

2020-2025年中国网络安全行业市场前景预测及投资战略咨询报告

报告大纲

一、报告简介

华经情报网发布的《2020-2025年中国网络安全行业市场前景预测及投资战略咨询报告》涵盖行业最新数据，市场热点，政策规划，竞争情报，市场前景预测，投资策略等内容。更辅以大量直观的图表帮助本行业企业准确把握行业发展态势、市场商机动向、正确制定企业竞争战略和投资策略。本报告依据国家统计局、海关总署和国家信息中心等渠道发布的权威数据，以及我中心对本行业的实地调研，结合了行业所处的环境，从理论到实践、从宏观到微观等多个角度进行市场调研分析。

官网地址：<https://www.huaon.com/detail/493962.html>

报告价格：电子版: 9000元 纸介版：9000元 电子和纸介版: 9200元

订购电话: 400-700-0142 010-80392465

电子邮箱: kf@huaon.com

联系人: 刘老师

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、报告目录及图表目录

网络安全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受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

本研究报告数据主要采用国家统计局数据，海关总署，问卷调查数据，商务部采集数据等数据库。其中宏观经济数据主要来自国家统计局，部分行业统计数据主要来自国家统计局及市场调研数据，企业数据主要来自于国统计局规模企业统计数据库及证券交易所等，价格数据主要来自于各类市场监测数据库。

报告目录：

第1章：中国网络安全行业发展综述

1.1 网络安全行业概述

1.1.1 网络安全概念分析

1.1.2 网络安全的特性分析

(1) 保密性

(2) 完整性

(3) 可用性

(4) 可控性

(5) 可审查性

1.1.3 网络安全主要类型分析

(1) 系统安全

(2) 网络的安全

(3) 信息传播安全

(4) 信息内容安全

1.1.4 网络安全产品和服务分类

(1) 依据主要功能及形态分类

(2) 依据安全防御生命周期技术能力分类

1.1.5 网络安全产业的概念分析

1.2 网络安全行业市场背景分析

1.2.1 需求端一：技术升级换代，安全隐忧增加

1.2.2 需求端二：多个地下产业链形成，网络安全威胁大

1.2.3 需求端三：网络安全突发事件造成的影响越来越大

1.2.4 需求端四：数字经济发展对网络和数据安全提出更高要求

1.2.5 政策端：国内外网络安全政策频发

1.2.6 技术端：网络安全防护技术发展

- (1) 常见的互联网安全防护技术
- (2) 网络技术发展的阶段分析
- (3) 前沿互联网安全防护技术发展

1.2.7 社会端：公安部等部门重拳出击打击网络诈骗

1.3 网络安全行业发展环境分析

1.3.1 行业政策环境分析

- (1) 网络安全主管部门
- (2) 国际政策
- (3) 国内政策

1.3.2 行业社会环境分析

- (1) 境内感染网络病毒终端数
- (2) 境内被篡改网站数量
- (3) 境内被植入后门网站数量
- (4) 安全漏洞数量

1.3.3 行业经济环境分析

- (1) 国内生产总值
- (2) 工业增加值
- (3) 固定资产投资
- (4) 对外贸易环境分析
- (5) 2019年宏观经济展望

1.3.4 行业技术环境分析

- (1) 行业专利申请量分析
- (2) 行业专利公开量分析
- (3) 技术领先企业分析
- (4) 行业热门技术分析

1.4 网络安全行业发展机遇与威胁分析

1.4.1 网络安全行业发展机遇分析

- (1) 国内网络安全产业规模高速增长，安全服务领域创新活跃
- (2) 重点城市加快产业布局，产业集群效应逐渐显现
- (3) 网络安全人才培养上升法律和战略高度，高校企业共同发力

