

2026-2032年中国AI+网络安全行业市场竞争现状 及发展趋向研判报告

报告大纲

一、报告简介

智研咨询发布的《2026-2032年中国AI+网络安全行业市场竞争现状及发展趋向研判报告》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.chyxx.com/research/1280272.html>

报告价格：电子版: 9800元 纸介版：9800元 电子和纸介版: 10000元

订购电话: 400-700-9383、010-60343812、010-60343813

电子邮箱: kefu@chyxx.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

智研咨询发布的《2026-2032年中国AI+网络安全行业市场竞争现状及发展趋向研判报》共十二章。首先介绍了AI+网络安全行业市场发展环境、AI+网络安全整体运行态势等，接着分析了AI+网络安全行业市场运行的现状，然后介绍了AI+网络安全市场竞争格局。随后，报告对AI+网络安全做了重点企业经营状况分析，最后分析了AI+网络安全行业发展趋势与投资预测。您若想对AI+网络安全产业有个系统的了解或者想投资AI+网络安全行业，本报告是您不可或缺的重要工具。

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家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：

第一章 AI+网络安全行业概述

1.1 AI+网络安全的定义与技术内涵

1.1.1 AI+网络安全的概念界定

1.1.2 与传统网络安全的本质区别

1.1.3 AI+网络安全的技术分层架构

1.2 AI赋能网络安全的核心技术特征

1.2.1 威胁检测智能化

1.2.2 安全运营自动化

1.2.3 攻击面管理动态化

1.2.4 安全知识沉淀体系化

1.2.5 对抗攻防升级

1.3 AI+网络安全的战略价值

1.3.1 国家网络空间安全的智能底座

1.3.2 数字经济基础设施的安全保障

1.3.3 网络安全产业转型升级的核心引擎

1.3.4 AI自身安全治理的技术支撑

1.4 AI+网络安全技术发展历程

1.4.1 全球技术演进

1.4.2 中国技术发展路径

1.4.3 关键里程碑事件梳理

1.5 本报告数据来源及研究方法

1.5.1 本报告数据来源

1.5.2 本报告研究方法

第二章 中国AI+网络安全行业发展政策研究

2.1 行业监管体系及机构职能

2.1.1 监管体系

2.1.2 核心监管机构

2.2 AI+网络安全行业标准建设

2.2.1 国际标准参与

2.2.2 国内标准研制现状

2.2.3 AI安全检测评估标准体系

2.2.4 大模型安全评测标准建设进展

2.2.5 标准体系瓶颈与完善方向

2.3 行业主要政策规划汇总及解读

2.4 政策影响分析

2.4.1 政策驱动下的合规需求爆发

2.4.2 AI安全产品与服务的准入制度

2.4.3 数据跨境流动与AI训练数据安全监管

2.4.4 当前政策体系的短板与完善方向

第三章 AI+网络安全产业成本拆解与降本路径

3.1 成本结构拆解

3.2 中长期降本路径

3.3 隐性成本与技术对冲

3.4 AI+网络安全成本研究小结

第四章 中国AI+网络安全行业现状调查

4.1 中国AI+网络安全行业发展历程

4.1.1 规则引擎时期（2015年以前）

4.1.2 机器学习引入期（2016-2020）

4.1.3 大模型赋能爆发期（2021-2024）

4.1.4 安全Agent原生阶段（2025至今）

4.2 行业运行现状

4.2.1 市场规模与增长态势

- 4.2.2 产业发展阶段
- 4.2.3 产业发展核心痛点
- 4.2.4 投融资动态
- 4.2.5 行业发展驱动因素
- 4.3 市场现状与落地验证情况
 - 4.3.1 国内AI安全产品渗透率
 - 4.3.2 典型客户采购行为变化
 - 4.3.3 中国AI安全企业营收规模分布
- 4.4 中国AI+网络安全主要玩家及产品谱系调查
 - 4.4.1 传统安全巨头AI转型
 - 4.4.2 AI原生安全新锐
 - 4.4.3 互联网大厂安全AI能力外溢
 - 4.4.4 国家队与科研院所
- 4.5 行业竞争格局调查
 - 4.5.1 市场份额与订单获取情况
 - 4.5.2 技术梯队划分
 - 4.5.3 竞争态势演变
- 4.6 中国AI+网络安全产业链分析
- 4.7 AI+网络安全行业现状调查小结

第五章 AI+网络安全产业链调查——上游（AI基础设施与安全数据）

- 5.1 AI算力基础设施
 - 5.1.1 安全推理GPU/加速卡现状与主要玩家
 - 5.1.2 安全专用推理芯片/边缘AI芯片
 - 5.1.3 算力国产化替代进程
- 5.2 安全数据资源与数据治理
 - 5.2.1 威胁情报数据
 - 5.2.2 安全日志与流量数据
 - 5.2.3 合成安全数据生成技术
 - 5.2.4 安全数据标注与治理服务
- 5.3 AI基础模型与预训练能力
 - 5.3.1 通用大模型在安全领域的适配现状
 - 5.3.2 安全领域垂直大模型发展现状
 - 5.3.3 开源安全模型生态
- 5.4 上游关键挑战

