elastic

Search. Observe. Protect.

EDR 对比XDR

终端检测与响应 (EDR) 和扩展检测与响应 (XDR)，它们虽然在首字母缩略词中仅相差一个字母，却为网络安全团队提供了截然不同的结果。下面我们详细列出了团队可从这两种解决方案中得到的预期结果。

EDR	XDR
• 专注于终端保护	• 通过跨终端、云、用户、网络和其他载体的多种集成，可实现广泛的检测
• 使用 Machine Learning 来检测和防御恶意软件和勒索软件	• EDR 功能 + Machine Learning 驱动的分析功能，可有效关联活动和识别威胁
• 集成功能最少的独立型工具	• 与其他多种工具集成的一体化安全平台，可为分析师提供单一参考点
• 不需要高级的安全成熟度	• 需要高级的安全成熟度/成熟的安全团队
• 在终端阻止攻击；提供检测告警、主机隔离、自动响应	• EDR 功能 + 跨多个威胁向量、环境和解决方案的扩展型集中管理和执行功能

虽然 EDR 更容易实施到安全团队的现有工具集中，但要提高团队对组织整个攻击面的监测、检测和响应能力，XDR 则要比 EDR 有效得多。

想知道哪种解决方案最适合您组织的需求？何不两者都兼而有之？借助 Elastic 安全的 Limitless XDR，可让 EDR 与 SIEM 和云安全一起，都成为综合解决方案的关键组件。**如需了解更多信息，请参见：**
elastic.co/cn/security

 | © 2021 Elasticsearch B.V.保留所有权利。