1.4.2 网络安全行业发展威胁分析

- (1) 网络网络安全攻击更加复杂多变，网络安全易攻难守
- (2) 产品种类繁多，行业规范需进一步统一
- (3) 网络安全核心技术有待加强

(4) 网络安全人才匮乏

第2章：威胁网络安全的典型地下产业链分析

2.1 互联网黑色产业链发展状况分析

2.1.1 互联网黑色产业链含义

2.1.2 互联网黑色产业链的成因分析

- (1) 取证困难，发现滞后
- (2) 跨域犯罪，难以追踪
- (3) 规则改变，利益驱动

2.1.3 互联网黑色产业链的发展现状

2.1.4 互联网黑色产业链的市场规模

2.1.5 互联网黑色产业链的类型分析

- (1) 移动端网络黑色产业链
- (2) PC端网络黑色产业链

2.1.6 互联网黑色产业链各环节发展分析

- (1) 上游“源头供货”市场及牟利方式分析
- (2) 中游“处理加工”市场及牟利方式分析
- (3) 下游“应用变现”市场及牟利方式分析

2.2 勒索病毒解密黑色产业链分析

2.2.1 勒索病毒的含义

2.2.2 勒索病毒的类型

2.2.3 勒索病毒的发展现状

2.2.4 勒索病毒的热门目标

2.2.5 勒索病毒解密黑色产业链市场规模

2.2.6 勒索病毒解密黑色产业链各环节分析

- (1) 勒索病毒解密黑色产业链上游
- (2) 勒索病毒解密黑色产业链中游
- (3) 勒索病毒解密黑色产业链下游

2.2.7 勒索病毒的热门事件

2.3 DDoS攻击黑色产业链分析

2.3.1 DDoS攻击的含义

2.3.2 DDoS攻击的发展规模

2.3.3 DDoS攻击的类型分析

- (1) 流量型攻击
- (2) 连接型攻击

(3) 特殊协议缺陷攻击

2.3.4 DDoS攻击黑色产业链分析

2.3.5 DDoS攻击的热门事件

2.4 网络诈骗地下产业链发展分析

2.4.1 网络诈骗的含义

2.4.2 网络诈骗的发展规模

(1) 网络诈骗举报数量

(2) 群众损失规模

2.4.3 网络诈骗的犯罪特点

(1) 犯罪方法简单

(2) 犯罪成本低

(3) 渗透性强

(4) 隐蔽性强

2.4.4 网络诈骗的受害群体

(1) 男人更易上当，女人受骗更深

(2) 90后最易受骗，60后损失最多

2.4.5 网络诈骗的类型分析

(1) 仿冒身份欺诈

(2) 购物类欺诈

(3) 利诱类欺诈

(4) 虚构险情欺诈

(5) 日常生活消费类欺诈

(6) 钓鱼、木马病毒类欺诈

(7) 其他新兴违法欺诈

2.4.6 网络诈骗的市场结构

2.4.7 网络诈骗地下产业链各环节分析

(1) 信息获取

(2) 批发销售

(3) 实施诈骗

(4) 分赃销赃

2.5 数字金融欺诈产业链分析

2.5.1 数字金融欺诈的含义

2.5.2 数字金融欺诈的发展历程

2.5.3 数字金融欺诈的类型

(1) 高利理财

(2) 网络借贷

(3) 网络众筹

(4) 消费金融

(5) 非法集资

2.5.4 数字金融欺诈总体形势分析

(1) 诈骗交易笔数呈下降趋势

(2) 诈骗作案收款账号数量显著下降

(3) 支付账号单笔被骗金额上升明显

(4) 诈骗案件金额呈现上升趋势

2.5.5 数字金融欺诈人群与区域特征分析

(1) 受骗人群画像特征分析

(2) 受骗人群区域分布特征

(3) 作案人群画像特征分析

(4) 作案人群区域分布特征

2.6 网络安全威胁的趋势分析

2.6.1 物联网设备将成为新的DDoS攻击目标

2.6.2 机器学习加剧攻防两方的对抗

2.6.3 数字勒索或成为未来主流网络犯罪手法

2.6.4 家庭设备或将成为勒索软件的劫持目标

2.6.5 网络黑产技术手段持续升级，威胁源更加多变

2.6.6 电信诈骗与移动木马结合，升级为移动木马诈骗

2.6.7 移动支付成主流，手机支付安全引关注

第3章：中国网络安全行业发展状况分析

3.1 全球网络安全行业发展分析

3.1.1 全球网络安全行业规模分析

3.1.2 全球网络安全行业融资规模分析

(1) 融资额和融资数量

(2) 融资细分领域分析

3.1.3 全球网络安全行业结构分析

3.1.4 全球网络安全行业竞争格局

3.1.5 主要国家/地区网络安全行业发展分析

(1) 美国网络安全行业发展分析

(2) 欧洲网络安全行业发展分析

(3) 日本网络安全行业发展分析

3.1.6 全球网络安全行业热门事件分析

- (1) 英特尔处理器曝“Meltdown”和“Spectre漏洞”
- (2) GitHub遭遇大规模Memcached DDoS攻击
- (3) 瑞士数据管理公司 Veeam 泄露 4.45 亿条用户数据
- (4) Facebook数据泄露震惊全球
- (5) 万豪酒店5亿用户开房信息泄露

