络安全发展现状.....18

第一节 中国网络安全发展现状.....18

一、市场发展前景好，规模及企业持续增长.....18

二、行业集中度低，国内厂商竞争力不强.....18

三、行业发展不均衡，产业布局有待优化.....18

四、技术持续发展，企业产品不断更新迭代.....19
第二节 中国网络安全市场规模.....21
第三节 中国网络安全市场企业数量.....22
第四节 中国网络安全产业结构.....22
第五节 中国网络安全发展驱动因素和限制条件分析.....24
一、驱动因素.....24
二、限制因素.....26
第三章 中国网络安全重点细分行业发展情况分析.....29
第一节 网络安全重点细分市场发展现状.....29
一、基本概述.....29
二、产业图谱.....30
第二节 细分市场发展阶段分析.....31
一、基础设施安全.....31
二、云安全.....34
三、数据安全.....38
四、应用安全.....42
五、安全运营.....45

六、工业互联网安全 49
七、信息技术应用创新 52
第四章 网络安全创新实践案例 57
第一节 西安国际医学中心医院 57
一、医院简介及网络安全核心痛点和诉求 57
二、网络安全软硬件设施布局及成效 58
第二节 华中科技大学同济医学院附属协和医院 60
一、医院简介及网络安全核心痛点和诉求 60
二、网络安全软硬件设施布局及成效 61
第三节 陕西榆林能源集团有限公司 62
一、企业简介及网络安全核心痛点和诉求 62
二、网络安全设施布局及成效 62
第四节 江铃汽车集团有限公司 66
一、企业简介及网络安全核心痛点和诉求 66
二、网络安全软硬件设施布局及成效 67
第五节 山东港口科技集团有限公司 68
一、企业简介及网络安全核心痛点和诉求 68

二、网络安全软硬件设施布局及成效 69

第五章 中国网络安全市场趋势预测 72

第一节 中国网络安全市场发展方向与热点分析 72

一、传统网络安全技术进一步升级演进 72

二、前沿安全技术不断与传统技术融合发展 72

三、数据安全成为网络安全重要组成部分 72

四、关键信息基础设施网络安全保护备受重视 73

五、零信任架构演进进入落地推广阶段 74

第二节 中国网络安全市场规模预测 74

第三节 中国网络安全市场需求趋势预测 75

一、关键行业信创持续推进，网络安全产品需求增加 75

二、产品向数据安全、安全管理、安全服务类延伸 75

三、网络安全市场需求持续向服务化转型 76

四、网络安全需求市场仍将以华北、华东、华南为主 76

五、政府部门是最大的网络安全产品用户 76

第四节 中国网络安全市场竞争趋势预测 77

一、网络安全行业集中度不高 77

二、网络安全企业分布区域集聚特征将更为明显.....77
第五节 中国网络安全市场前景分析.....78
一、国家持续加强网络安全顶层设计.....78
二、网络安全下游细分市场需求增长空间大.....79
三、网络威胁增加且日趋复杂化，带来新的安全需求.....79
第六章 推动我国网络安全产业发展的措施建议.....81
第一节 面向政府机构的建议.....81
一、开展关键信息基础设施重点防护和加固.....81
二、营造良好云原生安全产业发展环境.....81
三、细化数据安全管理规范及管控措施.....81
四、整合创新资源并完善创新体系.....82
第二节 面向企业的建议.....82
一、重视产品安全认证及可靠性评估.....82
二、优化边界安全、云安全等刚需产品性能.....83
三、积极布局信创、数据安全治理相关产品.....83

图表目录

图表 1 ： 网络安全主要特点 1

图表 2 ： 网络安全产品及服务分类 2

图表 3 ： 网络安全发展大事记 4

图表 4 ： 《“十四五”国家信息化规划》网络安全相关内容 7

图表 5 ： 中国网络安全行业部分政策汇总 9

图表 6 ： 中国网络安全制度体系 11

图表 7 ： 中国网络安全行业相关部分政策汇总 12

图表 8 ： 网络安全主要技术发展情况及代表企业统计 14

图表 9 ： 网络安全关键技术方向 16

图表 10 ： 网络安全行业重点企业发展历程 20

图表 11 ： 2020-2023 年前三季度中国网络安全市场规模统计 21

图表 12 ： 2020-2023 年前三季度中国网络安全市场企业数量统计 22

图表 13 ： 中国网络安全行业竞争梯队 23

图表 14 ： 中国网络安全重点细分行业基本信息 29

图表 15 ： 中国网络安全行业产业链图谱 31

图表 16 ：2020-2023 年前三季度中国基础设施安全领域网络安全市场规模统计

.....34

图表 17 ： 山石网科云安全主要产品 36

图表 18 ： 2020-2023 年前三季度中国云安全领域网络安全市场规模统计 38

图表 19 ： 山石网科数据安全治理方案框架图 41

图表 20 ： 2020-2023 年前三季度中国数据安全领域网络安全市场规模统计 . 42

图表 21 ： 2020-2023 年前三季度中国应用安全领域网络安全市场规模统计 . 45

图表 22 ： 2020-2023 年前三季度中国安全运营领域网络安全市场规模统计 . 49

图表 23 ：2020-2023 年前三季度中国工业互联网安全领域网络安全市场规模统计 52

图表 24 ： 山石网科国产化 XDR 安全运营架构 54

图表 25 ：2020-2023 年前三季度中国信息技术应用创新领域网络安全市场规模统计 56

图表 26 ： 西安国际医学中心医院网络安全核心痛点及诉求 57

图表 27 ： 西安国际医学中心医院网络安全创新实践成果 59

图表 28 ： 陕西榆林能源集团有限公司网络安全痛点及需求 62

图表 29 ： 陕西榆林能源集团有限公司网络安全智能安全运营系统平台 63

图表 30 ： 陕西榆林能源集团有限公司网络安全创新实践成果 65

图表 31 ： 江铃汽车集团有限公司网络安全痛点及需求 66

图表 32 ： 山东港口科技集团有限公司网络安全痛点及需求.....69

图表 33 ： 山东港口科技集团有限公司网络安全创新实践成果.....71

图表 34 ： 2023-2025 年中国网络安全市场规模预测.....75

图表 35 ： 中国网络安全行业企业分布图.....78

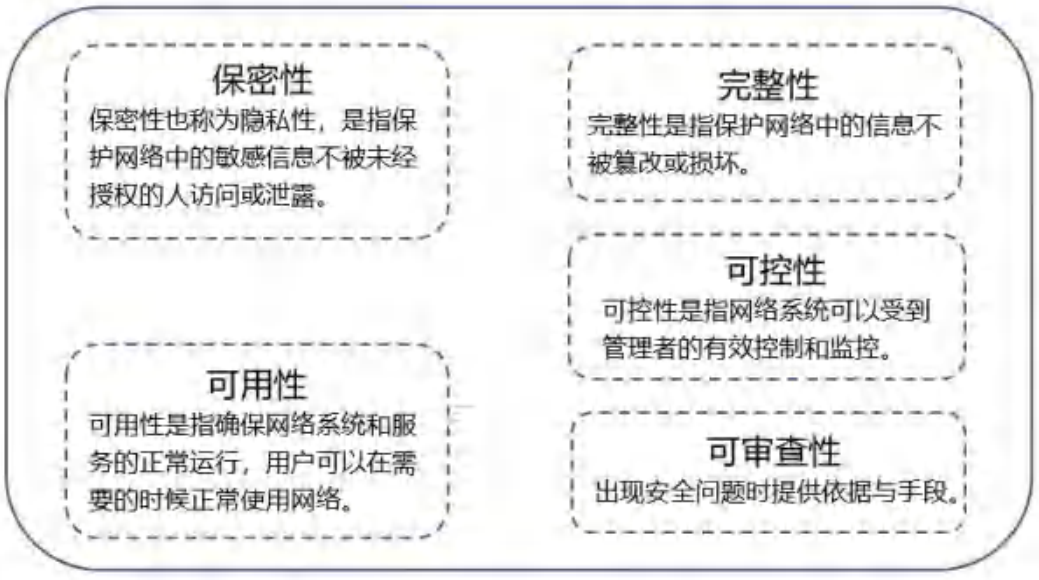
第一章 网络安全发展环境及背景

第一节 网络安全内涵

根据2017年6月实行的《中华人民共和国网络安全法》概念界定，“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障网络数据的完整性、保密性、可用性的能力。

网络安全可细分为网络设备安全、网络软件安全和网络信息安全。凡是涉及到网络上信息保密性、完整性、可用性、可认证性、可控性和可审查性的相关理论和技术都属于网络安全研究的范畴。

图表 1：网络安全主要特点



资料来源：项目组统计整理

按产品结构及形态分类，网络安全产业可分为网络安全硬件、网络安全软件和

网络安全服务三类。其中，网络安全硬件主要包括智能卡、防火墙、VPN、入侵防御等；安全软件包括身份管理和访问控制软件、安全性与漏洞管理软件、安全内容与威胁管理软件等；安全服务则主要由咨询服务、培训服务、实施服务、运维服务组成。

图表 2：网络安全产品及服务分类

资料来源：项目组统计整理

第二节 网络安全发展背景

一、全球背景

随着信息化对整个经济社会发展的融合、驱动作用日益明显，其所带来的网络空间威胁和风险日益增多。网络空间安全已成为关系国家安全、社会稳定和广大人民群众切身利益的重要问题。当前，全球大部分国家步入网络空间规划的建设阶段，

全球网络空间治理领域出现变革契机，同时网络空间威胁的规模不断扩大与发展，网络空间安全的问题愈加艰巨复杂。

欧美等发达国家围绕网络安全治理工作出台了多项法律法规进行保障，组成了覆盖网络与信息安全各个方面的管理和技术体系，伴随着各国网络安全意识的不断增强，提升网络安全监测预警、防御阻断、处置响应和追踪溯源的能力成为紧迫需求，各国均投入大量资金以促进网络安全技术发展。

2022年，受俄乌冲突影响，美英欧等国纷纷强化网络安全建设，出台相关战略规划，以立法推动零信任、量子技术等网络安全新兴技术研发，同时进一步完善网络安全机构体系，加速提升科研实力，提高自身“造血”能力。

2023年11月，英国政府宣布成立新的人工智能安全研究所，以促进人工智能技术安全发展方面的国际合作，该研究所将测试新兴前沿人工智能技术的安全性。英国政府的前沿人工智能特别工作组将演变为人工智能安全研究所，它将与图灵研究所进行合作，在新的人工智能模型推出后对其进行测试，以应对潜在的风险。英国还同意与美国联邦人工智能安全研究所和新加坡政府建立伙伴关系，就人工智能安全测试进行合作。

二、中国背景

随着中国第一台电子计算机的诞生，网络安全行业的发展亦拉开序幕。20世纪80、90年代，由于互联网开始商业化，首次出现了病毒攻击终端事件，故终端网络安全受到重视。在千禧年之后，随着互联网的商业化以及网民规模的快速增长，第二代网络安全技术诞生，核心为白名单机制，主要由于蠕虫、病毒可大规模通过网

络攻击，第一代的黑名单机制已无法奏效。

2014 年，网络安全上升为国家战略。2015 年之后，基于人工智能的大数据分析作为第三代网络安全技术诞生，2016 年《网络安全法》出台，网络安全行业进入“黄金十年”。2020 年以来，国家越来越重视网络安全问题，政策鼓励、制度体系不断完善，网络安全产业迎来较好发展。

图表 3：网络安全发展大事记

时间	重大事件	重要意义
1987 年	王运丰教授和李澄炯博士等中国科学家在北京计算机应用技术研究所（icA）创建第一个电子邮件节点。向德国发出了中国第一封电子邮件。	中国互联网发展史的开端
1988 年	1988 年发现小球病毒，当计算机系统时钟处于半点或整点，且系统在进行读盘操作即可触发，此时屏幕出现一个活蹦乱跳的小回点进行斜线运动，当碰到屏幕边沿或者文字就立刻反弹，同时削去碰到的部分文字。	新中国第一例电脑病毒
1994 年	公安部颁布了《中华人民共和国计算机信息系统安全保护条例》，从法规角度全面阐述了关于计算机信息系统安全相关的概念、理论、管理、监督、责任。	网络安全首部法律诞生，标志着信息系统等级保护工作正式开启
2000 年	国内的金山、瑞星、江民，国外的卡巴斯基、麦咖啡、诺顿等杀毒软件陷入持续的价格战。	杀毒软件市场混战时期
2006 年	蠕虫病毒“能猫烧香”出现，能终止大量反病毒软件和防火墙的运行，造成系统核心程序加载失败，并删除重要文件。中毒之后，许算机主界面上会出现一个举着三根香的熊猫。	最出名的“本土”病毒
2007 年	我国信息安全等级保护制度正式实施，并成为我国非涉密信息系统网络安全建设的重要标准。2007 年和 2008 年颁布实施的《信息安全子级保护管理办法》和《信息安全等级保护基本要求》，被称为“等保 1.0”。	“等保 1.0”颁布实施
2016 年	《中华人民共和国网络安全法》发布，是落实总体国家安全观的重要举措，在维护网络安全、维	《中华人民共和国网络安全法》是我国第一部网络

	护广大人民群众切身利益方面发挥了重要的作用。	安全的综合性立法，是我国第一部全面规范网络空间安全管理的基础性法律
2019年	国家市场监督管理总局召开新闻发布会，正式发布“等保2.0”，于2019年12月1日正式实施。	网络安全等级保护制度2.0标志着国家网络安全等级保护工作步入新时代
2019年	《中华人民共和国密码法》正式发布，从密码管理的基本原则、分类管理、商用密码从业单位管理、检测认证体系建设、网络运营者使用等多个角度进行了规范。	我国密码领域首部综合性、基础性法律
2021年	《中华人民共和国数据安全法》正式发布，就如何保障个人数据安全、如何用数据提升智能化服务、如何对数据进行分级保护等多方面提供法律依据。	我国数据领域的基础性法律，更是我国第一部有关数据安全的专门法律

资料来源：项目组统计整理

第三节 网络安全相关政策解读

一、网络安全规划

随着时代发展，网络安全的重要性愈加凸显。当前，我国网络安全发展呈现出制度体系化、基础设施化、风险交织化、边界融合化、工具数智化、治理主动化、监管常态化、环境清朗化等八大趋势，但也面临着网络安全在管理制度、安全技术、人才竞争、国际格局等方面的新挑战。基于此，国内关于网络安全方面的规划内容不断增多。

1、《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》

2021年3月发布的《中华人民共和国国民经济和社会发展第十四个五年规划和

2035 年远景目标纲要》是“十四五”期间国内发展的重要指导，其中网络安全已经确定成为未来中国发展建设工作的重点之一。《纲要》里共提及“网络安全”14 次，涉及数字经济、数字生态、国家安全、能源资源安全四大领域，并提出“健全国家网络安全法律法规和制度标准，加强重要领域数据资源、重要网络和信息系统安全保障；建立健全关键信息基础设施保护体系，提升安全防护和维护政治安全能力；加强网络安全风险评估和审查；加强网络安全基础设施建设，强化跨领域网络安全信息共享和工作协同，提升网络安全威胁发现、监测预警、应急指挥、攻击溯源能力；加强网络安全关键技术研发，加快人工智能安全技术创新，提升网络安全产业综合竞争力；加强网络安全宣传教育和人才培养。”

《纲要》将网络安全作为“十四五”期间重点工作内容，意味着“十四五”期间国家将大力支持、鼓励网络安全产业发展，更为丰富的网络安全法律规范、网络安全标准将被陆续制定并颁布执行，对重点领域的网络空间数据资源、信息资源等的保护也将会更为严格。

2、《“十四五”信息通信行业发展规划》

2021 年 11 月，工信部发布《“十四五”信息通信行业发展规划》（工信部规〔2021〕164 号），《规划》提出在安全保障体系和能力建设方面，着力完备网络基础设施保护和网络数据安全体系，持续提升新型数字基础设施安全管理水平，打造繁荣发展的网络安全产业和可信的网络生态环境，全面提升行业网络安全应急处置，构建国家网络安全新格局等 6 项重点任务，以支撑国家网络安全新格局形成。

3、《“十四五”大数据产业发展规划》

2021 年 11 月，工信部发布《“十四五”大数据产业发展规划》（工信部规〔2021〕179 号）。《规划》明确将开展数据安全铸盾行动，加强数据安全管理能力；推动建立数据安全管理制度，制定相关配套管理办法和标准规范，组织开展数据分类分级管理，制定重要数据保护目录，对重要数据进行备案管理、定期评估与重点保护；并加强数据跨境安全管理。

4、《“十四五”软件和信息技术服务业发展规划》

2021 年 11 月，工信部发布《“十四五”软件和信息技术服务业发展规划》（工信部规〔2021〕180 号）。《规划》要求，在安全保障方面，要强化安全服务保障开展软件数据安全、内容安全评估审查，加强软件源代码检测和安全漏洞管理能力，提升开源代码、第三方代码使用的安全风险防控能力；鼓励第三方服务机构，积极提升软件安全咨询、培训、测试、认证、审计、运维等服务能力。

5、《“十四五”国家信息化规划》

2021 年 12 月，中央网络安全和信息化委员会印发《“十四五”国家信息化规划》，强调要坚持安全和发展并重，以实现网络空间治理能力和安全保障能力显著增强为目标，深化关口前移、防患于未然的安全理念，加强网络安全信息统筹机制建设，开发网络安全技术及相关产品，提升网络安全自主防御能力。

