

2024-2030年中国网络安全 市场深度分析与投资前景分析报告

报告目录及图表目录

北京迪索共研咨询有限公司

www.cction.com

一、报告报价

《2024-2030年中国网络安全市场深度分析与投资前景分析报告》信息及时，资料详实，指导性强，具有独家，独到，独特的优势。旨在帮助客户掌握区域经济趋势，获得优质客户信息，准确、全面、迅速了解目前行业发展动向，从而提升工作效率和效果，是把握企业战略发展定位不可或缺的重要决策依据。

官方网站浏览地址：<http://www.cction.com/report/202310/414034.html>

报告价格：纸介版8000元 电子版8000元 纸介+电子8500元

北京迪索共研咨询有限公司

订购电话: 400-700-9228(免长话费) 010-69365838

海外报告销售: 010-69365838

Email: kefu@gonyn.com

联系人：李经理

特别说明：本PDF目录为计算机程序生成，格式美观性可能有欠缺；实际报告排版规则、美观。

二、说明、目录、图表目录

网络安全的是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改和泄露，系统连续、可靠、正常地运行，网络服务不中断。由此可以将网络安全理解为：通过采用各种技术和管理措施，使网络系统正常运行，从而确保网络数据的可用性、完整性和保密性。

全球方面，相关研究机构预测，2023年全球网络安全支出（包括企业产品和服务）将增长13.2%，在理想条件下，2023年的总支出预计将达到2238亿美元。2023年，网络安全服务（包括咨询、外包、部署、集成、维护和管理服务）的交付预计将增长14.1%，达到1443亿美元。这将占据2023年全球网络安全市场份额的64.5%。2023年，网络安全产品（包括终端安全、网络安全、网络和电子邮件安全、数据安全、权限管理以及漏洞与安全分析）的出货量将增长11.7%，达到795亿美元。这意味着技术领域会出现强劲增长，但与2022年相比，增长会有所放缓。

2021年我国网络安全产业规模达到1905.1亿元，较2020年增长16.6%，2022年产业规模约为2169.9亿元，增速约为13.9%，到2023年产业规模有望超2500亿元。人才方面，2022年10月，根据工信部发布《网络安全产业人才发展报告（2022年版）》。截至2022年7月，全国有500余所高校设立网络安全相关专业，尽管开设网络安全相关专业的高校数量在逐年攀升，但目前每年高校安全专业培养人才仍无法满足市场需求，人口缺口较大。

从融资事件来看，2022年国内网络安全相关企业融资事件约110起，涉及约100家网络安全企业，覆盖包括数据安全、工控安全、隐私计算、开发安全、零信任、安全运营、物联网安全、区块链、公共安全、智能网联汽车、身份安全等众多细分领域。多家企业在2022年成功IPO，另有部分企业完成了多次融资。

网络安全行业，正迎来顶层规划及法律法规的密集发布。为了做好网络安全法与相关法律法规的衔接协调，完善法律责任制度，保护个人、组织在网络空间的合法权益，维护国家安全和公共利益，国家网信办会同相关部门起草了《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》于2022年9月14日公布，向社会公开征求意见。工业和信息化部2022年10月印发《网络产品安全漏洞收集平台备案管理办法》。《办法》规定，漏洞收集平台备案通过工业和信息化部网络安全威胁和漏洞信息共享平台开展，采用网上备案方式进行。拟设立漏洞收集平台的组织或个人，应当通过工业和信息化部网络安全威胁和漏洞信息共享平台如实填报网络产品安全漏洞收集平台备案登记信息。该办法自2023年1月1日起施行。2022年11月，工业和信息化部会同银保监会起草了《关于促进网络安全保险规范健康发展的意见（征求意见稿）》并予以公示。《征求意见稿》旨在加快推动网络安全产业和金融服务融合发展，培

