卡巴斯基端点检测与响应 - 优选版

将您的端点防御能力提升到新的高度，并毫不费力地正面应对规避式威胁。

kaspersky 25 years

卡巴斯基端点检测与响应 — 优选版

是时候提升一个层次了。现在，您不仅准备好了用基本的反恶意软件技术保护您的组织，还能识别、分析并有效消除威胁，那些威胁意图躲避传统保护机制并隐藏在您的系统中，随时准备攻击。

挑战

躲避检测的威胁

规避式恶意软件、勒索软件、间谍软件和其他威胁越来越“聪明”，能够避开传统的检测机制，通过使用合法的系统工具和其他高级技术实施攻击。

勒索软件即服务

黑客可以用低廉的价格购买现成的工具并攻击任何对象——窃取数据，破坏您的基础架构，并索要越来越多的赎金。

有限的资源

随着基础架构变得越来越复杂和广泛，时间、金钱和监控范围等资源开始无法满足需求。我们不做鸡肋产品。

64% 的组织已经遭到了勒索软件的攻击。其中 79% 的组织向攻击者支付了赎金。

卡巴斯基，2022 年 5 月

“我们重视卡巴斯基的全面解决方案、可靠性和及时的服务与支持。它们保障了我们 IT 环境的正常运行。”

NEO 首席信息安全官 Marcelo Mendes，
阅读案例研究

我们如何帮助

卡巴斯基端点检测与响应 (EDR) - 优选版通过提供易于使用的高级检测、简化的调查和自动响应，帮助您识别、分析和消除规避式威胁。

高级保护

我们的高级检测机制包括机器学习、行为分析和云沙盒等技术。

通过简单的可视化分析工具，您可以完全了解威胁及其范围，并在造成任何损害之前，快速采取响应行动，阻止攻击。

一站式解决方案

下一代端点安全与简单易用的 EDR 相结合，可增强对笔记本电脑、工作站、服务器、云工作负载和虚拟环境的保护。

所有这些部署和管理都通过单个云或本地控制台在同一个位置进行。

简单高效

我们在创建 EDR 优选版时考虑了规模较小的网络安全团队的需求，他们希望提升自己的事件响应能力和专业技术，但又没有那么多时间。

我们对大多数任务进行优化并使其自动化，因此您可以将更多时间用在真正重要的事情上。

主要优势

- **防止多种类型的**威胁
- **帮助您的系统和数据**抵御规避式威胁
- **在当前威胁实施攻击之前**将其捕获
- **识别端点上的规避式威胁**
- **了解威胁**并快速分析
- **通过快速自动响应避免遭受损害**
- **借助简单易用的工具**节省时间和资源
- **保护每个端点：**笔记本电脑、服务器、云工作负载

关键功能

- 自带**下一代端点安全防护功能**
- **基于机器学习的**高级检测
- **入侵指标** (IoC) 扫描
- **可视化调查和分析**工具
- 所有必要的数据集中在**一个警报卡中**
- **内置响应**指导和自动化
- **单一云或本地控制台**和自动化
- 支持**工作站、虚拟和物理服务器、VDI 部署和公有云工作负载**

关键用例

我是否已经遭到攻击？

- **基于机器学习的高级检测**（包括云沙盒）可自动检测威胁。
- **从 securelist.com 或其他来源下载并扫描 IoC**，查找高级威胁。

我能清除它们吗？

- **利用多个响应选项**，可隔离主机、阻止文件执行或将其删除。
- **扫描其他主机**，查找所分析威胁的迹象。
- **跨主机应用自动响应**以识别威胁 (IoC)。

如何获得技能培训？

- **查看警报卡中的响应指南**。
- **访问威胁情报门户**并查看最新 TI。
- **在分析和响应威胁的同时提升您的专业知识**。

它是如何做到的？

- 在**可视化进程树中分析威胁**。
- 在**下钻图中跟踪它的操作**。
- **了解其根本原因和进入基础架构的入口点**。

我要如何阻止它再次发生？

- **学以致用** — 知道要屏蔽哪些 IP 和网站、修改哪些策略以及对哪些员工进行培训。
- **创建规则以抵御将来可能出现的**此类威胁，例如防止文件执行。

如何抵御所有常见威胁？

- **部署下一代端点安全技术**，可立即阻止大多数威胁。
- 通过漏洞和补丁管理加快修补。
- **利用端点控制自动缩小**攻击面并调整策略。

运作方式

如需快速演示，请观看**此视频**。

您所在的国家和地区是?