图表 4：《“十四五”国家信息化规划》网络安全相关内容

类型	内容
主攻方向	开发网络安全技术及相关产品，提升网络安全自主防御能力。完善相关法律法规和技术标准，规范各类数据资源采集、管理和使用，避免重要敏感信息泄露。强化新技术应用安全风险动态评估，逐步探索建立人工智能、区块链等新技术的治理原则和标准。

重点建设工程	建设基础网络、数据中心、云、数据、应用等一体协同的安全保障体系。开展通信网络安全防护，研究完善海量数据汇聚融合的风险识别与防护技术、数据脱敏技术、数据安全合规性评估认证、数据加密保护机制及相关技术检测手段。

资料来源：项目组统计整理

6、《“十四五”智能制造发展规划》

2021 年 12 月，工信部、国家发改委等八部门联合发布《“十四五”智能制造发展规划》（工信部联规〔2021〕207 号）。《规划》要求加强智能制造安全风险研判，同步推进网络安全、数据安全和功能安全，推动密码技术深入应用；实施企业网络安全分类分级管理，督促企业落实网络安全主体责任；完善国家、地方、企业多级工控信息安全监测预警网络，加快建设工业互联网安全技术监测服务体系；探索建立数据跨境传输备案与监管机制；建立符合政策标准要求的技术防护体系和安全管理制度。

7、《数字中国建设整体布局规划》

2023 年 2 月，中共中央、国务院发布《数字中国建设整体布局规划》，一是构筑自立自强的数字技术创新体系；二是筑牢可信可控的数字安全屏障，主要提到切实维护网络安全，完善网络安全法律法规和政策体系，增强数据安全保障能力，建立数据分类分级保护基础制度，健全网络数据监测预警和应急处置工作体系。

二、网络安全相关政策

1、网络安全行业政策

近年来，随着企事业单位业务以及人们的日常生活与数字世界的结合愈加紧密，

各类网络安全风险对现实生产生活秩序的威胁也愈加严峻。在各行业数字化安全需求不断扩大的同时，国家层面上也持续出台政策鼓励提升网络安全水平，例如《中华人民共和国网络安全法》、《网络安全审查办法》、《网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）》、《关于促进数据安全产业发展的指导意见》、《关于开展网络安全服务认证工作的实施意见》、《关于促进网络安全保险规范健康发展的意见》等，网络安全企业也迎来了较好的发展机遇。

图表 5：中国网络安全行业部分政策汇总

发布时间	发布部门	政策名称	政策解读
2016.11	全国人大常委会	《中华人民共和国网络安全法》	这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，是我国网络空间法治建设的重要里程碑，是依法治网、化解网络风险的法律重器，是让互联网在法治轨道上健康运行的重要保障。作为网络安全的“基本法”，其重大意义在于：一是明确了部门、企业、社会组织和个人的权利、义务和责任；二是规定了国家网络安全工作的基本原则、主要任务和重大指导思想和理念；三是将成熟的政策规定和措施上升为法律，为政府部门的工作提供了法律依据，体现了依法行政、依法治国要求；四是建立了国家网络安全的一系列基本制度，这些基本制度具有全局性、基础性特点，是推动网信工作、防范重大风险的强大基石。
2020.04	网信办、工信部等部门	《网络安全审查办法》	主要目的是为了确保关键信息基础设施供应链安全，维护国家安全。规定网络安全审查应坚持防范网络安全风险与促进先进技术应用相结合、过理公正透明与知识产权保护相结合、事前审查与持续监管相结合、企业承诺与社会监督相结合，从产品和服务安全性、可能带来的国家安全风险等方面进行审查。
2021.07	工信部	《网络安全产业高质量发展三年行动计划	《行动计划》提出，到 2023 年，网络安全产业规模超过 2500 亿元，年复合增长率超过 15%。提升中小企业、重点行业和关键行业基础设施网络安全防护水平，电信等重点行业网络安全投入占信息化

		（2021-2023 年）（征求意见稿）》	投入比例达 10%。网络安全关键核心技术实现突破，加快新兴技术与网络安全的融合创新，增强网络安全产品和服务创新能力，初步形成具有网络安全生态引领能力的领航企业。
2023.01	工信部、网信办、发改委、公安部等十六部门	《关于促进数据安全产业发展的指导意见》	一是提出促进数据安全产业发展的总体要求，并按 2025 年、2035 年两个阶段提出产业发展目标，其中，到 2025 年，数据安全产业规模超过 1500 亿元，年复合增长率超过 30%；到 2035 年，数据安全产业进入繁荣成熟期。二是明确促进数据安全产业发展的七项任务。三是提出加强组织协调、加大政策支撑和优化产业发展环境三方面保障措施。
2023.03	市场监督总局、中央网信办、工信部、公安部	《关于开展网络安全服务认证工作的实施意见》	明确提出现阶段网络安全服务认证目录包括检测评估、安全运维、安全咨询和等级保护测评等服务类别。
2023.07	工信部、国家金融监督管理总局	《关于促进网络安全保险规范健康发展的意见》	在产品创新方面，鼓励保险机构面向不同行业场景的差异化网络安全风险管理需求，开发多元化网络安全保险产品。服务创新方面，鼓励网络安全保险服务机构协同合作，探索构建以网络安全保险为核心的全流程网络安全风险管理解决方案。
2023.12	工信部	《关于组织开展网络安全保险服务试点工作的通知》	组织开展网络安全保险服务试点工作。该试点险种主要包括网络安全财产类保险和网络安全责任类保险两大类。结合我国网络安全保险发展实际，试点内容包括面向电信和互联网、工业互联网、车联网等重点行业的企业类保险和网络安全产品、信息技术产品，以及网络安全服务类保险。

资料来源：项目组统计整理

2、中国网络安全制度体系

网络安全是我国维护国家安全、社会稳定，保护企业和个人隐私的前提，国家高度重视网络安全。在网络强国战略思想指引下，我国网络安全工作取得了积极进

展，网络安全政策法规体系不断健全，网络安全工作体制机制也日益完善，有效促进了网络安全领域的技术创新和应用落地，为筑牢国家网络安全屏障、推进网络强国建设提供了有力支撑。

图表 6：中国网络安全制度体系

领域		法律制度名称
综合性、基础性法律		《中华人民共和国民法典》 《中华人民其和国网络安全法》
网络安全等级保护领域	专门性立法	《中华人民共和国密码法》 《中华人民共和国数据安全法》
	管理条例	《网络安全等级保护条例》
关键信息基础设施安全保护领域	管理条例	《关键信息基础设施安全保护条例》 《网络安全审查办法》
个人信息保护领域	专门性立法	《中华人民共和国个人信息保护法》 《中华人民共和国数据安全法》
数据出境管理领域	管理条例	《数据出境安全评估办法》 《信息安全技术数据出境安全评估指南》 《网络数据安全管理条例》
内容治理和信息服务领域	专门性立法	《中华人民共和国网络安全法》
	管理条例	《互联网新闻信息服务管理规定》 《具有舆论属性或社会动员能力的互联网信息服务安全评估规定》 《网络信息内容生态治理规定》

资料来源：项目组统计整理

3、下游/应用领域政策

在政策部署下，我国网络安全立法和监管持续推进，2020 年以来，我国网络安全法治建设取得初步成就，多部重量级法律法规出台，《数据安全法》、《关键信息基础设施安全保护条例》、《个人信息保护法》、《数据出境安全评估办法》、

《商用密码管理条例》等政策相继发布，我国在数据安全、个人信息保护、关键信息基础设施保护、数据出境及商用密码管理等领域实现有法可依、有章可循。

图表 7：中国网络安全行业相关部分政策汇总

发布时间	发布部门	政策名称	政策解读
2020.03	信安标委	《网络安全标准实践指南-远程办公安全防护》	针对远程办公系统使用方和用户分别提出了安全控制措施建议，旨在围绕网络安全法律法规政策、标准、网络安全热点和事件等主题，宣传网络安全相关标准及知识，提供标准化实践指引。
2021.06	全国人大常委会	《中华人民共和国数据安全法》	这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。提出建立数据分类分级保护制度、数据安全应急处置机制、数据安全审查制度、数据安全出口管制、数据投资贸易反制措施，提出开展数据活动必须履行数据安全保护义务，并明确数据安全相关法律责任。
2021.07	工信部、网信办、公安部	《网络产品安全漏洞管理规定》	明确网络产品提供者与网络运营者两类主体责任，明确漏洞发布要求、漏洞收集平台相关要求，并制定相关罚则。
2021.07	国务院	《关键信息基础设施安全保护条例》	这是我国首部专门针对关键信息基础设施安全保护工作的行政法规。明确了国家网信部门的统筹协调职责，将进一步增强关键信息基础设施保护工作的系统性、整体性和协同性，有利于筑牢国家网络安全屏障，为经济社会发展和人民群众福祉提供安全保障。《条例》的施行，标志着我国的关键基础设施信息化安全保护建设正式迈入新的阶段。
2021.08	全国人大常委会	《中华人民共和国个人信息保护法》	规范个人信息处理活动，构建了以“告知-知情-同意”为核心的个人信息处理规则，明确了敏感个人信息的认定与保护规则，明确了个人在个人信息处理活动中的权利。
2022.01	网信办	《数据出境安全评估办法》	明确适用对象、规定应当申报数据出境安全评估的情形、提出数据出境安全评估的具体要求。
2022.01	国务院	《“十四五”数字经济发展规划》	部署了八项重点任务，在数字经济安全体系方面，提出了三个方向的要求，一是增强网络安全防护能力、二是提升数据安全保障水平、三是切

			实有效防范各类风险，系统阐述了网络安全对于数字经济的独特作用及重要性。
2023.02	网信办	《个人信息出境标准合同办法》	明确通过订立标准合同的方式开展个人信息出境活动，应当坚持自主缔约与备案管理相结合、保护权益与防范风险相结合，保障个人信息跨境安全、自由流动。
2023.04	工信部、网信办、发改委等八部门	《关于推进 IPv6 技术演进和应用创新发展的实施意见》	在提升安全保障能力方面，坚持同步推进网络安全系统规划、建设、运行的原则，从强化 IPv6 网络安全防护、加快 IPv6 安全技术创新、推动 IPv6 安全应用三个方面进行了规划部署，为 IPv6 高质量发展提供安全保障。
2023.05	国务院	《商用密码管理条例》	一是完善了商用密码管理体制；二是促进商用密码科技创新与标准化建设；三是健全商用密码检测认证体系；四是加强电子认证服务使用密码和电子政务电子认证服务活动管理；五是规范商用密码进出口管理；六是促进商用密码应用，明确关键信息基础设施的商用密码使用要求和国家安全审查要求。

资料来源：项目组统计整理

第四节 网络安全相关技术发展情况

网络安全方面最基本的技术主要是防火墙技术、数据加密技术以及智能卡技术，随着技术发展以及下游领域网络安全要求提高，防火墙、数据加密以及智能卡等现有技术不断更新，入侵检测与防御系统（IDS/IPS）等新技术也持续被研发创新应用于网络安全细分领域。因而，现阶段我国网络安全领域应用的技术较多，包括防火墙技术、入侵检测技术、数据加密技术、身份认证技术、安全漏洞扫描技术、虚拟专用网技术、蜜罐技术、安全审计技术、防病毒技术、云安全技术等。同时，每种技术又随着技术发展拓展出不同的方向类型，这就导致我国网络安全行业细分领域高度分散，市场集中度不高。

图表 8：网络安全主要技术发展情况及代表企业统计

技术	内容	发展情况	代表企业
防火墙技术	用于隔离内部网络和外部网络，阻挡来自外部的非法访问和恶意攻击。	现阶段，防火墙技术已由最初的包过滤防火墙发展为状态检测防火墙，再到集成多种安全功能的 UTM（统一威胁管理）设备，最终发展到具备应用识别能力的 NGFW（下一代防火墙），且国内布局下一代防火墙技术的企业较多。	山石网科、天融信、启明星辰、网御星云、绿盟科技、安恒信息、蓝盾、华为等
入侵检测技术	用于检测网络中是否存在异常行为或恶意攻击，及时发现并采取相应的措施。	包括网络入侵检测系统（NIDS）和机遇主机的入侵检测系统（HIDS）；还可细分为边界 IDS、基于 VM（虚拟机）的 IDS、基于堆栈的 IDS、基于签名的 IDS 以及基于异常行为的 IDS 等。	山石网科、启明星辰、绿盟科技、网御星云、360、天融信、铱迅信息、蓝盾、杭州迪普等
数据加密技术	用于保护数据的安全性和机密性，防止数据被非法获取和篡改。	数据加密技术是最基本的安全技术，被誉为信息安全的核心。随着加密技术的不断发展和应用，加密数据工具日益增多，加密数据的应用也越来越广泛，为用户提供了更多样化的选择。	明朝万达、中安威士等
身份认证技术	用于验证用户的身份和权限，防止非法访问和恶意攻击。	身份认证技术是对信息接收方进行身份鉴别的技术，也是保障信息安全的重要手段。随着时代的发展，身份认证技术已从早期的口令发展为简单密码，后又发展为生物特征和多因素认证技术。目前已发展到无感知的身份认证技术。	竹云科技、芯盾时代、天钥科技等
安全漏洞扫描技术	用于检测网络中的安全漏洞和隐患，及时发现并修复漏洞。	漏洞扫描技术是一类重要的网络安全技术，它和防火墙、入侵检测系统互相配合，能够有效提高网络的安全性。其主要包括端口扫描技术和漏洞扫描技术。	山石网科、奇安信、绿盟科技、启明星辰、创信华通、蓝盾等
虚拟专用网技术	用于构建加密的虚拟网络，保证数据的传输安全性和机密性。	虚拟专用网技术具有高度的安全性，且可以简化网络设计、降低成本。目前国内虚拟专用网技术客户主要为企业。	山石网科、华为、阿里云等

蜜罐技术	用于诱捕攻击者，记录攻击者的行为和工具，以便进行分析和追踪。	蜜罐是一种安全威胁的主动防御技术。国内蜜罐诱捕技术最早的出现时间在2014年，但仅作为安全项目中的一个功能，并未成为独立产品被用户关注和采购。2016年陆续有专注于蜜罐诱捕技术能力的安全厂商进入市场，并推出具有单一标准化的蜜罐诱捕产品。2019年，在一系列大型的活动与安全事件推动下，蜜罐诱捕被各行业用户广泛关注。	山石网科、启明星辰、安恒、长亭科技、默安等
安全审计技术	用于对网络进行安全审计，检测和记录网络中的各种行为和事件。	IT治理、内控和风险管理的发展极大地促进了安全审计市场的发展。现阶段，安全审计细分领域不断扩大，包括主机审计、网络审计、数据库审计、运维审计、日志审计、业务审计、配置审计等方面。	天融信、绿盟科技、山石网科、奇安信等
防病毒技术	用于防范病毒、蠕虫等恶意软件的传播和破坏。	近些年，随着网络安全技术的不断提升，电脑病毒的数量和感染面积有所下降，但电脑病毒仍然存在，并不断发展。病毒现在不仅仅是破坏、篡改或删除文件，更多的是通过勒索，窃取信息等方式来实现目的。随着科技的不断进步和计算机的广泛应用，数据加密技术、防火墙技术、杀毒软件等防病毒技术也得到了极大的发展，但是病毒是不可能彻底消失的，这就要求防病毒技术要持续更新和创新发展，才能满足需求。	三六零、山石网科、金山、瑞星科技、江民科技、卡巴斯基技术等
云安全技术	用于保护云端数据的安全性和机密性，防范云端攻击和数据泄露。	随着各个行业和领域都在加速向云迁移和创新，如电商、金融、教育、医疗、游戏、社交等，云计算服务需求日益多样化和复杂化。为了满足不同的应用场景和用户需求，云安全技术也在不断创新和演进，中国企业使用或计划使用的主要云安	山石网科、奇安信、启明星辰、安恒信息、华为、三六零、天融信、华清信安等

		全技术包括边缘云、分布式云、多云、零信任等。	

资料来源：项目组统计整理

没有网络安全就没有国家安全，网络安全技术为维护国家网络安全提供了重要的技术基础，为支撑经济社会发展构建坚实的安全屏障。党的十九届五中全会明确了我国“十四五”期间发展的战略任务和 2035 年远景目标，强调要统筹发展和安全，全面加强网络安全保障体系和能力建设，对网络安全技术和防护能力提出了新的更高要求。以下为网络安全关键技术方向：

图表 9：网络安全关键技术方向

技术方向	技术子领域	实现时间		制约因素	
		实验室实现	社会推广	实验室制约因素	社会推广制约因素
网络攻击追踪溯源技术	数据安全	2023	2025	高层次人才及团队	国内示范推广
面对人工智能应用的网络安全技术	新一代新兴技术安全	2024	2028	高层次人才及团队	国内示范推广
大数据威胁情报分析技术	数据安全	2023	2025	产学研合作	国内示范推广
云环境下的数据存储安全技术	应用安全	2024	2025	产学研合作	产业链配套
信息内容的理解和研判技术	内容安全	2024	2027	高层次人才及团队	公众需求
网络安全主动防御技术	网络攻防	2024	2024	产学研合作	公众需求
网络虚拟身份管理技术	数据安全	2024	2025	国家政策支持	国内示范推广
车联网网络安全防护技术	新一代信息技术安全	2024	2027	产学研合作	公众需求