育网络安全保险新业态，促进企业加强网络安全风险管理，推动网络安全产业高质量发展。目前，大数据、云计算、物联网、工业互联网、移动互联网等技术的发展融合导致安全风险的复杂叠加并快速演化，安全技术走到IT创新突破的前沿，安全产业版图面临变革重构，虚拟化、可视化、智能化、服务化成为安全技术创新发展的主流。由于网络安全行业和IT投入直接相关，IT投入可预期将持续增长，而且，在政策及安全事件的驱动下，占总的IT投入比重有望提升，因此，从长期来看，这是一个市场空间长期向上的行业。

中企顾问网发布的《2024-2030年中国网络安全市场深度分析与投资前景分析报告》共十七章。首先介绍了网络安全的基本概念、体系结构及产品等内容，接着分析了国内外网络安全的发展环境与发展现状。并从云安全、工控安全、大数据安全、物联网安全、移动安全、工业互联网安全五个重要细分领域入手进行了深入分析；然后，报告对网络安全的下游应用以及技术方面也做了分析，随后，报告分析了国内外重点企业运营状况、产业投融资及投资案例；最后对网络安全产业的发展前景进行了科学的预测。

本研究报告数据主要来自于国家统计局、工信部、互联网数据中心（IDC）、中企顾问网、中企顾问网市场调查中心、以及国内外重点刊物等渠道，数据权威、详实、丰富，同时通过专业的分析预测模型，对行业核心发展指标进行科学地预测。您或贵单位若想对网络安全产业有个系统深入的了解、或者想投资网络安全相关行业，本报告将是您不可或缺的重要参考工具。

报告目录：

第一章 网络安全基本概述

1.1 网络安全概念界定

1.1.1 网络安全定义

1.1.2 网络安全特征

1.1.3 网络安全模型

1.2 网络安全体系结构

1.2.1 安全服务

1.2.2 安全机制

1.2.3 安全管理

1.3 网络安全产品介绍

1.3.1 网络安全产品分类

1.3.2 网络安全产品特点

1.3.3 网络安全产品定价

第二章 2021-2023年全球网络安全行业发展分析

2.1 2021-2023年全球网络安全产业发展分析

2.1.1 网络安全状况

2.1.2 行业发展热点

2.1.3 产业规模分析

2.1.4 产业结构分析

2.1.5 产业区域分布

2.1.6 企业营收情况

2.1.7 安全支出预测

2.1.8 产业发展趋势

2.2 2021-2023年全球网络安全产业技术投入分析

2.2.1 强化网络安全威慑能力

2.2.2 网络数据跨境流动投入

2.2.3 网络安全人才培养投入

2.2.4 强化网络安全资金支持

2.3 美国网络安全产业发展状况

2.3.1 行业发展历程

2.3.2 政策环境分析

2.3.3 产业布局现状

2.3.4 人才培养战略

2.3.5 网络安全预算

2.3.6 经验借鉴分析

2.3.7 美对外制裁及威胁

2.4 欧盟网络安全产业发展分析

2.4.1 产业发展环境

2.4.2 产业布局进展

2.4.3 产业发展现状

2.4.4 行业发展形势

2.4.5 行业发展举措

2.4.6 行业发展影响

2.4.7 产业战略规划

- 2.4.8 发展经验借鉴
- 2.5 澳大利亚网络安全产业发展分析
 - 2.5.1 政策环境分析
 - 2.5.2 网络安全现状
 - 2.5.3 资金投入分析
 - 2.5.4 产业发展规划
- 2.6 其他国家网络安全产业的发展
 - 2.6.1 英国
 - 2.6.2 新加坡
 - 2.6.3 以色列
 - 2.6.4 越南

