



2026-2032全球与中国AI模型安全测试平台市场调研报告

【行业】:软件及商业服务 【报告编码】:179264882806502

【出版时间】:2026-10-22 【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AI模型安全测试平台市场销售额达到了18.89亿美元，预计2032年将达到75.82亿美元，年复合增长率（CAGR）为22.0%（2026-2032）。

本文研究全球及中国市场AI模型安全测试平台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。

AI模型安全测试平台是面向机器学习模型、基础模型、生成式人工智能应用及自主智能体开展主动安全、安全性与对抗鲁棒性验证的软件平台。其测试对象覆盖模型权重与序列化文件、训练及微调数据、推理接口、系统提示词、检索增强生成链路、插件、工具调用、模型上下文协议服务器、记忆、权限及多智能体交互关系。平台核心能力通常涵盖模型文件与依赖扫描、对抗样本生成、提示注入与越狱测试、数据投毒与后门检测、模型反演与提取测试、自适应多轮攻击、场景化风险题库、自动化结果判定、漏洞复现及整改验证。产品主要以SaaS、API、专属云、本地化系统或网络安全平台集成模块交付，可用于模型开发、上线前验证、第三方模型验收、CI/CD安全门禁、版本回归测试、持续红队及审计证据生成，主要服务于科技、金融、政府、医疗、关键基础设施及其他部署高影响AI系统的组织。

核心总结

北美约占2025年市场收入的58%-64%

中国约占2025年市场收入的11%-16%

企业级专用平台年合同价值通常约为7.5万-30万美元

需求正由上线前评估转向智能体及AI工作流持续测试

行业发展趋势

AI模型安全测试平台正由静态越狱题库和一次性模型审查，演变为覆盖模型、应用、智能体及AI供应链的持续验证基础设施。自适应攻击智能体开始针对RAG链路、工具权限、记忆系统、MCP服务器及多智能体工作流执行多轮、多语言和上下文感知攻击；原本相对独立的模型文件扫描与行为红队测试也逐步汇入统一AI安全平台。客户需求从攻击数量转向可复现证据、低误报、业务场景适配、私有化部署、版本关联回归测试及开发流程集成。行业长期方向是形成“漏洞发现—工程整改—自动复测—发布决策—运行时策略更新”闭环。基础提示测试和常见漏洞扫描将趋于标准化，未知攻击发现、复杂权限验证、多模态评测及真实业务影响证明将成为差异化价值来源。

市场动态

驱动因素

企业加速部署RAG应用、代码助手、智能客服和自主流程智能体，持续扩大AI攻击面及系统复杂度。模型升级、提示词调整、知识库更新和工具接入均可能引入新风险，使安全测试由一次性评估转变为持续性需求。受监管行业还需要证明AI系统在全生命周期内保持安全、稳健和可追溯。NIST生成式AI风险管理框架强调上线前测试和对抗性演练，欧盟人工智能法案则强化稳健性及风险评估义务。这些因素推动AI模型安全测试正式进入AI开发、采购、发布和治理流程。

限制因素

市场普及受到产品边界不清、平台间缺乏可比性，以及安全测试与AI治理、可观测性、运行时防护和咨询合同难以拆分等因素限制。测试先进模型与智能体通常需要较高推理成本、专业攻击研究、行业数据集及人工复核，复杂发现也难以完全自动判定。开源扫描器和云平台内置评测工具对基础提示测试及标准化漏洞检查形成价格压力。中小客户在AI应用尚未进入关键业务前，可能继续依赖内部脚本或周期性服务；涉及敏感模型的组织若无法获得本地处理、隔离网部署及数据驻留支持，也可能推迟采购。

市场机遇

智能体与工具链安全测试构成最突出的增量机会，重点覆盖权限、记忆、跨智能体信任、MCP服务器、API操作以及外部内容触发的间接提示注入。模型供应链验证、恶意模型文件识别、第三方模型验收、多语言测试、多模态系统和行业专用攻击库同样具备发展空间。厂商可通过将测试发现转化为可复用回归用例、CI/CD发布门禁、整改建议、合规映射及运行时控制策略，提高单一客户合同价值。私有化部署和本地风险题库在金融、政府、国防、医疗、通信、能源等数据敏感或运营后果较高的行业具有更明确的商业机会。

行业风险与挑战

行业核心挑战是模型能力、防护机制、智能体架构及攻击方法快速演化，平台必须持续维护测试有效性。攻击数量多并不等同于覆盖质量高，厂商还需证明漏洞可利用性、结果可复现性、业务相关性及误报控制水平。现有标准化基准难以充分比较自适应攻击及复杂智能体行为，不同平台测试结果的一致性有限。测试功能又经常与AI安全态势管理、运行时护栏、治理或专业服务捆绑，增加收入归因和采购比较难度。行业整合有利于扩大渠道，但可能削弱测试独立性；基础功能快速商品化则要求专业厂商持续投入攻击研究并建立可量化的技术差异。

价值链分析

上游主要由基础模型、开源模型仓库、云计算及推理服务、安全框架、漏洞知识库、攻击数据集、评测基准和对抗机器学习研究构成，决定平台测试覆盖、推理成本、模型可访问程度以及新攻击方法产品化速度。中游厂商通过攻击生成引擎、模型与依赖扫描器、自动判定器、测试编排系统、报告工具、合规映射、工程集成和私有化部署能力，将研究成果转化为商业平台。主要成本来自安全研究、模型推理、产品研发、攻击库维护、企业系统集成及客户支持，持续更新能力对产品竞争力和毛利水平具有重要影响。

下游客户涵盖基础模型开发商、AI应用团队、网络安全部门、模型风险管理职能、审计机构及受监管企业。平台通过减少人工红队投入、在上线前发现可利用缺陷、降低第三方模型准入风险，并在系统变更后保留版本关联证据创造价值。企业级业务盈利能力主要取决于自动化程度、攻击知识复用、推理成本控制、续约率及开发与安全流程集成，而非单纯测试数量。专业厂商可依靠技术深度获得溢价，大型网络安全及云平台则依托渠道、组合合同和较低获客成本形成商业优势。

细分市场分析

按核心测试功能划分，自动化行为红队测试构成市场商业化中心，主要覆盖提示注入、越狱、敏感数据提取、不安全内容、RAG泄露及工具滥用。模型文件与供应链扫描形成相对独立的技术板块，重点检查序列化文件、依赖组件、恶意代码、后门和组件漏洞；对抗鲁棒性测试主要服务传统机器学习、视觉及语音模型。智能体与工具链安全测试是当前技术演进最快的方向，重点评估智能体行动、权限、记忆、MCP连接及多智能体攻击路径。随着客户寻求统一识别模型、应用、智能体及供应链风险，综合多功能平台的战略重要性持续上升。

