SOPHOS

EBOOK

EDR, XDR, MDR

What's the difference?
And which one is right for your business?

CONTENTS

EDR, XDR, MDR

What's the difference? And which one is right for your business?

IT and security leaders face mounting pressure to strengthen cyber resilience without overextending already limited teams or budgets. With threat volumes surging and attack sophistication accelerating, making smart investments in detection and response capabilities is imperative.

Whether you're operating on a global scale or managing a leaner team, aligning your security approach with your organization's risk profile and operational realities is key. For many leaders, choosing the right detection and response approach also means deciding whether to manage it yourself or work with a trusted partner.

Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), and Managed Detection and Response (MDR) each offer unique advantages, but the real challenge is identifying what delivers the most value for your organization. EDR and XDR are tools that help your team detect, investigate, and respond faster. MDR is a service that provides 24/7 monitoring and response through expert analysts, typically using XDR and other technologies.

Understanding what sets these approaches apart — and how they can complement each other — is the first step toward building a security strategy that protects you today and positions you for resilience tomorrow.

Why detection and response matters

Robust endpoint protection remains a critical first line of defense. However, sophisticated threat actors exploit legitimate credentials, impersonate trusted users, and abuse native IT tools to evade defenses. These attacks may not look malicious to a single preventative tool, and that's exactly why they succeed.

Detection and response capabilities, such as EDR, XDR, and MDR, fill this critical gap. They help you identify and neutralize threats that make it past prevention before they can escalate into full-blown incidents.

SOPHOS

WHAT IS EDR?

Endpoint Detection and Response (EDR) is part of a continuous endpoint security strategy. It helps teams monitor, detect, and respond to threats and security incidents on endpoint devices such as laptops, desktops, and servers.

Key benefits of EDR:

Provides real-time visibility into endpoint activity — such as file executions, process behavior, and lateral movement — so teams can quickly spot and stop threats before they spread.

Detects evasive threats by identifying behavioral indicators, helping you catch attacks that traditional prevention tools often miss.

Automates response actions like isolating affected endpoints or killing malicious processes, reducing dwell time and preventing attackers from gaining further access.

Explore how Sophos EDR can protect your endpoints and servers from advanced, human-led attacks, whether they are in the office, over the network, or in the cloud.

WHAT IS XDR?

Extended Detection and Response (XDR) elevates threat visibility by integrating data from across your security ecosystem beyond endpoints and servers. It includes firewalls, email, cloud infrastructure, identity systems, backup and recovery solutions, productivity tools, endpoints and servers, and more. XDR enables more effective correlation of suspicious activities, helping to identify sophisticated multi-vector attacks that siloed tools might miss.

Where EDR looks deeply at endpoints, XDR extends visibility and connects the dots across all systems. It provides a holistic view of an attack, making it easier to detect multi-stage, multi-vector threats that would otherwise go unnoticed.

Key benefits of XDR:

Correlates signals across multiple attack vectors to uncover patterns and prioritize high-fidelity alerts. This reduces noise and brings complex, multi-system threats into focus.

Streamlines investigation workflows so your team can respond faster and with confidence. Analysts gain clear visibility into how an attack unfolded — and how to prevent it from happening again.

Supports investigation and response workflows with AI-powered tools that accelerate analysis and remediation, enabling faster, more confident incident resolution.

Explore how Sophos XDR enables you to detect, investigate, and respond to suspicious activities across your entire ecosystem.

WHAT IS MDR?

Managed Detection and Response (MDR) is a service-led model that combines AI with expert-led human analysts to provide 24/7 monitoring, threat hunting, and incident response. It's especially valuable for organizations without 24/7 operations or those facing SOC coverage gaps, staffing challenges, or growing complexity.

MDR can function as a fully outsourced solution or a co-managed extension of your internal team — helping reduce dwell time and stop incidents like ransomware before they escalate.

Key benefits of MDR:

24/7 coverage. Threats don't follow a 9-to-5 schedule: 88% of ransomware attacks occur outside normal business hours. MDR ensures coverage at all hours.