第三章 2021-2023年中国网络安全行业发展环境分析

- 3.1 政策环境
 - 3.1.1 政策发展回顾
 - 3.1.2 政策发展现状
 - 3.1.3 重点政策汇总
 - 3.1.4 相关政策解读
 - 3.1.5 相关行业标准
 - 3.1.6 等级保护制度
 - 3.1.7 数据安全法颁布
 - 3.1.8 网络安全审查办法
 - 3.1.9 网络安全漏洞管理
 - 3.1.10 网络安全发展规划
 - 3.1.11 国家信息化规划
- 3.2 经济环境
 - 3.2.1 全球经济运行
 - 3.2.2 宏观经济概况
 - 3.2.3 对外经济分析
 - 3.2.4 工业经济运行
 - 3.2.5 经济转型升级
 - 3.2.6 宏观经济展望

3.3 互联网环境

3.3.1 互联网接入环境分析

3.3.2 网民规模及结构状况

3.3.3 互联网基础资源状况

3.3.4 互联网应用发展情况

3.4 新兴技术应用在网络安全领域的特点

3.4.1 人工智能

3.4.2 区块链

3.4.3 量子信息技术

3.4.4 5G

3.4.5 物联网

3.4.6 隐私计算

第四章 2021-2023年中国网络安全行业发展分析

4.1 中国互联网网络安全形势分析

4.1.1 互联网网络安全总体状况

4.1.2 网民网络安全事件发生状况

4.1.3 网站安全 and 信息安全漏洞

4.1.4 网络安全相关举报和受理

4.1.5 互联网网络安全监测分析

4.1.6 互联网网络安全威胁分析

4.2 中国网络安全行业发展现状综合分析

4.2.1 市场规模分析

4.2.2 市场区域分布

4.2.3 市场应用领域

4.2.4 营销网络建设

4.2.5 市场销售模式

4.2.6 市场竞争格局

4.2.7 企业布局动态

4.2.8 人才需求情况

4.2.9 国际合作进展

4.3 中国网络安全企业发展现状分析

- 4.3.1 企业数量规模
- 4.3.2 企业收入水平
- 4.3.3 企业业务类型
- 4.3.4 典型企业排名
- 4.4 中国部分省市网络安全产业区域布局分析
 - 4.4.1 北京市
 - 4.4.2 上海市
 - 4.4.3 浙江省
 - 4.4.4 广东省
 - 4.4.5 山东省
 - 4.4.6 河南省
 - 4.4.7 山西省
- 4.5 中国网络安全行业发展面临的挑战
 - 4.5.1 国内网络安全风险挑战
 - 4.5.2 网络安全监管力度不够
 - 4.5.3 网络安全产业发展问题
 - 4.5.4 “新基建”带来的新挑战
 - 4.5.5 网络安全技术体系短板
- 4.6 中国网络安全行业发展对策建议
 - 4.6.1 大力开展新型基础设施建设
 - 4.6.2 着力优化专业人才供给结构
 - 4.6.3 全力推动产学研用联动发展
 - 4.6.4 加快培育多种类型市场主体
 - 4.6.5 逐步统一产业统计核算口径
 - 4.6.6 不断促进国内企业走向全球

第五章 2021-2023年云安全行业发展分析

- 5.1 云安全相关概述
 - 5.1.1 云安全含义
 - 5.1.2 云安全本质
 - 5.1.3 云安全特点
 - 5.1.4 云安全产品

- 5.1.5 云安全技术
- 5.1.6 云安全策略
- 5.2 2021-2023年全球云安全行业发展分析
 - 5.2.1 云计算市场分析
 - 5.2.2 云安全监管环境
 - 5.2.3 云安全市场规模
 - 5.2.4 云安全市场现状
 - 5.2.5 云安全竞争格局
 - 5.2.6 云安全企业布局
 - 5.2.7 云安全事件动态
 - 5.2.8 云安全发展趋势
- 5.3 2021-2023年中国云安全行业发展分析
 - 5.3.1 云计算市场分析
 - 5.3.2 云安全市场特点
 - 5.3.3 云安全市场规模
 - 5.3.4 云安全产品部署
 - 5.3.5 云安全竞争格局
 - 5.3.6 云安全市场驱动因素
 - 5.3.7 云安全发展趋势
- 5.4 中国云安全典型企业分析
 - 5.4.1 百度智能云
 - 5.4.2 阿里云
 - 5.4.3 华为云
 - 5.4.4 安恒云