3.1.7 全球网络安全行业前景与趋势

- (1) 安全信息与事件管理渐成气候
- (2) 云计算在安全服务上的应用日益普遍

3.2 中国网络安全行业发展状况分析

3.2.1 网络安全行业状态描述总结

3.2.2 网络安全行业经济特性分析

3.2.3 网络安全行业市场规模分析

3.2.4 网络安全行业竞争格局分析

- (1) 整体竞争格局分析
- (2) 互联网巨头竞争格局
- (3) 云设备商竞争格局分析
- (4) 创业公司竞争格局分析
- (5) 未来竞争趋势分析

3.2.5 网络安全行业市场关注热点分析

- (1) 关键信息基础设施保护
- (2) 大数据安全
- (3) 个人信息保护
- (4) 网络安全标准
- (5) 网络安全人才培养

3.2.6 网络安全行业区域发展分析

3.2.7 网络安全行业发展痛点分析

3.3 中国网络安全行业总体监测情况分析

3.3.1 网络病毒拦截监测情况分析

- (1) 病毒拦截总体情况
- (2) 拦截病毒类型分析
- (3) 病毒感染地域分析

3.3.2 网络漏洞监测情况分析

- (1) 最新漏洞态势研判情况
- (2) 漏洞报送情况统计

- (3) 漏洞严重程度统计

- (4) 漏洞要闻速递

3.3.3 反网络黑产诈骗监测情况分析

- (1) 举报垃圾短信条数

- (2) 骚扰电话用户标记量

- (3) 拦截恶意网址

3.4 中国网络安全应急响应发展现状分析

3.4.1 网络安全应急响应含义

3.4.2 网络安全应急响应的措施

- (1) 准备工作

- (2) 事件监测

- (3) 抑制处置

- (4) 应急场景演练

3.4.3 网络安全应急响应发展现状

3.4.4 网络安全应急响应的热点领域

- (1) 态势感知

- (2) 网络攻击与溯源

3.4.5 网络应急响应发展的痛点分析

- (1) 网络安全应急响应管理制度不健全

- (2) 网络安全应急响应管理职责不明确

- (3) 网络安全应急响应意识较薄弱

3.5 互联网巨头应对网络安全的举措分析

3.5.1 腾讯应对网络安全的举措分析

- (1) 企业内部布局

- (2) 商业联盟布局

- (3) 新兴领域布局

- (4) 创业公司布局

3.5.2 百度应对网络安全的举措分析

- (1) 企业内部布局

- (2) 举办网络安全竞赛

- (3) 创业公司布局

3.5.3 阿里应对网络安全的举措分析

- (1) 企业内部布局

- (2) 组建网络安全联盟

- (3) 云安全布局

(4) 创业公司布局

第4章：网络安全行业细分市场发展状况分析

4.1 网络安全设备市场发展分析

4.1.1 防火墙/VPN市场分析

- (1) 防火墙/VPN市场现状
- (2) 防火墙/VPN市场格局
- (3) 防火墙/VPN市场趋势

4.1.2 IDS/IPS市场分析

- (1) IDS/IPS市场现状
- (2) IDS/IPS市场格局
- (3) IDS/IPS市场趋势

4.1.3 UTM市场分析

- (1) UTM市场现状
- (2) UTM市场格局
- (3) UTM市场趋势

4.2 网络安全软件市场发展分析

4.2.1 WEB业务安全产品市场分析

- (1) WEB业务概述
- (2) WEB市场现状
- (3) WEB市场趋势

4.2.2 安全管理平台市场分析

- (1) 安全管理平台市场概述
- (2) 安全管理平台市场格局
- (3) 安全管理平台市场趋势

4.2.3 终端安全管理市场分析

- (1) 终端安全管理市场现状
- (2) 终端安全管理市场格局
- (3) 终端安全管理市场趋势

4.3 网络安全服务市场发展分析

4.3.1 安全服务市场概述

4.3.2 安全服务市场现状

4.3.3 安全服务市场格局

4.3.4 安全服务市场趋势

第5章：网络安全行业细分领域需求市场分析

5.1 政府领域网络安全需求分析

5.1.1 政府领域网络安全需求特征分析

- (1) 政务领域需求
- (2) 税务领域需求
- (3) 工商领域需求

5.1.2 政府领域网络安全需求现状分析

5.1.3 政府领域网络安全需求潜力分析

5.2 金融领域网络安全需求分析

5.2.1 金融领域网络安全需求特征分析

- (1) 传统金融领域
- (2) 数字金融领域

5.2.2 金融领域网络安全需求现状分析

5.2.3 互联网金融领域网络安全分析

- (1) 互联网金融发展情况
- (2) 互联网金融平台运营监测数据
- (3) 互联网金融漏洞类型
- (4) 互联网金融网站攻击类型