可信计算技术	应用安全	2025	2028	研发资金	产业链配套
工业控制系统的安全防护技术	应用安全	2023	2024	产学研合作	产业链配套

资料来源：项目组统计整理

第二章 中国网络安全发展现状

第一节 中国网络安全发展现状

一、市场发展前景好，规模及企业持续增长

中国网络安全市场起步晚，产业整体规模及增长幅度有限。近年来，在国家政策法规支持下，政府部门和机构加大在网络安全上的投入，数字经济蓬勃发展带动市场需求逐渐增强，为网络安全产业规模提升注入新的驱动力。2020-2022 年，中国网络安全市场规模由 718.8 亿元增长至 920.0 亿元。企业方面，随着信息化产业发展、数字化融合，我国网络安全需求持续增多，加之政策刺激，国内网络安全企业数量也有所增长，现阶段行业内企业数量已超过 4000 家，且随着数字化、信息化发展，未来国内网络安全需求还将增长，企业数量也将进一步增加。

二、行业集中度低，国内厂商竞争力不强

近年来，虽然我国网络安全产业快速发展，但是，产业总体规模仍然较小，在全球市场份额中占比仍较低。在市场规模有限的情况下，我国约有四千余家网络安全从业公司，产业竞争十分激烈，激烈的竞争并没有造就强大的头部企业，行业集中度低。从全球网络安全市场看，美国占据网络安全领域的主导地位，诞生了一批如思科、赛门铁克、迈克菲和火眼等在网络安全产品和服务提供商，其从业公司在市场规模、技术实力、产品性能和服务水平上远远领先国内企业，拥有强大的国际竞争力。

三、行业发展不均衡，产业布局有待优化

基于政策扶持、需求扩张、应用升级等多方面驱动，我国网络安全产业发展进入快车道。网络安全产业呈现出重点领域发展壮大、新模式新业态不断涌现、产业集聚发展加速等特点，形成了良好的发展局面。但由于我国网络安全行业起步较晚，加之各地区、各细分领域、各应用领域发展不一，网络安全行业呈现不均衡、不协调的发展态势。

从细分产品来看，我国网络安全产品细分领域较多，各领域发展不均衡，其中基础设施安全领域和云安全、信息技术应用创新领域市场规模较大，2022年该三大领域网络安全市场规模合计为445.9亿元，占网络安全总规模的48.47%；而数据安全、应用安全、安全运营、工业互联网等领域市场规模相对较小。

从需求区域方面来看，我国网络安全客户分布与GDP有较强相关性，呈现区域集聚效应，华东、华北和华南地区经济较发达，对网络安全的投入较大，是我国网络安全主要需求区域，2022年三地区需求占比合计超过70%。华中、西南、西北等地区需求占比较低。

从下游应用领域来看，网络安全市场项目分布广泛，涉及政府、教育、医疗卫生、公检法司、能源化工、企业、电信、金融、交通等多个领域，其中，政府领域因客户数量多，政策监管严格，项目需求量大，在行业中占据主导地位；其他下游领域需求还需进一步释放。

四、技术持续发展，企业产品不断更新迭代

网络安全是一个动态的过程，随着网络变得高度关联、相互依赖，网络安全的威胁来源和攻击手段不断变化，加之网络应用的广泛普及和数据量的增长，也对网

络安全防护能力提出新要求。此外，IT 技术的发展会导致防守两端的技术都在进步，新技术会被应用于新的攻击手段，防守端也需要新的技术来应对。因而，随着云计算、物联网、人工智能等新技术的快速发展，网络安全技术需要不断更新迭代以适应新的网络环境和安全需求。

随着竞争加剧，国内网络安全行业越来越多的企业加大研发投入、布局新技术、推出新产品，例如山石网科在 2020 年成立安全技术研究院，并于 2023 年与龙芯中科联合成立信创安全实验室，共同研发、探索新技术；启明星辰于 2022 年与龙芯中科联合成立信创安全实验室；深信服 2021 年发布 DaaS 桌面即服务；奇安信 2023 年推出奇安天盾数据安全保护系统、奇安信零信任工作系统、大模型卫士等多款创新产品。

图表 10：网络安全行业重点企业发展历程

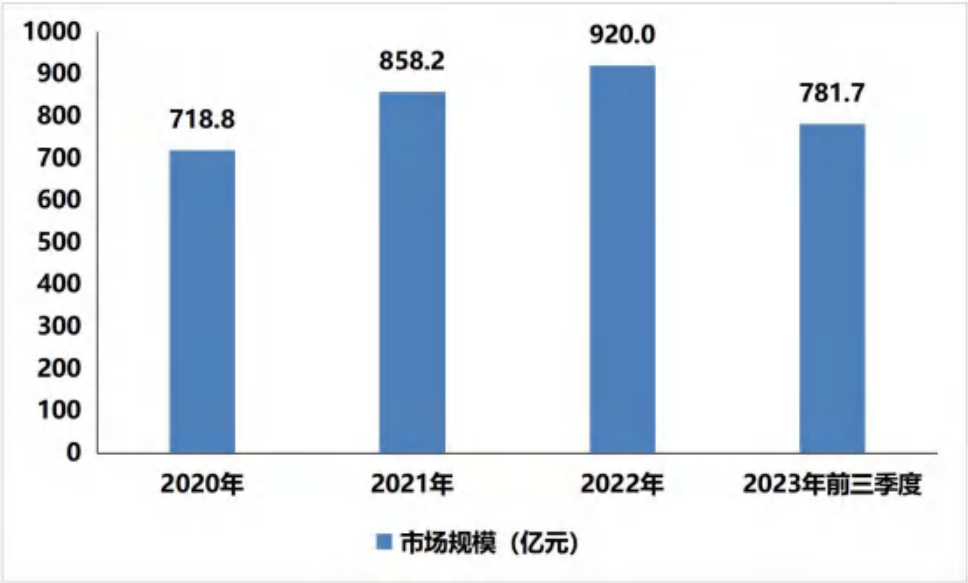
	1990-1999	2000-2009	2010-2019	2020-至今
山石网科		2007年，山石网科成立 2009年，SG系列模块化多核安全网关首批通过国家信息安全产品认证（三级）	2011年，山石网科成立苏州研发中心和全球技术支持中心 2019年，山石网科在上交所挂牌上市	2020年，山石网科成立安全技术研究院 2023年，山石网科与龙芯中科联合成立信创安全实验室
启明星辰	1996年，启明星辰公司成立 1997年，启明星辰研发中心成立	2005年，推出国内第一款自主知识产品的UTM产品—天清汉马USG多功能安全网关	2010年，启明星辰在深交所挂牌上市	2022年，启明星辰集团与中国移动集团达成投资合作
深信服		2000年，深信服科技正式注册成立 2007年，连续4年入围Gartner魔力象限	2011年，国内率先推出下一代防火墙 2018年，于深交所创业板上市	2020年，发布SASE、零信任VPN、ARM超融合架构、云原生平台、云计算平台 2021年，发布DaaS桌面即服务
奇安信			2014年，奇安信成立 2016年，开始参与国家级网络安全保障	2020年，登陆科创板 2021年，组建网络安全中国代表队

资料来源：项目组统计整理

第二节 中国网络安全市场规模

近三年，基于政策扶持、需求扩张、应用升级等方面驱动，我国网络安全产业进入“快车道”，产品体系日益完善，技术创新高度活跃，企业数量持续增加，行业综合实力不断增强，市场规模也随之呈现增长态势。具体来看，2020 年，受疫情封控等因素影响，人们居家办公、学习时间增多，网络使用量激增，面临的网络安全问题随之增加，带动网络安全规模增长；2021 年以来，国内接连出台个人信息保护、数据安全等方面网络安全保护法规、意见，在网络安全政策法规驱动下，国内网络安全市场规模呈现持续增长态势。2022 年，受宏观经济下行趋势影响，国内网络安全行业市场需求在经历多年快速增长后，出现增速放缓现象，其市场规模增速也随之放缓，中国网络安全市场规模增长至 920.0 亿元。

图表 11：2020-2023 年前三季度中国网络安全市场规模统计

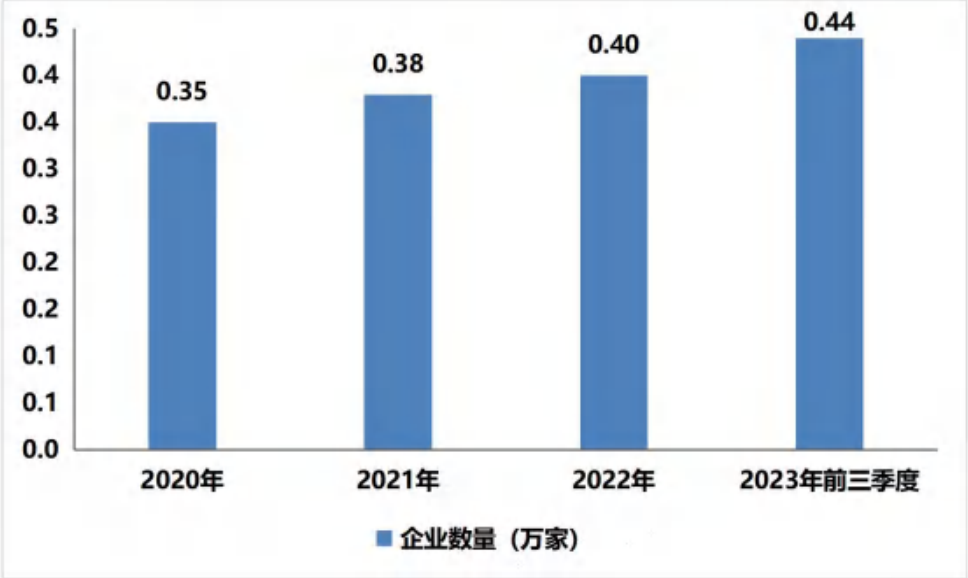


数据来源：项目组统计整理

第三节 中国网络安全市场企业数量

随着疫情平稳转段、网络安全相关政策法规和标准规范相继落地、网络安全治理日臻完善等正向激励效能显现，中国网络安全市场需求持续扩大，产业取得积极进展，技术创新明显提升，动态行为分析等一批前沿技术取得创新突破；同时，网络安全产业链条不断完善、产业基础能力稳步提升。2023 年前三季度，中国网络安全企业数量增长至 0.44 万家，覆盖网络安全设备、安全服务、安全软件、安全集成等网络安全各环节，产业链上下游协同效应进一步增强。

图表 12：2020-2023 年前三季度中国网络安全市场企业数量统计



数据来源：项目组统计整理

第四节 中国网络安全产业结构

从产品类型来看，网络安全产品包括基础设施安全产品、云安全产品、数据安全产品、应用安全产品、安全运营产品、工业互联网安全产品、信息技术应用创新产品等细分类型。其中，基础设施安全产品、云安全产品、信息技术应用创新产品

是需求量较大的细分领域，2022 年这三大领域网络安全市场规模均超过 100 亿元；而数据安全产品、应用安全产品、安全运营产品、工业互联网安全产品 2022 年规模均不足 100 亿元。

现阶段，我国网络安全行业市场空间已颇具规模，多年来保持了快速增长态势。良好的发展前景及市场机遇也吸引了较多参与者，市场竞争较为激烈。现有企业中，奇安信、启明星辰、深信服、天融信等企业安全业务收入高于 30 亿元，处于行业第一梯队；绿盟科技、山石网科、安恒信息、三六零、亚新安全等企业安全业务收入低于 30 亿元但又大于 5 亿元，处于第二梯队。此外，还有大量安全业务收入低于 5 亿元的中小型网络信息安全企业。总的来看，我国网络安全行业整体市场仍较为分散。

图表 13：中国网络安全行业竞争梯队

资料来源：项目组统计整理

从地域方面来看，华北、华东、华南地区经济发达，网络安全意识高、投入大，是我国网络安全主要需求区域，2022 年三大地区需求占比达到 70%左右，其他地区

网络安全需求占比合计仅在 30%左右。同时，华北、华东、华南地区也是我国网络安全企业主要分布地区，例如奇安信、启明星辰、北信源等龙头厂商分布与华北地区；山石网科、中孚信息、亚信安全、安恒信息、迪普科技位于华东地区；深信服、天融信等厂商位于华南地区。

第五节 中国网络安全发展驱动因素和限制条件分析

一、驱动因素

1、安全管理、安全服务需求逐渐上升

随着生产生活数字化程度不断加深，网络安全合规要求不断提高，诸多动力将驱动我国网络安全市场不断扩张。一是处于数字化转型加速期的企业面对更加复杂严峻的网络安全环境，必须加大网络安全投入，满足安全合规要求，保障业务稳定安全。二是个人信息保护更加深入人心，对网络的安全性要求更高。三是元宇宙等新概念的提出创造了新的网络安全需求。

同时，数字经济和大数据等新兴产业是我国“十四五”期间重点发展的产业，随着数字经济、大数据产业等“十四五”发展规划陆续出台，各行各业将加快数字化改造，我国数字经济将迎来蓬勃发展，“数字中国”建设也将深入推进，网络安全产业作为保障数字经济和大数据等产业安全的重要工具，其需求也将持续增多，市场规模不断扩大。预计 2025 年，我国网络安全市场规模将增长至 1588.7 亿元。

2、AI 等新兴技术赋能网络安全产品

人工智能（AI）技术是近年来备受关注的热门技术之一，它已经在各个领域展

示出了巨大的潜力和影响力。而在网络安全领域，人工智能的兴起也将带动重要的改变。例如人工智能通过学习和分析大量的数据，可以快速发现和识别潜在的攻击行为，从而提前采取相应的防御措施；利用深度学习技术，人工智能可以对大量的网络攻击数据进行分析，识别出隐藏的攻击模式，并提供更加精准的威胁情报。此外，人工智能也可以提供更加大的身份认证和访问控制能力，进一步保障网络安全。

目前，国内多个网络安全企业已将AI应用到网络安全产品及服务中，例如山石网科推出基于AI技术的三大威胁检测能力：入侵防御检测、僵尸网络防御检测、恶意加密流量的智能检测；华为推出基于自进化的AI检测引擎—华为HiSec Insight安全态势感知系统，该系统可对整个企业网络安全态势进行精准预测，以提升网络的威胁处置能力和安全运维效率的网络安全态势感知系统，是华为面向企业全场景智能威胁检测推出的安全大脑。

除人工智能技术外，量子信息技术也将在网络安全领域中发挥更大的作用。例如可利用量子态的叠加性和量子不可克隆原理可进行绝对安全的量子保密通信。近年来，量子保密通信技术与物联网、大数据、人工智能以及5G等现代ICT技术的融合不断加速，量子安全服务已在政务、金融、能源等领域持续落地。美国政府通过签署政策指令推动量子技术的研究开发，帮助美国加密标准向后量子密码学过渡，加速建设安全、稳定的量子网络；欧盟积极发布相关发展战略，整合多个国家现有超算资源，建设覆盖整个欧洲的量子网络。总的来看，人工智能、量子信息等新兴技术应用可为网络安全提供更丰富的工具，提高网络安全技术水平，推进行业技术发展。

3、政策法律体系不断完善，行业发展更有保障

网络安全是筑牢可信可控数字中国安全屏障的重要保障，也是以新安全格局保障新发展格局的战略需求、推动国家安全体系和能力现代化建设的必要条件，其发展受到国家政策的大力支持。在《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》等一系列法律法规加速落地的同时，网络安全相关立法继续向体系化、纵深化发展。《网络安全审查办法》、《互联网信息服务算法推荐管理规定》、《数据出境安全评估办法》颁布实施，在坚定维护网络空间安全的同时，也刺激了网络安全产业加速发展。同时，人工智能、自动驾驶、元宇宙等新概念、新技术、新业态的兴起与推广给网络安全法律体系建设提出了更高要求，细分领域的立法仍处于“进行时”。

网络安全相关法律法规由“立”向“行”演进。2021 年以来，网络安全领域执法检查活动更加频繁，执法更加严厉，典型网络安全司法判例和执法案例不断涌现。网络安全审查已逐渐成为我国网络安全生态治理的常态化内容，相关执法实践也越来越成熟，网络安全与数据保护逐渐成为企业必须正视的重大合规问题，刺激了数据合规、安全合规等服务需求，成为网络安全产业新的增长点。

二、限制因素

1、网络安全法律体系不够完善

第一，法律法规仍待细化落实。尽管网络安全法律体系逐步建立健全，但是每部新法案从开始实施到完善落实，都需要一定的过渡期。新法内的一些具体规定要具体“落地”，都需要完善一系列措施及配套政策。《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等出台后，仍需要制定相关的配套措施，针对

需要明确的重点问题进一步细化，明确《中华人民共和国数据安全法》的制度及具体要求与标准，进一步提高实操性，才能提供实践指导。

第二，法律法规配套仍需加强。总体来说，网络安全领域的立法质量不断提高，法律的操作性、规范性不断增强，但现有网络安全领域配套法律法规仍需完善。一方面，法律配套制度涉及部门多，协调难度大，影响因素交错复杂，客观上会带来一定的困难。另一方面，网络技术发展迅猛，情况变化很快，这也给法律法规配套的制定和落实带来一定的挑战。

2、核心技术自主可控能力不够强

自主可控是确保网络安全的必要条件。目前，我国在网信领域（如芯片和基础软件等方面）仍存在一些短板。芯片方面，其短板在于制造工艺、装备、材料、设计工具等方面。以AI芯片为例，我国起步晚，在算法方面缺乏原始创新，目前仍依赖进口。基础软件方面，操作系统大部分依赖Windows，国产操作系统很少；大型工业基础软件，如集成电路涉及软件基本上是进口，自主研发的较少。我国亟需“扬长处，补短板”，努力突破“卡脖子”问题，提升自主可控能力，保障网络安全。

