kaspersky

EDR vs MDR vs XDR

EDR
Endpoint Detection and Response

Identifies new, unknown and evasive threats bypassing endpoint protection, and automates routine security tasks

MDR
Managed Detection and Response

Delivers continuous managed protection against even the most complex and innovative non-malware threats

XDR
Extended Detection and Response

Proactively detects complex threats across multiple infrastructure levels, and automatically responds to and counters these threats

How it works

- Enables advanced detection and hunting for threats bypassing prevention mechanisms
- Enhances threat visibility and visualization
- Simplifies root cause analysis
- Delivers centralized, automated response

- Gathers telemetry from security products, proactively analyzes system activity metadata for any signs of an active or impending attack, and provides managed or guided response

- Integrates multiple tools and security applications
- Monitors data on endpoints, networks, clouds, web servers, mail servers etc. to detect and eliminate complex threats
- Simplifies information security management through automating cross-product interaction

Who's it best for?

- Businesses with an in-house IT security team requiring granular endpoint visibility and centralized response to reduce manual handling tasks

- Companies seeking to expand internal IT security capacity by offloading key detection and response tasks
- Organizations that might not have the budget or specialist staff available to build their own internal SOC

Security mature organizations wanting a single platform delivering:

- A coherent picture of what's happening throughout their infrastructure
- Built-in threat hunting and threat intelligence
- Superior incident prioritization and fewer false positive alerts

Business value

- Gives security personnel the unified visibility and control they need to actively hunt for threats instead of waiting for alerts
- Maximizes existing IT security teams' capacities by automating an array of analysis, investigation and response processes
- Drives cost efficiencies by enabling IT security teams to work more effectively without having to juggle multiple tools and consoles

- Solves the cybersecurity talent crisis ensuring instant protection against complex threats
- Enables outsourcing of incident management processes to better focus limited and expensive in-house resources on the critical outcomes delivered
- Reduces overall security costs without the need to deploy complex security solutions and employ a range of in-house security specialists

- Provides holistic protection against the evolving threat landscape
- Ecosystem approach maximizes efficiency of the cybersecurity tools involved, saves resources and reduces risk
- Simplifies the work of IT security specialists and gives them the additional context needed to investigate multi-vector attacks
- Minimizes MTTD and MTTR - crucial in combating complex threats and targeted attacks
- Enables centralized and automated response across the entire security technology stack

If yours is a security mature organization looking to benefit from XDR capabilities, take a look at Kaspersky Expert Security

Learn More