



2026-2032全球与中国人工智能网络安全解决方案市场调研报告

【行业】:软件及商业服务 【报告编码】:178883392726907

【出版时间】:2026-09-08 【订购热线】:+86 180 2246 3983

【电子邮件】:market@winmarketresearch.com

【报告价格】: ¥18900.00 中文电子版
¥18900.00 英文电子版
¥37800.00 中文+英文电子版

内容摘要

根据统计及预测，2025年全球人工智能网络安全解决方案市场销售额达到了70.00亿美元，预计2032年将达到186.0亿美元，年复合增长率（CAGR）为15.1%（2026-2032）。地区层面来看，中国市场在过去几年变化较快，2025年市场规模为百万美元，约占全球的%，预计2032年将达到百万美元，届时全球占比将达到%。

本文研究全球及中国市场人工智能网络安全解决方案现状及未来发展趋势，侧重分析全球及中国市场的主要企业，同时对比北美、欧洲、中国、日本、东南亚和印度等地区的现状及未来发展趋势。

人工智能网络安全解决方案是以智能分析、行为识别、自动威胁响应、身份访问控制和跨环境安全编排为核心的综合安全平台，可保护企业云上负载、分支网络、远程用户、数据中心、应用系统和混合基础设施。2025年行业平均毛利率约为70%。在上游环节，关键投入包括服务器、交换机和存储设备，代表性供应商包括Dell Technologies、Cisco Systems和SK hynix，为平台提供算力、网络交换和数据存储资源。中游环节主要围绕智能安全模型集成、威胁情报处理、行为分析、安全策略编排、流量分析、身份集成、日志管理、自动化事件响应、高可用部署、安全规则更新和平台运营展开，这些能力共同决定检测准确性、响应效率、防护覆盖范围、服务稳定性、扩展性和客户黏性。下游主要用于银行金融服务与保险、零售、信息技术和电信领域，可保护云上工作负载、分支网络、线上交易系统、客户数据、远程访问环境、应用系统和混合企业网络，代表客户包括JPMorgan Chase、Walmart和Verizon。

人工智能网络安全解决方案的需求，将更多来自企业在云端、应用、远程访问和分布式基础设施中提升威胁判断速度的需求。银行金融服务与保险领域关注交易安全、欺诈信号、合规监测和敏感客户数据保护；零售行业需要加强电商平台、支付系统、门店网络和会员数据防护；信息技术与电信行业则面对更大流量、更复杂用户和持续攻击面。后续竞争将集中在检测准确性、自动响应、身份上下文、误报控制、告警可解释性、合规报表以及与现有安全运营体系的集成能力。

本文重点分析在全球及中国有重要角色的企业，分析这些企业人工智能网络安全解决方案产品的市场规模、市场份额、市场定位、产品类型以及发展规划等。

主要企业包括：

Palo Alto Networks (美国)

Fortinet (美国)

Check Point Software Technologies (以色列)

Zscaler (美国)

Cisco (美国)

Cloudflare (美国)

Netskope (美国)

Cato Networks (以色列)

Amazon Web Services (美国)

Microsoft Azure (美国)

Google Cloud (美国)

Oracle Cloud Infrastructure (美国)

Trend Micro (日本)

Akamai Technologies (美国)

腾讯云 (中国)

阿里云 (中国)

华为云 (中国)

按照不同产品类型，包括如下几个类别：

防火墙即服务平台

云原生下一代防火墙平台

云Web应用防火墙平台

其他

按照不同管理架构，包括如下几个类别：

集中式防火墙

分布式防火墙

其他

按照不同吞吐能力，包括如下几个类别：

吞吐量