kaspersky

卡巴斯基
托管检测和响应

先于风险
保护业务

卡巴斯基托管检测和响应是一项专家主导的服务，提供全天候监控、检测、调查以及针对复杂网络攻击的快速响应。该服务将人工检测与全球威胁情报相结合，以此增强组织现有的安全体系。无论企业规模或行业背景，该服务均可提升 IT 与 OT 环境的整体安全性。

依托全天候托管服务提升安全韧性

随着远程办公的普及、数字化协作的激增、安全人才的稀缺，加之网络威胁已能轻易绕过传统自动防御，各种规模的企业都面临着严峻的防御压力。在当前环境下，对每起事件做出快速、有效的响应至关重要。

当今网络威胁概览[1]

1 初始攻击路径

31% 有效账户利用

13% 信任关系劫持

39% 公共应用的漏洞利用

2 内网渗透与目标达成

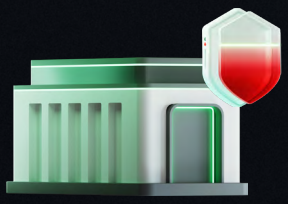
在缺乏系统配置规范的基础设施中，攻击者常利用合法工具 (如 Mimikatz、PsExec、SoftPerfect Network Scanner) 进行渗透。

3 影响

42% 文件被加密

17% 遭遇数据泄露

11% 植入持久化后门以备后续攻击



事实表明，攻击者在得手后往往会再次潜入。

攻击持续时间

快速	平均水平	长期持续型
45%	20%	35%
不超过 1 天	13 天	253 天

核心优势

从部署之初，即可为端点、网络、云端等各类攻击面提供持续的高级防护。

直接对接全球专家资源，获取全天候 SOC 运营支持，无需自行组建、配置或维护内部安全中心。

将监控、研判与调查工作委托给专业团队，减轻内部安全人员的工作量。

通过专家经验、威胁情报与 AI 的结合，在事件影响业务前实现有效拦截，保障安全结果。

卡巴斯基 MDR 成功检测并拦截了一次零日攻击，及时化解了可能导致业务严重中断的风险。

GTO Grandeza de México

Daniel Huerta Santos
瓜纳华托州政府网络安全经理

阅读详情

1 卡巴斯基 MDR 和事件响应报告

卡巴斯基 MDR 提供的服务

上线即享高级威胁持续防护

卡巴斯基 MDR 支持快速部署，无需额外基础设施。依托专家团队与威胁情报，实现跨领域的多维检测。服务基于数十亿条遥测信号，提供主动威胁搜索、根因分析及快速自动化处置，从部署之初即可防范已知与零日威胁。

专家驱动与情报增强的安全运营

借助卡巴斯基 MDR，您的安全运营将由拥有丰富实战经验和行业认证的全球专家团队接管。通过整合市场领先的威胁情报与 AI 技术，专家团队能够深入研判每一条警报，加速检测并缩短平均响应时间 (MTTR)。

提升运营效率，实现成本可控

- 卡巴斯基 MDR 能够规避从零构建内部 SOC 的高昂成本与复杂流程。自行组建 SOC 往往耗费巨大，且可能导致关键的安全能力建设推迟数月甚至数年。
- 对于已有 SOC 的组织，该服务可分担全天候监控、告警研判及事件分类等繁重任务，从而将您的分析师从琐事中解脱出来，专注于更高价值的战略性安全事务。

核心功能

- 为尚未建立 SecOps 体系的组织提供即插即用的全天候防护
- 通过协同管理模式，增强内部安全团队的实战能力
- 针对工业控制系统等 OT 环境提供深度防御
- 为嵌入式设备及系统提供持续的定向安全保障

30 分钟
我们的平均 MTTR[2]

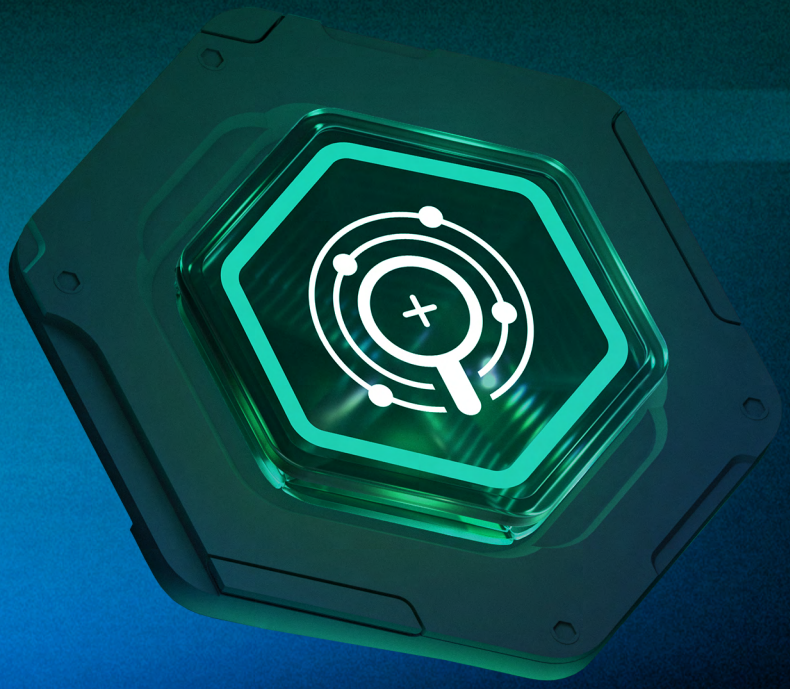
30%
的警报由 AI 自动分析师自动处理[1]

不超过 15 分钟
激活卡巴斯基 MDR 所需的时间

长达 2 年
即可完成内部安全运营的从零部署

70%
的安全团队难以应对安全工具产生的大量警报[3]

2 根据我们的年度 MDR 分析师报告
3 2024 年现代信息安全专业人员画像



卡巴斯基
托管检测和响应

预约演示

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。

#卡巴斯基
#引领未来