按被测对象划分，基础模型与大语言模型应用目前覆盖最广泛的商业需求，自主智能体及多智能体系统则成为新测试要求的主要来源。上线前验证仍是重要采购环节，但随着模型、提示词、检索配置及工作流频繁变化，CI/CD回归测试和生产持续测试的重要性正在上升。公有云SaaS有利于快速采用，专属云、VPC、本地化及隔离网部署则在高风险行业保持较强地位。因此，能够同时覆盖云端与私有环境的混合交付能力正由附加选项转变为重要竞争要素。

下游市场机会

科技企业与基础模型开发商仍是重要早期客户，需要在发布前评估新模型版本、微调方法、API和智能体能力。中期更大的机会来自将AI由试验转入客户触点和运营流程的企业。金融机构关注数据泄露、违规建议、模型操纵及第三方模型风险；政府与国防用户重视私有化、可审计性及权限控制；医疗与生命科学机构更关注敏感信息和高后果输出；关键基础设施运营商需要验证工具执行及运营边界。零售、媒体和专业服务行业构成覆盖更广但价格敏感度较高的市场，主要需求集中在智能客服、内容生成、内部知识系统及流程智能体。

地区分析

北美是最大区域市场，约占2025年市场收入的58%–64%，其领先地位来自基础模型开发商、网络安全平台、云厂商、风险资本支持的专业企业及大型终端客户高度集中。以色列及中东整体收入规模相对较小，但在攻击模拟、智能体安全以及红队测试与运行时控制联动方面具有较高技术密度。欧洲则在第三方独立保障、隐私保护、审计证据及监管适配方面形成差异化优势，推动可重复、可留痕测试需求增长。

中国约占2025年市场收入的11%–16%，市场路线更侧重私有化部署、中文风险题库、内容安全评测、本地标准及政企项目交付。亚太其他地区的供给较为分散，印度和新加坡具备部分专业能力，日本、韩国和中国台湾更多依赖云平台、网络安全企业及专业服务商内嵌测试功能，独立平台数量相对有限。因此，区域扩张不仅需要产品语言本地化，还需要本地攻击数据、数据驻留、监管映射及项目交付能力。

竞争格局

市场竞争呈现平台化整合与专业化创新并存的结构。大型网络安全集团及云厂商依托企业渠道、存量客户、组合采购，以及测试、治理和运行时控制的一体化能力参与竞争。并购正在加快技术汇聚：Protect AI已并入Palo Alto Networks，Robust Intelligence成为Cisco AI Defense的重要技术基础，SPLX则为Zscaler补充自动化红队能力。独立专业厂商主要依靠更深入的攻击研究、模型无关测试、开发者 workflow、较低误报，以及在智能体、MCP、模型供应链和前沿模型评估方面的专长竞争；中国厂商则依靠本地部署、中文测试、监管适配及政企交付网络建立差异化。当前市场尚未形成稳定寡头格局，42家已确认核心商业主体与12家扩展厂商并存。未来竞争优势将取决于厂商能否在保持测试独立性和可量化攻击有效性的同时，把测试发现转化为可复现回归测试、工程整改、发布决策及运行时策略。

报告范围

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AI模型安全测试平台产品的市场规模、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, Inc.

Cisco Systems, Inc.
Microsoft Corporation
HiddenLayer, Inc.
Amazon Web Services, Inc.
Zscaler, Inc.
Check Point Software Technologies Ltd.
Google LLC
Gray Swan AI, Inc.
Noma Security Ltd.
International Business Machines Corporation
Promptfoo, Inc.
Giskard AI SAS
Mindgard Ltd.
Cranium AI, Inc.
Lasso Security Ltd.
Pillar Security Technologies Ltd.
Straiker, Inc.
SentinelOne, Inc.
Tenable Holdings, Inc.
Adversa AI Ltd.
Vijil, Inc.
北京瑞莱智慧科技有限公司
杭州安恒信息技术股份有限公司
绿盟科技集团股份有限公司
启明星辰信息技术集团股份有限公司
中国电信股份有限公司
北京火山引擎科技有限公司
杭州数圭通科技有限公司
Resaro Limited

