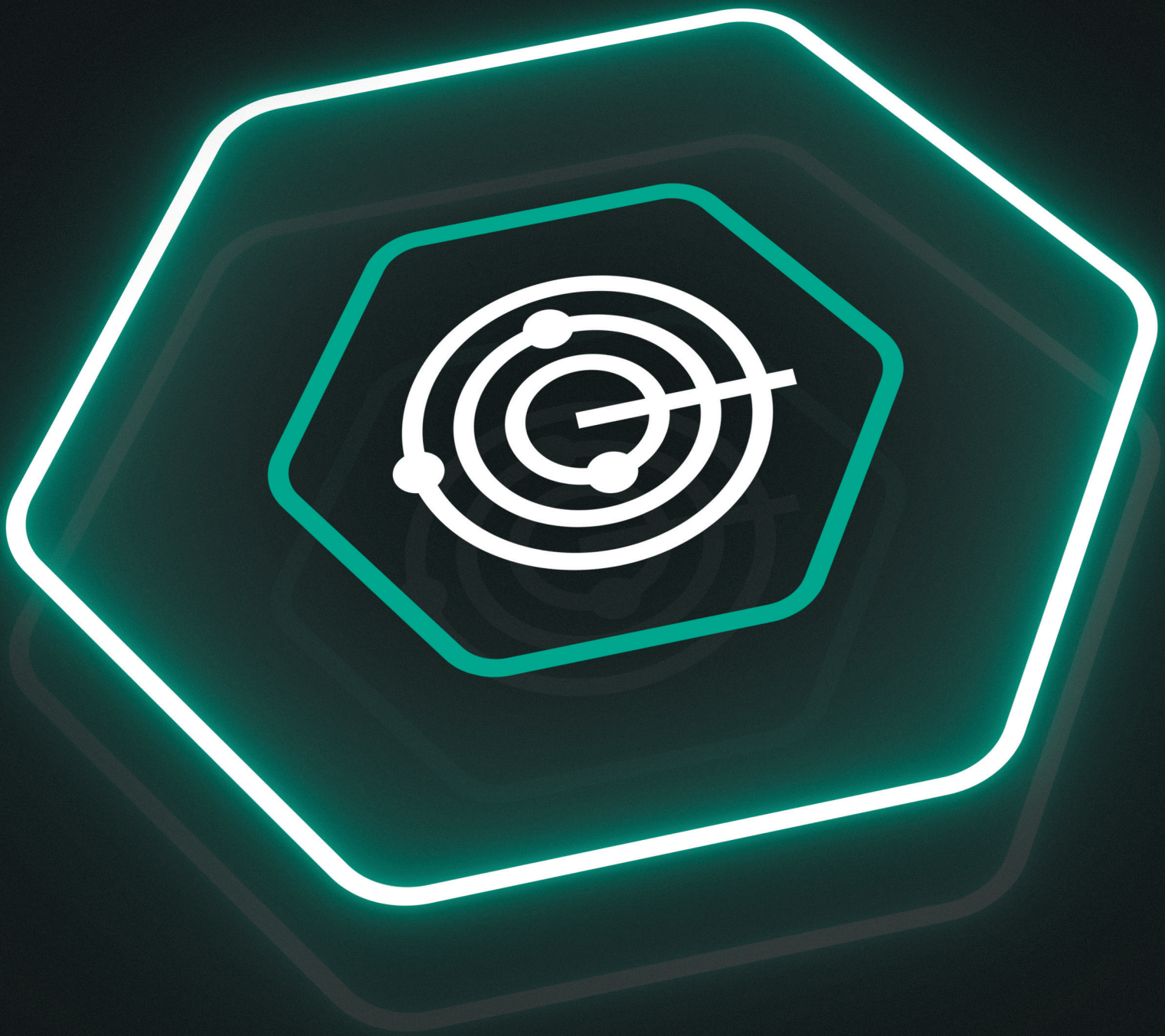


卡巴斯基反针对性攻击平台

kaspersky 引领未来

当今的网络犯罪分子专门设计独特和创新的系统渗透和破坏方法。随着威胁不断演变并变得更加复杂和具有破坏性，快速检测和最快、最适当的响应都变得至关重要。

企业必须不断反思其 IT 安全防御措施，

才能比日益增长的网络威胁领先一步，并限制所产生的任何经济损失。

卡巴斯基反针对性攻击平台：

- **减少**识别和响应威胁所需的时间
- **简化**威胁分析和事件响应
- **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 安全人员来执行其他关键任务
- **支持**全面的合规性

