

通过有效、用户友好且经济高效的扩展安全功能，为您不断增长的业务提供支持

卡巴斯基新一代安全 XDR 优选版

kaspersky cybersecurity true to business

面向中小型企业

充分利用资源，提高事件响应的有效性

以中小型企业为目标的网络威胁正变得更加复杂和激烈。攻击者越来越多地利用合法的系统工具和先进的技术来躲避检测。同时，没有意识到网络安全风险的员工很容易受到网络钓鱼和社会工程攻击，造成财务和声誉损失。

与此同时，有限的资源（包括紧张的预算和熟练员工短缺）使得防御这些威胁更加困难。因此，拥有先进而易于使用的工具，为企业提供适当级别的保护至关重要。

卡巴斯基新一代安全 XDR 优选版适用于拥有完善 IT 基础设施和合理网络安全预算的中小型企业。无论安全管理工作由规模更大的 IT 团队统筹，还是交由专业的小型团队负责，该解决方案均配备便于管理的工具，能够实现专业的安全防护，同时避免给现有资源带来过度负荷。

利用卡巴斯基新一代安全 XDR 优选版扩展安全性

该解决方案专为小型安全团队设计，可提升事件响应能力并培养专业知识，而不会增加耗时的常规任务负担。可自动执行多个流程，让您的团队专注于更重要的事务。

卡巴斯基新一代安全 XDR 优选版可轻松集成到现有的基础设施中，无需添加新的系统组件。



检测、分析和响应

- 行为检测
- 警报聚合
- 云沙盒
- 威胁证据发现 (IoC) 和定制 IoC
- 根本原因分析
- 响应操作范围

端点保护功能

- 增强的反恶意软件
- 扩展硬化
- 漏洞评估
- 端点控制
- 数据保护
- 补丁管理

从专业的端点保护和云安全到 IT 任务自动化和关键 XDR 功能：

专业的**端点保护**

借助经行业实践验证、基于机器学习技术构建的反勒索软件与反恶意软件工具所提供的自动化防护支持，抵御已知及未知威胁的侵袭，杜绝业务中断风险。

通过系统强化和培训修复漏洞

通过基于用户行为的系统强化减少攻击面，并通过集中管理漏洞、补丁和加密节省时间。此外，我们还提供您的团队所需的所有培训，以充分利用新的安全功能。

扩展您的**检测和响应**能力

深入了解威胁及其在端点内外的行动方式。使用自动化和引导式响应来反击攻击，使用基本调查工具追踪其活动。

培训整个团队在安全方面发挥积极作用

为您的 IT 员工和非技术人员提供保持安全的知识和技能。在强化 IT 安全团队专业防线的同时，在全公司范围内培育根植于心的安全意识文化。

利用我们基于云的系统进行**文件处理**

借助我们的云沙盒集成服务，轻松调查恶意文件并获得更多上下文和详细信息。只需上传潜在恶意样本，即可通过产品界面在数秒内检查其声誉状况，并利用生成的数据开展后续的 IoC 扫描。

利用可以信赖的云安全控制影子 IT

通过控制影子 IT，减少漏洞并保护数据和员工。了解哪些云服务正在使用中，阻止未经授权的访问，并识别 Microsoft 365 应用中存储了哪些敏感数据。

支持**多种交付模式，灵活选用**

通过基于云的部署和自动化工具降低总拥有成本，或在本地安装以实现完全控制。

卡巴斯基新一代安全 XDR 优选版——卡巴斯基新一代安全产品线的一部分

卡巴斯基新一代安全是一个分层产品解决方案，适用于各种规模的企业。卡巴斯基新一代安全优选版专为中小型企业量身定制。此类企业拥有专业精干的网络安全团队，期望在规避系统复杂性的前提下增强安全防护。该方案以端点防护为基础，融合端点检测与响应能力，并支持平滑升级至 XDR 或 MXDR，帮助企业逐步构建更成熟的网络安全体系。

为何选择卡巴斯基新一代安全优选版?

建立在我们专业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。我们久经考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，从而提高效率。

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专业。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，精准契合现实世界中的安全防护需求。

基于人工智能技术的多层防御

卡巴斯基使用预测算法、集群技术、神经网路、统计模型和专家算法提升检测速度和改进准确性。

与您同步成长的网络安全

卡巴斯基新一代安全解决方案可保护各种规模的企业。随着需求增长，您可以轻易从关键端点保护扩展至更高层级的高级和专家级解决方案。



www.kaspersky.com.cn

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

了解更多

#卡巴斯基
#安全为本 商道唯真