按照不同产品类型，包括如下几个类别：

- 自动化行为红队测试
- 对抗鲁棒性测试
- 模型文件与供应链扫描
- 智能体与工具链安全测试
- 其他

按照不同被测对象，包括如下几个类别：

- 传统机器学习模型
- 基础模型
- RAG与对话应用
- 自主AI智能体
- 其他

按照不同部署方式，包括如下几个类别：

- 公有云SaaS
- 专属云
- 本地化
- 其他

按照不同应用，主要包括如下几个方面：

- 科技与基础模型厂商
- 银行及金融服务与保险
- 政府与国防
- 其他

重点关注如下几个地区

- 北美
- 欧洲
- 中国
- 日本
- 东南亚
- 印度

章节概要

第1章：报告统计范围、产品细分及全球总体规模及增长率等数据

第2章：全球不同应用AI模型安全测试平台市场规模及份额等

第3章：全球AI模型安全测试平台主要地区市场规模及份额等

第4章：全球范围内AI模型安全测试平台主要企业竞争分析，主要包括AI模型安全测试平台收入、市场份额及行业集中度分析

第5章：中国市场AI模型安全测试平台主要企业竞争分析，主要包括AI模型安全测试平台收入、市场份额及行业集中度分析

第6章：全球主要企业基本情况介绍，包括公司简介、AI模型安全测试平台产品、收入及最新动态等

第7章：行业发展机遇和风险分析

第8章：报告结论

报告目录

1 AI模型安全测试平台市场概述

1.1 AI模型安全测试平台市场概述

1.2 不同产品类型AI模型安全测试平台分析

1.2.1 自动化行为红队测试

1.2.2 对抗鲁棒性测试

1.2.3 模型文件与供应链扫描

1.2.4 智能体与工具链安全测试

1.2.5 其他

1.2.6 全球市场不同产品类型AI模型安全测试平台销售额对比（2021 VS 2025 VS 2032）

1.2.7 全球不同产品类型AI模型安全测试平台销售额及预测（2021-2032）

1.2.7.1 全球不同产品类型AI模型安全测试平台销售额及市场份额（2021-2026）

1.2.7.2 全球不同产品类型AI模型安全测试平台销售额预测（2027-2032）

1.2.8 中国不同产品类型AI模型安全测试平台销售额及预测（2021-2032）

1.2.8.1 中国不同产品类型AI模型安全测试平台销售额及市场份额（2021-2026）

1.2.8.2 中国不同产品类型AI模型安全测试平台销售额预测（2027-2032）

1.3 不同被测对象AI模型安全测试平台分析

1.3.1 传统机器学习模型

1.3.2 基础模型

1.3.3 RAG与对话应用

1.3.4 自主AI智能体

1.3.5 其他

1.3.6 全球市场不同被测对象AI模型安全测试平台销售额对比（2021 VS 2025 VS 2032）

1.3.7 全球不同被测对象AI模型安全测试平台销售额及预测（2021-2032）

1.3.7.1 全球不同被测对象AI模型安全测试平台销售额及市场份额（2021-2026）

1.3.7.2 全球不同被测对象AI模型安全测试平台销售额预测（2027-2032）

1.3.8 中国不同被测对象AI模型安全测试平台销售额及预测（2021-2032）

1.3.8.1 中国不同被测对象AI模型安全测试平台销售额及市场份额（2021-2026）

1.3.8.2 中国不同被测对象AI模型安全测试平台销售额预测（2027-2032）

1.4 不同部署方式AI模型安全测试平台分析

1.4.1 公有云SaaS

1.4.2 专属云

1.4.3 本地化

1.4.4 其他

1.4.5 全球市场不同部署方式AI模型安全测试平台销售额对比（2021 VS 2025 VS 2032）

1.4.6 全球不同部署方式AI模型安全测试平台销售额及预测（2021-2032）

1.4.6.1 全球不同部署方式AI模型安全测试平台销售额及市场份额（2021-2026）

1.4.6.2 全球不同部署方式AI模型安全测试平台销售额预测（2027-2032）

1.4.7 中国不同部署方式AI模型安全测试平台销售额及预测（2021-2032）

1.4.7.1 中国不同部署方式AI模型安全测试平台销售额及市场份额（2021-2026）

1.4.7.2 中国不同部署方式AI模型安全测试平台销售额预测（2027-2032）

2 不同应用分析

2.1 从不同应用，AI模型安全测试平台主要包括如下几个方面

2.1.1 科技与基础模型厂商

2.1.2 银行及金融服务与保险

- 2.1.3 政府与国防
- 2.1.4 其他
- 2.2 全球市场不同应用AI模型安全测试平台销售额对比（2021 VS 2025 VS 2032）
- 2.3 全球不同应用AI模型安全测试平台销售额及预测（2021-2032）
 - 2.3.1 全球不同应用AI模型安全测试平台销售额及市场份额（2021-2026）
 - 2.3.2 全球不同应用AI模型安全测试平台销售额预测（2027-2032）
- 2.4 中国不同应用AI模型安全测试平台销售额及预测（2021-2032）
 - 2.4.1 中国不同应用AI模型安全测试平台销售额及市场份额（2021-2026）
 - 2.4.2 中国不同应用AI模型安全测试平台销售额预测（2027-2032）
- 3 全球AI模型安全测试平台主要地区分析
 - 3.1 全球主要地区AI模型安全测试平台市场规模分析：2021 VS 2025 VS 2032
 - 3.1.1 全球主要地区AI模型安全测试平台销售额及份额（2021-2026）
 - 3.1.2 全球主要地区AI模型安全测试平台销售额及份额预测（2027-2032）
 - 3.2 北美AI模型安全测试平台销售额及预测（2021-2032）
 - 3.3 欧洲AI模型安全测试平台销售额及预测（2021-2032）
 - 3.4 中国AI模型安全测试平台销售额及预测（2021-2032）
 - 3.5 日本AI模型安全测试平台销售额及预测（2021-2032）
 - 3.6 东南亚AI模型安全测试平台销售额及预测（2021-2032）
 - 3.7 印度AI模型安全测试平台销售额及预测（2021-2032）
- 4 全球主要企业市场占有率
 - 4.1 全球主要企业AI模型安全测试平台销售额及市场份额
 - 4.2 全球AI模型安全测试平台主要企业竞争态势
 - 4.2.1 AI模型安全测试平台行业集中度分析：2025年全球Top 5厂商市场份额
 - 4.2.2 全球AI模型安全测试平台第一梯队、第二梯队和第三梯队企业及市场份额
 - 4.3 2025年全球主要厂商AI模型安全测试平台收入排名
 - 4.4 全球主要厂商AI模型安全测试平台总部及市场区域分布
 - 4.5 全球主要厂商AI模型安全测试平台产品类型及应用
 - 4.6 全球主要厂商AI模型安全测试平台商业化日期
 - 4.7 新增投资及市场并购活动
 - 4.8 AI模型安全测试平台全球领先企业SWOT分析
- 5 中国市场AI模型安全测试平台主要企业分析
 - 5.1 中国AI模型安全测试平台销售额及市场份额（2021-2026）
 - 5.2 中国AI模型安全测试平台Top 3和Top 5企业市场份额
- 6 主要企业简介
 - 6.1 Palo Alto Networks, Inc.
 - 6.1.1 Palo Alto Networks, Inc.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手
 - 6.1.2 Palo Alto Networks, Inc. AI模型安全测试平台产品及服务介绍
 - 6.1.3 Palo Alto Networks, Inc. AI模型安全测试平台收入及毛利率（2021-2026）&（百万美元）
 - 6.1.4 Palo Alto Networks, Inc.公司简介及主要业务
 - 6.1.5 Palo Alto Networks, Inc.企业最新动态
 - 6.2 Cisco Systems, Inc.
 - 6.2.1 Cisco Systems, Inc.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手
 - 6.2.2 Cisco Systems, Inc. AI模型安全测试平台产品及服务介绍
 - 6.2.3 Cisco Systems, Inc. AI模型安全测试平台收入及毛利率（2021-2026）&（百万美元）
 - 6.2.4 Cisco Systems, Inc.公司简介及主要业务
 - 6.2.5 Cisco Systems, Inc.企业最新动态
 - 6.3 Microsoft Corporation
 - 6.3.1 Microsoft Corporation公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手
 - 6.3.2 Microsoft Corporation AI模型安全测试平台产品及服务介绍
 - 6.3.3 Microsoft Corporation AI模型安全测试平台收入及毛利率（2021-2026）&（百万美元）
 - 6.3.4 Microsoft Corporation公司简介及主要业务
 - 6.3.5 Microsoft Corporation企业最新动态
 - 6.4 HiddenLayer, Inc.
 - 6.4.1 HiddenLayer, Inc.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手
 - 6.4.2 HiddenLayer, Inc. AI模型安全测试平台产品及服务介绍
 - 6.4.3 HiddenLayer, Inc. AI模型安全测试平台收入及毛利率（2021-2026）&（百万美元）
 - 6.4.4 HiddenLayer, Inc.公司简介及主要业务
 - 6.5 Amazon Web Services, Inc.
 - 6.5.1 Amazon Web Services, Inc.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手
 - 6.5.2 Amazon Web Services, Inc. AI模型安全测试平台产品及服务介绍