第六章 2021-2023年工控安全行业发展分析

- 6.1 工控安全相关概述
 - 6.1.1 工控安全基本介绍
 - 6.1.2 工控安全主要分类
 - 6.1.3 工控系统安全重要性
- 6.2 工业控制系统发展综述
 - 6.2.1 工业控制系统含义

- 6.2.2 工业控制系统特点
- 6.2.3 ICS体系结构分析
- 6.2.4 ICS安防状况分析
- 6.2.5 ICS系统潜在风险
- 6.2.6 ICS安全防护问题
- 6.2.7 ICS实施安防策略
- 6.3 2021-2023年工控安全行业发展状况分析
 - 6.3.1 工控安全政策法规
 - 6.3.2 工业信息安全规模
 - 6.3.3 工控安全市场规模
 - 6.3.4 典型工控安全事件
 - 6.3.5 工控系统安全漏洞
 - 6.3.6 联网工控设备分布
 - 6.3.7 工控系统攻击分析
 - 6.3.8 工控安全发展不足
 - 6.3.9 工控安全发展潜力
- 6.4 典型工控安全解决方案
 - 6.4.1 电力工控安全
 - 6.4.2 制造业工控安全
 - 6.4.3 市政工控安全

第七章 2021-2023年大数据安全行业发展分析

- 7.1 大数据安全相关概述
 - 7.1.1 大数据安全概念界定
 - 7.1.2 大数据安全问题挑战
 - 7.1.3 大数据安全保障框架
 - 7.1.4 大数据安全防护体系
- 7.2 2021-2023年全球大数据安全行业发展分析
 - 7.2.1 大数据安全行业相关政策
 - 7.2.2 大数据安全市场发展规模
 - 7.2.3 大数据安全行业发展形势
 - 7.2.4 大数据安全行业典型事件

- 7.2.5 大数据安全行业面临挑战
- 7.2.6 大数据安全行业发展展望
- 7.3 2021-2023年中国大数据安全行业发展分析
 - 7.3.1 政策环境分析
 - 7.3.2 行业发展现状
 - 7.3.3 市场规模分析
 - 7.3.4 行业发展特点
 - 7.3.5 行业竞争分析
 - 7.3.6 体系建设成果
 - 7.3.7 行业应用展望
- 7.4 贵州省大数据安全行业发展分析
 - 7.4.1 大数据中心产业集群建设
 - 7.4.2 大数据安全发展状况分析
 - 7.4.3 大数据安全区域发展布局
 - 7.4.4 大数据安全发展具体举措
 - 7.4.5 大数据安全认证机构设立
- 7.5 大数据安全关键技术发展状况分析
 - 7.5.1 设备系统安全技术
 - 7.5.2 密码学及隐私保护算法
 - 7.5.3 认证和访问控制技术
 - 7.5.4 高可靠数据保护技术
 - 7.5.5 数据安全管理工作技术
 - 7.5.6 数据库技术
 - 7.5.7 人工智能技术
- 7.6 大数据安全典型厂商
 - 7.6.1 中国联通
 - 7.6.2 蚂蚁集团
 - 7.6.3 百度
 - 7.6.4 天翼云
- 7.7 大数据安全解决方案
 - 7.7.1 安全问题
 - 7.7.2 防护思路

