卡巴斯基端点检测和响应

kaspersky 引领未来

网络犯罪分子正变得越来越狡猾，能够成功绕过现有防护。您企业的每个领域都可能面临风险，进而干扰业务关键流程，损害生产力并增加运营成本。

利用卡巴斯基 EDR，您的组织可以：

- 有效**监控**威胁 – 不只是恶意软件
- 有效**检测**威胁 – 使用先进技术
- 集中**汇总**原始数据和裁定
- 对攻击做出快速**响应**
- **根据已发现的威胁阻止**恶意操作

...所有操作都通过直观的 Web 界面进行，调查和响应更加容易。

首先增强端点防御

对于网络犯罪分子来说，公司端点仍然是主要目标，它们将数据、用户和公司系统聚合在一起以生成和实施业务流程。为了保护公司端点并防止它们被用作基础设施的进入点，您的 IT 安全团队应该寻求措施，增强现有的防御能力。要实施从自动化常见威胁阻止到敏捷恰当应对复杂事件的完整端点保护周期，需要经先进的防御功能补充的预防技术。

卡巴斯基端点检测和响应 (EDR) 使用户能够全面掌握公司网络中的所有端点，并提供卓越的防御措施，支持例行任务的自动化，以便了解、确定优先级、调查和清除复杂威胁与类似于 APT 的攻击。

卡巴斯基 EDR 和 IDC 的 2020 年端点安全报告的关键信息*

- 薄弱的 EPP 解决方案会摧毁 EDR 工具的价值

  卡巴斯基通过单一代理提供强大的完整端点防御 (EPP+EDR)

- 人员和时间因而成为衡量 EDR 工具投资回报的新指标

  卡巴斯基将高级自动化应用于复杂问题，从而解放您的安全专家的宝贵时间

- EDR 必须利用端点外部的数据

  卡巴斯基通过单一工具增加了基于邮件和基于 Web 的高级威胁发现和可视性，提高了 EDR 的有效性。

亮点

- 卡巴斯基 EDR 的强大 EDR 功能增强了我们久经考验、屡获殊荣的旗舰端点保护平台 (EPP) – **卡巴斯基企业安全解决方案**，进一步提升了您的整体安全级别。单个代理即可提供对常见威胁的自动防护，以及针对复杂攻击的高级防御，从而简化事件处理流程，并将维护要求降到最低。端点无额外负担，也没有进一步成本 – 确保您的工作站和服务器受到完全保护，远离最复杂的针对性攻击。
- 卡巴斯基 EDR 可以减少初始证据收集所需的时间，提供完整的遥测分析，并最大程度地实现 EDR 流程自动化，从而缩短整体事件响应时间，无需吸引额外的 IT 安全资源。
- 卡巴斯基 EDR 可以融入**卡巴斯基反针对性攻击平台**，将 EDR 功能和网络级高级威胁发现相结合。IT 安全专家拥有在端点和网络级别处理高级多维威胁发现、应用前沿技术、进行有效调查和实现快速集中响应所需的所有工具 — 全部通过一个解决方案实现。

* IDC 观点，《2020 年端点安全：EPP 再度崛起，EDR 成为众望所归》

如果您的组织希望实现以下目标，卡巴斯基 EDR 将是理想选择：

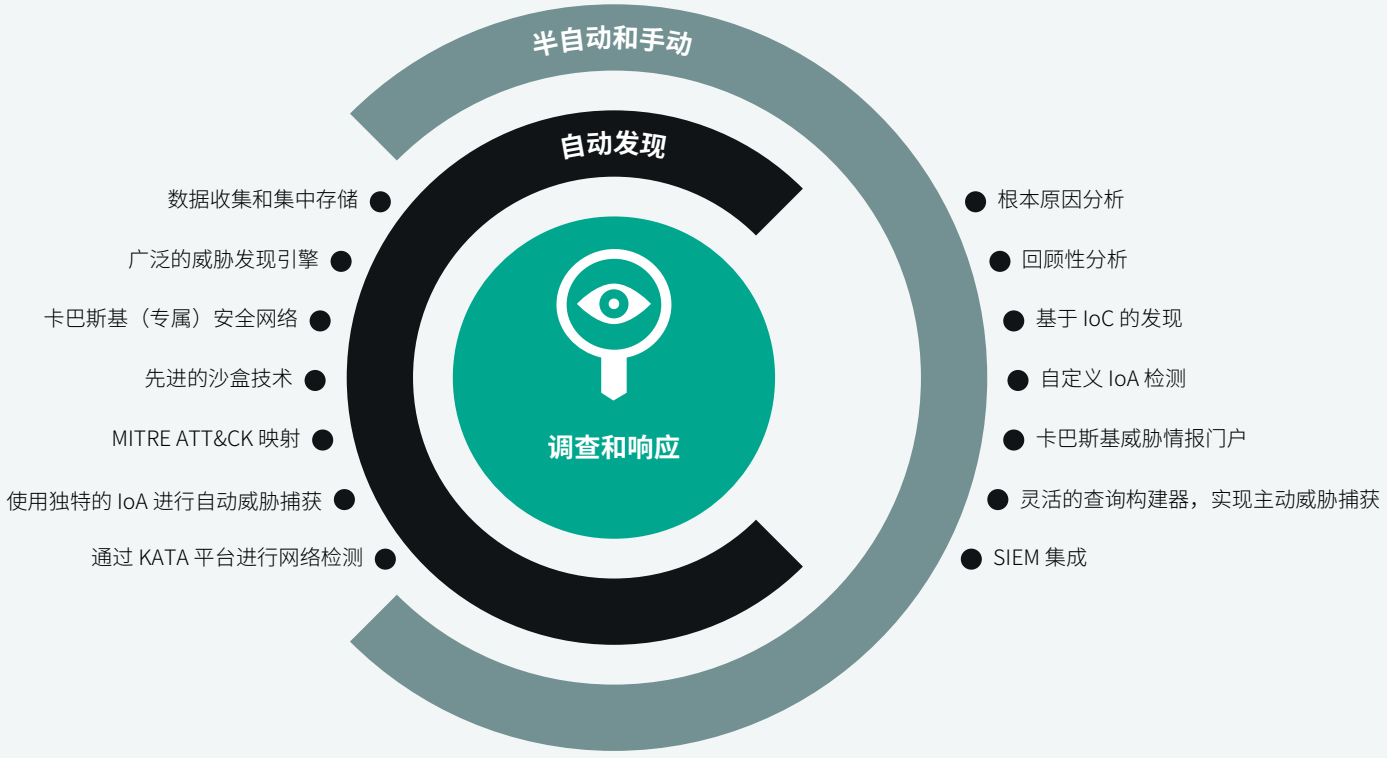
- 通过易于使用的企业解决方案升级您的安全性，以实现事件响应
- 自动执行威胁识别和响应 – 调查过程中不会出现业务中断
- 通过先进技术增强端点可视性和威胁检测
- 了解威胁行为者为实现其目标而采用的特定策略、技术和程序 (TTP)，从而实现更有效的防御和安全资源分配
- 建立统一且有效的威胁捕获、事件管理和响应流程
- 提高内部 SOC 的效率 – 不浪费时间分析无关的端点日志
- 通过执行端点日志、警报审核和调查结果记录来帮助实现合规性