6.5.3 Amazon Web Services, Inc. AI模型安全测试平台收入及毛利率（2021-2026）&（百万美元）

6.5.4 Amazon Web Services, Inc.公司简介及主要业务

6.5.5 Amazon Web Services, Inc.企业最新动态

6.6 Zscaler, Inc.

6.6.1 Zscaler, Inc.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

6.6.2 Zscaler, Inc. AI模型安全测试平台产品及服务介绍

6.6.3 Zscaler, Inc. AI模型安全测试平台收入及毛利率（2021-2026）&（百万美元）

6.6.4 Zscaler, Inc.公司简介及主要业务

6.6.5 Zscaler, Inc.企业最新动态

6.7 Check Point Software Technologies Ltd.

6.7.1 Check Point Software Technologies Ltd.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

6.7.2 Check Point Software Technologies Ltd. AI模型安全测试平台产品及服务介绍

6.7.3 Check Point Software Technologies Ltd. AI模型安全测试平台收入及毛利率（2021-2026）&（百万美元）

6.7.4 Check Point Software Technologies Ltd.公司简介及主要业务

6.7.5 Check Point Software Technologies Ltd.企业最新动态

6.8 Google LLC

6.8.1 Google LLC公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

6.8.2 Google LLC AI模型安全测试平台产品及服务介绍

6.8.3 Google LLC AI模型安全测试平台收入及毛利率（2021-2026）&（百万美元）

6.8.4 Google LLC公司简介及主要业务

6.8.5 Google LLC企业最新动态

6.9 Gray Swan AI, Inc.

6.9.1 Gray Swan AI, Inc.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

6.9.2 Gray Swan AI, Inc. AI模型安全测试平台产品及服务介绍

6.9.3 Gray Swan AI, Inc. AI模型安全测试平台收入及毛利率（2021-2026）&（百万美元）

6.9.4 Gray Swan AI, Inc.公司简介及主要业务

6.9.5 Gray Swan AI, Inc.企业最新动态

6.10 Noma Security Ltd.

6.10.1 Noma Security Ltd.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

6.10.2 Noma Security Ltd. AI模型安全测试平台产品及服务介绍

6.10.3 Noma Security Ltd. AI模型安全测试平台收入及毛利率（2021-2026）&（百万美元）

6.10.4 Noma Security Ltd.公司简介及主要业务

6.10.5 Noma Security Ltd.企业最新动态

6.11 International Business Machines Corporation

6.11.1 International Business Machines Corporation公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

6.11.2 International Business Machines Corporation AI模型安全测试平台产品及服务介绍

6.11.3 International Business Machines Corporation AI模型安全测试平台收入及毛利率（2021-2026）&（百万美元）

6.11.4 International Business Machines Corporation公司简介及主要业务

6.11.5 International Business Machines Corporation企业最新动态

6.12 Promptfoo, Inc.

6.12.1 Promptfoo, Inc.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

6.12.2 Promptfoo, Inc. AI模型安全测试平台产品及服务介绍

6.12.3 Promptfoo, Inc. AI模型安全测试平台收入及毛利率（2021-2026）&（百万美元）

6.12.4 Promptfoo, Inc.公司简介及主要业务

6.12.5 Promptfoo, Inc.企业最新动态

6.13 Giskard AI SAS

6.13.1 Giskard AI SAS公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

6.13.2 Giskard AI SAS AI模型安全测试平台产品及服务介绍

6.13.3 Giskard AI SAS AI模型安全测试平台收入及毛利率（2021-2026）&（百万美元）

6.13.4 Giskard AI SAS公司简介及主要业务

6.13.5 Giskard AI SAS企业最新动态

6.14 Mindgard Ltd.

6.14.1 Mindgard Ltd.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

6.14.2 Mindgard Ltd. AI模型安全测试平台产品及服务介绍

6.14.3 Mindgard Ltd. AI模型安全测试平台收入及毛利率（2021-2026）&（百万美元）

6.14.4 Mindgard Ltd.公司简介及主要业务

6.14.5 Mindgard Ltd.企业最新动态

6.15 Cranium AI, Inc.

6.15.1 Cranium AI, Inc.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

6.15.2 Cranium AI, Inc. AI模型安全测试平台产品及服务介绍

6.15.3 Cranium AI, Inc. AI模型安全测试平台收入及毛利率（2021-2026）&（百万美元）

6.15.4 Cranium AI, Inc.公司简介及主要业务

6.15.5 Cranium AI, Inc.企业最新动态

6.16 Lasso Security Ltd.

6.16.1 Lasso Security Ltd.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

6.16.2 Lasso Security Ltd. AI模型安全测试平台产品及服务介绍

6.16.3 Lasso Security Ltd. AI模型安全测试平台收入及毛利率（2021-2026）&（百万美元）

6.16.4 Lasso Security Ltd.公司简介及主要业务

6.16.5 Lasso Security Ltd.企业最新动态

6.17 Pillar Security Technologies Ltd.

6.17.1 Pillar Security Technologies Ltd.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

6.17.2 Pillar Security Technologies Ltd. AI模型安全测试平台产品及服务介绍

6.17.3 Pillar Security Technologies Ltd. AI模型安全测试平台收入及毛利率（2021-2026）&（百万美元）

6.17.4 Pillar Security Technologies Ltd.公司简介及主要业务

6.17.5 Pillar Security Technologies Ltd.企业最新动态