Access to expert security analysts who understand attacker behavior and act decisively. These specialists handle incidents daily, prioritizing and containing threats to keep your business running smoothly.

Freedom from alert fatigue and manual triage. MDR cuts through the noise, so your team can focus on strategic initiatives instead of chasing false positives.

Rapid resolution when it matters most. In high-stakes incidents like ransomware, MDR teams can detect and contain threats before internal teams even know they exist — preventing disruption and reducing risk.

Discover how Sophos MDR, with its open, AI-powered platform and expert analysts, can complement your team and meet you where you are in your security journey.

WHEN TO CONSIDER EDR, XDR, OR MDR

Solution	You might consider if...	It may not be the best fit if...
EDR	• You need robust endpoint detection and response. • You're looking to elevate your defenses beyond preventive endpoint protection tools. • You're building a layered defense that can support future XDR or MDR integration.	• You need broader visibility across your entire environment (cloud, identity, network, backup, etc.). • You're expecting 24/7 detection and response without outsourcing or adding headcount.
XDR	• You need a unified view across all key attack vectors, including endpoint, firewall, network, cloud, identity, backup, and productivity tools. • You want faster threat correlation and reduced alert fatigue. • You want to get more ROI from your existing and future security and IT technology investments.	• You are only monitoring endpoints and servers. • You need more hands-on support than your team can provide. • You don't have the necessary in-house resources to manage an XDR platform.
MDR	• You need expert-led, 24/7 threat detection and response. • You're experiencing alert fatigue, talent shortages, or burnout. • You want a proactive partner to investigate and neutralize threats on your behalf. • You want to improve your cyber insurance position, potentially lowering premiums and increasing coverage.	• You already have mature security operations with full staffing and in-house capabilities, providing robust 24/7/365 coverage. • You're not ready to outsource parts of your detection and response operations.

ADDITIONAL CONSIDERATIONS BEFORE YOU DECIDE

As you weigh your options, there are a few critical factors that can shape whether EDR, XDR, or MDR is the right fit, and which partner can deliver on that promise.

Threat intelligence matters

The effectiveness of any detection and response solution depends on the quality of the threat intelligence that powers it. The broader, deeper, and fresher the intel, the faster threats can be spotted and stopped. Make sure any vendor you consider can explain the sources and scope of their threat data.

Service should be more than a promise

Even the best technology can fall short without responsive support. Whether you're self-managing or leveraging a partner for managed services, you need to know help is available when you need it. Ask vendors how support works in practice: Who responds, how fast, what's included, and how to get help during an active incident.

Cost isn't always what it seems

Don't assume one path is inherently more expensive. Pricing varies widely depending on how each solution is implemented and supported. Focus on your specific needs and consider your current staffing and existing investments, including potential tradeoffs between technologies and cost of in-house vs. outsourced resources.

Detection and response solutions, particularly MDR, can play a role in influencing cyber insurance costs. Many insurers now look favorably on organizations with 24/7 threat monitoring and response in place, which can result in reduced premiums or improved coverage terms.

A comprehensive ROI analysis that factors in operational savings, risk reduction, and even insurance benefits can help you uncover the true cost and value of each approach.

THE BOTTOM LINE

$1.53 Million

The average cost to recover from a ransomware attack — and that's before factoring in any ransom payments.*

40%

of organizations hit by ransomware say a lack of cybersecurity expertise contributed to the attack.*

The stakes are too high for guesswork.

Choosing the right detection and response strategy isn't just about technology, it's about enabling your people, protecting your operations, and building a resilient cyber defense that lasts.

*2025 Sophos State of Ransomware Report

SOPHOS

SOPHOS
DEFEAT CYBERATTACKS

LEARN MORE ABOUT SOPHOS SOLUTIONS AND SERVICES

Sophos helps you better detect and respond to threats today and as your security needs evolve.

Speak to a Sophos expert and let's work on finding the right solution for your business, together.