kaspersky



AI 赋能
卡巴斯基解决方案

卡巴斯基的 AI 探索始于 2005 年。早在 AI 热潮兴起之前，我们便已利用机器学习解决核心安全问题。如今，这份长期积累已成为我们的独特优势。

AI 只是工具，专业经验才是真正的优势。

在 AI 热潮席卷行业的今天，几乎所有厂商都在放大 AI 的想象空间。而卡巴斯基始终坚持更务实的理念：AI 不是“万能解法”，而是一种需要以可信数据和专业经验为基础的工具。

AI Technology Research

AI 已融入我们的产品基因

- 卡巴斯基设有专门的 AI 技术研究中心
- 拥有超过 **20年** 的 AI 创新积累
- 从使用 **AI 提升安全防护能力**开始，我们也同步持续研究 AI 带来的安全威胁

持续监测 AI 威胁态势

依托近 30 年的威胁研究经验，卡巴斯基能够透过市场噪音，专注识别并应对真实风险：

- 追踪利用 AI 热点实施诈骗的行为
- 持续监测网络犯罪分子如何借助 AI 提升攻击效率与规模
- 预测 AI 威胁的发展趋势，构建更强大的防护能力
- 强化系统对 AI 驱动型威胁的安全防御

久经验证的专业实力

拥有 **130 余项 AI 相关专利**

- 《欧盟人工智能公约》签署成员之一
- 制定了《AI 安全开发指南》
- 基于 AI 的威胁检测机制，是卡巴斯基产品在各类独立测试中持续保持优秀表现的重要支撑

TOP 3

经过广泛测试，并在多年独立验证中持续展现可靠表现。

扫码了解更多



我们的 AI 战略：两大核心方向

卡巴斯基围绕两项关键使命，持续推进全球 AI 研发与创新。

AI 驱动的网络安全

我们利用 AI 帮助企业抵御各类网络威胁——从大规模恶意软件攻击，到经过 AI 强化的高级攻击。

AI 的安全防护

随着企业不断引入 AI 的使用，新的攻击面也随之出现。卡巴斯基 AI CERT 可帮助企业保护各类 AI 系统的安全，涵盖从大语言模型 (LLM) 到工业 AI 模型，防范提示词注入、数据投毒、模型窃取以及供应链攻击等风险。

核心基础：数据 + 专家 + AI



AI 的能力上限，取决于其背后的数据基础与专家支持。卡巴斯基网络安全持续汇聚全球的匿名化威胁遥测数据，并由安全研究人员与事件响应专家不断分析和丰富。这一持续迭代的机制，使我们的 AI 模型保持准确性与稳健性。

AI 实战应用：更强的安全能力，更智能的 SecOps

① 用于威胁检测的 AI：低调而高效

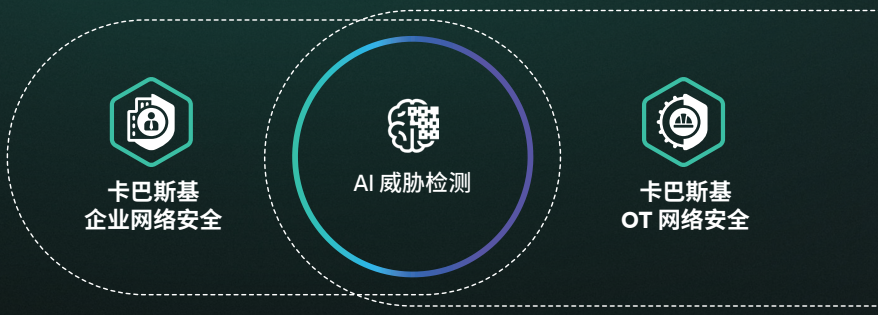
多层 AI 能力已深度融入卡巴斯基 IT 与 OT 安全产品体系，在后台持续运行，帮助拦截恶意软件、勒索软件、网络钓鱼及其他攻击，降低其对业务造成影响的风险。

