kaspersky

EDR
端点检测和响应

识别绕过端点保护的新型、未知的和规避式威胁，并自动执行日常安全任务

VS

托管检测与响应
托管检测和响应

即使面对最复杂、最具创新性的非恶意软件威胁，也能提供持续的托管保护

VS

扩展检测与响应
扩展检测和响应

主动检测多层基础设施的复杂威胁，并自动响应和解决这些威胁

运作方式

- 支持对绕过防御机制的威胁进行高级检测和搜寻
- 增强威胁可见性和可视化
- 简化根本原因分析
- 提供集中式自动化响应

- 收集安全产品的遥测数据，主动分析系统活动元数据以找出任何正在发生或即将发生的攻击迹象，并提供托管或引导式响应

- 集成多个工具和安全应用程序
- 监控端点、网络、云端、Web 服务器和邮件服务器等的数据，以检测和清除复杂威胁
- 通过自动化跨产品交互来简化信息安全管理

它最适合的对象是谁？

- 拥有内部 IT 安全团队但需要借助粒度化的端点可见性和集中响应来减少手动处理任务的企业

- 希望通过减轻关键检测和响应任务的负担来扩展内部 IT 安全能力的公司
- 可能没有预算或专业人员来建立自己内部 SOC 的组织

安全防御较为成熟的企业希望通过单一平台提供：

- 连贯显示整个基础设施的动态
- 内置威胁捕获和威胁情报
- 出色的事件优先级划定和更少的误报

商业价值

- 为安全团队提供他们需要的统一可见性和控制能力，让他们可以主动搜寻威胁而不是等待警报
- 通过自动执行一系列分析、调查和响应流程，最大程度地提高现有 IT 安全团队的能力
- 提升 IT 安全团队的工作效率，而无需同时使用多个工具和控制台，进一步推动成本效率

- 解决网络安全人才危机，确保即时防御复杂威胁
- 支持事件管理流程的外包，以更好地将有限且宝贵的内部资源集中在交付关键成果上
- 降低总体安全成本，无需部署复杂的安全解决方案并聘请一系列内部安全专家

- 针对不断变化的威胁环境提供全方位保护
- 着眼整个生态系统，最大限度地提高所使用的网络安全工具的效率，节省资源并降低风险
- 简化 IT 安全专家的工作，并为他们提供调查多媒介攻击所需的额外背景信息
- 尽量缩短 MTTD 和 MTTR，这对于抵御复杂威胁和针对性攻击至关重要
- 在整个安全技术堆栈中实现集中式自动化响应

如果您是一家安全防御体系较为成熟的组织，希望借助 XDR 的功能进一步筑牢安全防线，不妨了解一下

Kaspersky Expert Security

了解更多