

2026-2031年中国入侵检测系统行业全景调研与发展趋势预测报告

报告简介

入侵检测系统行业作为网络安全防御体系的核心组件与主动安全防护的关键技术支撑，是保障国家关键信息基础设施安全、维护数字经济稳定运行的战略性基础产业。本报告所研究的入侵检测系统(IDS)行业，是指通过监控网络流量或系统活动，识别违反安全策略行为或潜在攻击迹象，并实时告警或主动响应的安全防护软件与硬件产业，涵盖基于网络的入侵检测系统(NIDS)、基于主机的入侵检测系统(HIDS)、基于应用的入侵检测系统(AIDS)及分布式入侵检测系统等形态，并延伸至威胁情报分析、安全态势感知及自动化响应编排等高级功能。该行业横跨计算机网络、密码学、人工智能、大数据分析及安全攻防等多个高技术领域，具有技术迭代极快、攻防对抗性强、误报漏报敏感、合规要求严苛等典型特征。随着网络攻击手段智能化、供应链攻击频发及关键基础设施数字化程度加深，入侵检测已从传统的边界防御补充手段向云网端一体化智能安全运营的核心能力演进，其产业价值正从单一检测告警向威胁狩猎、攻击面管理及安全决策支持深度延伸。

当前中国入侵检测系统产业正处于从“规则驱动”向“智能驱动”转型、从“单品部署”向“平台运营”升级的关键攻坚期。经过多年发展，我国已在特征库匹配、异常流量检测及特定行业场景适配方面形成技术积累，部分企业在基于机器学习的恶意代码检测、加密流量分析及威胁情报关联方面取得突破，国产替代在政务、金融、能源等关键行业稳步推进，安全运营中心(SOC)建设带动检测能力集中化。展望“十五五”时期，中国入侵检测系统行业将迎来关基保护强化与AI安全攻防共振的战略机遇。技术演进维度，基于生成式AI的攻击模拟与防御对抗、多源异构数据的关联分析与攻击链重构、以及安全大模型的推理决策能力，将推动入侵检测从“特征匹配”向“行为理解”乃至“意图预测”能力跃迁；场景拓展维度，随着工业互联网、车联网及智慧城市关键基础设施的数字化，面向OT环境、边缘计算及云原生架构的轻量化、嵌入式检测能力将快速成熟；运营变革维度，XDR(扩展检测与响应)平台的普及、安全智能体的自动化处置能力及安全运营即服务(SOCaaS)模式的推广，将重塑企业安全建设模式与产业价值分配；生态协同维度，威胁情报共享机制、安全漏洞协同处置及产学研联合攻防演练的深化，将提升整体网络安全防御

韧性;合规驱动维度，关基保护条例、数据安全法等及等保2.0的深入实施，将持续释放高端检测能力的刚性需求。

本研究咨询报告由北京中道泰和信息咨询有限公司领衔撰写，在大量周密的市场调研基础上，主要依据了国家统计局、国家商务部、国家发改委、国家经济信息中心、国务院发展研究中心、国家海关总署、全国商业信息中心、中国经济景气监测中心、51行业报告网、全国及海外相关报刊杂志的基础信息以及入侵检测系统行业研究单位等公布和提供的大量资料。报告对我国入侵检测系统行业的供需状况、发展现状、子行业发展变化等进行了分析，重点分析了国内外入侵检测系统行业的发展现状、如何面对行业的发展挑战、行业的发展建议、行业竞争力，以及行业的投资分析和趋势预测等等。报告还综合了入侵检测系统行业的整体发展动态，对行业在产品方面提供了参考建议和具体解决办法。报告对于入侵检测系统产品生产企业、经销商、行业管理部门以及拟进入该行业的投资者具有重要的参考价值，对于研究我国入侵检测系统行业发展规律、提高企业的运营效率、促进企业的发展壮大有学术和实践的双重意义。 本报告也可以用于专精特新“小巨人”申请申报。

