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

图表目录

图表：2026-2031年中国入侵检测系统行业核心指标预测汇总