3、网络安全人才供需失衡

当前，我国网络安全领域人才不足，已成为阻碍我国产业发展的主要因素，特别是实战型人才培养方面，存在显著的需求缺口。此外，由于高校缺乏实战环境，过于注重理论知识传授而轻视实践能力培养，所培养的网络安全人才往往无法迅速融入实际工作，大部分企业认为自己缺乏网络安全实战人才。攻防实战人才必须具备在实际业务环境中，利用网络安全技术和工具进行安全监督和解析、危险度评估

或风险评估与衡量、渗透测试事件研判等业务能力，这对网络安全攻防实战人才的培养路径提出了高标准、高要求。

同时，我国还缺乏网络安全人才发展规划。随着全球信息化进程的推进，众多国家已经认识到网络安全的重要性，并纷纷制定国家网络安全战略。然而，相较于美国等发达国家在网络安全人才培养方面的系统性和层次性，我国在这方面起步较晚。尽管我国已经发布了一些网络安全战略规划文件，强调了人才培养的重要性，但总体上来说，仍缺乏网络安全人才培养的整体规划和顶层设计。

第三章 中国网络安全重点细分行业发展情况分析

第一节 网络安全重点细分市场发展现状

一、基本概述

以下是网络安全重点细分市场范围界定：

图表 14：中国网络安全重点细分行业基本信息

细分市场	简介
基础设施安全	指面向公众提供网络信息服务或支撑能源、通信、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统安全等。
云安全	云安全行业包括了云计算基础架构的安全、云计算服务平台的安全和云计算软件的安全。云安全是云计算技术在安全领域的应用，亦是安全技术在云计算领域的应用。
数据安全	数据安全是保护数字信息资产免遭未经授权的访问、披露、修改或盗窃，能够保护数据免受意外或故意威胁，并在组织的整个生命周期中保持其机密性、完整性和可用性。
应用安全	应用安全就是保障应用程序使用过程和结果的安全。针对应用程序或工具在使用过程中可能出现计算、传输数据的泄露和失窃，通过其他安全工具或策略来消除隐患。 应用安全旨在防止应用程序内的数据或代码被盗或劫持，包含在应用程序开发和设计过程中发生的安全注意事项，但也涉及在应用程序部署后保护应用程序的系统和方法。
安全运营	从狭义层面来看，安全运营是以 IT 资产为核心，以威胁事件管理为关键流程，利用安全运营平台，建立的一套实时的 IT 资产风险评估模型，是进行事件发现、风险分析、预警管理和应急响应处置的集中安全管理体系。 从广义层面来看，安全运营是一个将技术、流程和人有机结合的复杂系统工程，通过对已有安全产品、工具和服务产出的数据进行有效的分析，持续输出价值，解决安全问题，以确保网络安全为最终目标。

工业互联网安全	工业互联网安全指保护工业互联网系统、设备和数据免受未经授权的访问、损坏、干扰或泄露的一系列措施和实践。由于工业互联网涉及关键基础设施、生产过程和重要数据，其安全性至关重要。
信息技术应用创新	即信创，是数据安全、网络安全的基础，也是新基建的重要组成部分。信创体系覆盖 2+8+N 个领域，即党、政与金融、电力、电信、石油、交通、教育、医疗、航空航天 8 个关于国计民生的重要行业，以及 N 个消费市场。

资料来源：项目组统计整理

二、产业图谱

网络安全产业链上游是涉及网络安全的相关设备/系统，包括芯片、内存等基础硬件；操作系统、数据库、中间件等软件系统，以及引擎、算法等基础能力；中游是网络安全产品和服务厂商，如山石网科、亚信安全、腾讯云、华云、安恒信息、启明星辰等；下游是网络安全产品及服务应用领域，包括政府、教育、医疗、能源、金融、电信、制造等。

图表 15：中国网络安全行业产业链图谱

资料来源：项目组统计整理

第二节 细分市场发展阶段分析

一、基础设施安全

1、发展现状

2016 年 4 月，习近平总书记在网络安全和信息化工作座谈会上对关键信息基础设施保护和网络安全检查工作时指出：“金融、能源、电力、通信、交通等领域的关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重，也是可能遭到重点攻击的目标”，要求“要全面加强网络安全检查，摸清家底，认清风险，找出漏洞，通报结果，督促整改”。2016 年 12 月 27 日，国家互联网信息办公室发布并实施了《国家网络空间安全战略》，提出要加强对国家关键信息基础设施的保

护。

随着网络安全日益受到重视，各个企业的网络安全保护意识日益增强，我国针对网络安全违法犯罪行为的打击力度也逐渐加大。其中，关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重，在当前的情势下，加快提升关键信息基础设施安全保护能力成为国家的一项重要工作。

2021 年，《关键信息基础设施安全保护条例》正式发布，明确了关键信息基础设施的范围，以及运营者的责任义务。2023 年 5 月，《信息安全技术 关键信息基础设施安全保护要求》国家标准正式实施，为各行业各领域关键信息基础设施的识别认定、安全防护能力建设、检测评估、监测预警、主动防御、事件处置体系建设等工作提供有效技术遵循，为保障关键信息基础设施全生命周期安全提供标准化支撑。

国家互联网信息办公室发布《数字中国发展报告（2022 年）》显示，2022 年，我国网络基础设施、算力基础设施、应用基础设施规模和服务能力快速增长，一体化协同发展水平稳步提升。“双千兆”网络深度覆盖进程加速，网络基础设施覆盖区域持续下沉；算力基础设施规模世界领先，“东数西算”工程全面开展；工业互联网、车联网、能源互联网等应用基础设施加速赋能高质量融合发展。

总体上，近些年，为支撑和保障关键信息基础设施安全保护工作的顺利和有效开展，相关法律法规政策和标准体系从国家各个层面均在逐步的构建和完善中，同时各企事业单位也在不断加强基础设施安全的投入，进而推动了中国基础设施安全市场规模的持续增长。

2、特点

（1）安全问题层出不穷，且影响重大

关键信息基础设施作为网络空间的“神经中枢”，其功能稳定与服务持续是维护国家安全和社会稳定的关键所在，一旦遭受攻击可能会导致系统关键服务运行中断、通信设备瘫痪以及大规模数据信息泄露等重大影响。例如，2020年以来，委内瑞拉电网攻击、美国天然气管道商遭攻击、欧洲能源巨头遭受勒索软件攻击、乌克兰多个政府机构以及两家大型银行的网站遭到DDoS网络攻击、北京健康宝遭境外黑客组织大规模流量攻击、武汉地震监测中心遭某国情报机构恶意网络攻击等事件，网络攻击事件频发，涉及电力、水利、能源、金融、医疗、交通等关键信息基础设施领域，网络安全事件层出不穷。

（2）面临新挑战

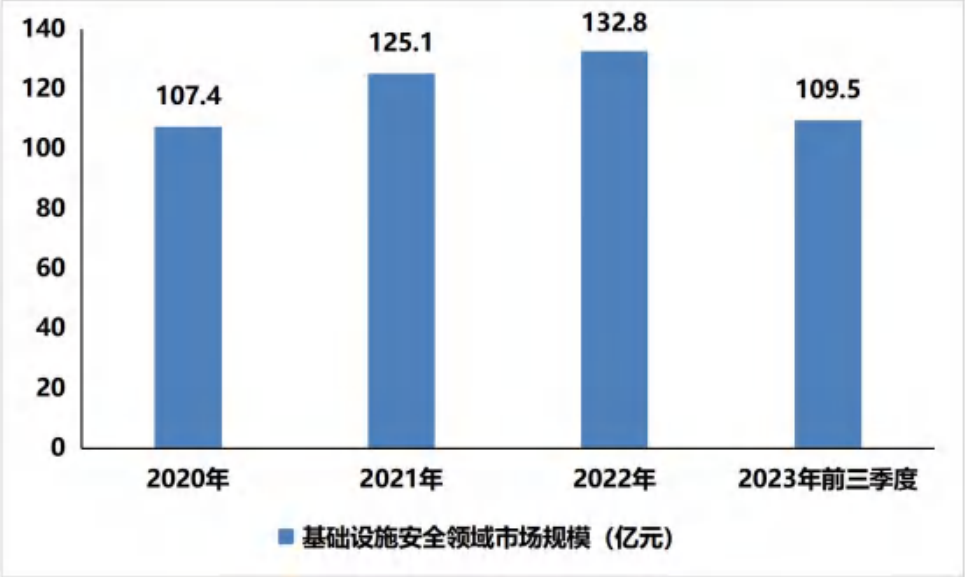
当前，百年未有之大变局加速演进，受地区安全局势变化、意识形态斗争等因素影响，我国网络安全关键基础设施保护工作面临错综复杂的新形势和新挑战。一是高级可持续性威胁攻击的技术和武器快速发展，指向性和杀伤力不断增强，高级可持续性威胁攻击加剧，网络安全防御愈加艰难。二是随着信息化技术的快速发展，新技术和新应用加速发展，但是由于其自身安全和使用安全未经过广泛深入的研究和论证，这类新兴技术和应用成为恶意攻击者发起网络攻击的高风险目标，网络安全新风险日益显现。三是生成式人工智能异军突起，且呈加速发展态势，利用该技术制造的大模型网络工具或可轻易制作黑客攻击脚本和难辨真伪的网络钓鱼邮件，使得网络攻击门槛显著降低，对关键基础设施保护工作构成较大冲击，引发更多的

不稳定因素。四是网络设备研发制造全球化，供应链安全问题更加复杂，极大增加了关键基础设施行业领域软硬件产品供应链的攻击面，导致我国关键基础设施供应链安全面临着严峻而复杂的挑战。

3、市场规模

近些年，国际环境越来越复杂，国内外基础设施安全事件频发，针对我国基础设施开展的网络攻击行为越来越多，我国企事业单位不得不持续提升基础设施安全能力，同时叠加国家对基础设施安全的重视程度越来越高，不断完善基础设施安全相关法律法规和标准，中国基础设施安全行业市场规模持续增长。2023 年前三季度，中国基础设施安全市场规模达到 109.5 亿元。

图表 16：2020-2023 年前三季度中国基础设施安全领域网络安全市场规模统计



数据来源：项目组统计整理

二、云安全

1、发展现状

2008年5月，趋势科技在美国正式推出了“云安全”技术。但是中国云安全行业的发展略晚于美国市场2-3年，即2011年萌芽，2014年众多技术驱动的创业型公司加入到该领域，同时2014年阿里云等公有云厂商正式上线云安全服务，行业逐渐进入快速发展阶段。2015年，山石网科公司发布云计算安全产品“山石云·格”和“山石云·界”。2018年，初创公司与公有云安全厂商竞合关系逐步形成，安全服务初创公司接入公有云厂商，云安全良性生态逐渐形成。

近些年，国家陆续颁布了《网络安全法》、《数据安全法》、《关键信息基础设施保护条例》等法律法规，国家对于网络安全、数据安全、信息基础设施安全的重视，有力提升了各行业的安全防护意识。同时，随着我国云安全技术本身愈发成熟，山石网科、安恒信息、三六零等企业在新兴云安全技术的应用上不断追赶，有力地支撑了国内云安全市场的发展。

在政策和技术的推动下，同时随着我国数字经济高速发展，受数字政府、智慧城市、工业互联网、企业数字化转型等应用影响，伴随着云服务模式的深化应用，细分领域和场景的安全实践带来云安全市场需求的快速增长。

2、特点

（1）市场规模高速增长

我国云安全行业发展虽然仅有10年左右时间，但是近年来，在云计算和网络安全产业的蓬勃发展下，我国云安全行业市场规模呈现高速增长态势，2020-2022年中国云安全市场规模保持40%以上的复合增速高速增长，同时云安全在网络安全市场总体规模中占比不断上升，2022年已接近20%。

（2）云安全形势依然严峻

云安全形势依然严峻，尤其是高度利用云计算技术，将重要业务迁移到云端的企业，正面临例如数据泄露、隐私泄露、服务中断、设备管理等一系列问题。这些问题如果不得到解决，可能会引发严重的隐私侵犯问题，影响企业用户的信任和安全感，再加上如果系统遭受攻击从而将引发业务中断，会导致服务不可用，影响用户体验和业务连续性，企业声誉受到严重影响，甚至可能导致企业面临财务损失。

（3）新产品持续推出

虚拟机、容器、服务网格、多集群间通信、多云和混合云、Serverless 等新技术不断涌现，对云安全技术提出了越来越多的要求，我国云安全企业也持续推出新产品以满足快速变化的市场需求。以山石网科为例，其于 2015 年发布云计算安全产品“山石云·格”和“山石云·界”，分别为用户提供云计算网络之间的安全隔离和安全防护、云内东西向流量的网络微隔离防护能力；2021 年发布云安全新品——山石云铠，为云环境提供主机与容器安全防护能力，在云计算安全版图补全“容器安全”板块，完成主流虚拟化技术及云服务场景网络安全产品的全面覆盖。目前，山石网科将安全 SD-WAN、私有云安全、公有云安全、云安全审计和云安全运营等优势方案能力集成进企业多云、混合云网络安全解决方案中，帮助企业多云、混合云用户构建全面、可靠、稳定的网络安全环境。

图表 17：山石网科云安全主要产品

方案	特性
安全 SD-WAN	为企业广域网络提供先进的防护能力，以应对企业多云、混合云广域组网所面临的各种挑战。
私有云安全	兼容各类主流虚拟化和云平台环境，可通过在私有云部署山石云·界、

	山石云·格、山石云铠、山石云·集、山石 vWAF 及审计探针等产品实现私有云网络层、应用层、数据层的威胁检测与安全防护。
公有云安全	可为多云、混合云用户提供公有云内丰富的安全防护能力，为用户构建安全的公有云业务防护体系，落实租户安全等级保护要求。 多云、混合云用户的公有云租户可选购满足自身防护需求的山石网科公有云安全产品，如山石云·界虚拟化防火墙、山石云 Web 应用防火墙、云漏洞扫描等，从而实现租户内差异化、精细化的 IaaS 安全防护能力。 通过公有云安全管理中心，租户能够方便实现山石网科公有云安全产品的下单、资产管理和用量计费，并且可以全面掌握云安全态势，实现便捷、高效的安全运维与租户纵深安全防护。
多云、混合云安全审计	山石网科云数据库审计与防护系统可对多云、混合云租户内的云数据库访问行为进行独立审计和安全控制，帮助用户应对来自外部和内部的数据库安全威胁，满足等保要求中关于安全计算环境的数据完整性和数据保密性要求。 山石网科云堡垒机将运维管理和运维安全理念相融合，通过身份认证、权限控制、账户管理、操作审计等多种手段，完成企业多云、混合云内核心资产的统一认证、统一授权、统一审计，全方位提升运维风险控制能力。 山石网科云日志审计产品可为多云、混合云用户提供上网访问行为的监管与审计功能，配合山石云·界的 NAT、IPS、上网行为分析等功能，能够有效记录接入用户的网络日志和安全日志，帮助用户解决网络出口日志审计的困扰，满足《网络安全法》及行业的监管要求。
多云、混合云安全管理与运营	针对主机安全管理，山石云鉴主机安全管理系统围绕主机检测、响应、预防进行可持续安全运营，实现主机安全全生命周期管理。 针对多云、混合云安全运营，山石云景云端安全运营与管理平台围绕业务系统，把持续的威胁检测、威胁分析和响应处置固化到日常企业安全运营的工作中，帮助企业多云、混合云环境构建起以主动监测、快速预警、有效联动、准确处置为特点的闭环式动态安全运营体系。

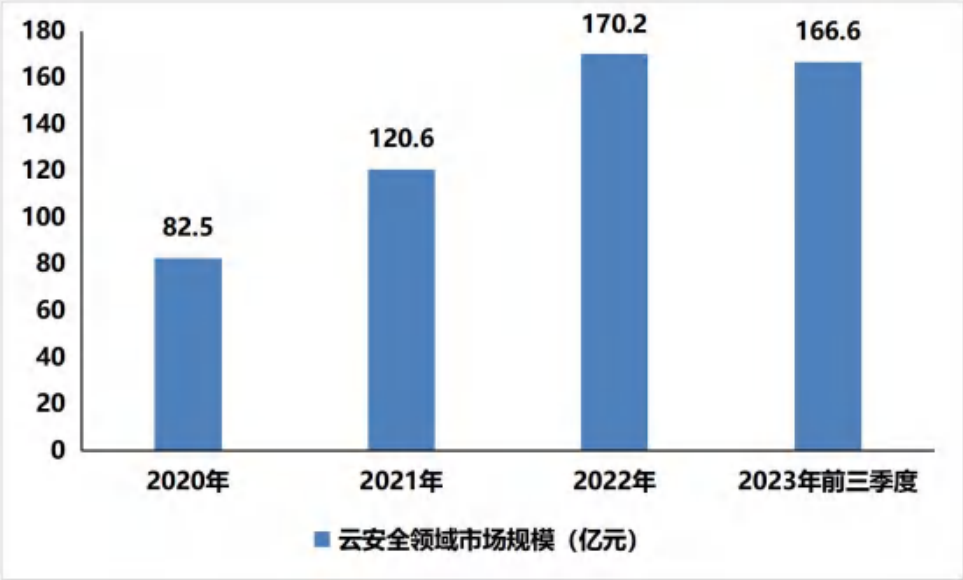
资料来源：项目组统计整理

3、市场规模

2020-2022 年，随着中国云计算技术的快速发展以及公有云、私有云、混合云的迅速推广应用，中国云安全需求越来越强烈，推动了中国云安全市场规模的高速增

长，2022 年，中国云安全市场规模大的 170.2 亿元，同比增长 41.1%。2023 年前三季度，中国云安全市场规模依然保持高速增长，达到 166.6 亿元。