报告目录

第一章 入侵检测系统行业概述

第一节 入侵检测系统的定义与功能

一、入侵检测系统的基本概念界定

二、ids与ips的技术区别与联系

三、入侵检测在网络安全体系中的定位

第二节 入侵检测系统的主要分类

一、按检测技术分类

二、按部署位置分类

三、按工作模式分类

第三节 入侵检测系统产业链结构

- 一、上游：芯片、操作系统、数据库、威胁情报
- 二、中游：ids/ips产品研发、生产、集成
- 三、下游：政府、金融、电信、能源、企业、云服务商

第二章 全球入侵检测系统市场发展现状

第一节 全球入侵检测系统市场规模分析

- 一、2023-2025年全球市场规模及增速
- 二、硬件、软件、服务结构占比
- 三、2026-2031年全球市场增长预测

第二节 全球入侵检测技术演进趋势

- 一、ai/ml驱动的智能检测
- 二、云原生与saas化部署
- 三、威胁情报与协同防御

第三节 全球产业格局与区域特征

- 一、美国技术领先与厂商集中
- 二、欧洲合规驱动与隐私保护
- 三、亚太市场快速增长与本土化

第三章 中国入侵检测系统行业发展环境

第一节 网络安全威胁环境

- 一、apt攻击与高级持续性威胁
- 二、勒索软件与供应链攻击
- 三、物联网与工控安全威胁

第二节 政策法规与合规环境

一、网络安全等级保护制度

二、关键信息基础设施保护

三、数据安全与个人信息保护

第三节 数字化转型与it环境

一、企业上云与混合it架构

二、远程办公与零信任架构

三、5g与边缘计算安全

第四章 中国入侵检测系统市场供需分析

第一节 市场需求结构分析

一、政府与公共部门需求

二、金融行业需求

三、电信与互联网行业需求

四、能源与工业需求

五、医疗与教育行业需求

第二节 市场供给能力分析

一、国内ids/ips厂商数量与分布

二、产品技术成熟度与功能覆盖

三、威胁情报与检测能力

第三节 供需匹配与缺口分析

一、高端检测引擎供给不足

二、行业定制化解决方案欠缺

三、云原生安全能力待提升

第五章 中国入侵检测系统市场规模与增长预测

第一节 2023-2025年市场规模回顾

- 一、整体市场规模及增速
- 二、硬件、软件、云服务结构
- 三、行业分布与区域特征

第二节 2026-2031年市场规模预测

- 一、总量规模预测模型
- 二、细分产品形态增长预测
- 三、云服务与托管安全服务增长

第三节 市场增长驱动因素

- 一、等保2.0与关基保护强制要求
- 二、网络攻击频率与 sophistication 提升
- 三、云化与数字化安全需求

第六章 网络入侵检测/防御系统 (nids/nips) 市场分析

第一节 nids/nips技术架构

- 一、旁路检测与串联防御
- 二、深度包检测(dpi)技术
- 三、流量分析与行为建模

第二节 硬件设备市场

- 一、盒式与框式设备
- 二、吞吐量与检测性能
- 三、国产芯片与自主可控

第三节 软件与虚拟化部署

一、软件定义nids/nips

二、虚拟化与容器化部署

三、nfv与云网融合

第七章 主机入侵检测/防御系统 (hids/hips) 市场分析

第一节 hids/hips技术特征

一、系统调用监控与文件完整性

二、内存保护与恶意代码检测

三、主机行为分析与edr融合

第二节 服务器与终端防护

一、服务器工作负载保护

二、终端检测与响应(edr)

三、统一端点安全(ues)

第三节 容器与云工作负载安全

一、容器运行时安全

二、无服务器函数安全

三、cwpp与hips融合

第八章 应用入侵检测系统 (aids) 与web安全

第一节 web应用防火墙(waf)集成

一、owasp top 10防护

二、api安全与bot管理

三、waap与云原生waf

第二节 数据库活动监控(dam)

一、sql注入与异常查询检测

二、数据库审计与合规

三、敏感数据访问监控

第三节 应用运行时自我保护(rasp)

一、应用层攻击实时阻断

二、与aids的协同

三、devsecops集成

第九章 智能检测与ai驱动技术

第一节 机器学习在入侵检测中的应用

一、异常行为建模与基线学习

二、恶意流量分类与预测

三、误报率优化与自适应

第二节 深度学习与高级威胁检测

一、流量指纹与协议识别

二、加密流量分析(eti)

三、对抗样本与模型安全

第三节 威胁情报与协同防御

一、ioc共享与情报消费

二、att&ck框架映射

三、soar与自动化响应

第十章 云原生与saas化入侵检测

第一节 云原生ids/ips架构

一、微服务与sidecar部署

二、服务网格安全集成

三、ebpf与内核级监控

第二节 安全即服务(secaas)

