



卡斯基新一代安全
EDR 专家版



卡斯基新一代安全
XDR 专家版



为您的端点基础设施
提供前沿的网络安全防护

卡斯基 新一代安全 EDR 专家版

kaspersky

针对高级威胁的多方位端点防御



卡斯基新一代安全 EDR 专家版适合各个行业、不同规模且拥有内部专业IT安全团队的组织，可提升威胁检测与调查的深度，加速响应速度，并在海量端点的场景下实现具备取证价值的可见性。

在如今高度互联的数字环境中，端点仍是网络攻击的主要入口。要领先于现代威胁，组织仅依靠传统防控已远远不够，还需要具备先进的威胁检测、调查和响应能力。

卡斯基新一代安全 EDR 专家版是一款端点检测和响应解决方案，可与端点防护产品无缝集成，用于阻止大规模攻击并识别高级威胁。它能够自动检测可疑活动，支持安全事件调查，并为安全团队提供必要工具以实现快速、有效的响应。

卡斯基新一代安全 EDR 专家版面向大型分布式 IT 基础设施设计，助力企业快速遏制威胁并全面消除安全事件。它通过单一代理即可实现多方面的端点防护，不仅能简化运维、降低维护与支持工作，还能在维持系统性能的同时提升整体安全态势。



久经验证，屡获殊荣

我们的技术定期接受权威独立测试实验室的严苛检验，产品品质亦获行业专业分析机构高度认可。同时，屡获国际权威奖项殊荣。



为您的团队配备专业 EDR

- 通过屡获殊荣的 EPP 和前沿的 EDR 功能，提高您的安全防护效率
- 加强您对端点基础设施的控制
- 改进对高级威胁的检测和补救措施
- 通过资源分配的优化，帮助建立威胁检测、事件管理和响应流程
- 为您遵守监管要求和标准提供支持

EDR



2 检测时间

基于 IoC、IoA 和自定义规则的威胁发现

利用全球威胁情报提升检测能力

主动威胁捕获和回顾性分析



3 调查

深入调查和根本原因分析

基础数字取证工具包



4 事件响应

支持各种响应操作

EPP



1 防御

强大的检测引擎

多层安全控制措施和数据保护

漏洞和补丁管理

行为分析和自适应异常控制

核心功能

卡巴斯基新一代安全 EDR 专家版可为企业提供基础设施内端点的全景式概览，并在威胁调查全流程实现可视化追踪。其搭载的检测引擎和根本原因分析工具，可确保威胁识别与调查工作兼具高效性与精准性。

回顾性分析以及 MITRE ATT&CK 知识库检测关联，让您能够识别攻击者所使用的战术和技术。该产品还提供主动威胁搜索功能和卡巴斯基威胁情报门户的访问权限，助力安全专家复现攻击路径，有效应对各类复杂网络攻击。

EPP



前沿预防技术， 涵盖基于机器学习 (ML) 的创新技术手段

- 自动阻止威胁
- 自动恢复
- 防止加密尝试
- 防止漏洞被利用
- 防止凭证被盗



安全和数据 控制措施

- 应用程序控制
- 网页控制
- 设备控制
- 自适应异常控制
- 加密和策略管理
- 便携式设备加密



漏洞评估 和补丁管理

- 高级补丁管理
- 漏洞评估
- 授权许可管理
- 集中式应用程序和操作系统部署
- 远程管理工具
- 资产清查

EDR



自动检测 高级威胁

- 数据收集和存储
- 基于攻击指标 (IoA) 规则的高级检测机制
- 自动访问威胁情报 (KSN)
- 回顾性分析
- MITRE ATT&CK 映射



入侵指标 (IoC) 搜索和 威胁捕获

- 完全可见性和控制
- 事件优先级排序
- IoC 扫描
- YARA 规则
- 可访问威胁查找
- 灵活的查询构建器，
实现主动威胁捕获



事件响应

- 事件响应工具
- 自动化响应任务设置
- 响应建议
- 威胁控制
- 集中式事件本地化

卡巴斯基新一代安全 EDR 专家版——卡巴斯基新一代安全系列解决方案的组成部分

卡巴斯基新一代安全解决方案采用分层架构设计，适配各规模企业的网络安全需求。它包含两大产品体系，其中卡巴斯基新一代安全专家版，为配备专业网络安全团队或安全运营中心的企业量身打造，支持按需配置高级 EDR 与 XDR 功能，依托智能化自动化处理机制及弹性扩展架构，助力企业安全团队实现安全运营效能的提升。

为何选择卡巴斯基新一代安全解决方案？



基于人工智能技术的多层防御

卡巴斯基采用基于统计、结构和行为原理的 AI 驱动检测技术组合，能够自动识别威胁，能够自动检测威胁，提高检测速度和准确性。人工智能为资产风险评分提供关键技术支撑。这些技术有助于降低网络事件影响，有效优化 MTTD 和 MTTR。



以深厚的知识、技能和专业知识为后盾

卡巴斯基新一代安全解决方案，依托于卡巴斯基全球安全团队数十载沉淀的丰富经验与深厚知识。我们的专业团队成员紧密协作，全力攻克复杂多变的网络威胁难题，持续迭代优化支撑产品的核心技术。这种以专家为主导的研发模式，有力保障了我们的解决方案兼具可靠性与创新性，精准契合当下的安全防护需求。



与您同步成长的网络安全

卡巴斯基新一代安全解决方案，为各规模企业提供安全防护。随着需求增长，您可以轻松从关键端点保护扩展至更高级别的高级和专家级解决方案。



建立在我们一流的端点解决方案基础之上

十多年来，卡巴斯基产品一直在各种独立测试和评审中雄踞榜首。我们久经经验的自动端点保护方案可减少安全团队需要分析的警报数量，从而大幅提高效率。



www.kaspersky.com.cn

© 2026 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。

了解详情

#卡巴斯基
#引领未来