图表 18：2020-2023 年前三季度中国云安全领域网络安全市场规模统计



数据来源：项目组统计整理

三、数据安全

1、发展现状

随着信息技术和人类生产生活交汇融合，各类数据迅猛增长、海量聚集，对经济发展、人民生活产生了重大而深刻的影响，数据安全也已成为事关国家安全与经济社会发展的重大问题。

近年来，国家多次发布相关法规法案，将保障数据安全放到了重点突出的位置。2021 年 6 月 10 日，我国《数据安全法》正式发布，并于 2021 年 9 月 1 日起施行。《数据安全法》重点确立了数据安全保护的各项基本制度，完善了数据分类分级、重要数据保护、跨境数据流动和数据交易管理等多项重要制度，形成了我国数据安

全的顶层设计。

数据安全需求的提升是推动行业快速发展的根本因素。随着我国整体信息化水平持续提升，经济和社会对信息化的依赖程度日益提高，而随着身份盗用、交易诈骗、资源滥用、网络钓鱼等安全事件频繁发生，政府、企业、个人对数据安全的关注程度日益增强，社会对数据安全的需求与日俱增，政府部门、重点行业在数据安全产品和服务上的投入也不断增加，促进了数据安全行业的持续增长。2022年，中国数据安全市场规模达到48.5亿元。

2、特点

（1）增速快、细分领域多

近些年，我国数据安全行业快速发展，2020-2022年市场规模增速保持在20%以上，但是数据安全的细分赛道众多，可划分为四个大类18个技术领域，涉及数据安全治理、数据安全态势感知、数据服务、大数据安全管控与防护、API安全、数据库防火墙、数据库审计、数据库加密、数据库运维、数据库保密检查、文档加密、数据脱敏、DLP、数据水印、数据备份/恢复/销毁、APP隐私检测与保护、隐私计算、隐私管理。

（2）外部数据安全威胁持续升级

业务数字化、信息系统云化、安全边界模糊化等正在加速演进的时代发展趋势，使得企业或组织面临的外部数据安全威胁也在相应发生变化。在数据时代，通过漏洞利用、防护绕过等手段侵入企业或组织的内部网络实现数据窃取或破坏的安全事件仍常有发生，但随着网络安全防护设施的普及和加强，明显增加了侵入内部网络

的难度，伴生而来的新的攻击和外部数据安全威胁层出不穷，导致数据的窃取、篡改和非法使用等威胁。

（3）内部数据安全风险日益严峻

相比持续升级的外部数据安全威胁，日益严峻的内部数据安全风险更是让企业或组织感到迫在眉睫。其主要风险包括内部人员有意或无意行为引发的数据安全风险、敏感个人信息非法利用严重侵害个人权益、业务频繁变化引起的数据误用、滥用等。

（4）国内厂商占据主导

数据安全领域细分领域较多，部分细分领域之间的技术关联性不强，而数据安全技术密集型的特点，导致企业很难在不同的细分领域同时发力。但是在总体的数据安全市场中，国内安全公司一直在安全硬件市场中占有主导地位，份额已经超过一半，其产品的性能和功能完全可以和国外产品相抗衡。如山石网科作为中国网络安全行业的技术创新领导厂商的代表，在《网络安全法》正式实施的 2017 年，便加大数据安全相关产品研发力度，山石网科数据库审计与防护系统、山石网科数据泄露防护系统、山石网科静态数据脱敏系统、山石网科数据安全综合治理平台等十余款产品先后面世，帮助客户构建贴合自身情况的数据安全防护体系。

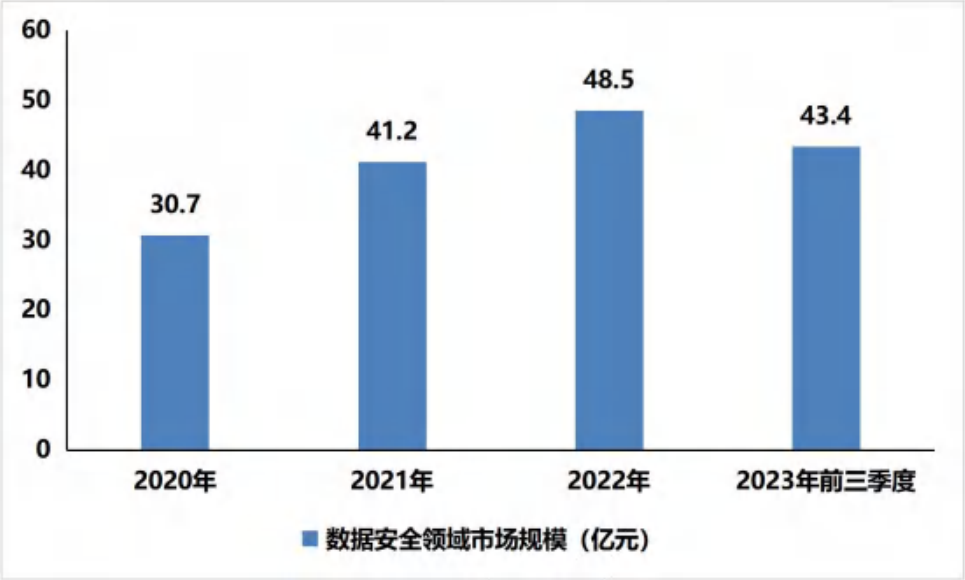
图表 19：山石网科数据安全治理方案框架图

资料来源：项目组统计整理

3、市场规模

数据安全行业产品涉及软硬件级服务，通过采用强大的数据保护策略、身份和访问管理（IAM）、管理控制、物理安全、合规性法规以及各种其他技术和技术来保护数据免受网络威胁和破坏。2020-2022 年，随着我国数据安全问题越来越突出，中国政府、企事业单位以及个人对数据安全越来越重视，同时中国数据安全行业产品越来越丰富，推动了中国数据安全市场规模的持续增长，2022 年，中国数据安全市场规模达到 48.5 亿元。2023 年前三季度，中国数据安全市场规模为 43.4 亿元。

图表 20：2020-2023 年前三季度中国数据安全领域网络安全市场规模统计



数据来源：项目组统计整理

四、应用安全

1、发展现状

应用安全产品主要包括以下几类：

WEB 应用防火墙：WEB 应用防火墙是集 WEB 防护、网页保护、负载均衡、应用交付于一体的 WEB 整体安全防护设备的产品，主要功能是事前主动防御，事中进行智能响应，事后进行行为审计。如山石网科 Web 应用防火墙（WAF）采用双安全引擎等多种先进技术，能够有效抵御 SQL 注入、跨站、挂马、恶意扫描等常见 Web 攻击，同时，还支持 Web 应用加速、应用负载均衡、Bypass 和 HA 等功能，为 Web 应用提供全方位的防护解决方案。

WEB 应用安全扫描及监控：Web 应用扫描器通过 Web 前端与 Web 应用程序通信，可以自动检查 Web 应用程序，探测、分析其响应，从而发现潜在的安全问题和

架构缺陷。Web 安全监控系统主要采用类似于搜索引擎的爬虫技术，通过网络远程周期性、自动化对目标网站/网站群进行检测。

网页防篡改：由发布服务器程序、同步服务器程序、交互页面远程控制台等部分组成，同时还可以选择配置防篡改模块。发布服务器程序（更新端）负责将合法的网页文件通过安全通信发送到 WEB 服务器；同步服务器程序（监控端）负责接收发布服务器发送来的合法网页变化，并保存其数字水印，监视本机未经许可的文件变化并向服务器请求恢复变化的文件；远程控制台（管理端）提供远程方式对发布服务器的管理及日志内容查看；防篡改模块（IIS Filter）内嵌在 IIS WEB 服务器软件里，对所有的网页文件请求进行合法性检查，并对所有发送的网页进行数字水印比对；内容保护过程对浏览器的网页浏览请求，防篡改模块检查其头部信息，检查请求的文件是否在监视列表中。

邮件安全：邮件安全软件的核心功能是阻止或隔离恶意软件、网络钓鱼攻击和垃圾邮件，很多产品甚至还为出站电子邮件提供数据丢失防护和电子邮件加密功能。

API 安全：API 是一些预先定义的接口（如函数、HTTP 接口），或指软件系统不同组成部分衔接的约定。用来提供应用程序与开发人员基于某软件或硬件得以访问的一组例程，而又无需访问源码，或理解内部工作机制的细节。

随着 Web2.0、社交网络、微博等一系列新型的互联网产品的诞生，基于 Web 环境的互联网应用越来越广泛，企业信息化的过程中各种应用都架设在 Web 平台上，Web 业务的迅速发展也引起黑客们的强烈关注，接踵而至的就是 Web 安全威胁的凸显，黑客利用网站操作系统的漏洞和 Web 服务程序的 SQL 注入漏洞等得到 Web 服

务器的控制权限，轻则篡改网页内容，重则窃取重要内部数据，更为严重的则是在网页中植入恶意代码，使得网站访问者受到侵害。我国 web 应用安全问题一直比较严峻。

同时，随着移动通信技术的飞速发展，移动应用成为了经济活动和民生需求必不可少的工具，全面覆盖到金融、医疗、教育、办公、交通等各个领域，移动应用种类和数量呈爆发式增长，但是随着移动应用数量的增长，各类不合规应用不断出现，非法搜集、存储、传输、处理和使用用户个人信息的问题原来越严重。

国家互联网应急中心发布的《2020 年上半年我国互联网网络安全监测数据分析报告》显示，我国网络受到恶意程序、漏洞风险、DDoS 攻击等方面的风险，其中安全漏洞方面，应用程序漏洞（占 48.5%）、Web 应用漏洞（占 26.5%），远超网络设备、操作系统等方面的漏洞。我国应用安全受到的威胁越来越多，安全形式非常严峻。

2、特点

（1）web 安全事件频发

随着互联网信息化的不断发展，web 应用得到迅速发展，为互联网的发展发挥着非常重要的作用，但是一方面由于 TCP/IP 的设计没有考虑安全问题，使得在网络上传输的数据是没有任何安全防护的，另一方面是我国用户在 web 应用方面的安全意识较低，导致国内 web 应用安全事件频发，且攻击类型多样，黑客攻击、资产被盗、安全漏洞、私钥窃取、钓鱼攻击问题比较严重。

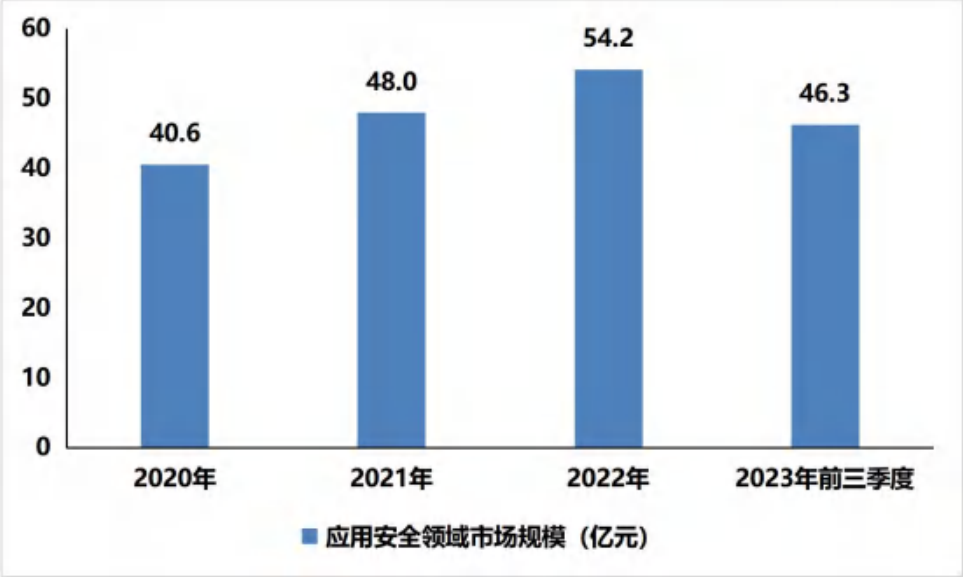
（2）移动应用安全问题迅速增长

近些年，随着智能手机、智能穿戴设备等的迅速普及，大量的移动应用被开发和上线。与传统 PC 相比，移动设备的开放性、多样性以及安全性问题，为欺诈分子提供了更多的攻击方式和手段，使得移动设备更容易受到攻击。此外，许多用户对移动设备安全问题缺乏意识，导致我国移动应用安全问题随着移动应用规模的增长而迅速增长。

3、市场规模

2020-2022 年，随着我国 web 应用和移动设备安全问题越来越严重，国家和企业都在大力宣传推广网络应用安全保护，用户和企事业单位的应用安全意识持续提升，进而推动了中国应用安全产品和服务需求的增长，中国应用安全市场规模呈现持续增长态势。2023 年前三季度，中国应用安全市场规模为 46.3 亿元。

图表 21：2020-2023 年前三季度中国应用安全领域网络安全市场规模统计



数据来源：项目组统计整理

五、安全运营

1、发展现状

安全运营是保障企业的业务系统持续安全运行的过程，并通过运营能力对各类数据实现统一管理、分析，可以对业务系统的安全持续优化。因此，安全运营是将企业的网络安全建设化零为整，统一的进行安全管理。

当前企业网络管理人员基本上都具备了一定的网络安全意识，初步形成了一套网络安全运营机制，对日常网络安全运营工作具有一定的应对能力。

对于像银行、能源等头部企业，在安全建设上的特点是预算充裕、对业务的安全要求极高、普遍拥有规模不小的内部安全团队。在安全建设方面，他们也能够根据自己的业务系统去构建自身的安全防御体系，这类群体不仅自身非常重视安全运营，而且也拥有安全运营的能力。

腰部企业的特点是有一定的安全预算，对安全的关注重点在于合规，这一点同头部企业有着明显的区别，但在内部安全团队建设方面，可能就只有几个专职甚至兼职的人员去做。这决定了这类客户的安全能力普遍较弱，安全团队从人员数量到人员素养都难以进行高效的安全运营。

中小企业是体量最大的群体。在数字化转型的过程中，更多拥抱数字化的其实是中小企业。这类群体的特点是，对业务的重视程度高于其他方面，因此在安全相关方面投入普遍较少，即便有预算也非常紧张，而在安全人员的配置方面几乎没有。因此，这类企业主要是通过购买简单的、标准的安全产品或安全服务来解决安全问题，其自身是很难有能力去做安全运营的。

新技术的大量引入和企业业务模式的变化也导致近年来网络安全事件发生更加

频繁，勒索病毒、蠕虫木马、漏洞攻击、扫描渗透等网络攻击手段层出不穷。单靠被动响应，中小企业无法及时发现风险源头，也无法快速实现业务恢复，企业业务也因此会造成巨大损失。即使部署了大量的安全设备，企业也缺乏全局视角的安全管理和故障响应能力，因此中小企业的网络安全运营面临着严峻的挑战。

近些年，以山石网科、华清信安等为代表的网络安全公司针对国内运营安全的痛点和难点，开发了运营安全相关产品或解决方案，相比于传统的安全建设，其安全运营产品可以让企业安全建设更简单。例如华清信安TDR智能安全运营通过SaaS模式部署，最快可以实现分钟级接入；山石网科XDR安全运营解决方案是以国产化山石智源智能安全运营平台为核心，融合国产化NDR、防火墙、EDR等安全产品的威胁检测和处置能力，可提供统一视图、实时监测、关联分析、全局溯源和自动化响应等功能，帮助组织更好地检测、响应和应对各种网络威胁和安全事件，并保证安全运营的“可靠”。

现阶段，从安全运营中心的运营成本及安全能力考虑，国内安全运营市场也衍生出了托管安全服务的新方式。为了弥补专业安全分析人员短缺，采购第三方安全运营服务已经成为机构提升和完善安全运营能力的有效手段，服务范围包括部署在本地、外部数据中心和云上的托管安全服务，服务模式通常包括驻场服务、远程服务、SaaS类服务等。

如山石网科推出的山石云景——云端安全运营与管理平台，该产品是一款为解决中小企业客户所面临的网络安全运营挑战而开发的、SaaS化的安全运营管理平台，从产品、技术、平台和人员这四个维度，可以在云端为广大中小企业用户提供便捷、高效、高性价比的增值安全运营服务，实现在云端的一站式安全运营管理。

2、特点

（1）安全运营是从整体进行安全建设

安全运营对于企业来说，安全防护的方式发生改变，不只是采购某一个安全产品，更是系统化的从整体对企业安全进行运营管理。不同厂商、不同类型的安全产品存在数据不互通的问题，形成安全“数据孤岛”，导致企业的网络安全往往是点状分散式管理，面对更隐蔽、更复杂的网络威胁往往难以快速发现和响应。安全运营通过统一管理运营，将点链接成面，形成更可靠的安全防护屏障。

（2）安全运营是动态的

运营者需要进行长周期的对企业安全进行系统化的管理，这包括安全产品的升级、应急响应处置流程的优化、安全策略和规则的调整等。根据企业自身业务的变化调整，对企业的安全需求进行动态评估，及时调整安全策略以保障企业网络安全。