5.2.4 金融领域网络安全需求潜力分析

5.3 运营商领域网络安全需求分析

5.3.1 运营商领域网络安全需求特征分析

5.3.2 运营商领域网络安全需求现状分析

- (1) 门户网站安全
- (2) 互联网安全评估整改
- (3) 白环境
- (4) 网络异常流量清洗
- (5) 互联网数据中心

5.3.3 运营商领域网络安全需求潜力分析

5.4 教育领域网络安全需求分析

5.4.1 教育领域网络安全需求特征分析

5.4.2 教育领域网络安全需求现状分析

5.4.3 教育领域网络安全需求潜力分析

5.5 军工领域网络安全需求潜力分析

5.5.1 军工领域网络安全需求现状分析

5.5.2 军工领域网络安全需求潜力分析

5.6 通信领域网络安全需求分析

5.6.1 通信领域网络安全需求现状分析

- (1) 5G通信安全需求
- (2) 融合通信安全需求

5.6.2 通信领域网络安全需求潜力分析

5.7 航空航天领域网络安全需求分析

5.7.1 航空航天领域网络安全需求特征

- (1) 航空航天对网络依赖程度较高
- (2) 攻击航空网络系统危害后果更严重

5.7.2 航空航天领域网络安全需求现状

5.7.3 航空航天领域网络安全需求潜力

第6章：中国网络安全大领域需求市场分析

6.1 人工智能行业网络安全需求分析

6.1.1 人工智能行业发展现状分析

6.1.2 人工智能行业网络安全需求特征分析

- (1) 组件安全需求
- (2) 技术应用安全需求

6.1.3 人工智能行业网络安全发展现状

- (1) 应用范围日益广泛
- (2) 应用深度还处于初级阶段

6.1.4 人工智能行业网络安全发展趋势

- (1) 加大人工智能安全技术研究，提升人工智能安全防护能力
- (2) 促进人工智能企业与网络安全企业协作，提升技术应用深度和产品成熟度

6.2 物联网行业网络安全需求分析

6.2.1 物联网行业发展现状分析

6.2.2 物联网行业网络安全需求特征分析

- (1) 设备安全需求
- (2) 隐私保护需求
- (3) 通信安全需求

6.2.3 物联网行业网络安全发展现状

6.2.4 物联网行业网络安全发展趋势

- (1) 以攻促防推进物联网安全技术发展
- (2) 联合行业力量打造物联网安全生态

6.3 云安全行业市场需求分析

6.3.1 云安全行业市场需求特征分析

- (1) 中小企业上云还处于初级阶段
- (2) 数据安全需求
- (3) 平台安全需求

6.3.2 云安全行业市场规模分析

6.3.3 云安全行业竞争格局

- (1) 公有云领域
- (2) 私有云领域

6.3.4 云安全行业发展趋势

6.4 区块链行业网络安全需求分析

6.4.1 区块链行业发展现状分析

- (1) 区块链发展现状
- (2) 区块链行业市场规模

6.4.2 区块链行业网络安全需求特征

- (1) 区块链机制安全需求
- (2) 生态安全需求
- (3) 使用安全需求

6.4.3 区块链行业网络安全发展现状

6.4.4 区块链行业网络安全发展趋势

6.5 大数据行业网络安全需求分析

6.5.1 大数据行业发展现状分析

6.5.2 大数据行业网络安全需求特征分析

- (1) 平台安全需求
- (2) 数据安全需求
- (3) 隐私保护安全需求

6.5.3 大数据行业网络安全发展现状

- (1) 平台安全发展现状
- (2) 数据安全发展现状
- (3) 隐私保护发展现状

6.5.4 大数据行业网络安全发展趋势

- (1) 构建大数据安全综合防御体系
- (2) 强化大数据平台安全保护
- (3) 完善数据安全技术体系
- (4) 加强隐私保护核心技术产业化投入

第7章：中国网络安全行业领先企业案例分析

7.1 网络安全行业企业发展总体概况

7.2 国内网络安全领先企业案例分析

7.2.1 哈尔滨安天科技集团股份有限公司经营状况分析

- (1) 企业发展简况分析
- (2) 企业经营情况分析
- (3) 企业技术能力分析
- (4) 企业网络安全业务分析
- (5) 企业销售渠道与网络分析

7.2.2 北京山石网科信息技术有限公司经营状况分析

- (1) 企业发展简况分析
- (2) 企业经营情况分析
- (3) 企业技术能力分析
- (4) 企业网络安全业务分析
- (5) 企业销售渠道与网络分析

7.2.3 杭州安恒信息技术股份有限公司经营状况分析

- (1) 企业发展简况分析
- (2) 企业经营情况分析
- (3) 企业技术能力分析
- (4) 企业网络安全业务分析
- (5) 企业销售渠道与网络分析