一、托管检测与响应(mdr)

二、云访问安全代理(casb)集成

三、sase与边缘安全

第三节 多云与混合云安全

一、跨云统一安全策略

二、云工作负载态势管理(cwpp)

三、云安全态势管理(cspm)联动

第十一章 入侵检测系统行业竞争格局

第一节 行业竞争态势分析

一、市场集中度与cr5

二、综合安全厂商与专业厂商

三、硬件、软件、云服务分化

第二节 国内主要企业竞争力

一、传统网络安全厂商

二、新兴云安全厂商

三、威胁情报与ai安全厂商

第三节 国际竞争与合作

- 一、国际厂商在华布局
- 二、国产替代与自主可控
- 三、技术引进与生态合作

第十二章 入侵检测系统成本与价格分析

第一节 成本结构分析

- 一、研发与威胁情报投入
- 二、硬件与芯片成本
- 三、云服务与运营成本

第二节 价格形成机制

- 一、产品许可与订阅模式
- 二、性能规格与定价
- 三、行业解决方案溢价

第三节 成本优化路径

- 一、硬件国产化与芯片替代
- 二、ai模型效率优化
- 三、云化与规模化降本

第十三章 入侵检测系统行业风险分析

第一节 技术风险

- 一、ai模型误报与漏报
- 二、加密流量检测挑战
- 三、供应链与0day漏洞

第二节 市场与竞争风险

一、同质化竞争与价格战

二、云厂商安全服务挤压

三、人才短缺与流动

第三节 政策与合规风险

一、数据出境安全审查

二、密码与自主可控要求

三、行业监管标准变化

第十四章 入侵检测系统行业投资机会分析

第一节 细分技术投资机会

一、ai驱动智能检测引擎

二、云原生安全架构

三、威胁情报与主动防御

第二节 应用场景投资机会

一、工业互联网安全

二、车联网与物联网安全

三、数据安全与隐私计算

第三节 商业模式投资机会

一、mdr与托管安全服务

二、安全运营中心(soc)即服务

三、威胁情报订阅服务

第十五章 2026-2031年入侵检测系统行业发展趋势与建议

第一节 技术发展趋势

一、ai原生与自主进化

二、零信任架构深度融合

三、量子安全与后量子密码

第二节 市场发展趋势

一、从边界防御到持续验证

二、从单点产品到平台化

三、从合规驱动到价值驱动

第三节 战略建议

一、对安全厂商的战略建议

二、对行业用户的建议

三、对投资者的建议

图表目录

图表：ids/ips技术分类与部署架构

图表：入侵检测系统产业链结构图

图表：2023-2025年全球入侵检测系统市场规模及增速

图表：全球网络安全市场ids/ips占比

图表：2026-2031年全球入侵检测系统市场规模预测

图表：主要国家网络安全支出结构对比

图表：中国网络安全威胁事件统计

图表：2025年中国入侵检测系统需求结构

图表：各行业网络安全建设投入占比

图表：国内ids/ips厂商技术能力评估

图表：2023-2025年中国入侵检测系统市场规模

图表：2026-2031年中国入侵检测系统市场规模预测

图表：2026-2031年细分产品形态增长预测

图表：nids/nips主要性能指标对比

图表：国产芯片在ids设备中的应用

图表：edr与hids/hips技术融合趋势

图表：云工作负载安全(cwpp)功能覆盖

图表：容器安全与主机安全协同

图表：waap与waf技术演进对比

图表：应用层攻击检测技术栈

图表：ai/ml在入侵检测中的应用场景

图表：加密流量检测(eti)技术原理

图表：云原生安全架构与sidecar部署

图表：secaas与传统安全模式对比

图表：2025年中国入侵检测系统市场集中度

图表：入侵检测系统行业竞争格局矩阵

图表：入侵检测系统成本结构与定价模式

图表：重点行业ids/ips采购价格区间

图表：入侵检测系统行业风险因素评估矩阵

图表：入侵检测系统细分领域投资价值评估

图表：入侵检测系统技术演进与零信任融合路线图

图表：2026-2031年中国入侵检测系统行业核心指标预测汇总

把握投资 决策经营！

咨询订购 请拨打 400-886-7071 (免长途费) Email : kf@51baogao.cn

报告编号：4067016

本文地址：<https://www.51baogao.cn/baogao/20260328/4067016.shtml>

在线订购：[点击这里](#)