7.7.3 方案设计

7.7.4 解决方案

第八章 2021-2023年物联网安全行业发展分析

8.1 物联网安全相关概述

8.1.1 物联网基本介绍

8.1.2 物联网安全分类

8.1.3 物联网安全特征

8.1.4 物联网安全防御体系

8.2 2021-2023年全球物联网安全行业发展分析

8.2.1 物联网市场规模分析

8.2.2 物联网连接设备分析

8.2.3 物联网安全发展环境

8.2.4 物联网安全事件回顾

8.2.5 物联网安全市场规模

8.2.6 物联网安全发展动态

8.3 2021-2023年中国物联网安全行业发展分析

8.3.1 物联网行业发展分析

8.3.2 物联网安全相关政策

8.3.3 物联网安全市场规模

8.3.4 物联网安全用户规模

8.3.5 物联网安全风险分析

8.3.6 物联网安全发展前景

8.3.7 物联网安全发展展望

8.4 物联网安全防护策略分析

8.4.1 瞄准内生安全

8.4.2 加速新技术的应用

8.4.3 建立泛在化部署体系

8.4.4 加强全方位安全防护

8.4.5 强化供应链安全

第九章 2021-2023年移动安全行业发展分析

- 9.1 移动互联网综述
 - 9.1.1 移动互联网基本概述
 - 9.1.2 移动互联网发展现状
 - 9.1.3 移动互联网发展特点
 - 9.1.4 移动互联网安全重要性
 - 9.1.5 移动互联网主要问题
 - 9.1.6 移动互联网防范措施
 - 9.1.7 移动互联网发展趋势
- 9.2 2021-2023年中国移动安全行业发展分析
 - 9.2.1 移动安全市场规模
 - 9.2.2 移动安全市场特点
 - 9.2.3 移动安全威胁类型
 - 9.2.4 移动安全典型事件
 - 9.2.5 移动安全发展趋势
- 9.3 移动应用安全发展状况分析
 - 9.3.1 移动应用发展概况
 - 9.3.2 移动应用漏洞概况
 - 9.3.3 移动恶意应用概况
 - 9.3.4 应用嵌入SDK概况
 - 9.3.5 技术安全保护概况
 - 9.3.6 应用安全监管概况
 - 9.3.7 应用信息保护建议
- 9.4 移动支付安全发展状况分析
 - 9.4.1 移动支付基本概述
 - 9.4.2 移动支付行业现状
 - 9.4.3 移动支付用户规模
 - 9.4.4 移动支付安全现状
 - 9.4.5 支付安全性分析
 - 9.4.6 移动支付安全建议

第十章 2021-2023年工业互联网安全行业发展分析

- 10.1 工业互联网发展综述

- 10.1.1 工业互联网基本含义
- 10.1.2 工业互联网政策环境
- 10.1.3 工业互联网发展概况
- 10.1.4 工业互联网产业现状
- 10.1.5 工业互联网产业生态
- 10.1.6 工业互联网平台分析
- 10.1.7 工业互联网区域发展
- 10.1.8 工业互联网融合发展
- 10.1.9 工业互联网发展趋势
- 10.2 工业互联网安全行业发展综述
- 10.2.1 工业互联网安全内涵
- 10.2.2 工业互联网安全形势
- 10.2.3 与传统工业信息安全的关系
- 10.2.4 工业互联网安全相关政策
- 10.3 工业互联网安全防护需求分析
- 10.3.1 海量和异构工业设备接入及设备资源受限
- 10.3.2 不同架构工业云协调运维和快速部署
- 10.3.3 工业微服务多样化和多服务复杂协同
- 10.3.4 工业应用协同工作和开放定制
- 10.3.5 工业数据多源异构和大规模访问与共享
- 10.4 2021-2023年中国工业互联网安全行业发展分析
- 10.4.1 行业发展状况
- 10.4.2 市场规模分析
- 10.4.3 市场发展特点
- 10.4.4 发展问题分析
- 10.4.5 发展建议分析
- 10.4.6 发展趋势分析
- 10.4.7 行业发展展望
- 10.5 2021-2023年中国工业互联网安全现状
- 10.5.1 工业主机安全风险
- 10.5.2 工控设备安全风险
- 10.5.3 数控设备安全风险