7.2.4 北京神州绿盟网络安全科技股份有限公司经营状况分析

- (1) 企业发展简况分析
- (2) 企业经营情况分析
- (3) 企业技术能力分析
- (4) 企业网络安全业务分析
- (5) 企业销售渠道与网络分析

7.2.5 启明星辰信息技术集团股份有限公司经营状况分析

- (1) 企业发展简况分析
- (2) 企业经营情况分析
- (3) 企业技术能力分析
- (4) 企业网络安全业务分析
- (5) 企业销售渠道与网络分析

7.2.6 北京北信源软件股份有限公司经营状况分析

- (1) 企业发展简况分析

(2) 企业经营情况分析

(3) 企业技术能力分析

(4) 企业网络安全业务分析

(5) 企业销售渠道与网络分析

7.2.7 北京神州泰岳软件股份有限公司经营状况分析

(1) 企业发展简况分析

(2) 企业经营情况分析

(3) 企业技术能力分析

(4) 企业网络安全业务分析

(5) 企业销售渠道与网络分析

7.2.8 深圳市优网科技有限公司

(1) 企业发展简况分析

(2) 企业组织机构分析

(3) 企业经营情况分析

(4) 企业主营业务分析

(5) 企业销售渠道与网络分析

7.2.9 飞天诚信科技股份有限公司

(1) 企业发展简况分析

(2) 企业经营情况分析

(3) 企业产品结构分析

(4) 企业产品应用分析

(5) 企业销售渠道与网络分析

7.2.10 任子行网络技术股份有限公司经营情况分析

(1) 企业发展简况分析

(2) 企业经营情况分析

(3) 企业经营模式分析

(4) 企业资质能力分析

(5) 企业网络安全产品方案分析

第8章：网络安全行业投资潜力与策略规划

8.1 网络安全行业发展前景预测（AK ZJH）

8.1.1 行业发展环境分析

(1) 政策支持分析

(2) 技术推动分析

(3) 市场需求分析

8.1.2 行业发展前景预测

8.2 网络安全行业发展趋势预测

8.2.1 行业整体趋势预测

8.2.2 企业发展趋势预测

- (1) 品牌集中度将提高
- (2) 企业多元化发展
- (3) 国内企业将快速崛起

8.2.3 产品发展趋势预测

8.2.4 技术发展趋势预测

- (1) 态势感知迈向产品应用阶段
- (2) 虚拟化技术推动安全产品形态演进
- (3) 人工智能有望驱动网络安全技术革新

8.3 网络安全行业投资潜力分析

8.3.1 行业投资热潮分析

8.3.2 行业投资推动因素

- (1) 区域政策扶持推动
- (2) 财政支持推动
- (3) 产业联盟推动

8.3.3 行业投资主体分析

8.3.4 行业投资切入方式

8.3.5 行业投资壁垒分析

- (1) 技术壁垒
- (2) 人才壁垒
- (3) 品牌壁垒
- (4) 资质壁垒

8.3.6 行业投资现状分析

8.4 网络安全行业投资策略规划

8.4.1 行业投资方式策略

8.4.2 行业投资领域策略

- (1) 安全即服务
- (2) 大数据驱动的威胁情报
- (3) 企业级移动安全

8.4.3 行业产品创新策略

- (1) Virsec Trusted Execution
- (2) 趋势科技Writing Style DNA

- (3) Forcepoint Dynamic Data Protection
- (4) Unisys Stealth
- (5) Tripwire Container Analyzer Service
- (6) SonicWall NSv Virtual Firewall
- (7) Centrify Next-Gen Access
- (8) CylanceOptics
- (9) Kenna Application Risk Module
- (10) CrowdStrike Falcon Endpoint Protection Complete

8.4.4 行业商业模式策略

图表目录：

图表1：网络舆论危机信息传播模式

图表2：网络安全产品和服务

图表3：2015-2019年我国网民规模数量及增长（单位：亿人，%）

图表4：2019年以来部分重大网络安全突发事件

图表5：防火墙工作原理示意图

图表6：VPN分类标准

图表7：网络安全技术的发展阶段

图表8：2015-2019年有关网络安全技术的主要会议及会议内容

图表9：2015-2019年打击电信诈骗专项行动成果（单位：万个，万人，万张，亿元）

图表10：2015-2019年有关网络安全技术的主要会议及会议内容

更多图表见正文.....

详细请访问：<https://www.huaon.com/detail/493962.html>