6.18 Straiker, Inc.

6.18.1 Straiker, Inc.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

6.18.2 Straiker, Inc. AI模型安全测试平台产品及服务介绍

6.18.3 Straiker, Inc. AI模型安全测试平台收入及毛利率（2021-2026）&（百万美元）

6.18.4 Straiker, Inc.公司简介及主要业务

6.18.5 Straiker, Inc.企业最新动态

6.19 SentinelOne, Inc.

6.19.1 SentinelOne, Inc.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

6.19.2 SentinelOne, Inc. AI模型安全测试平台产品及服务介绍

6.19.3 SentinelOne, Inc. AI模型安全测试平台收入及毛利率（2021-2026）&（百万美元）

6.19.4 SentinelOne, Inc.公司简介及主要业务

6.19.5 SentinelOne, Inc.企业最新动态

6.20 Tenable Holdings, Inc.

6.20.1 Tenable Holdings, Inc.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

6.20.2 Tenable Holdings, Inc. AI模型安全测试平台产品及服务介绍

6.20.3 Tenable Holdings, Inc. AI模型安全测试平台收入及毛利率（2021-2026）&（百万美元）

6.20.4 Tenable Holdings, Inc.公司简介及主要业务

6.20.5 Tenable Holdings, Inc.企业最新动态

6.21 Adversa AI Ltd.

6.21.1 Adversa AI Ltd.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

6.21.2 Adversa AI Ltd. AI模型安全测试平台产品及服务介绍

6.21.3 Adversa AI Ltd. AI模型安全测试平台收入及毛利率（2021-2026）&（百万美元）

6.21.4 Adversa AI Ltd.公司简介及主要业务

6.21.5 Adversa AI Ltd.企业最新动态

6.22 Vijil, Inc.

6.22.1 Vijil, Inc.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

6.22.2 Vijil, Inc. AI模型安全测试平台产品及服务介绍

6.22.3 Vijil, Inc. AI模型安全测试平台收入及毛利率（2021-2026）&（百万美元）

6.22.4 Vijil, Inc.公司简介及主要业务

6.22.5 Vijil, Inc.企业最新动态

6.23 北京瑞莱智慧科技有限公司

6.23.1 北京瑞莱智慧科技有限公司公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

6.23.2 北京瑞莱智慧科技有限公司 AI模型安全测试平台产品及服务介绍

6.23.3 北京瑞莱智慧科技有限公司 AI模型安全测试平台收入及毛利率（2021-2026）&（百万美元）

6.23.4 北京瑞莱智慧科技有限公司公司简介及主要业务

6.23.5 北京瑞莱智慧科技有限公司企业最新动态

6.24 杭州安恒信息技术股份有限公司

6.24.1 杭州安恒信息技术股份有限公司公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

6.24.2 杭州安恒信息技术股份有限公司 AI模型安全测试平台产品及服务介绍

6.24.3 杭州安恒信息技术股份有限公司 AI模型安全测试平台收入及毛利率（2021-2026）&（百万美元）

6.24.4 杭州安恒信息技术股份有限公司公司简介及主要业务

6.24.5 杭州安恒信息技术股份有限公司企业最新动态

6.25 绿盟科技集团股份有限公司

6.25.1 绿盟科技集团股份有限公司公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

- 6.25.2 绿盟科技集团股份有限公司 AI模型安全测试平台产品及服务介绍
- 6.25.3 绿盟科技集团股份有限公司 AI模型安全测试平台收入及毛利率（2021-2026）&（百万美元）
- 6.25.4 绿盟科技集团股份有限公司公司简介及主要业务
- 6.25.5 绿盟科技集团股份有限公司企业最新动态
- 6.26 启明星辰信息技术集团股份有限公司
- 6.26.1 启明星辰信息技术集团股份有限公司公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手
- 6.26.2 启明星辰信息技术集团股份有限公司 AI模型安全测试平台产品及服务介绍
- 6.26.3 启明星辰信息技术集团股份有限公司 AI模型安全测试平台收入及毛利率（2021-2026）&（百万美元）
- 6.26.4 启明星辰信息技术集团股份有限公司公司简介及主要业务
- 6.26.5 启明星辰信息技术集团股份有限公司企业最新动态
- 6.27 中国电信股份有限公司
- 6.27.1 中国电信股份有限公司公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手
- 6.27.2 中国电信股份有限公司 AI模型安全测试平台产品及服务介绍
- 6.27.3 中国电信股份有限公司 AI模型安全测试平台收入及毛利率（2021-2026）&（百万美元）
- 6.27.4 中国电信股份有限公司公司简介及主要业务
- 6.27.5 中国电信股份有限公司企业最新动态
- 6.28 北京火山引擎科技有限公司
- 6.28.1 北京火山引擎科技有限公司公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手
- 6.28.2 北京火山引擎科技有限公司 AI模型安全测试平台产品及服务介绍
- 6.28.3 北京火山引擎科技有限公司 AI模型安全测试平台收入及毛利率（2021-2026）&（百万美元）
- 6.28.4 北京火山引擎科技有限公司公司简介及主要业务
- 6.28.5 北京火山引擎科技有限公司企业最新动态
- 6.29 杭州数圭通科技有限公司
- 6.29.1 杭州数圭通科技有限公司公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手
- 6.29.2 杭州数圭通科技有限公司 AI模型安全测试平台产品及服务介绍
- 6.29.3 杭州数圭通科技有限公司 AI模型安全测试平台收入及毛利率（2021-2026）&（百万美元）
- 6.29.4 杭州数圭通科技有限公司公司简介及主要业务
- 6.29.5 杭州数圭通科技有限公司企业最新动态
- 6.30 Resaro Limited
- 6.30.1 Resaro Limited公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手
- 6.30.2 Resaro Limited AI模型安全测试平台产品及服务介绍
- 6.30.3 Resaro Limited AI模型安全测试平台收入及毛利率（2021-2026）&（百万美元）
- 6.30.4 Resaro Limited公司简介及主要业务
- 6.30.5 Resaro Limited企业最新动态
- 7 行业发展机遇和风险分析
- 7.1 AI模型安全测试平台行业发展机遇及主要驱动因素
- 7.2 AI模型安全测试平台行业发展面临的风险
- 7.3 AI模型安全测试平台行业政策分析
- 8 研究结果
- 9 研究方法与数据来源
- 9.1 研究方法
- 9.2 数据来源
- 9.2.1 二手信息来源
- 9.2.2 一手信息来源
- 9.3 数据交互验证
- 9.4 免责声明

报告图表

表格目录

- 表 1：自动化行为红队测试主要企业列表
- 表 2：对抗鲁棒性测试主要企业列表
- 表 3：模型文件与供应链扫描主要企业列表
- 表 4：智能体与工具链安全测试主要企业列表
- 表 5：其他主要企业列表