- 5.4.1 安全领域高质量训练语料稀缺
- 5.4.2 高端AI算力“卡脖子”现状
- 5.4.3 安全数据标注的专业性壁垒
- 5.4.4 模型可解释性与安全合规性矛盾
- 5.5 上游产业链研究总结

第六章 AI+网络安全产业链调查——中游（AI安全产品与平台集成）

- 6.1 AI赋能安全检测类产品
 - 6.1.1 AI驱动的入侵检测/防御系统（AI-IDS/IPS）
 - 6.1.2 AI恶意软件检测与沙箱分析
 - 6.1.3 AI驱动的网络流量分析（NTA/NDR）
 - 6.1.4 AI漏洞挖掘与自动化渗透
- 6.2 AI赋能安全运营类产品
 - 6.2.1 AI安全运营中心（AISOC）
 - 6.2.2 安全编排自动化与响应（SOAR）+ AI
 - 6.2.3 AI安全告警分诊与降噪
 - 6.2.4 安全大模型助手/安全Copilot
- 6.3 AI赋能数据安全与隐私保护
 - 6.3.1 AI驱动的数据分类分级
 - 6.3.2 AI驱动的数据泄露检测（DLP智能化）
 - 6.3.3 联邦学习/隐私计算在安全场景的应用
 - 6.3.4 AI驱动的隐私合规自动化
- 6.4 AI赋能身份与访问管理（IAM）
 - 6.4.1 AI驱动的行为异常检测（UEBA）
 - 6.4.2 智能化零信任架构
 - 6.4.3 AI深度伪造检测与反欺诈
- 6.5 Security for AI（AI自身的安全防护）
 - 6.5.1 AI模型安全评测与红队测试
 - 6.5.2 大模型防火墙与内容安全
 - 6.5.3 AI供应链安全检测
 - 6.5.4 对抗样本防御与模型鲁棒性加固
- 6.6 中游集成与平台化趋势
 - 6.6.1 安全厂商的平台化战略
 - 6.6.2 大模型+小模型协同架构
 - 6.6.3 中游产业链发展关键挑战

