elastic

Search. Observe. Protect.

EDR vs. XDR

Endpoint Detection & Response (EDR) and Extended Detection & Response (XDR) – though only one letter apart in acronyms — provide substantially different outcomes for cybersecurity teams. Here, we break down what teams can expect out of the two solutions.

EDR	XDR
• Focused protection on endpoints	• Broad detection through a diverse set of integrations across endpoints, cloud, user, network, and other vectors
• Uses machine learning to detect and prevent against malware and ransomware	• EDR capabilities + machine learning-powered analytics to correlate activity and identify threats
• Standalone tool with minimal integration capabilities	• Unified security platform that integrates across other tools, serving as a single reference point for analysts
• Doesn't require advanced security maturity	• Requires advanced security maturity/ established security team
• Blocks attacks at the endpoint; provides detection alerts, host isolation, automated response	• EDR capabilities + scaled centralized management and execution capabilities across multiple threat vectors, environments, and solutions

While EDR is more readily implemented into a security team's existing toolset, XDR is far more effective at boosting teams' ability to monitor, detect, and respond across the organization's full attack surface.

Wondering which solution is best for your organization's needs? Why not both? With Elastic Security's Limitless XDR, EDR is a key component — alongside SIEM and cloud security — of the comprehensive solution. **Learn more at: elastic.co/security**