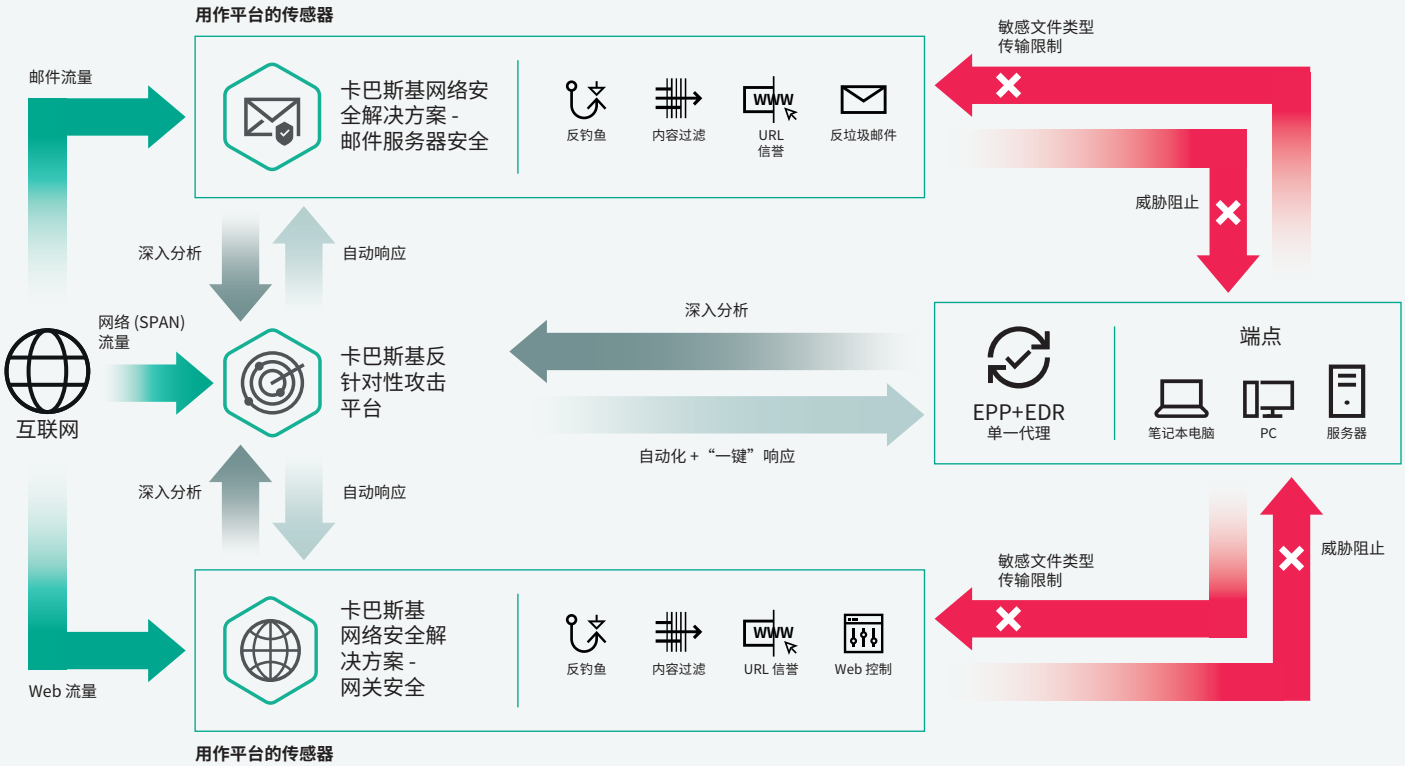
统一的解决方案实现无与伦比的网络安全

职业网络犯罪分子现在常使用多向量方法。卡巴斯基反针对性攻击平台结合了网络级高级威胁发现和 EDR 功能，同时为 IT 安全专家提供处理高级多维威胁发现、应用前沿技术、进行有效调查、主动捕获威胁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。

最复杂的攻击在您的关注和控制之下

该平台作为扩展的检测和响应解决方案，提供一体化 APT 防护，由我们的威胁情报提供支持并映射到 MITRE ATT&CK 框架。所有潜在威胁入口点 – 网络、Web、邮件、PC、笔记本电脑、服务器和虚拟机 – 都在您的控制之下。