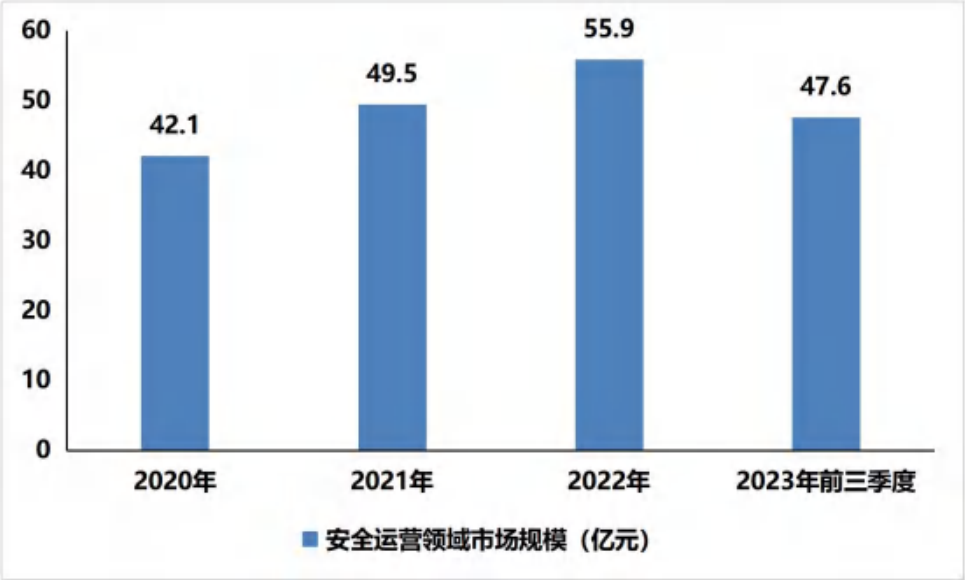
（3）安全运营的实现需要全方位的资源协同

安全运营体现建设不仅仅是一个安全产品，还需要专业人员、产品、云、地、机的有效结合。云作为当下大多数企业网络安全防护的主要场景，云上的威胁检测、主动防御、态势感知、风险预警等能力在结合本地的安全团队实现全方位的协同运营。通过资源的全方位协同运营，覆盖企业的资产安全管理、安全风险评估、威胁检测与管理、安全事件的响应及处置、安全检查和风险防范，形成企业安全闭环管理运营。

3、市场规模

数字化发展带来的网络威胁日益增加，在网络安全法律法规的严格要求下，许多企业安全建设已经发生转变，越来越多的企业主动开始进行安全建设。相对于传统安全防护，安全运营由于可以通过主动防御、纵深防护等措施，提高威胁检测效率，更好的帮助企业提升安全防护能力，被越来越多的企业所选择。2020-2022 年，中国安全运营市场规模持续增长，2023 年上半年，中国安全运营市场规模为 47.6 亿元。

图表 22：2020-2023 年前三季度中国安全运营领域网络安全市场规模统计



数据来源：项目组统计整理

六、工业互联网安全

1、发展现状

工业互联网是第四次工业革命的关键支撑和竞争焦点。近些年，工业互联网已经成为少数发达国家利用网络攻击遏制别国发展、胁迫他国服从的重要手段，给国际正常秩序以及国家的安全稳定、经济发展、居民生活造成了严重威胁和巨大损失。

例如，2018 年美国 4 家天然气输气管道公司的客户通信系统受到网络攻击，造成系统关闭数小时；2019 年，挪威海德鲁公司（NorskHydro）遭遇网络攻击导致生产中断、工厂关闭；2020 年，委内瑞拉国家电网干线遭到攻击，致使全国大规模停电；新型冠状病毒肺炎疫情暴发以后，仅 2020 年上半年发现的针对我国工业互联网的恶意网络攻击行为就高达 1356.3 万次，涉及企业达 2039 家。

因此，我国亟需加快发展工业互联网安全产业，形成有效可靠的安全防护与保障能力，为国家间的合作与竞争提供基础支撑。

2020 年，我国工业信息安全主管部门和行业监管部门密集出台了《关于推动工业互联网加快发展的通知》、《“工业互联网+安全生产”行动计划（2021-2023 年）》等多项与工业互联网安全相关的政策，指导工业互联网安全保障工作的具体实施。

近些年，我国工业互联网安全政策和标准日益完善，垂直行业工业信息安全建设提速，工业企业安全意识全面增强，工业信息安全保障技术水平显著提升，推动了工业互联网安全产业的全面发展。2022 年，我国工业互联网安全市场规模达 94.6 亿元，增长率达 25%。

2、特点

（1）仍然处于快速增长期

2022 年，我国工业互联网安全产业资本、技术、人才加速聚合，企业间不断加快优势资源整合，产学研持续联动。2020-2022 年，中国工业互联网安全市场规模保持高速增长，年均增速达到 30%左右，我国工业互联网安全行业仍均处于快速增长期。

（2）潜在攻击类型多、安全防护工作复杂

工业互联网面临着木马、病毒、入侵攻击、物理攻击、供应链攻击等多种攻击方式的一种或多种，攻击者可能试图入侵、破坏或干扰工业系统和网络。同时工业互联网安全又比较复杂，要确保工业系统和设备的安全，需要综合运用物理安全、网络安全、身份认证、数据加密等多种措施，并进行持续的监测、审计和更新。

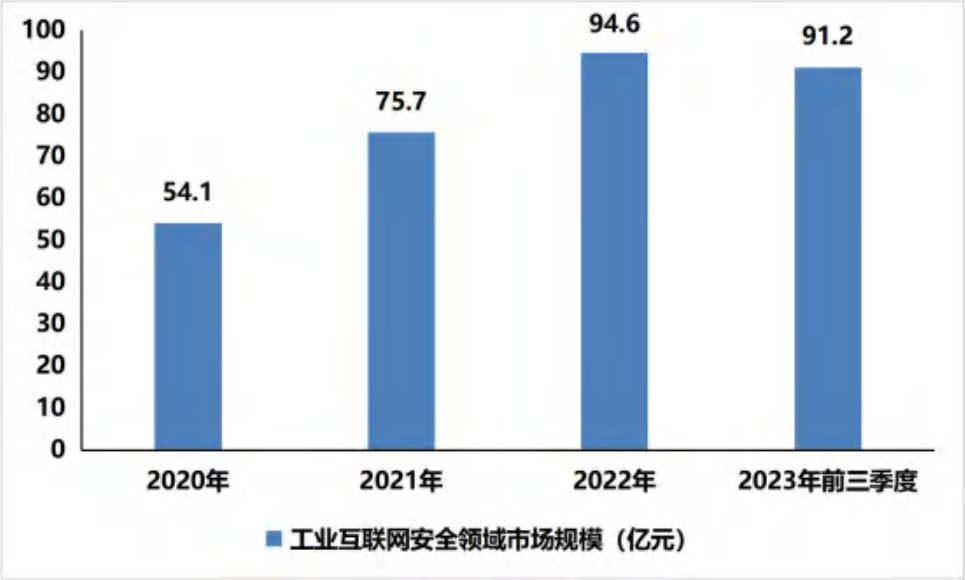
（3）企业多、产品类型多样

目前，国内布局工业互联网安全领域的企业较多，以山石网科、启明星辰、电科网安等为代表的老牌工业信息安全业务企业竞争力相对较强，不同企业在工业互联网安全领域布局业务类型多样，涵盖软件产品、硬件设备产品、安全解决方案及安全服务等。代表产品如山石网科的“Trust -E”工业互联网安全解决方案，该方案包含工业防火墙、工业网闸、工业安全监测审计系统、工业安全主机卫士系统、工业互联网安全态势分析与管理平台等，是一套涵盖工业互联网边缘层、控制层、应用层与平台层的整体解决方案。

3、市场规模

工业互联网安全可以有效降低系统遭受攻击和损害的风险，确保工业生产的稳定和可靠运行。2020-2022年，在建设制造强国、网络强国、数字中国的战略需求下，我国在工业互联网安全方面的重视程度和投入力度持续提升，同时由于技术和威胁的不断演进，企业在工业互联网安全方面持续投入，以保护工业系统和国家的安全，进而推动了中国工业互联网安全市场规模的持续快速增长。2023年前三季度，中国工业互联网安全市场规模为91.2亿元。

图表 23：2020-2023 年前三季度中国工业互联网安全领域网络安全市场规模统计



数据来源：项目组统计整理

七、信息技术应用创新

1、发展现状

信息技术应用创新即“信创”，其核心是通过国产和自主创新实现信息技术产业的“自主可控、安全可信、高效可用”。

我国政府自 2017 年以来已经连续四年将“数字经济”写入政府工作报告，并在十四五规划纲要中提出“以数字化转型整体驱动生产方式、生活方式和治理方式变革”，数字化转型从企业（组织）层面上升为国家战略。近些年，从数字政务、数字政府到数字中国，从国家党政机关到国防军工，再到各大央国企，都在与时俱进的进行数字化转型升级，数字化转型中的数据安全是重中之重，涉及到国家的安全及军事机密。

但是我国很多技术因为一些原因越来越受制于人，尤其是上游核心技术，不断

被西方国家“卡脖子”。同时，中国大部分的软件应用都是使用西方国家的产品，国家及企业所有的数据隐私都掌握在西方国家厂商的后台手中，这对于中国的数据安全极为不利。为了解决西方国家在科学技术“卡脖子”的问题，以及国家数据安全的问题，信息技术应用创新产业应运而生。

近些年，国家陆续出台一系列政策支持信息技术应用创新产业发展，如《“十四五”数字经济发展规划》、《“十四五”国家信息化规划》等。与此同时，部分省份也要求“十四五”期间打造信创产品、发展信创产业，并对信创企业予以奖励和补贴，积极推动国产信创产品大范围使用。信创已成为国家战略的重要组成部分。

自主可控是我们国家信创的核心和信息化建设的关键环节，是保护信息安全的重要目标之一，在信息安全方面意义重大。我国本土网络安全企业持续加大研发投入，不断推出自主可控的信创领域网络安全产品。如山石网科基于多年的硬件自主设计、软件自主研发经验，依托丰富的安全产品线，推出了国产化安全运营平台和多个国产化安全组件，通过“X”种自主可控的安全解决方案，构建全新XDR架构下的安全运营，以实现“可靠”安全运营；推出基于国产芯片的国产化防火墙产品K1280和K6580，覆盖2Gbps-100Gbps应用场景，并发布了多款基于国产关键元器件的入侵检测和防御系统等边界安全产品，持续丰富边界安全产品信创布局。

图表 24：山石网科国产化 XDR 安全运营架构

资料来源：项目组统计整理

目前，我国信创从党政领域试点应用，逐渐向国计民生行业加速渗透，中石化、中交集团、中国稀土、中储粮等央国企及行业信创大单频现，信创产品及解决方案持续落地，信创产业产品采购步入常态化阶段。

2、特点

（1）信创领域安全漏洞和病毒问题更加严峻。

由于信创大量基于开源框架复用，面临着软件供应链、信创漏洞研究缺失等问题。和传统终端环境一样，信创终端同样存在着木马、病毒、恶意软件肆虐，勒索、挖矿病毒横行等情况。国外成熟操作系统、数据库或中间件可在大量黑客或用户的攻击使用下，能够获得更充分的测试，而国内由于目前使用场景、用户量较少等原因，导致测试不充分，潜在的安全漏洞问题更严峻。

（2）信创安全普遍还是外挂式安全，并没有与数字化深度融合

目前，信创安全普遍与信创重构相脱节，更偏重于生态、适配和业务迁移，缺少了与数字化的深入融合。外挂式安全类似防火墙，主要作用为外部物理防御，没有从内生性内部环节流程上保障安全-没有前期规划部署，需要后期根据需求去适配。真正的安全一定是从客户业务中自己生长出来的，在5G环境下是必然的趋势，很多场景下产品不再适合做外挂安全。

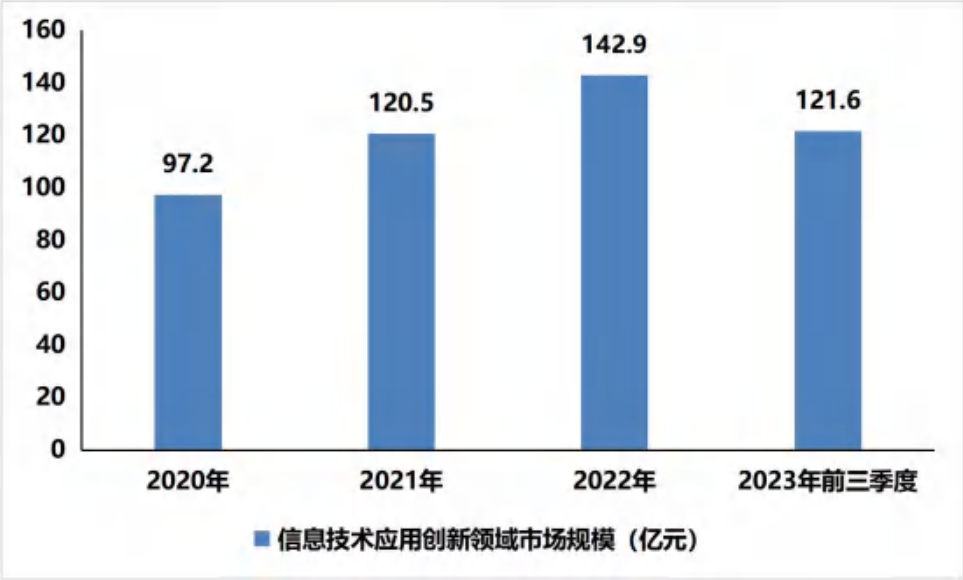
（3）信创安全缺乏全局和前瞻视角

具体表现在“重替代、轻安全规划”，“重功能、轻安全融合”，“重单品、轻体系建设”等，面对网络攻击依然停留在事后补救的“补丁式防护”，缺少围绕体系化建设的咨询、规划、评估。信创环境下整套安全体系需要重建，而不仅仅是局限在安全漏洞和病毒的问题。目前网络安全的状态是在原有防护原来的基础上做修补，而不是真正的把安全产品围绕云计算或者数字化转型进行安全产品的深度融合。

3、市场规模

近些年，国家非常重视我国信息技术的自主可控，鼓励和支持企业持续推进信息技术应用创新，2020-2022年，随着我国党政以及重点行业不断加强信息技术应用创新方面的投入，中国信息技术应用创新领域网络安全市场规模持续增长，2023年前三季度，中国信息技术应用创新领域网络安全市场规模为121.6亿元。

图表 25：2020-2023 年前三季度中国信息技术应用创新领域网络安全市场规模统计



数据来源：项目组统计整理

第四章 网络安全创新实践案例

第一节 西安国际医学中心医院

一、医院简介及网络安全核心痛点和诉求

西安国际医学中心医院是一所集医疗、科研、教学、预防、保健、康复、健康管理为一体，通过国际 JCI 认证，按照三级甲等医院标准建设的综合医院，是西北大学、陕西中医药大学附属医院、温州医科大学教学医院，是全球著名医疗机构-美国妙佑医疗国际（Mayo Clinic）联盟成员医院。

西安国际医学中心医院日均诊疗服务人数多，截至 2023 年 9 月 25 日，西安国际医学中心医院 4 年累计服务门急诊患者 235 万人次。这使得西安国际医学中心医院接入终端数量大，系统访问需求较多。

然而，2022 年之前，西安国际医学中心医院并无有效手段进行敏感数据的脱敏及数据的分类分级治理，互联网出口侧也无流量清洗设备，防护手段较为单一，因此无法分析主机是否可信、是否存在潜在风险、对网络风险进行预警、对网络漏洞及异常行为进行处理，更无法对数据进行分级治理。

图表 26：西安国际医学中心医院网络安全核心痛点及诉求

序号	网络安全核心痛点
1	院区接入终端数量大，访问系统次数较多，无法分析主机是否可信或者是否存在潜在风险
2	院区的安全建设仅在区域网关防护层面，缺乏对院区整网资产的风险感知、威胁感知、漏洞感知及全院联动处置的安全运营能力
3	互联网出口侧无流量清洗设备，防护手段较为单一
4	无有效手段进行敏感数据的脱敏及数据分类分级治理，数据安全防护体系尚不完善

资料来源：项目组统计整理

二、网络安全软硬件设施布局及成效

1、构建全院网络安全态势感知及安全运营体系

2022 年以来，西安国际医学中心医院通过上线山石网科态势感知安全运营系统、漏洞扫描系统，并利用其进行全流量威胁分析与漏洞分析，实现提前预警、网络风险前置的目的。

医院借助漏洞扫描系统定期执行漏洞扫描任务的同时，还将漏洞弱点情况与态势感知平台资产进行关联，为态势感知分析提供多样的数据来源与风险依据，从而更加精准的呈现资产风险状况。

此外，西安国际医学中心医院上线的态势感知安全运营系统还能够与边界防火墙、数据中心防火墙等异构品牌设备进行自动化剧本联动，下发阻断安全策略，由防火墙进行攻击拦截、行为拦截，最终形成从资产梳理、异常行为分析、高级威胁分析、漏洞弱点分析到云端情报感知、全院自动化联动阻断的安全运营体系。

2、构筑数据安全治理体系，形成数据安全治理模型

西安国际医学中心医院通过上线数据分类分级治理平台、数据脱敏系统，对数据信息进行安全等级分化，防止数据中的敏感信息泄露，初步构建了数据安全治理体系，形成数据安全治理模型。之后，西安国际医学中心医院计划扩展数据安全治理模型中的安全组件，以医院实际情况完善优化模型并逐步提升数据安全防护能力。