- 10.5.4 工业机器人安全风险
- 10.5.5 工业物联网设备安全风险
- 10.6 工业互联网安全解决方案案例分析
 - 10.6.1 工业互联网数据安全解决方案
 - 10.6.2 轨道交通行业安全解决方案
 - 10.6.3 汽车制造行业安全解决方案
 - 10.6.4 电子制造企业安全解决方案
 - 10.6.5 风电集控中心安全解决方案
 - 10.6.6 城市污水处理安全解决方案

第十一章 2021-2023年网络安全行业下游应用分析

- 11.1 电信业
 - 11.1.1 政策环境分析
 - 11.1.2 电信网络安全需求
 - 11.1.3 电信网络安全状况
 - 11.1.4 电信运营商安全布局
 - 11.1.5 电信业网络安全问题
 - 11.1.6 电信网络安全发展目标
 - 11.1.7 电信网络安全防范措施
- 11.2 金融业
 - 11.2.1 金融业政策环境分析
 - 11.2.2 金融网络安全需求背景
 - 11.2.3 金融业网络安全技术
 - 11.2.4 金融业网信安全框架
 - 11.2.5 金融业网络安全策略
 - 11.2.6 金融业网络安全事件
 - 11.2.7 金融业网络安全趋势
- 11.3 电子政务
 - 11.3.1 电子政务政策环境分析
 - 11.3.2 电子政务运行状况分析
 - 11.3.3 电子政务网络安全问题
 - 11.3.4 电子政务网络安全威胁

- 11.3.5 电子政务安全运营体系
- 11.3.6 电子政务主要防范措施
- 11.3.7 电子政务安全发展目标
- 11.4 能源行业
 - 11.4.1 能源行业典型安全事件
 - 11.4.2 电力行业网络政策环境
 - 11.4.3 电力网络安全威胁分析
 - 11.4.4 电力系统网络安全层面
 - 11.4.5 电力网络安全应对策略
 - 11.4.6 能源网络安全发展建议
- 11.5 快递行业
 - 11.5.1 快递行业发展状况
 - 11.5.2 隐私单面建设现状
 - 11.5.3 信息安全特点分析
 - 11.5.4 信息安全应对策略

第十二章 网络安全技术分析

- 12.1 防火墙技术
 - 12.1.1 防火墙基本概述
 - 12.1.2 防火墙主要类型
 - 12.1.3 防火墙基本特性
 - 12.1.4 防火墙主要功能
 - 12.1.5 防火墙技术分析
 - 12.1.6 大型企业防火墙
- 12.2 身份认证技术
 - 12.2.1 基本概述
 - 12.2.2 安全风险
 - 12.2.3 组合认证
- 12.3 数据加密技术
 - 12.3.1 基本概述
 - 12.3.2 技术应用
- 12.4 入侵检测技术分析

- 12.4.1 基本概述
- 12.4.2 主要类型
- 12.4.3 面临困境
- 12.4.4 发展方向
- 12.5 访问控制技术
 - 12.5.1 计算机网络访问控制
 - 12.5.2 自主访问控制技术
 - 12.5.3 强制访问控制技术
 - 12.5.4 角色访问控制技术

第十三章 2021-2023年网络安全行业国外重点企业经营分析

13.1 雷神科技公司 (Raytheon Technologies Corp.)

- 13.1.1 企业发展概况
- 13.1.2 2021年企业经营状况分析
- 13.1.3 2022年企业经营状况分析
- 13.1.4 2023年企业经营状况分析

13.2 思科系统公司 (Cisco Systems, Inc.)

