EDR vs XDR

AGILEBLUE

Endpoint Detection and Response (EDR) and eXtended Detection and Response (XDR) - though very similar acronyms - provides substantially different outcomes for cybersecurity teams.

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 organizations full attack surface.

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 plus 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 plus scaled centralized management and execution capabilities across multiple threat vectors, environments, and solutions

Deciding which solution is best for your organization? Why not both?

With AgileBlue's SOC|XDR platform, EDR is a key component of our all-in-one solution. Ready to get started? Send us an email with your information and a member from our team will be in touch to demonstrate how AgileBlue can detect cyber threats before you're breached.

sales@agileblue.com