有反恶意软件，还不够吗?

加强端点保护

无论您是使用卡巴斯基还是第三方端点保护，现在都是考虑实施 EDR 的最佳时机。

这不仅仅是为了提高检测和预防能力，也是为了应对规避式威胁 - 识别、分析和清除它们。

详细了解如何防范规避式威胁，请参阅《关于实现最佳安全级别的买家指南》。

已经在使用卡巴斯基?

提高您的安全性

我们正在不断改进产品。为了能充分使用产品的最新功能，请及时升级或迁移到云端，将繁琐的日常操作交给我们处理。

最新版本的卡巴斯基 EDR 优选版提供以下功能：

- **警报卡中的引导式响应！**
- **在执行响应之前进行系统关键对象检查！**
- **警报卡中的威胁情报文件声誉！**
- **无限深度的过程树分析！**

点击此处详细了解新功能。

还未使用过卡巴斯基产品?

提高您的安全性

卡巴斯基 EDR 优选版凭借以下优势获得了全球数千家企业的青睐：

- **通过单个产品提供强大的 EPP 和基础 EDR 功能**
- **专为小型网络安全团队设计的简单易用的 EDR 功能**
- **支持云端或本地部署的轻量级灵活解决方案**

查看卡巴斯基优选安全 — 基于 EDR 和 MDR 技术的规避式威胁综合性解决方案

循序渐进

您使用的工具应该能完全满足您的网络安全和业务需求，对于您的团队和现有资源而言也是理想之选。因此，我们简化了选择网络安全级别的过程，相信这是您目前的主要关注点。您可以根据组织目前的情况，从三种不同的方案中进行选择。

Kaspersky Security Foundations

自动拦截绝大多数威胁。

- **全方位自动防御常见威胁（占网络攻击的绝大多数）引起的事件。**
- **为任何规模和复杂性的组织筑牢综合防御战略的基础阶段。**
- **为拥有小型 IT 团队和新兴安全专业知识的组织提供可靠的端点保护。**

» 了解更多

Kaspersky Optimum Security

如果您符合以下情况，就可以建立抵御规避式威胁的能力：

- **拥有具备基础网络安全专业知识的小型 IT 安全团队。**
- **IT 环境的规模和复杂性都在不断增长，攻击面也由此扩大。**
- **需要加强保护，但缺乏网络安全资源。**
- **加强事件响应能力的需求日益增长。**

» 了解更多

Kaspersky Expert Security

为组织应对复杂和类 APT 攻击做好准备：

- **存在复杂的分布式 IT 环境。**
- **拥有成熟的 IT 安全团队，或完备的安全运营中心 (SOC)。**
- **由于安全事件和数据泄露的成本较高，因此高度重视风险防控。**
- **所从事的领域受到严格监管。**

» 了解更多

我们公司的价值主张

我们是一家全球性的私营网络安全公司，在全球拥有数十万客户及合作伙伴，坚守**透明度和独立性**。25 年来，我们一直在构建工具并提供服务，用**测试最多、获奖最多的技术**，确保您的安全。

IDC

《IDC MarketScape：2021 全球大型企业现代端点安全供应商评估》

主要参与者

AV-Test

高级端点保护：勒索软件防护测试

100% 防护

Radicati Group

高级持续性威胁 (APT) 市场象限

顶尖参与者

如果您有更高的需求

请查看**卡巴斯基 EDR 专家版**，这是一款强大的 EDR 工具，可以为您的专家提供深入的威胁捕获能力、广泛的定制和卓越的检测机制。

进一步了解

要了解卡巴斯基EDR 优选版如何在节约您的安全团队和资源的同时解决网络威胁，请访问
www.kaspersky.com/enterprise-security/edr-security-software-solution

网络威胁新闻： securelist.com
IT 安全新闻： business.kaspersky.com
中小企业的 IT 安全： kaspersky.com/business
企业的 IT 安全： kaspersky.com/enterprise

kaspersky.com.cn