表 6:	全球市场不同产品类型AI模型安全测试平台销售额及增长率对比 (2021 VS 2025 VS 2032) & (百万美元)
表 7:	全球不同产品类型AI模型安全测试平台销售额列表 (2021-2026) & (百万美元)
表 8:	全球不同产品类型AI模型安全测试平台销售额市场份额列表 (2021-2026)
表 9:	全球不同产品类型AI模型安全测试平台销售额预测 (2027-2032) & (百万美元)
表 10:	全球不同产品类型AI模型安全测试平台销售额市场份额预测 (2027-2032)
表 11:	中国不同产品类型AI模型安全测试平台销售额列表 (2021-2026) & (百万美元)
表 12:	中国不同产品类型AI模型安全测试平台销售额市场份额列表 (2021-2026)
表 13:	中国不同产品类型AI模型安全测试平台销售额预测 (2027-2032) & (百万美元)
表 14:	中国不同产品类型AI模型安全测试平台销售额市场份额预测 (2027-2032)
表 15:	传统机器学习模型主要企业列表
表 16:	基础模型主要企业列表
表 17:	RAG与对话应用主要企业列表
表 18:	自主AI智能体主要企业列表
表 19:	其他主要企业列表
表 20:	全球市场不同被测对象AI模型安全测试平台销售额及增长率对比 (2021 VS 2025 VS 2032) & (百万美元)
表 21:	全球不同被测对象AI模型安全测试平台销售额列表 (2021-2026) & (百万美元)
表 22:	全球不同被测对象AI模型安全测试平台销售额市场份额列表 (2021-2026)
表 23:	全球不同被测对象AI模型安全测试平台销售额预测 (2027-2032) & (百万美元)
表 24:	全球不同被测对象AI模型安全测试平台销售额市场份额预测 (2027-2032)
表 25:	中国不同被测对象AI模型安全测试平台销售额列表 (2021-2026) & (百万美元)
表 26:	中国不同被测对象AI模型安全测试平台销售额市场份额列表 (2021-2026)
表 27:	中国不同被测对象AI模型安全测试平台销售额预测 (2027-2032) & (百万美元)
表 28:	中国不同被测对象AI模型安全测试平台销售额市场份额预测 (2027-2032)
表 29:	公有云SaaS主要企业列表
表 30:	专属云主要企业列表
表 31:	本地化主要企业列表
表 32:	其他主要企业列表
表 33:	全球市场不同部署方式AI模型安全测试平台销售额及增长率对比 (2021 VS 2025 VS 2032) & (百万美元)
表 34:	全球不同部署方式AI模型安全测试平台销售额列表 (2021-2026) & (百万美元)
表 35:	全球不同部署方式AI模型安全测试平台销售额市场份额列表 (2021-2026)
表 36:	全球不同部署方式AI模型安全测试平台销售额预测 (2027-2032) & (百万美元)
表 37:	全球不同部署方式AI模型安全测试平台销售额市场份额预测 (2027-2032)
表 38:	中国不同部署方式AI模型安全测试平台销售额列表 (2021-2026) & (百万美元)
表 39:	中国不同部署方式AI模型安全测试平台销售额市场份额列表 (2021-2026)
表 40:	中国不同部署方式AI模型安全测试平台销售额预测 (2027-2032) & (百万美元)
表 41:	中国不同部署方式AI模型安全测试平台销售额市场份额预测 (2027-2032)
表 42:	全球市场不同应用AI模型安全测试平台销售额及增长率对比 (2021 VS 2025 VS 2032) & (百万美元)
表 43:	全球不同应用AI模型安全测试平台销售额列表 (2021-2026) & (百万美元)
表 44:	全球不同应用AI模型安全测试平台销售额市场份额列表 (2021-2026)
表 45:	全球不同应用AI模型安全测试平台销售额预测 (2027-2032) & (百万美元)
表 46:	全球不同应用AI模型安全测试平台市场份额预测 (2027-2032)
表 47:	中国不同应用AI模型安全测试平台销售额列表 (2021-2026) & (百万美元)
表 48:	中国不同应用AI模型安全测试平台销售额市场份额列表 (2021-2026)
表 49:	中国不同应用AI模型安全测试平台销售额预测 (2027-2032) & (百万美元)
表 50:	中国不同应用AI模型安全测试平台销售额市场份额预测 (2027-2032)
表 51:	全球主要地区AI模型安全测试平台销售额: (2021 VS 2025 VS 2032) & (百万美元)
表 52:	全球主要地区AI模型安全测试平台销售额列表 (2021-2026) & (百万美元)
表 53:	全球主要地区AI模型安全测试平台销售额及份额列表 (2021-2026)
表 54:	全球主要地区AI模型安全测试平台销售额列表预测 (2027-2032) & (百万美元)
表 55:	全球主要地区AI模型安全测试平台销售额及份额列表预测 (2027-2032)
表 56:	全球主要企业AI模型安全测试平台销售额 (2021-2026) & (百万美元)
表 57:	全球主要企业AI模型安全测试平台销售份额对比 (2021-2026)
表 58:	2025年全球AI模型安全测试平台主要厂商市场地位 (第一梯队、第二梯队和第三梯队)
表 59:	2025年全球主要厂商AI模型安全测试平台收入排名 (百万美元)
表 60:	全球主要厂商AI模型安全测试平台总部及市场区域分布
表 61:	全球主要厂商AI模型安全测试平台产品类型及应用
表 62:	全球主要厂商AI模型安全测试平台商业化日期
表 63:	全球AI模型安全测试平台市场投资、并购等现状分析
表 64:	中国主要企业AI模型安全测试平台销售额列表 (2021-2026) & (百万美元)
表 65:	中国主要企业AI模型安全测试平台销售份额对比 (2021-2026)

表 66: Palo Alto Networks, Inc.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手
表 67: Palo Alto Networks, Inc. AI模型安全测试平台产品及服务介绍
表 68: Palo Alto Networks, Inc. AI模型安全测试平台收入及毛利率 (2021-2026) & (百万美元)
表 69: Palo Alto Networks, Inc.公司简介及主要业务
表 70: Palo Alto Networks, Inc.企业最新动态
表 71: Cisco Systems, Inc.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手
表 72: Cisco Systems, Inc. AI模型安全测试平台产品及服务介绍
表 73: Cisco Systems, Inc. AI模型安全测试平台收入及毛利率 (2021-2026) & (百万美元)
表 74: Cisco Systems, Inc.公司简介及主要业务
表 75: Cisco Systems, Inc.企业最新动态
表 76: Microsoft Corporation公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手
表 77: Microsoft Corporation AI模型安全测试平台产品及服务介绍
表 78: Microsoft Corporation AI模型安全测试平台收入及毛利率 (2021-2026) & (百万美元)
表 79: Microsoft Corporation公司简介及主要业务
表 80: Microsoft Corporation企业最新动态
表 81: HiddenLayer, Inc.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手
表 82: HiddenLayer, Inc. AI模型安全测试平台产品及服务介绍
表 83: HiddenLayer, Inc. AI模型安全测试平台收入及毛利率 (2021-2026) & (百万美元)
表 84: HiddenLayer, Inc.公司简介及主要业务
表 85: Amazon Web Services, Inc.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手
表 86: Amazon Web Services, Inc. AI模型安全测试平台产品及服务介绍
表 87: Amazon Web Services, Inc. AI模型安全测试平台收入及毛利率 (2021-2026) & (百万美元)
表 88: Amazon Web Services, Inc.公司简介及主要业务
表 89: Amazon Web Services, Inc.企业最新动态
表 90: Zscaler, Inc.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手
表 91: Zscaler, Inc. AI模型安全测试平台产品及服务介绍
表 92: Zscaler, Inc. AI模型安全测试平台收入及毛利率 (2021-2026) & (百万美元)
表 93: Zscaler, Inc.公司简介及主要业务
表 94: Zscaler, Inc.企业最新动态
表 95: Check Point Software Technologies Ltd.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手
表 96: Check Point Software Technologies Ltd. AI模型安全测试平台产品及服务介绍
表 97: Check Point Software Technologies Ltd. AI模型安全测试平台收入及毛利率 (2021-2026) & (百万美元)
表 98: Check Point Software Technologies Ltd.公司简介及主要业务
表 99: Check Point Software Technologies Ltd.企业最新动态
表 100: Google LLC公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手
表 101: Google LLC AI模型安全测试平台产品及服务介绍
表 102: Google LLC AI模型安全测试平台收入及毛利率 (2021-2026) & (百万美元)
表 103: Google LLC公司简介及主要业务
表 104: Google LLC企业最新动态
表 105: Gray Swan AI, Inc.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手
表 106: Gray Swan AI, Inc. AI模型安全测试平台产品及服务介绍
表 107: Gray Swan AI, Inc. AI模型安全测试平台收入及毛利率 (2021-2026) & (百万美元)
表 108: Gray Swan AI, Inc.公司简介及主要业务
表 109: Gray Swan AI, Inc.企业最新动态
表 110: Noma Security Ltd.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手
表 111: Noma Security Ltd. AI模型安全测试平台产品及服务介绍
表 112: Noma Security Ltd. AI模型安全测试平台收入及毛利率 (2021-2026) & (百万美元)
表 113: Noma Security Ltd.公司简介及主要业务
表 114: Noma Security Ltd.企业最新动态
表 115: International Business Machines Corporation公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手
表 116: International Business Machines Corporation AI模型安全测试平台产品及服务介绍
表 117: International Business Machines Corporation AI模型安全测试平台收入及毛利率 (2021-2026) & (百万美元)
表 118: International Business Machines Corporation公司简介及主要业务
表 119: International Business Machines Corporation企业最新动态
表 120: Promptfoo, Inc.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手
表 121: Promptfoo, Inc. AI模型安全测试平台产品及服务介绍
表 122: Promptfoo, Inc. AI模型安全测试平台收入及毛利率 (2021-2026) & (百万美元)
表 123: Promptfoo, Inc.公司简介及主要业务

