



The MSP's Guide to EDR and MDR Security

Dominate Cybersecurity

Let's be honest. You want Superman guarding your data, not some Average Joe. Unlock next-level security with EDR and MDR. This guide equips MSPs with the tools, features and strategies to implement and sell these solutions. Explore your all-in-one guide to building client trust and scaling your business growth.

Understanding EDR and MDR

We're talking about the difference between losing millions in breach repairs or massive business profits. Here's what makes EDR and MDR the powerhouse of cyber protection.

EDR: Eliminate Threats on Site

Endpoint Detection and Response (EDR) is your frontline cyber defense. It scans and eliminates threats across all endpoints—laptops, phones, servers and any device with internet access. It stops ransomware, malware and other bad actors from compromising crucial data.

How EDR Works

Let's say a user clicked a malicious link. No problem. EDR detects and destroys the malware in real-time. Unlike traditional antivirus, EDR actively hunts down unfamiliar threats before they become unstoppable breaches. Think of EDR as your 24/7 digital bodyguard, eliminating attacks on command.

EDR Key Features:

- Detects real-time threats and monitors network 24/7
- Collects and manages comprehensive data
- Identifies system vulnerabilities
- Actively searches for hidden malware
- Integrates seamlessly with existing security tools

What Is MDR?

Managed Detection Response (MDR) is a threat response system operated and overseen by a team of cyber experts and analysts. Instead of one bodyguard, imagine a multitude of defense guards that spot, repair and fortify your security, ensuring you stay ahead of threats.

MDR offers a suite of security services under the watch of an expert team. Clients benefit from EDR threat-hunting solutions, real-time alerts and advanced intelligence to mitigate attacks and make their networks impenetrable.

How MDR Works

Cyberattacks don't clock out, and neither does MDR. When breaches happen outside of business hours, MDR rapidly neutralizes the threat. This allows the external team to patch security gaps, preventing downtime. MDR is ideal for MSPs lacking round-the-clock staffing or clients needing elite security.

EDR Key Features:

- Managed 24/7 by expert-security team
- Collects and manages comprehensive data
- Identifies system vulnerabilities
- Actively searches for hidden malware
- Integrates seamlessly with existing security tools



The MSP's Guide to EDR and MDR Security

EDR vs. MDR

Feature	EDR	MDR
Service	Endpoint threat detection and response	Team-managed threat detection and response
Operations	Requires MSP or IT staff expertise	Monitored by third-party cybersecurity team
Threat Detection Time	Instant and automated	Immediate with external oversight
Ideal for	Organizations looking to supplement smaller IT staff	Organizations needing large security operations center
Cost	Subscription-based	Subscription-based

How Does This Affect Me?

Small businesses are one of the most common targets for ransomware attacks. With scams up 42%,¹ bad actors are leveling up. A single breach could mean months of recovery or lost business. Clients look to MSPs as their business shield and safeguard. Cybersecurity isn't a maybe, it's a must-have.

EDR and MDR are key components for CIS Controls and dominate as a cybersecurity powerhouse. Deliver these services and watch your client retention and revenue increase, scaling your business like never before.

\$9.36 million

In 2024, the average cost of a data breach in the United States was \$9.36 million.²

72%

72% of businesses worldwide were impacted by ransomware attacks in 2023.³

61%

61% of SMBs were victims of a cyberattack in 2023.³

How Do I Sell EDR and MDR Solutions?

Effectively selling EDR and MDR means hitting clients with the hard truth.

SMBs are cybercriminals' number one target, and a breach is bound to happen. If someone hijacks their customer data or infiltrates their network, do they have a plan of action?

Can they afford to face millions in damages or lose their business? Show clients that the reward of cybersecurity is greater than the risk of leaving it to chance. Deliver customized plans that ease their worries and expand your services.



The MSP's Guide to EDR and MDR Security

Overcoming Challenges

Cybersecurity can feel intimidating, leaving clients hesitant to move forward. Here's how EDR and MDR break down the barriers:

- **Complexity:** EDR and MDR simplify security with streamlined operations that manage threats. They're the perfect choice for clients who want a robust system without the cost of an IT team.
- **Integration:** EDR and MDR integrate seamlessly into existing IT environments and strengthen your current defenses.
- **Flexibility:** EDR adapts to your client's unique systems and compliance needs. MDR puts a team of experts in charge of your security and compliance. Clients receive a tailored approach, ensuring perfect system conditions.

Maximize Cybersecurity with Pax8

Growing threats demand stronger security. To protect clients' endpoints, Pax8 delivers powerful EDR and MDR solutions, including SentinelOne and CrowdStrike. Talk with a security consultant and access Pax8 security resources to start growing your security practice and reducing your clients' risks.

Schedule a call

Explore Pax8 security resources

Sources:

1. [World Economic Forum](#)
2. [IBM Cost of a Data Breach Report 2024](#)
3. [The State of Ransomware 2024](#)
4. [Black Fog: The State of Ransomware 2024](#)