卡巴斯基反针对性攻击平台与**卡巴斯基企业安全解决方案**完全集成，与卡巴斯基 EDR 共用一个代理。它还与**卡巴斯基网络安全解决方案 - 邮件服务器安全**和**卡巴斯基网络安全解决方案 - 网关安全**集成，这两个解决方案为平台提供传感器，可自动响应更复杂的电子邮件和网络威胁。



值得信赖的安全解决方案，提供完整的隐私

所有对象分析均在现场执行，没有出站数据流，而卡巴斯基专属安全网络提供实时入站信誉更新，同时保持公司数据完全隔离。

统一平台，通过以下方式加速数字转型创新：

- **整体业务连续性。**我们从一开始就将安全性和合规性纳入新流程
- **对公司 IT 基础架构的**完全可视性
- **最大的灵活性**，允许在任何需要可视性和控制的物理和虚拟环境中部署
- **自动执行威胁发现和响应任务**，优化安全性、事件响应和 SOC 团队的成本效益
- **与现有安全产品紧密、直接地集成**，从而提高整体安全级别并保护传统安全投资

主要功能：

多层传感器架构 – 通过网络、Web 和电子邮件传感器以及端点代理的组合实现全方位可视性。

广泛的威胁发现引擎 – 使用网络传感器（网络流量分析）和端点代理（EDR 功能）的数据，以实现快速裁定并减少误报。

高级沙盒 – 为深入分析威胁活动提供一个安全的环境，支持操作系统组件的随机化、虚拟机中的时间加速、反规避技术、用户活动模拟以及映射到 MITRE ATT&CK 知识库的结果 – 所有这些都有助于高效的基于行为的检测。

回顾性分析 – 即使在无法访问受损端点或数据已被加密的情况下，也可以通过自动化数据、对象和裁定集合以及集中存储进行分析。

两种模式的威胁情报交互 – 与卡巴斯基安全网络的全球信誉数据进行自动比较，以及通过卡巴斯基威胁情报门户手动进行威胁捕获和调查查询。

实时自动威胁捕获 – 事件与卡巴斯基威胁捕获者生成的一套独特的攻击指标 (IoA) 相关联，并映射到 MITRE ATT&CK 矩阵，提供清晰的事件描述、示例和响应建议。

利用我们强大灵活的查询构建器进行主动威胁捕获 – 分析人员可以构建复杂的查询，以搜索非典型行为和可疑活动，以及特定于您的基础设施的威胁。

简而言之

可靠的数据保护、IT 基础设施安全性以及业务流程稳定性和合规性是当今企业实现可持续发展的前提条件。

卡巴斯基反针对性攻击平台可以帮助像贵组织这样的拥有成熟 IT 安全机制的组织，它能帮您构建可靠的防御机制，保护您的企业基础设施免受 APT 式威胁和定向攻击的侵扰，并为实现法规合规性提供支持，而且不需要额外的 IT 安全资源。借助能够最大程度利用自动化技术、最大限度提升成果质量的统一解决方案，您就可以快速识别、调查和响应复杂事件，从而帮助 IT 安全团队或 SOC 团队摆脱手动任务，提升其工作效率。

经验证是业界最有效的解决方案

SE Labs 对卡巴斯基反针对性攻击平台进行了一系列黑客攻击测试，**并给出了 3A 的评分**。

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

作为全球仅有的 6 家获得 Gartner Peer Insights 2020 年 EDR 解决方案客户选择奖的供应商之一（客户对我们的扩展 EDR 解决方案的最极致称赞）– 以卡巴斯基 EDR 为核心的卡巴斯基反针对性攻击平台。

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。

在独立的 “ICSA Labs: 高级威胁防御（2019 年第 3 季度）” 测试中，卡巴斯基反针对性攻击平台**实现了 100% 检测率和零误报**。

检测质量已经 MITRE ATT&CK 评估确认

卡巴斯基反针对性攻击平台的核心要素（卡巴斯基 EDR）参与了 MITRE 第二轮评估 (APT29)，并在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。

如需了解更多信息，请访问 kaspersky.com/MITRE

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

Radicati Group 将卡巴斯基评为**其 2020 年高级持续性威胁 (APT) 防护市场象限中的顶尖参与者**。

如需进一步了解卡巴斯基反针对性攻击平台，请访问：

kaspersky.com/enterprise-security/anti-targeted-attack-platform

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.