这一体系结合了统计型、静态及行为分析等 AI / ML 模型，可同时运行于云端与客户本地系统，在不过度依赖云端机制或持续联网的情况下，更有效地识别新型威胁变种。

威胁数量持续增长：

每天检测到 500,000 个恶意对象

卡巴斯基检测数据



② 用于 SecOps 的 AI：赋能团队，而非取代团队

安全人才短缺问题日益突出，SOC 分析师也长期面临海量告警带来的压力。卡巴斯基面向 SecOps 的 AI 能力，可有效提升团队效率，帮助分析师更智能地开展研判、更高效地完成调查与更快速地响应安全事件。

2.1 面向安全运营的 AI 自动化能力

DLL 劫持检测

基于全球匿名化 DLL 加载遥测数据建立正常行为基线，并对异常行为进行分析与告警，辅助分析师快速识别风险。

账号盗用检测

通过学习账号的正常行为模式建立基线，用于识别异常活动。

AI 风险评分

基于主机正常活动建立行为模型，识别可能表明系统遭受入侵的异常告警链，并自动进行优先级排序，帮助分析师降低干扰，更聚焦高优先级威胁。

适用于：

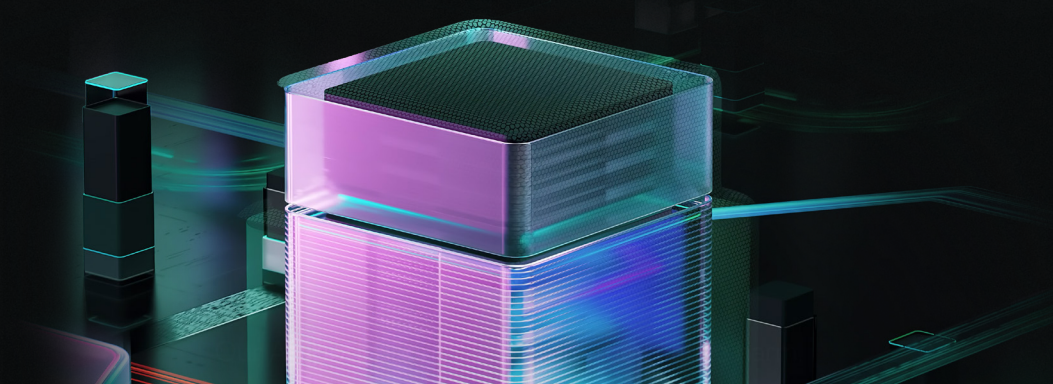
- 卡巴斯基 新一代安全 XDR 专家版
- 卡巴斯基 统一监控和分析平台

AI 驱动的托管安全服务

在 AI 自动分析的辅助下，卡巴斯基分析师团队能够实现 7×24 小时持续安全运营，并进一步缩短平均响应时间 (MTTR)。根据卡巴斯基 MDR 统计数据，AI 自动分析技术可帮助卡巴斯基 SOC 专家减少约 25% 的工作负载。

适用于：

- 卡巴斯基 新一代安全 MXDR 优选版
- 卡巴斯基 托管检测和响应



2.2 面向安全运营的 GenAI 辅助能力

KIRA: SecOps 场景下的 GenAI 智能助手

卡巴斯基调查和响应助手 (KIRA) 是一套面向安全运营场景打造的 GenAI 工具体系。它支持接入兼容 OpenAI 标准的大语言模型 (LLM)，让企业能够基于自身数据与实际需求灵活选择和部署。



事件摘要生成
一键生成完整攻击链的自然语言事件摘要。

按需脚本分析
快速还原并分析混淆恶意代码，秒级理解其行为逻辑。

自然语言威胁搜索
可直接使用自然语言提问，并自动生成结构化查询语句，降低使用门槛。

卡巴斯基
新一代安全
XDR 专家版

卡巴斯基
统一监控和
分析平台

容器镜像扫描结果摘要
提供清晰、完整的镜像说明，包括风险分析与最终评估结果。

卡巴斯基
容器安全

GenAI 辅助威胁情报
我们的 GenAI 助手可从海量 OSINT（开源情报）数据中提取关键信息，将原始数据整理为简洁易读的情报报告，帮助团队更快建立态势感知能力。

卡巴斯基
威胁情报平台



AI 驱动的网络安全
以更智能的方式应对网络威胁

扫码了解更多

www.kaspersky.com.cn

© 2026 年 AO 卡巴斯基实验室。
注册商标和服务商标归其各自所有者所有。

#卡巴斯基