表 124: Promptfoo, Inc.企业最新动态

表 125: Giskard AI SAS公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

表 126: Giskard AI SAS AI模型安全测试平台产品及服务介绍

表 127: Giskard AI SAS AI模型安全测试平台收入及毛利率 (2021-2026) & (百万美元)

表 128: Giskard AI SAS公司简介及主要业务

表 129: Giskard AI SAS企业最新动态

表 130: Mindgard Ltd.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

表 131: Mindgard Ltd. AI模型安全测试平台产品及服务介绍

表 132: Mindgard Ltd. AI模型安全测试平台收入及毛利率 (2021-2026) & (百万美元)

表 133: Mindgard Ltd.公司简介及主要业务

表 134: Mindgard Ltd.企业最新动态

表 135: Cranium AI, Inc.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

表 136: Cranium AI, Inc. AI模型安全测试平台产品及服务介绍

表 137: Cranium AI, Inc. AI模型安全测试平台收入及毛利率 (2021-2026) & (百万美元)

表 138: Cranium AI, Inc.公司简介及主要业务

表 139: Cranium AI, Inc.企业最新动态

表 140: Lasso Security Ltd.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

表 141: Lasso Security Ltd. AI模型安全测试平台产品及服务介绍

表 142: Lasso Security Ltd. AI模型安全测试平台收入及毛利率 (2021-2026) & (百万美元)

表 143: Lasso Security Ltd.公司简介及主要业务

表 144: Lasso Security Ltd.企业最新动态

表 145: Pillar Security Technologies Ltd.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

表 146: Pillar Security Technologies Ltd. AI模型安全测试平台产品及服务介绍

表 147: Pillar Security Technologies Ltd. AI模型安全测试平台收入及毛利率 (2021-2026) & (百万美元)

表 148: Pillar Security Technologies Ltd.公司简介及主要业务

表 149: Pillar Security Technologies Ltd.企业最新动态

表 150: Straiker, Inc.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

表 151: Straiker, Inc. AI模型安全测试平台产品及服务介绍

表 152: Straiker, Inc. AI模型安全测试平台收入及毛利率 (2021-2026) & (百万美元)

表 153: Straiker, Inc.公司简介及主要业务

表 154: Straiker, Inc.企业最新动态

表 155: SentinelOne, Inc.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

表 156: SentinelOne, Inc. AI模型安全测试平台产品及服务介绍

表 157: SentinelOne, Inc. AI模型安全测试平台收入及毛利率 (2021-2026) & (百万美元)

表 158: SentinelOne, Inc.公司简介及主要业务

表 159: SentinelOne, Inc.企业最新动态

表 160: Tenable Holdings, Inc.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

表 161: Tenable Holdings, Inc. AI模型安全测试平台产品及服务介绍

表 162: Tenable Holdings, Inc. AI模型安全测试平台收入及毛利率 (2021-2026) & (百万美元)

表 163: Tenable Holdings, Inc.公司简介及主要业务

表 164: Tenable Holdings, Inc.企业最新动态

表 165: Adversa AI Ltd.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

表 166: Adversa AI Ltd. AI模型安全测试平台产品及服务介绍

表 167: Adversa AI Ltd. AI模型安全测试平台收入及毛利率 (2021-2026) & (百万美元)

表 168: Adversa AI Ltd.公司简介及主要业务

表 169: Adversa AI Ltd.企业最新动态

表 170: Vijil, Inc.公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

表 171: Vijil, Inc. AI模型安全测试平台产品及服务介绍

表 172: Vijil, Inc. AI模型安全测试平台收入及毛利率 (2021-2026) & (百万美元)

表 173: Vijil, Inc.公司简介及主要业务

表 174: Vijil, Inc.企业最新动态

表 175: 北京瑞莱智慧科技有限公司公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

表 176: 北京瑞莱智慧科技有限公司 AI模型安全测试平台产品及服务介绍

表 177: 北京瑞莱智慧科技有限公司 AI模型安全测试平台收入及毛利率 (2021-2026) & (百万美元)

表 178: 北京瑞莱智慧科技有限公司公司简介及主要业务

表 179: 北京瑞莱智慧科技有限公司企业最新动态

表 180: 杭州安恒信息技术股份有限公司公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

表 181: 杭州安恒信息技术股份有限公司 AI模型安全测试平台产品及服务介绍

表 182: 杭州安恒信息技术股份有限公司 AI模型安全测试平台收入及毛利率 (2021-2026) & (百万美元)

表 183: 杭州安恒信息技术股份有限公司公司简介及主要业务

表 184: 杭州安恒信息技术股份有限公司企业最新动态

表 185: 绿盟科技集团股份有限公司公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

表 186: 绿盟科技集团股份有限公司 AI模型安全测试平台产品及服务介绍

表 187: 绿盟科技集团股份有限公司 AI模型安全测试平台收入及毛利率 (2021-2026) & (百万美元)

表 188: 绿盟科技集团股份有限公司公司简介及主要业务

表 189: 绿盟科技集团股份有限公司企业最新动态

表 190: 启明星辰信息技术集团股份有限公司公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

表 191: 启明星辰信息技术集团股份有限公司 AI模型安全测试平台产品及服务介绍

表 192: 启明星辰信息技术集团股份有限公司 AI模型安全测试平台收入及毛利率 (2021-2026) & (百万美元)