迅速发现并遏制最复杂的威胁

卡巴斯基 EDR 提供高级端点保护并提高 SOC 效率，实现高级威胁发现并提供对回顾性数据的访问，即使在无法访问受损端点或数据在攻击过程中被加密的情况下也是如此。通过我们独特的攻击指标 (IoA)、MITRE ATT&CK 的充实数据和灵活的查询构建器，以及访问我们的威胁情报门户知识库，增强了调查功能 – 所有这些都促进了有效的威胁捕获和快速的事件响应，从而限制和预防损失。

用例：

- 在整个网络上主动搜索入侵证据
- 在入侵者可能造成重大损害和破坏之前，快速检测入侵并进行补救
- 通过无缝的工作流程对数千个端点的事件进行快速调查和集中管理
- 验证其他安全解决方案发现的警报和潜在事件
- 自动执行例行操作 – 有助于尽量减少手动任务，释放资源并减少“警报过载”的可能性



卡巴斯基 EDR 在企业中的业务优势：

- 帮助消除安全漏洞并减少攻击 “停留时间”
- 在威胁检测和响应过程中自动执行手动任务
- 解放 IT 和 IT 安全人员来执行其他关键任务
- 简化威胁分析和事件响应
- 减少识别和响应威胁所需的时间
- 帮助实现完全合规性

如果您想要更多功能... 卡巴斯基托管检测和响应

在卡巴斯基 EDR 中添加完全托管和量身定制的全天候防御，这意味着您的 IT 安全资源可以得到节省，只需将事件相关的处理任务转移给卡巴斯基，或者在您的内部团队缺乏有足够资质的安全专家来满足特定要求时寻求我们的专家判断和独特的威胁捕获专业知识。

Gartner peerinsights customers' choice 2020™

Gartner Peer Insights 的 2020 年 EDR 解决方案客户选择奖将卡巴斯基评选为最佳供应商

卡巴斯基是全球仅有的 6 家获得 Gartner Peer Insights 2020 年端点检测和响应解决方案客户选择奖的供应商之一，我们的服务和支持在所有供应商中获得最高评价，这是客户对卡巴斯基 EDR 最极致的称赞。

Gartner 免责声明

Gartner Peer Insights “客户选择奖” 由最终用户评论的主观意见、评级和根据记录在案的方法应用的数据构成；它们既不代表也不构成 Gartner 或其附属机构认可的观点。

MITRE | ATT&CK®

检测质量已经 MITRE ATT&CK 评估确认

认识到策略、技术和程序 (TTP) 分析在复杂事件调查中的重要性，以及 MITRE ATT&CK 在当今安全市场中的作用：

- 卡巴斯基 EDR 参与了 MITRE 评估第二轮 (APT29)，并在第二轮范围内的检测应用于当今针对性攻击关键阶段的主要 ATT&CK 技术方面展现出高水平的性能。
- 卡巴斯基 EDR 的检测充实了 MITRE ATT&CK 知识库中的数据，可深入分析对手的 TTP。

如需了解更多信息，请访问 kaspersky.com/MITRE

如需进一步了解卡巴斯基 EDR，请访问：

kaspersky.com/enterprise-security/endpoint-detection-response-edr

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

www.kaspersky.com.cn

我们屡获殊荣。我们独立评测。我们价格透明。我们致力于打造一个通过科技改善生活的更加安全的世界。我们保护世界安全的目的，是让地球上的每个人都能享受它带来的无限机会。确保网络安全，创造更安全的明天。

如需了解更多信息，请访问
kaspersky.com/transparency

Proven. Transparent. Independent.