6.7 中游产业链研究总结

第七章 AI+网络安全产业链调查——下游应用场景（关键基础设施安全防护）

7.1 关键基础设施安全防护需求分析

7.1.1 关基保护条例下的合规刚需

7.1.2 能源、金融、交通、通信等重点行业AI安全需求差异

7.2 AI赋能网络安全态势感知

7.2.1 全域威胁态势实时感知

7.2.2 攻击链自动还原与溯源

7.3 AI赋能安全应急响应

7.3.1 自动化事件响应与处置

7.3.2 安全事件智能研判与报告生成

7.4 行业主要玩家与典型案例

7.4.1 主要玩家

7.4.2 典型案例

7.5 2026-2032年AI+网络安全在关基防护领域应用市场空间测算

7.6 AI+网络安全在关基防护领域应用发展趋势

7.6.1 从被动防御到主动免疫

7.6.2 安全大模型赋能行业级安全大脑

7.7 AI+网络安全在关基防护领域应用研究小结

第八章 AI+网络安全产业链调查——下游应用场景（企业安全运营智能化）

8.1 企业安全运营痛点与智能化需求

8.1.1 告警疲劳与安全人才缺口

8.1.2 安全运营效率提升诉求

8.2 AI驱动的安全运营中心（SOC）升级

8.2.1 智能告警分诊与优先级排序

8.2.2 AI辅助威胁狩猎

8.2.3 自然语言交互式安全查询

8.3 AI赋能云安全与SaaS安全

8.3.1 云工作负载保护平台（CWPP）+ AI

8.3.2 云安全态势管理（CSPM）智能化

8.3.3 SaaS安全接入代理（CASB）+ AI

8.4 中小企业安全普惠化

8.4.1 AI降低安全服务使用门槛

8.4.2 安全托管服务（MSS）+ AI的商业模式创新

8.5 主要玩家与典型案例

8.5.1 主要玩家

8.5.2 典型案例

8.6 2026-2032年AI+网络安全在企业安全运营领域应用市场空间测算

8.7 AI+网络安全在企业安全运营领域应用发展趋势

8.8 AI+网络安全在企业安全运营领域应用研究小结

第九章 AI+网络安全产业链调查——下游应用场景（AI安全治理与合规）

9.1 AI安全治理需求分析

9.1.1 生成式AI服务的安全合规要求

9.1.2 AI大模型备案与安全评估

9.1.3 AI伦理与可信AI评测

9.2 AI内容安全与深度伪造治理

9.2.1 AI生成内容（AIGC）检测技术

9.2.2 深度伪造检测与溯源

9.2.3 AI生成式钓鱼邮件/社工攻击防御

9.3 数据安全与隐私保护合规

9.3.1 AI训练数据合规审查

9.3.2 个人信息保护合规自动化

9.3.3 数据跨境安全评估

9.4 主要玩家与典型案例

9.4.1 主要玩家

9.4.2 典型案例

9.5 2026-2032年AI+网络安全在AI安全治理领域应用市场空间测算

9.6 AI+网络安全在AI安全治理领域应用发展趋势

9.6.1 从合规驱动到内生安全

9.6.2 AI治理平台化与自动化

9.7 AI+网络安全在AI安全治理领域应用研究小结

第十章 中国AI+网络安全行业重点企业推荐

10.1 深信服科技股份有限公司

10.1.1 企业概况

10.1.2 企业优势分析

10.1.3 产品/服务特色

10.1.4 公司经营状况

10.1.5 公司发展规划

10.2 安恒信息技术股份有限公司

10.2.1 企业概况

10.2.2 企业优势分析

10.2.3 产品/服务特色

10.2.4 公司经营状况

10.2.5 公司发展规划

10.3 启明星辰信息技术集团股份有限公司

10.3.1 企业概况

10.3.2 企业优势分析

10.3.3 产品/服务特色

10.3.4 公司经营状况

10.3.5 公司发展规划

10.4 天融信科技集团股份有限公司

10.4.1 企业概况

10.4.2 企业优势分析

10.4.3 产品/服务特色

10.4.4 公司经营状况

10.4.5 公司发展规划

10.5 微步在线技术（北京）有限公司

10.5.1 企业概况

10.5.2 企业优势分析

10.5.3 产品/服务特色

10.5.4 公司经营状况

10.5.5 公司发展规划

10.6 华云安（北京）技术有限公司

10.6.1 企业概况

10.6.2 企业优势分析

10.6.3 产品/服务特色

10.6.4 公司经营状况

10.6.5 公司发展规划

10.7 北京瑞莱智慧科技有限公司（RealAI）

10.7.1 企业概况

10.7.2 企业优势分析

10.7.3 产品/服务特色

10.7.4 公司经营状况

10.7.5 公司发展规划

10.8 斗象科技（深圳）有限公司

10.8.1 企业概况

10.8.2 企业优势分析

10.8.3 产品/服务特色

10.8.4 公司经营状况

10.8.5 公司发展规划

10.9 华为技术有限公司

10.9.1 企业概况

10.9.2 企业优势分析

10.9.3 产品/服务特色

10.9.4 公司经营状况

10.9.5 公司发展规划

10.10 长亭科技（北京）有限公司

10.10.1 企业概况

10.10.2 企业优势分析

10.10.3 产品/服务特色

10.10.4 公司经营状况

10.10.5 公司发展规划

第十一章 AI+网络安全行业发展前景与市场空间测算

11.1 行业发展趋势

11.1.1 技术趋势

11.1.2 产品趋势

11.1.3 产业趋势

11.1.4 竞争趋势

11.2 行业发展主要风险

11.2.1 AI幻觉导致安全误判的风险

11.2.2 AI被攻击者利用的安全攻防升级风险

11.2.3 算力成本与商业模式可持续性风险

11.2.4 合规政策快速变化的风险

11.2.5 AI安全人才严重短缺的风险

11.3 2026-2032年市场空间测算

11.3.1 全球AI+网络安全市场规模预测

11.3.2 中国AI+网络安全市场规模测算

(1) 基于网络安全整体市场中AI渗透率的测算

(2) 基于关键下游行业采购需求的测算

11.3.3 细分市场空间

(1) AI安全检测市场

(2) AI安全运营市场

(3) AI数据安全市场

(4) AI安全治理与合规市场

第十二章 中国AI+网络安全产业研究总结与投资机会透视

12.1 研究总结

12.1.1 市场特点总结

12.1.2 技术趋势总结

12.1.3 企业格局总结

12.2 2026-2032年投资机会多维透视

12.2.1 市场痛点分析

12.2.2 行业爆发点分析

12.2.3 产业链投资机会

12.2.4 新进入者投资机会

12.3 产业发展策略与投资建议

12.3.1 强化安全领域AI基础模型自主能力

12.3.2 推动安全数据开放共享与标准统一

12.3.3 鼓励“安全大模型+安全Agent”创新模式

12.3.4 构建AI安全攻防演练与评测体系

12.3.5 培育复合型AI安全人才梯队

12.4 产业发展壁垒

12.4.1 技术壁垒

12.4.2 数据壁垒

12.4.3 人才壁垒

12.4.4 准入壁垒

12.4.5 生态壁垒

详细请访问：<https://www.chyxx.com/research/1280272.html>