- 13.2.1 企业发展概况
- 13.2.2 2022财年企业经营状况分析
- 13.2.3 2023财年企业经营状况分析
- 13.2.4 2023财年企业经营状况分析

13.3 派拓网络 (Palo Alto Networks)

- 13.3.1 企业发展概况
- 13.3.2 2022财年企业经营状况分析
- 13.3.3 2023财年企业经营状况分析
- 13.3.4 2023财年企业经营状况分析

13.4 洛克希德·马丁公司 (Lockheed Martin)

- 13.4.1 企业发展概况
- 13.4.2 2021财年企业经营状况分析
- 13.4.3 2022财年企业经营状况分析
- 13.4.4 2023财年企业经营状况分析

13.5 Check Point软件技术有限公司

- 13.5.1 企业发展概况
- 13.5.2 2021年企业经营状况分析
- 13.5.3 2022年企业经营状况分析
- 13.5.4 2023年企业经营状况分析
- 13.6 Splunk, Inc.
- 13.6.1 企业发展概况
- 13.6.2 2021财年企业经营状况分析
- 13.6.3 2022财年企业经营状况分析
- 13.6.4 2023财年企业经营状况分析

第十四章 2020-2023年网络安全行业国内重点企业经营分析

14.1 启明星辰信息技术集团股份有限公司

- 14.1.1 企业发展概况
- 14.1.2 企业业务布局
- 14.1.3 经营效益分析
- 14.1.4 业务经营分析
- 14.1.5 财务状况分析
- 14.1.6 核心竞争力分析
- 14.1.7 公司发展战略
- 14.1.8 未来前景展望

14.2 深信服科技股份有限公司

- 14.2.1 企业发展概况
- 14.2.2 企业业务布局
- 14.2.3 经营效益分析
- 14.2.4 业务经营分析
- 14.2.5 财务状况分析
- 14.2.6 核心竞争力分析
- 14.2.7 公司发展战略
- 14.2.8 未来前景展望

14.3 成都卫士通信息产业股份有限公司

- 14.3.1 企业发展概况
- 14.3.2 经营效益分析

- 14.3.3 业务经营分析
- 14.3.4 财务状况分析
- 14.3.5 核心竞争力分析
- 14.3.6 公司发展战略
- 14.3.7 未来前景展望
- 14.4 北京神州绿盟信息安全科技股份有限公司
 - 14.4.1 企业发展概况
 - 14.4.2 安全业务发展
 - 14.4.3 经营效益分析
 - 14.4.4 业务经营分析
 - 14.4.5 财务状况分析
 - 14.4.6 核心竞争力分析
 - 14.4.7 未来前景展望
- 14.5 蓝盾信息安全技术股份有限公司
 - 14.5.1 企业发展概况
- 14.6 新华三集团
 - 14.6.1 企业发展概况
 - 14.6.2 网络安全布局
 - 14.6.3 产品矩阵布局
 - 14.6.4 企业发展成就
 - 14.6.5 企业项目动态
 - 14.6.6 企业战略布局
- 14.7 安天科技股份有限公司
 - 14.7.1 企业发展概况
 - 14.7.2 企业发展成果
 - 14.7.3 企业融资动态
 - 14.7.4 企业产品优势
 - 14.7.5 企业合作动态
- 14.8 三六零安全科技股份有限公司
 - 14.8.1 企业发展概况
 - 14.8.2 驱动因素分析
 - 14.8.3 网络安全布局

- 14.8.4 经营效益分析
- 14.8.5 业务经营分析
- 14.8.6 财务状况分析
- 14.8.7 核心竞争力分析
- 14.8.8 未来前景展望

第十五章 中国网络安全行业项目投资案例深度解析

15.1 任子行网络安全项目

- 15.1.1 项目基本情况
- 15.1.2 项目投资必要性
- 15.1.3 项目投资可行性
- 15.1.4 项目实施主体
- 15.1.5 项目投资概算
- 15.1.6 项目经济效益

15.2 森根科技无线网络安全治理平台研发及产业化项目

- 15.2.1 项目基本情况
- 15.2.2 项目投资概算
- 15.2.3 项目实施进度
- 15.2.4 项目审批情况
- 15.2.5 环境保护分析
- 15.2.6 项目经济效益

15.3 蓝盾大安全研发与产业化基地项目

- 15.3.1 项目基本情况
- 15.3.2 项目实施背景
- 15.3.3 项目投资计划
- 15.3.4 项目投资价值
- 15.3.5 项目建设方案
- 15.3.6 项目实施主体
- 15.3.7 项目经济效应