图表 27：西安国际医学中心医院网络安全创新实践成果

资料来源：项目组统计整理

第二节 华中科技大学同济医学院附属协和医院

一、医院简介及网络安全核心痛点和诉求

华中科技大学同济医学院附属协和医院是扎根武汉历史最悠久的集医疗、教学、科研于一体的国家卫生健康委员会直属大型综合性医院。医院获批质子诊疗系统配置许可，抢占癌症放疗制高点；配置 PET-MR、PET-CT、达芬奇机器人、射波刀等高端医疗设备，率先将混合现实信息技术、人工生物角膜等应用于临床手术实践。此外，医院拥有教育部重点实验室 1 个、卫生部重点实验室 1 个、省级重点实验室 3 个；连续 7 年中标国家自然科学基金数 100 余项，居国内医疗机构前三；获国家科技进步二等奖 6 项。近年来，医院加快国际化进程，与德、英、美、日等 20 多个国家和地区建立了广泛的交流协作关系。

在信息化方面，华中科技大学同济医学院附属协和医院围绕“医疗管理”“临床服务”“运营管理”“行政后勤”“基础保障”建设了 5 大体系 128 个子系统。在医院数字化运营管理领域，华中科技大学同济医学院附属协和医院以智慧管理分级评估标准体系为核心、金银湖院区为试点，完成智慧后勤、智慧安防、智慧医工、智慧病房、智慧门诊、指挥调度中心六位一体的智慧医院架构设计，基于数字孪生技术整合医院现有信息系统数据资源，实现医院运营管理决策支出。

随着数据安全的重要性不断提高，协和医院对医疗健康数据的安全持续投入，针对医疗健康大数据的共享与使用、医疗健康大数据的安全管理体系、落实数据安全法分类分级管理制度三个方向提出了具体要求。但如何针对三大方向进行实际的落地，需要专业的数据安全治理，咨询服务团队的支持。

二、网络安全软硬件设施布局及成效

华中科技大学同济医学院附属协和医院前期的信息安全建设工作，主要集中在网络安全的建设和升级，重点内容有边界、内外网以及外联等区域的安全防护，针对应用系统的安全防护以及移动办公、远程运维的防护等，并未专门面向数据资产上线全生命周期监控及防护工具。

为提高数据安全治理水平，协和医院采购了山石网科数据安全综合治理平台以及数据库审计与防护系统、应用（API）系统安全审计平台产品，搭配数据安全分类分级服务、数据安全风险评估服务，从而实现数据安全集中化管理、数据监测可视化、数据运作高效化、数据分类分级，成功构建医疗数据管理体系和动态化细粒度的医疗数据生命周期监控与追溯机制，解决医疗数据汇聚与共享安全威胁，促进医疗数据价值安全释放。

第三节 陕西榆林能源集团有限公司

一、企业简介及网络安全核心痛点和诉求

陕西榆林能源集团有限公司是 2012 年 7 月组建成立的市属国有独资企业，自成立以来，通过资产整合、收购兼并、投资新建等多种途径，形成煤炭产运销、综合能源、精细化工、战略型新兴产业，以及金融和环保“4+2”产业发展模式。

目前，榆能集团煤炭核定产能 3000 万吨，中转发运能力 6000 万吨，火电装机 4390MW、在建 700MW，光伏发电装机 100MW、在建 300MW，化工产品产能 170 万吨、在建 40 万吨，有计算机生产线 1 条、新能源汽车生产基地 1 处；位列中国能源企业 500 强第 120 位、中国煤炭企业 50 强第 26 位、陕西百强企业第 17 位。

陕西榆林能源集团有限公司分支单位较多，网络安全运营管理难度大，再加上集团内部缺乏专业网络技术人才，其亟需优化调整网络安全设施，以解决网络安全运维难度大、成本高、无法及时对故障进行定位、运维效率低等问题。

图表 28：陕西榆林能源集团有限公司网络安全痛点及需求

序号	网络安全核心痛点
1	缺乏专业网络技术人才，网络安全运维难度大
2	无法灵活使用网络资源，及时高效对故障进行定位
3	网络运维成本高、效率低

资料来源：项目组统计整理

二、网络安全设施布局及成效

1、上线网络安全智能安全运营系统平台

为提高网络安全运维效率、降低运维成本，榆能集团上线山石网科开发的网络安全智能安全运营系统平台。该平台主要由智能安全运营系统平台、探针、全网安全设备组成，可部署在网络任意位置，用于接收全网流量和日志信息。其中，威胁探针旁路部署在用户内网中镜像分析流量，安全设备部署在相应位置，可发送日志至智能安全运营系统平台，对现网安全设备可以进行日志采集以及 IP、端口五元组策略下发，阻断威胁行为。

同时，该智能安全运营系统平台可直接联动现网已有山石网科内网防火墙及安全防护模块，实现自动化的智能联动处置、自动化响应及编排，有效减少运维人员的安全设备配置工作量。

图表 29：陕西榆林能源集团有限公司网络安全智能安全运营系统平台

资料来源：项目组统计整理

2、实现智能运维、组网设备集中管控

榆能集团将网络安全智能安全运营系统平台作为网络安全管理中枢，进行自动资产管理、安全事件梳理、分析溯源、处置响应等操作，并定期总结集团安全运营情况，为集团信息化管理提供抓手，同时为集团网络进行协同调度提供依据。

榆能集团通过一套可视化网络调度控制器（部署于集团总部），将所有组网网关设备与之互联，对设备进行统一管理和控制，从而实现广域网的控制平面和转发平面分离。集团内部所有的设备配置、隧道建立、状态监控等操作都可以通过控制器完成而无需登录每台设备进行操作，从而实现灵活便捷地使用网络资源，高效组建、运营和运维整个集团网络的目的。

此外，通过使用网络调度控制器，榆能集团网络线路成本降低 70%以上，专线链路性能提升 50%以上；开通分支与总部的连接仅需分钟级别，支撑业务快速发展；实现可视化运维，使管理员对链路状态一目了然，高效实现故障定位。

图表 30：陕西榆林能源集团有限公司网络安全创新实践成果

资料来源：项目组统计整理

第四节 江铃汽车集团有限公司

一、企业简介及网络安全核心痛点和诉求

江铃汽车集团有限公司创立于 1947 年，是一家集汽车研发、制造和销售于一体的集团公司，有整车、零部件、服务金融三大业务板块，主要产品有轻客、轻卡、皮卡、SUV、新能源轿车、客车和各种类型的改装车，具备完善的零部件产业链，位列中国企业 500 强第 249 位、中国制造业企业 500 强第 123 位、中国战略性新兴产业领军企业第 94 位。

江铃集团本部作为省、市重点工业企业网络安全受检查单位，同时也承担集团成员企业网络安全监管职责，但缺乏有效网络安全威胁感知和防护手段，网络安全工作均是事后处置，且集团子公司安全问题经常反复出现、问题无法快速溯源和高效解决，存在网络漏洞脆弱性难加固、内外部威胁不可控、被动响应等痛点，需要强化主动防御能力，以确保网络安全事件及时响应、核心数据安全可靠、关键业务稳定运行。

图表 31：江铃汽车集团有限公司网络安全痛点及需求

序号	网络安全核心痛点
1	缺乏网络安全威胁感知和防护手段，网络安全工作均是事后处置，没有事前修复
2	各类安全设备没有统一平台，使用效率低，无法快速溯源发现关键问题节点
3	通报给子公司的安全问题反复出现，问题无法快速、有效的进行闭环
4	系统补丁、弱密码等问题修复缓慢，并且难以监控
5	测试环境、开发环境、老旧系统导致的网络安全问题时有发生

资料来源：项目组统计整理

二、网络安全软硬件设施布局及成效

江铃汽车集团有限公司基于集团内部专线骨干网，以集团核心机房为中心，搭建山石网科态势感知平台，增加 WEB 应用防火墙及漏扫设备，并在各相关子公司重点网络区域放置探针，配以远端全天候值守服务团队协助，实时监测安全威胁，研判、预警、协助处置安全事件，从而降低资产漏洞脆弱性风险，减少被黑客利用的机会；持续保持事件响应机制，有效精准抵御高级威胁，强化主动防御能力，提升网络安全水平。

第五节 山东港口科技集团有限公司

一、企业简介及网络安全核心痛点和诉求

山东港口科技集团有限公司（简称“山港科技”）是山东省港口集团有限公司直属一级集团，注册资本 2 亿元，于 2020 年 3 月 18 日山港科技正式注册成立，是山东港口倾力打造的智慧绿色港口建设综合服务商，拥有省级研发中心 2 个，市级研发中心 2 个，具有双软认证以及 CMMI 3、ITSS 3、DCMM 2 等资质。

山港科技融合青岛港、日照港、烟台港、渤海湾港深耕港航信息化业务 40 余年积累的经验和技术底蕴，依托山东港口一体化改革以来形成的平台优势及丰富的业务场景资源，聚焦港航软件服务、智慧绿色港口业务咨询、数字化平台服务、码头智能化、港口新基建五个业务方向，秉承“用户至上、服务生态、奋斗为本、开拓创新”发展理念，致力于成为一流的智慧绿色港口建设综合服务商。

在网络安全方面，山港科技母集团在网络基础安全层、协同响应层、安全运营层均存在安全问题，主要体现在：山港科技母集团各港口、版块集团之间安全建设标准不统一，加之集团与各个港口、版块集团之前的网络处于互联互通状态，权限控制颗粒度较粗，容易出现横向攻击，安全风险面增大，无法做到有效的区域逻辑隔离；现有防火墙、IPS、WAF 等防护类设备无法自动联动，不能高效率处理网络安全事件，难以发现隐蔽安全事件等；安全防护设备集中管控能力较弱，数据孤岛严重，威胁检测、攻击溯源能力不强等。对此，山港科技亟需开展港区骨干网边界安全建设、私有云横向微隔离、应用安全防护、攻防演练等措施，以提高自身及母集团的网络安全水平。

图表 32：山东港口科技集团有限公司网络安全痛点及需求

序号	网络安全核心痛点
1	山港科技母集团与各个港口、版块集团网络基础安全层权限控制颗粒度较粗，导致容易出现横向攻击、安全风险面增大，无法做到有效的区域逻辑隔离
2	现有防火墙、IPS、WAF 等防护类设备无法形成自动联动机制，网络安全技术之间的整合度低、联动性不强，无法高效应对、处理网络安全事件
3	安全操作主要依赖手动创建和维护，发现隐蔽的安全事件困难，造成在遭遇到突发攻击后需要封禁处置周期过长，无法做到安全事件发生时及时做到全面的协同响应
4	安全防护设备集中管控能力较弱，无法做到及时有效的威胁监测以及安全事件的追踪溯源
5	未形成纳管全域安全数据资产，使数据充分应用于安全风险决策、安全运营管理，存在安全数据孤岛，对于复杂多源异构网络安全数据做不到统一数据标准，也未能对各类安全设备、系统数据进行处理、治理、存储、分析等操作，资产发现、漏洞扫描、访问控制、威胁检测、攻击溯源能力较弱

资料来源：项目组统计整理

二、网络安全软硬件设施布局及成效

1、完成骨干网边界隔离，解决横向业务交互障碍

2022 年之前，山港科技及其母集团尚未根据业务调整统筹规划网络安全设施建设，资产发现、漏洞扫描、访问控制、威胁检测、攻击溯源能力较弱。对此，山港科技通过构建“一张网”，在集团侧完成骨干网边界隔离，利用 SRV6 通道实现各港口板块网络互联，并借助山石网科分布式高端数据中心防火墙实现全集团横向互联业务安全隔离以及业务分层访问控制，大大降低横向暴露面，有效防止集团内部横向威胁扩散。

山港科技母集团与各个港口、版块集团合并后，核心数据中心业务 IP 段存在重合，导致骨干网互通后无法直接进行互访，为此，山港科技通过山石网科应用交付平台，实现横向业务代理发布，各自隐藏数据中心冲突 IP 地址，促进各港口板块业

务融合发展，解决横向业务交互障碍。

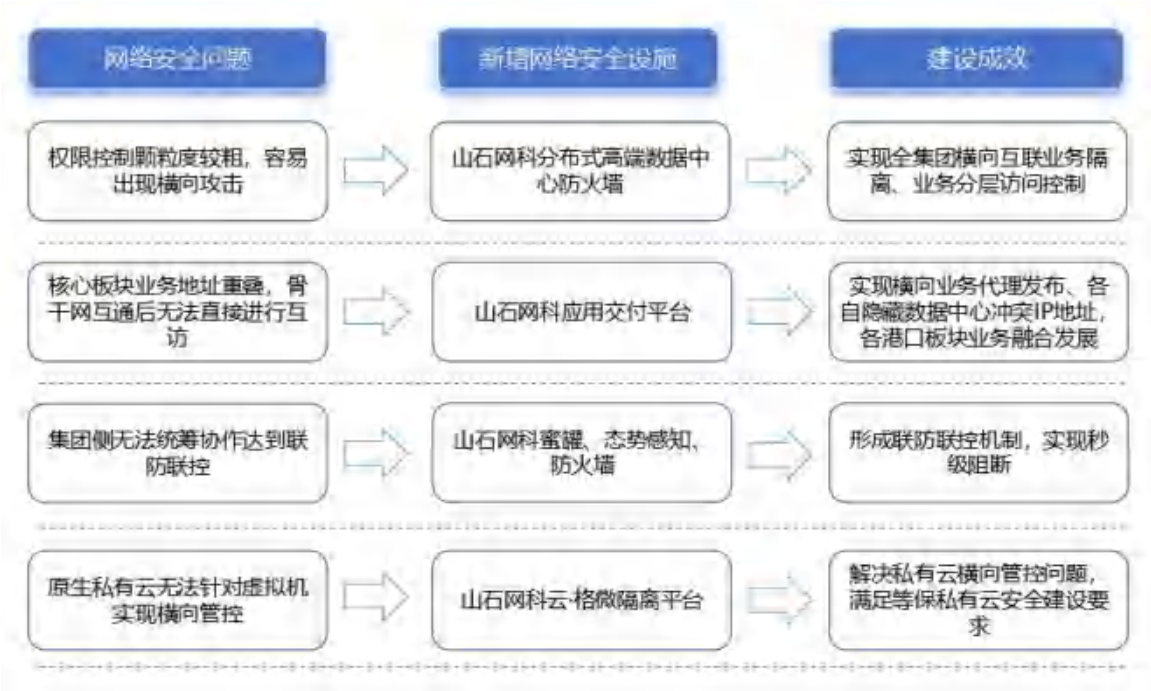
2、构建主动安全防护体系，强化自动化防护能力

由于山港科技母集团与各个港口、版块集团各自具有互联网出口，各自构建安全防御体系，无法统筹协作达到联防联控。为提高山港科技及其母集团安全防护级别、强化自动化防护能力，山港科技利用山石网科的蜜罐、态势感知、防火墙形成联防联控机制，对内外发布多个蜜罐业务，诱导攻击者，获取攻击者信息，数据上报至态势感知后，通过自动化编排下发防火墙黑名单，实现秒级阻断。

3、建设私有云微隔离能力，实现横向可视化管控

山港科技母集团核心业务均由私有云承载，原生私有云无法针对虚拟机实现横向管控，若有一台服务器失陷将会影响整个私有云。利用山石网科云·格微隔离平台，针对私有云内所有虚拟机进行横向访问控制，形成可视化链条，从而针对虚拟机之间实现入侵防御、病毒过滤等安全防护，解决私有云横向管控问题，满足等保私有云安全建设要求。

图表 33：山东港口科技集团有限公司网络安全创新实践成果



资料来源：项目组统计整理

第五章 中国网络安全市场趋势预测

第一节 中国网络安全市场发展方向与热点分析

一、传统网络安全技术进一步升级演进

由于网络安全防护内容越来越复杂、网络安全环境动态变化，以防火墙、密码算法、入侵检测及防御技术、漏洞扫描和修复技术等代表的传统网络安全技术无法适应网络威胁日益频繁、网络环境瞬息万变带来的安全防护需求。这促使网络安全企业持续迭代更新防火墙技术、入侵检测及防御技术、漏洞扫描和修复技术等，如山石网科通过构建山石云数据库，自研僵尸网络防御 AI 引擎，融合“自研安全系统“、全并行分布式架构设计”、 ‘’ 高性能安全加速芯片 ‘’ 、“流量分析和检测技术”等方式推动防火墙产品升级。

二、前沿安全技术不断与传统技术融合发展

目前，网络安全行业前沿安全技术与传统网络安全技术融合发展已成为重要趋势，如融入 AI 技术的防火墙、入侵防御、僵木蠕监测、态势感知、数据防泄漏、智能内网威胁分析产品等；基于大数据模型、人工智能的恶意样本检测与分析、攻击行为发现与溯源、安全情报推理与生成、自动化漏洞挖掘与评估、智能化安全服务与运营等。整体上看，传统网络安全技术与前沿安全技术的融合发展可实现网络安全防护效果的放大、叠加、倍增。

三、数据安全成为网络安全重要组成部分

伴随数字经济发展，全球数据安全事件频发，催生了数据安全市场需求。为保

障数据安全，我国陆续颁布《网络安全法》、《十四五规划纲要》、《数据安全法》、《个人信息保护法》等政策法规，加强对数据安全的监管，各关键行业用户也提升了对数据安全的重视程度。

其中，2022年12月国务院发布的《关于构建更加完善的要素市场化配置体制机制的意见》将数据纳入生产要素的范围，并强调把安全贯穿数据治理的全过程；2023年1月工信部等十六部门联合发布的《关于促进数据安全产业发展的指导意见》，提出到2025年，数据安全产业规模超过1500亿元，年复合增长率超过30%；到2035年，数据安全产业进入繁荣成熟期。

