elastic

Search. Observe. Protect.

EDR vs. XDR

Endpoint Detection & Response (EDR) und Extended Detection & Response (XDR) klingen zwar sehr ähnlich, liefern aber sehr unterschiedliche Ergebnisse für Cybersicherheitsteams. Hier finden Sie eine Aufschlüsselung davon, was Teams von den beiden Lösungen erwarten können.

EDR	XDR
• Gezielter Schutz für Endpunkte	• Umfassende Erkennung mit vielfältigen Integrationen für Endpunkte, Cloud, Nutzer, Netzwerke und andere Vektoren
• Verwendet Machine Learning, um Malware und Ransomware zu erkennen und abzuwehren	• EDR-Funktionen + Analytics mit Machine Learning, um Aktivitäten zu korrelieren und Bedrohungen zu identifizieren
• Eigenständiges Tool mit minimalen Integrationsfunktionen	• Einheitliche Sicherheitsplattform als Integration für andere Tools und als zentrale Anlaufstelle für Analysten
• Kein ausgereiftes Sicherheitskonzept erforderlich	• Ausgereiftes Sicherheitskonzept/ vorhandenes Sicherheitsteam erforderlich
• Blockiert Angriffe auf dem Endpunkt, bietet Erkennungswarnungen, Host-Isolierung, automatisierte Abwehr	• EDR-Funktionen + skalierte zentralisierte Verwaltungs- und Ausführungsfunktionen über mehrere Bedrohungsvektoren, Umgebungen und Lösungen hinweg

EDR lässt sich zwar einfacher in die bestehenden Tools von Sicherheitsteams integrieren, aber mit XDR können die Teams wesentlich effektiver die gesamte Angriffsfläche des Unternehmens überwachen, um Bedrohungen zu erkennen und abzuwehren.

Welche Lösung ist also für Ihr Unternehmen am besten geeignet? Warum nicht beide? Mit Limitless XDR von Elastic Security ist EDR, neben SIEM und Cloud Security, eine der drei Hauptkomponenten dieser umfassenden Lösung. **Weitere Informationen: elastic.co/de/security**