15.4 永信至诚网络安全人才培养项目

- 15.4.1 项目基本概述
- 15.4.2 项目投资价值

- 15.4.3 项目建设内容
- 15.4.4 项目进度安排
- 15.4.5 项目投资概算
- 15.5 启明星辰网络安全领域项目投资分析
 - 15.5.1 济南安全运营中心建设项目
 - 15.5.2 杭州安全运营中心建设项目
 - 15.5.3 昆明安全运营中心和网络安全培训学院建设项目
 - 15.5.4 郑州安全运营中心和网络培训学院建设项目

第十六章 2024-2030年中国网络安全行业投资潜力分析

- 16.1 全球网络安全行业投融资状况分析
 - 16.1.1 主要上市企业市值
 - 16.1.2 行业整体投融资情况
 - 16.1.3 行业投融资时间分布
 - 16.1.4 投融资技术领域分布
 - 16.1.5 行业并购交易活动态势
- 16.2 中国网络安全行业投融资状况分析
 - 16.2.1 行业投资数量
 - 16.2.2 行业投资金额
 - 16.2.3 行业融资轮次
 - 16.2.4 行业投资领域
 - 16.2.5 融资事件汇总
 - 16.2.6 企业上市进展
 - 16.2.7 行业并购态势
- 16.3 中国网络信息安全行业投资价值评估分析
 - 16.3.1 投资价值综合评估
 - 16.3.2 市场机会矩阵分析
 - 16.3.3 进入市场时机判断
- 16.4 中国网络信息安全行业投资壁垒分析
 - 16.4.1 竞争壁垒
 - 16.4.2 技术壁垒
 - 16.4.3 资金壁垒

16.4.4 政策壁垒

16.5 2024-2030年网络信息安全行业的投资建议

16.5.1 项目投资建议

16.5.2 行业风险提示

第十七章 2024-2030年中国网络安全行业发展前景及趋势预测分析

17.1 中国网络安全行业发展前景展望

17.1.1 网络安全行业发展趋势

17.1.2 网络安全技术发展趋势

17.1.3 网络安全行业变革趋势

17.1.4 “十四五”网络安全发展机会

17.1.5 “十四五”网络安全前景展望

17.2 2024-2030年中国网络安全产业预测分析

17.2.1 2024-2030年中国网络安全产业影响因素分析

17.2.2 2024-2030年中国网络安全市场规模预测

图表目录

图表1 网络安全模型图

图表2 OSI参考模型和TCP/CP参考模型协议对应关系

图表3 网络安全产品的基本分类

图表4 端点安全结构图

图表5 网络安全结构图

图表6 应用安全结构图

图表7 数据安全结构图

图表8 身份与访问管理结构类

图表9 安全管理结构图

图表10 云的结构图

图表11 大数据结构图

图表12 物联网结构图

图表13 移动结构图

图表14 产品主要技术特点

图表15 产品主要应用场景

- 图表16 产品主要应用场景
- 图表17 产品主要应用场景
- 图表18 产品主要应用场景
- 图表19 软件开发流程
- 图表20 竞争导向的企业定价流程
- 图表21 网络安全产品定价方法总结
- 图表22 2020-2026年全球网络安全市场规模及预测
- 图表23 2020-2021年全球网络安全市场结构
- 图表24 2021年全球网络安全软件市场结构
- 图表25 2021年全球网络安全终端用户支出地区分布
- 图表26 2021年全球主要网络安全公司营收增速
- 图表27 2021年全球主要网络安全公司多为亏损状态
- 图表28 2021年全球主要网络安全公司维持高研发及高销售投入
- 图表29 美国网络安全产业发展历程
- 图表30 2011-2020年美国“网络威慑”立场的演变历程

详细请访问：<http://www.cction.com/report/202310/414034.html>