卡巴斯基 Next EDR 优选版

将您的端点防御能力提升到新的高度，正面应对规避式威胁

kaspersky

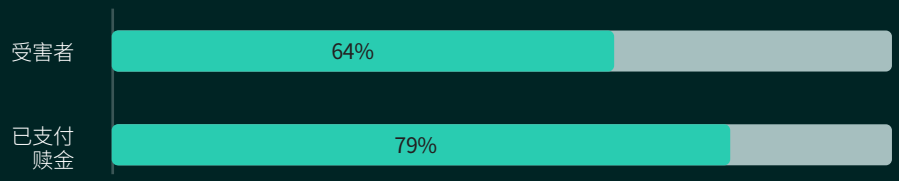
巴斯基 Next EDR 优选版

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。

企业高管如何看待勒索软件威胁，卡巴斯基，2022 年 5 月

是时候提升一个层次了。
识别、分析和消除用来规避传统保护的威胁



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”，能够在攻击中使用合法的系统工具和其他高级技术来避开传统检测。

勒索软件即服务

如今的黑客可以购买现成的工具和攻击任何人：偷窃数据、损害基础架构和索取不断增长的赎金。

有限的资源

基础架构变得更加复杂和多样化，而资源（时间、金钱和人）却短缺。这是昂贵的冷板凳软件的温床。

“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 的首席信息安全官 Marcelo Mendes

阅读案例研究

我们如何帮助

卡巴斯基 Next 是我们的旗舰产品线，旨在帮助您轻松构建更好的安全体系。无论您是在寻找必不可少的 EDR 功能还是为将来采用 XDR 铺路，卡巴斯基 Next 都近在咫尺，它提供适应性良好、强健的云原生保护，具有无与伦比的网络安全成就。

卡巴斯基 Next 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功能，帮助您识别、分析和消除规避式威胁。

高级保护

我们的先进检测机制包括行为分析和机器学习

所有这些与简单的可视化分析工具和快速响应操作结合，使您可以全面理解威胁及其范围，并在造成任何损害之前停止攻击。

借助于 云发现 和阻止能力以及 MS Office 365 Security，攻击面减少在端点上和云中完成。

一站式解决方案

下一代端点安全与简单的 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。

只需部署和管理一个控制台，在云中或本地。

简单高效

我们在创建 卡巴斯基 Next 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，但又没有许多时间。

我们会自动化和优化大部分任务，这样您就可以将时间花在处理重要东西上。我们提供您和您的 IT 团队需要的培训，以最充分地利用您的新安全能力。

现在您可以：

- 提前防止网络威胁
- 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损害
- 借助简单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
- 使用专业或专家视图控制台，由您选择！

现在您拥有：

- 下一代端点安全
- 基于机器学习的高级检测能力
- 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
- 支持所有工作站、虚拟和物理服务器、VDI 部署和公有云工作负载
- 经过完整产品培训的 IT 安全工作人员

最重要的时候有这些问题的答案

我是否已经遭到攻击？

- 应用基于机器学习的高级检测
- 从 securelist.com 或其他来源下载并扫描 IoC，查找高级威胁

它是如何做到的？

- 在可视化进程树中分析威胁
- 在下钻图中了解它的操作
- 了解其根本原因和进入基础架构的入口点

如何消除威胁？

- **利用多个响应选项**，可隔离主机、阻止文件执行或将文件删除
- **扫描其他主机**，查找所分析威胁的任何迹象
- **发现威胁 (IoC) 时在各主机上自动应用响应**

其他威胁怎么办？

- **部署下一代端点安全技术**，可立即阻止大多数威胁
- **自动减少您的攻击面**和调整您的策略
- **控制您的用户可以使用的应用程序和设备**

如何在将来防止这种事情发生？

- **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
- **保护您的云：发现、限制和阻止访问**未经授权的云资源、服务、即时通讯软件等。
- **了解并控制** MS SharePoint Online、OneDrive 和 Teams

如何更好地做到这些？

- **使用警报卡中的响应指南**
- **访问我们的威胁情报门户**并查看最新 TI
- **通过分析和响应威胁提升您的专业知识**
- **使用内置的培训**和认证内容，其中包含在模拟环境中的互动任务。

怎么能抽出时间处理所有这些事情？

- **自动化漏洞和补丁管理**，这是保持端点安全的关键方法
- **对所有员工执行远程管理原生加密**以保护公司数据安全
- **自动化耗时的安全和 IT** 管理任务

巴斯基 Next
EDR 优选版

巩固防御
通过关键调查和响应，
提升您的网络安全

为您提供
· 增强的可视性和响应功能
· 扩展的云上安全性
· 企业级控制

[1] 入侵指标

卡巴斯基 Next –
您有备无患的安全方案

卡巴斯基 Next EDR 优选版属于我们的 卡巴斯基 Next 产品线，提供强大的端点保护和控制，既有 EDR 的透明和速度，又有 XDR 的全面可见性和强大工具包，其根据您最关键的网络安全需求分为三个简单的产品等级。随着您需求的增长，您可以轻松切换产品层级，升级安全功能。

进一步介绍

卡巴斯基 Next 各产品层级的主要功能：

卡巴斯基 Next EDR 基础版

构建网络安全强大核心的最直接方法。

- 基于机器学习的强大端点保护能力
- 自动修复
- 多项自动化功能
- 灵活的安全控件
- EDR 根本原因分析工具

巴斯基 Next EDR 优选版

建立您对规避式威胁的防御能力和专业知识。

- 关键的 EDR 功能提供可见性、分析和响应能力
- 强大的端点保护
- 改进的控件、补丁管理和云安全
- 面向 IT 人员的卡巴斯基网络安全培训

卡巴斯基 Next XDR 专家版

让您的业务免遭最复杂的高级威胁。

- 与您现有的安全基础设施无缝整合
- 实时洞察和深入了解威胁
- 高级威胁检测
- 跨资产关联
- 自动响应

为何选择 卡巴斯基?

我们是一家全球性的私营网络安全公司，在全球拥有成千上万名客户及合作伙伴，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 集团
高级持续性威胁 (APT) 市场象限
顶尖参与者

进一步了解

若要进一步了解 卡巴斯基 Next EDR 优选版如何应对网络威胁，同时支持您的安全团队和节省资源，请访问 https://go.kaspersky.com/next.

进一步了解 卡巴斯基 Next EDR 优选版

卡巴斯基 Next EDR 优选版

卡巴斯基 Next EDR 基础版 了解更多

卡巴斯基 Next XDR 专家版 了解更多

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
大型企业的 IT 安全：kaspersky.com/enterprise

kaspersky.com.cn

了解有关 卡巴斯基 Next 的更多信息：
https://go.kaspersky.com/next

在我们的交互式工具中完成一个简短调查，选择最适合您的层级：
https://go.kaspersky.com/Kaspersky_Next_Tool