由此来看，数据已经成为重要的生产要素，而数据安全作为保障数据要素价值的前提，未来在数字化转型加速、数据的流存节点和区域变得繁杂、数据流动量呈指数级增长、数据使用方式日益多样化、数据要素市场建设加速推进的背景下，将成为网络安全的重要组成部分，并迎来快速增长。

四、关键信息基础设施网络安全保护备受重视

近年来，世界不稳定、不确定因素日益增多、国际格局复杂多变，针对关键信息基础设施的高级可持续威胁、数据窃取等事件频发，国家网络安全形势复杂严峻，加之我国关键信息基础设施存在网络安全态势感知、监测预警、追踪溯源能力不足等风险隐患，难以有效应对国家级、有组织的高强度网络攻击。

因此，国家出台多项政策推动各行业、各领域提升关键信息基础设施安全保护水平的同时，还发布关键信息基础设施安全标准，不断强化关键信息基础设施安全防护，健全完善网络安全管理制度，并要求组织开展演习演练、安全检测和风险评

估，及时发现深层次问题隐患和威胁。

五、零信任架构演进进入落地推广阶段

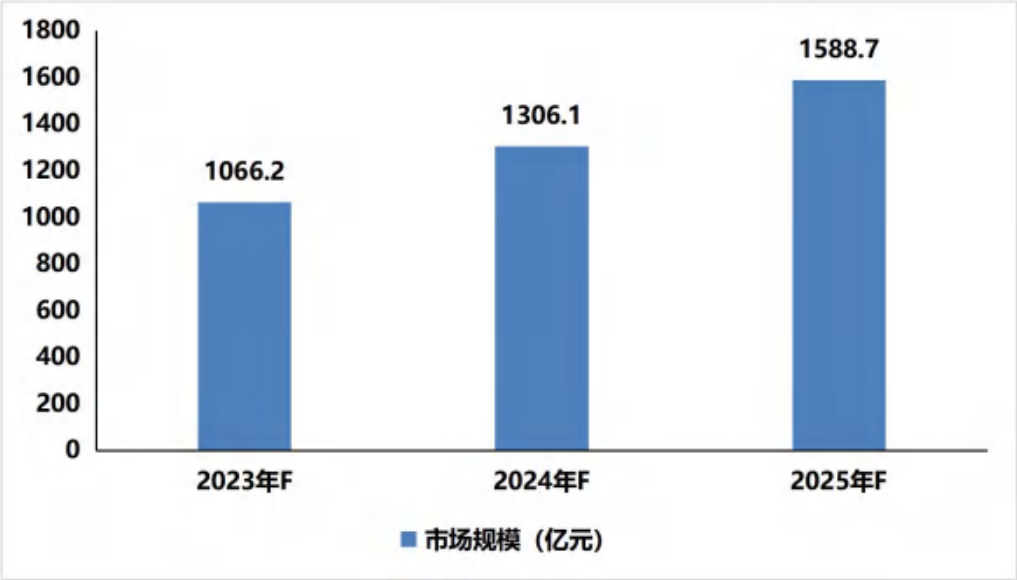
目前，网络安全行业面临的最大挑战是私有应用程序的访问端口十分分散，以及内部用户的权限过多，要求用户“从零开始构建信任安全体系”，基于权限最小化原则进行设计，根据访问的风险等级进行动态身份认证和授权。

在网络环境不断变化的客观形势下，国内网络安全企业纷纷开始布局零信任相关产品，如山石云·格，以及其他网络安全企业开发的零信任安全管控平台、零信任 VPN、零信任安全解决方案、基于“零信任+”的流量威胁管控平台等。与此同时，在需求端，我国中央部委、国家机关、大中型企业已开始探索实践零信任安全架构。

第二节 中国网络安全市场规模预测

预计 2023-2025 年，伴随着国家网络安全产业发展政策环境持续优化，国家安全体系和能力建设进一步完善；产业数字化转型加速推进，数字经济快速发展，信息技术与社会各领域融合日益深入；云计算、物联网、大数据、5G 等新兴技术不断发展，网络边界逐渐模糊，安全防护内容愈加复杂，中国网络安全市场规模将逐年扩大。其中，预计 2023 年，中国网络安全市场规模为 1066.2 亿元；预计 2025 年，中国网络安全市场规模为 1588.7 亿元。

图表 34：2023-2025 年中国网络安全市场规模预测



资料来源：项目组统计整理

第三节 中国网络安全市场需求趋势预测

一、关键行业信创持续推进，网络安全产品需求增加

随着国际形势的复杂演变，安全可信、自主可控成为国内政府、金融、能源等民生与关键信息基础设施领域信息技术发展的重要指导方针，推动信创从党政领域转向金融、电信、电力、石油、医疗、教育等行业领域，并使得政府、电信、金融等领域对网络安全产品和一体化解决方案需求越发明显。预计 2023-2025 年，与信创强相关的终端安全产品、网络安全产品以及信创中催生出的网络安全产品都将受益于信创行业发展爆发新一轮采购需求。

二、产品向数据安全、安全管理、安全服务类延伸

目前国内信息安全市场上的主流安全产品仍是以硬件形态呈现的网络边界层安全产品，包括防火墙、统一威胁管理平台（UTM）、入侵检测和入侵防御（IDP）、

虚拟专用网络（VPN）、安全内容管理（SCM）等。

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

三、网络安全市场需求持续向服务化转型

现阶段，网络威胁不仅日益频繁，而且越来越复杂，且灾难性攻击表明网络风险是重大威胁，促使企业开始把安全视为一项重要的商业风险，并越来越看重网络信息安全服务的持续性，加之虚拟化及云服务理念的不断渗透，我国网络安全行业产品交付形式正从“以硬件交付安全产品、人工交付安全服务”向“以云化、SaaS 化方式交付技术和服务”的模式转变。

四、网络安全需求市场仍将以华北、华东、华南为主

相较于其他地区，华北、华东和华南经济发达，在网络安全方面投入力度较大，区域内以广东、浙江、北京、江苏、山东、安徽、福建等为代表的省份网络安全项目数量较多，是国内最主要的网络安全产品及服务需求区域。2022 年，上述三大区域网络安全需求规模占比合计达到 70%左右。预计未来，受各地区经济发展水平、数字经济及信创行业发展规模等影响，华北、华东、华南地区仍将是国内最主要的网络安全需求市场。除上述地区外，川渝地区网络安全需求增长快速，有望成为国内网络安全需求市场新增长点。

五、政府部门是最大的网络安全产品用户

政府部门的信息系统涉及国计民生和国家安全，如果信息泄露或被篡改，将造成严重的后果，影响公众信任，甚至可能引发社会不稳定。因此，政府部门对网络安全产品需求量最为强烈，是国内最大的网络安全产品用户。预计未来几年，在党政信创持续发展背景下，政府部门仍将是网络安全行业最主要的用户之一。除政府外，教育、医疗、能源等与国计民生紧密相关的行业也将是网络安全主要应用领域。

第四节 中国网络安全市场竞争趋势预测

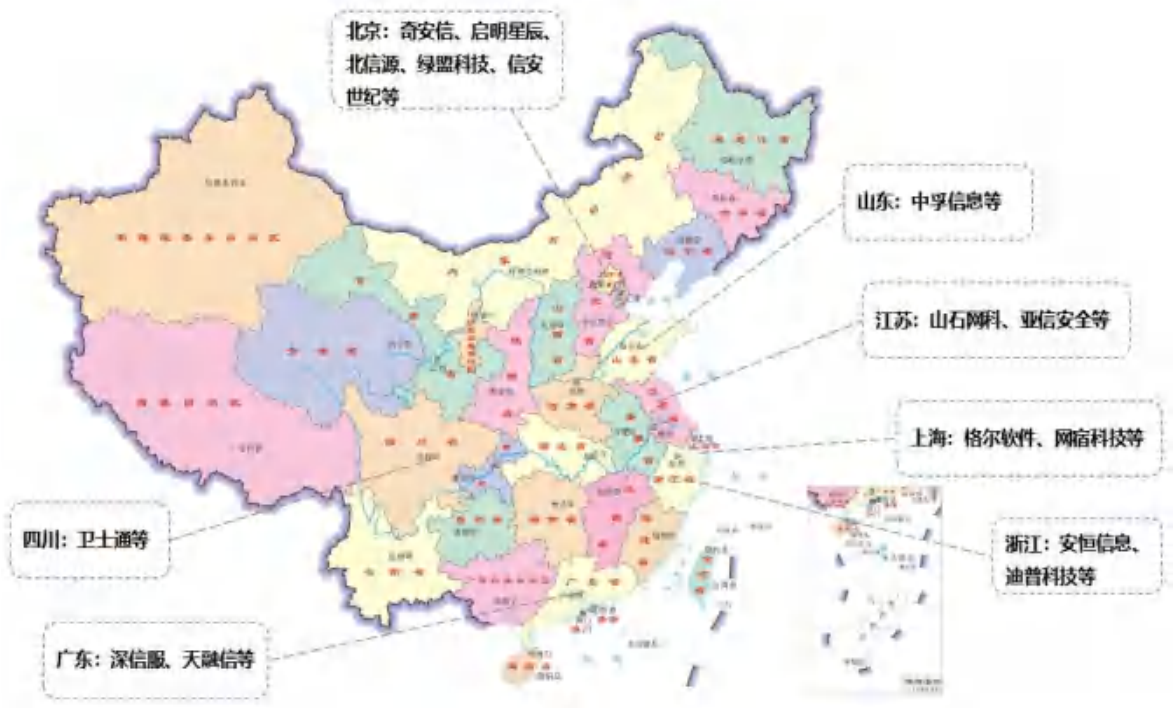
一、网络安全行业集中度不高

网络安全涉及范围广，市场容量大，行业内企业数量多，截至2023年前三季度，我国网络安全行业企业数量增至0.44万家，行业集中度不高。在激烈的市场竞争中，国内网络安全领军企业通过技术、产品、品牌等优势构筑起更高的进入门槛，推动网络安全市场集中度不断提高。预计2023-2025年，我国网络安全行业领先企业凭借强大的技术研发创新能力、资金实力、品牌影响力在国内市场的占有率仍将保持小幅增长趋势，国内网络安全市场集中度也将进一步提高。

二、网络安全企业分布区域集聚特征将更为明显

网络安全行业客户分布呈现聚集效应，主要位于京津冀、长三角和珠三角地区，叠加京津冀、长三角和珠三角地区网络安全配套产业较为完善，创新资源较为丰富，现阶段，中国网络安全行业主要聚集在北京、广东、上海、江苏、浙江等省市，如山石网科、奇安信、启明星辰、格尔软件、深信服、天融信、亚信安全、安恒信息等。预计未来几年，中国网络安全行业企业仍主要聚集在京津冀、长三角和珠三角地区。

图表 35：中国网络安全行业企业分布图



资料来源：项目组统计整理

第五节 中国网络安全市场前景分析

一、国家持续加强网络安全顶层设计

近年来，我国持续加强网络安全顶层设计，出台《数据安全法》、《密码法》、《个人信息保护法》、《网络安全法》，构成信息安全产业的顶层政策体系，使得企业在安全投入方面有法可依。

与此同时，2021 年 8 月发布的《关键信息基础设施安全保护条例》明确了关基领域网安建设的重要性，强化了关基领域大型企业相关领导的责任意识，为网络安全产业的需求拉动带来了实质上的提振。

2022 年 1 月发布的《“十四五”数字经济发展规划》，要求增强网络安全防护

能力、提升数据安全保障水平、切实有效防范各类风险；提升网络安全应急处置能力，加强关键信息基础设施网络安全防护能力，推动数据安全、关键行业信息基础设施防护市场需求持续增长。

整体上看，中国国家对网络安全的重视度不断提升，网络安全行业政策环境持续优化，为网络安全行业发展提供了充足保障。

二、网络安全下游细分市场需求增长空间大

一方面，下游行业网络安全的实施细则陆续出台，如《关于进一步加强新能源汽车企业安全体系建设的指导意见》、《金融数据安全评估规范》、《车联网网络安全和数据安全标准体系建设指南》等，将驱动下游各细分市场合规类网络安全产品需求进一步增长。

另一方面，伴随着数字化转型逐渐深入和信息技术快速发展，传统安全建设已无法满足企业数字化建设要求，主要是因为在数字化转型背景下，数据价值在不同业务场景中得到挖掘利用，并且信息技术深入到业务运营中。因此要求企业将网络安全工作覆盖、匹配复杂的业务应用场景，并针对不同的业务特点制定相应的安全策略以及及时响应各种复杂环境下出现的各种安全事件。这将促使教育、医疗、能源、电信、金融等行业企业加大网络安全建设投入力度，为网络安全行业带来新的需求。

三、网络威胁增加且日趋复杂化，带来新的安全需求

截至2022年，CNNVD合计发布漏洞信息199465条，其中2022年新增漏洞信息24801条。从漏洞危害情况来看，2022年新增漏洞中，超危漏洞4200个，高危

漏洞 9968 个，中危漏洞 10146 个，低危漏洞 487 个。整体上看，我国网络新增漏洞保持连年增长态势，且超高危级漏洞占比呈持续上升趋势，面临的漏洞威胁形势依然严峻。

除网络漏洞外，重要数据被窃取泄露也是我国网络安全治理中的急难险重问题，尤其是公民隐私数据、“新基建”数据的窃密。此外，网络攻击无孔不入，境外国家级黑客组织的猖獗活动将愈发增多、愈演愈烈，我国网络安全处于并将长期处于前所未有的战略承压期和高危风险期，这一特征在相当长一段时间内不会改变。

重要行业、重点机构、“新基建”领域频频遭受境外网络攻击，数据安全事件高发频发，将带来新的网络安全产品和服务需求。

第六章 推动我国网络安全产业发展的措施建议

第一节 面向政府机构的建议

一、开展关键信息基础设施重点防护和加固

我国早在2016年便开启全国范围内的关键信息基础设施网络安全检查工作，并建立健全国家网络安全应急协调和通报工作机制，强化监测预警能力，梳理水利、能源、油气、交通、电信、金融等关键信息基础设施建设、运行、管理情况及安全保护状况，及时发现隐患、修补漏洞，采取多种措施保护关键信息基础设施安全。未来一段时间，我国仍将进一步强化网络安全检查，以便于全面掌握网络基础设施、重要业务系统和重要数据等资源底数和网络资产，建立动态关键信息基础设施档案，针对核心系统进行重点防护和加固，对网络进行精细化管理。

二、营造良好云原生安全产业发展环境

随着数字化转型加速推进，越来越的企业将其数据和应用迁移至云环境中，为保护云环境中的数据和应用，云原生安全至关重要，已成为云安全的最新趋势。因此，需要充分发挥政府在云原生安全产业发展方面的积极作用，着力营造良好的云原生安全产业发展环境，集成整合资源，推动云原生安全技术提升，为云原生安全产品大规模应用构建良好的支撑体系。

三、细化数据安全管理规范及管控措施

除《数据安全法》以及各行业数据安全管理规范外，国家部门及各行业协会组织可进一步细化数据安全管理制度，制定并实施数据安全评估机制、数据标准规范

等，同时在数据安全管理过程中采取精细化、差异化、有针对性的安全保护措施，对数据采集、存储、处理和应用等各环节进行隐患分析，及时消除风险，确保数据全生命周期的安全。

四、整合创新资源并完善创新体系

充分利用国家和省市专项资金加大支持引导力度，以高等院校与科研院所为主体，联合国内网络安全行业主要企业和研发机构，集聚创新资源、知识基础、共性技术研发力量打造领先的创新技术体系。综合政府、企业、高校、科研院所、用户、资金等要素提升网络安全产业的创新孵化与成果转化服务，提高引进、消化、吸收和集成再创新能力；继续加强知识产权保护利用、标准制定和相关评估测评等工作，打造优越的创新制度体系。

第二节 面向企业的建议

一、重视产品安全认证及可靠性评估

国家已于2017-2018年发布《网络关键设备和网络安全专用产品目录(第一批)》、《网络关键设备和网络安全专用产品安全认证实施规则》（CNCA-CCIS-2018），并于 2020 年正式发布《网络安全审查办法》，于 2022 年发布新修订的《网络安全审查办法》。由此来看，国家对网络安全产品的安全性、可靠性评估机制正在逐步完善。另外，为保障关键信息基础设施安全，《关键信息基础设施安全保护条例》明确规定“运营者应当优先采购安全可信的网络产品和服务”。对此，企业应积极主动开展产品安全认证，以适应网络安全产业发展需要、满足政策法规要求，助力国内网络安全防护水平提升。

二、优化边界安全、云安全等刚需产品性能

网络安全行业需求侧围绕着国家的相关热点法规政策展开，边界安全、云安全、安全运营及服务、态势感知等属于网络安全行业刚需产品，尽管需求增速较低，但需求量依然庞大。基于此，网络安全行业企业可持续根据行业属性和客户需求进行产品及服务的迭代优化，如开发载有ASIC芯片技术的防火墙，以及多端口、灵活配置的防火墙；为用户提供覆盖私有云、公有云、多云、混合云，并支持物理服务器、虚机、容器等全场景的云计算安全解决方案等。

三、积极布局信创、数据安全治理相关产品

网络安全是信创的关键环节，新一轮信创将直接带动安全采购需求显著增加，如终端准入、资产管理、虚拟补丁等终端安全产品；信创防火墙、IDPS等网关类安全硬件产品；加密类产品、web应用安全产品等。除信创相关网络安全产品外，数据安全治理能力是保障数字经济持续发展的关键，网络安全企业可开发并持续优化数据库加密与访问控制系统、应用（API）数据安全审计系统、数据库审计与防护系统、静态数据脱敏系统等产品。