表 193: 启明星辰信息技术集团股份有限公司公司简介及主要业务

表 194: 启明星辰信息技术集团股份有限公司企业最新动态

表 195: 中国电信股份有限公司公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

表 196: 中国电信股份有限公司 AI模型安全测试平台产品及服务介绍

表 197: 中国电信股份有限公司 AI模型安全测试平台收入及毛利率 (2021-2026) & (百万美元)

表 198: 中国电信股份有限公司公司简介及主要业务

表 199: 中国电信股份有限公司企业最新动态

表 200: 北京火山引擎科技有限公司公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

表 201: 北京火山引擎科技有限公司 AI模型安全测试平台产品及服务介绍

表 202: 北京火山引擎科技有限公司 AI模型安全测试平台收入及毛利率 (2021-2026) & (百万美元)

表 203: 北京火山引擎科技有限公司公司简介及主要业务

表 204: 北京火山引擎科技有限公司企业最新动态

表 205: 杭州数圭通科技有限公司公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

表 206: 杭州数圭通科技有限公司 AI模型安全测试平台产品及服务介绍

表 207: 杭州数圭通科技有限公司 AI模型安全测试平台收入及毛利率 (2021-2026) & (百万美元)

表 208: 杭州数圭通科技有限公司公司简介及主要业务

表 209: 杭州数圭通科技有限公司企业最新动态

表 210: Resaro Limited公司信息、总部、AI模型安全测试平台市场地位以及主要的竞争对手

表 211: Resaro Limited AI模型安全测试平台产品及服务介绍

表 212: Resaro Limited AI模型安全测试平台收入及毛利率 (2021-2026) & (百万美元)

表 213: Resaro Limited公司简介及主要业务

表 214: Resaro Limited企业最新动态

表 215: AI模型安全测试平台行业发展机遇及主要驱动因素

表 216: AI模型安全测试平台行业发展面临的风险

表 217: AI模型安全测试平台行业政策分析

表 218: 研究范围

表 219: 本文分析师列表

图表目录

图 1: AI模型安全测试平台产品图片

图 2: 全球市场AI模型安全测试平台市场规模 (销售额) , 2021 VS 2025 VS 2032 (百万美元)

图 3: 全球AI模型安全测试平台市场销售额预测: (百万美元) & (2021-2032)

图 4: 中国市场AI模型安全测试平台销售额及未来趋势 (2021-2032) & (百万美元)

图 5: 自动化行为红队测试 产品图片

图 6: 全球自动化行为红队测试规模及增长率 (2021-2032) & (百万美元)

图 7: 对抗鲁棒性测试产品图片

图 8: 全球对抗鲁棒性测试规模及增长率 (2021-2032) & (百万美元)

图 9: 模型文件与供应链扫描产品图片

图 10: 全球模型文件与供应链扫描规模及增长率 (2021-2032) & (百万美元)

图 11: 智能体与工具链安全测试产品图片

图 12: 全球智能体与工具链安全测试规模及增长率 (2021-2032) & (百万美元)

图 13: 其他产品图片

图 14: 全球其他规模及增长率 (2021-2032) & (百万美元)

图 15: 全球不同产品类型AI模型安全测试平台市场份额2025 & 2032

图 16: 全球不同产品类型AI模型安全测试平台市场份额2021 & 2025

图 17: 全球不同产品类型AI模型安全测试平台市场份额预测2026 & 2032

图 18: 中国不同产品类型AI模型安全测试平台市场份额2021 & 2025

图 19: 中国不同产品类型AI模型安全测试平台市场份额预测2026 & 2032

图 20: 传统机器学习模型 产品图片

图 21: 全球传统机器学习模型规模及增长率 (2021-2032) & (百万美元)

图 22: 基础模型产品图片

图 23: 全球基础模型规模及增长率 (2021-2032) & (百万美元)

图 24: RAG与对话应用产品图片

图 25: 全球RAG与对话应用规模及增长率 (2021-2032) & (百万美元)

图 26: 自主AI智能体产品图片

图 27: 全球自主AI智能体规模及增长率 (2021-2032) & (百万美元)

图 28: 其他产品图片

图 29: 全球其他规模及增长率 (2021-2032) & (百万美元)

图 30: 全球不同被测对象AI模型安全测试平台市场份额2025 & 2032

图 31: 全球不同被测对象AI模型安全测试平台市场份额2021 & 2025

图 32: 全球不同被测对象AI模型安全测试平台市场份额预测2026 & 2032

图 33: 中国不同被测对象AI模型安全测试平台市场份额2021 & 2025

图 34: 中国不同被测对象AI模型安全测试平台市场份额预测2026 & 2032

图 35: 公有云SaaS 产品图片

图 36: 全球公有云SaaS规模及增长率 (2021-2032) & (百万美元)

图 37: 专属云产品图片

图 38: 全球专属云规模及增长率 (2021-2032) & (百万美元)

图 39: 本地化产品图片

图 40: 全球本地化规模及增长率 (2021-2032) & (百万美元)

图 41: 其他产品图片

图 42: 全球其他规模及增长率 (2021-2032) & (百万美元)

图 43: 全球不同部署方式AI模型安全测试平台市场份额2025 & 2032

图 44: 全球不同部署方式AI模型安全测试平台市场份额2021 & 2025

图 45: 全球不同部署方式AI模型安全测试平台市场份额预测2026 & 2032

图 46: 中国不同部署方式AI模型安全测试平台市场份额2021 & 2025

图 47: 中国不同部署方式AI模型安全测试平台市场份额预测2026 & 2032

图 48: 科技与基础模型厂商

图 49: 银行及金融服务与保险

图 50: 政府与国防

图 51: 其他

图 52: 全球不同应用AI模型安全测试平台市场份额2025 VS 2032

图 53: 全球不同应用AI模型安全测试平台市场份额2021 & 2025

图 54: 全球主要地区AI模型安全测试平台销售额市场份额 (2021 VS 2025)

图 55: 北美AI模型安全测试平台销售额及预测 (2021-2032) & (百万美元)

图 56: 欧洲AI模型安全测试平台销售额及预测 (2021-2032) & (百万美元)

图 57: 中国AI模型安全测试平台销售额及预测 (2021-2032) & (百万美元)

图 58: 日本AI模型安全测试平台销售额及预测 (2021-2032) & (百万美元)

图 59: 东南亚AI模型安全测试平台销售额及预测 (2021-2032) & (百万美元)

图 60: 印度AI模型安全测试平台销售额及预测 (2021-2032) & (百万美元)

图 61: 2025年全球前五大厂商AI模型安全测试平台市场份额

图 62: 2025年全球AI模型安全测试平台第一梯队、第二梯队和第三梯队厂商及市场份额

图 63: AI模型安全测试平台全球领先企业SWOT分析

图 64: 2025年中国排名前三和前五AI模型安全测试平台企业市场份额

图 65: 关键采访目标

图 66: 自下而上及自上而下验证

图 67: 资料三角测定