THREATDOWN™

EDR vs MDR vs XDR:
The Decision Guide

How to choose the best fit for your organization's security needs

THREATDOWN™

Table of Contents

THREATDOWN™

Introduction: The Detection and Response Dilemma

The pressure inside an organization's security operations continues to climb. Analysts flag overload as their top issue, and 83% attribute it to alert volume, false positives, and limited context.[1] Staffing gaps add more pressure, and 67% of organizations confirm they do not have enough people to keep up.[2] Adversaries recognize the imbalance and take advantage of the widening gap between threat volume and team capacity.

Detection and response technologies—EDR, MDR, and XDR—address these challenges, but they do so in fundamentally different ways. If there's a mismatch between your solution and your organization's reality, it can mean either overpaying for capabilities you can't use or underprotecting assets because your team is overwhelmed.

This guide provides clarity. You'll learn what each solution does, how they compare, and which one fits your organization's current reality.

What you'll find inside:

- Clear definitions of EDR, MDR, and XDR
- Side-by-side capability comparisons
- A decision framework based on your team's resources
- A maturity model showing when to adopt each solution

[1] Devo, The Evolution Toward an Alertless SOC
[2] Programs, Cybersecurity Talent & Workforce Shortage Stats

THREATDOWN™

Understanding The Three Detection and Response Solutions

Keeping up with today's cyberthreats requires both vigilance and the ability to manage increasingly complex security environments. Detection and response tools support that effort by helping you monitor activity, evaluate suspicious behavior, and act on potential threats within your environment.

EDR, MDR, and XDR can alleviate challenges most small business cybersecurity teams face, such as alert fatigue and limited resources. Although detection and response tools share similar purposes, they are not all equal. Every threat detection and response capability has its own advantages when it comes to addressing the needs of your business and catching threats that have thwarted traditional security layers. Let's dive into the basics of three common detection and response solutions:

Endpoint Detection & Response (EDR)

EDR solutions cover all endpoint monitoring and activity through threat hunting, data analysis, and remediation to stop a range of cyberattacks. These attacks include malware, ransomware, brute force, and zero-day intrusions.

Endpoint detection and response solutions offer:

- Centralized visibility across all endpoints in an organization
- Real-time continuous monitoring of endpoint activities
- Advanced threat detection using behavioral analysis and machine learning
- Automated response capabilities for identified threats
- Detailed forensic information for security investigations

EDR provides holistic visibility into the attack surface of all endpoints and can detect threats that circumvent legacy endpoint protection platforms (EPP). It forms the foundation for scalable cybersecurity maturity.

Managed Detection & Response (MDR)

MDR is a service that offers a suite of outsourced capabilities to deliver round-the-clock, 24/7 monitoring and detection, proactive threat hunting, prioritization of alerts, correlated data analysis, managed threat investigation, and remediation. MDR is popularly thought of as an in-house Security Operations Center (SOC) alternative or SOC-as-a-service. It blends a human element of highly-skilled experts with threat intelligence technologies.

MDR service capabilities typically include:

- Strategic security recommendations and reporting
- 24/7 security monitoring by trained security analysts
- Threat hunting services to proactively identify hidden threats
- Expert threat investigation and validation
- Guided or fully-managed incident response

MDR helps businesses obtain outsourced, high-skilled cybersecurity experts at an affordable cost. Regardless of size and level of expertise, your current IT team can work with Managed Detection and Response to close the skill gap in specialized security talent. Small businesses seeking to build security maturity, handle complex threats, and relieve in-house alert fatigue benefit significantly from Managed Detection and Response.

THREATDOWN™

Understanding The Three Detection and Response Solutions (continued)

Extended Detection & Response (XDR)

XDR is a proactive cybersecurity solution that provides unified visibility over endpoints, networks, and the cloud through aggregating siloed data across an organization's security stack.

Typically, XDR services offer:

- Simplified security stack management through consolidation
- Unified visibility across endpoints, networks, cloud workloads, email, and applications
- Cross-platform threat detection that correlates data from multiple security tools
- Automated response capabilities that span the entire IT infrastructure
- Advanced analytics that identify complex attack patterns across security domains

THREATDOWN™

Side-by-Side Comparison

Core Capabilities

	EDR	MDR	XDR
Primary Focus	Endpoint threat monitoring and response	Managed service with human expertise	Cross-platform data correlation
Coverage Scope	Endpoints only	Endpoints (primary)	Endpoints, network, cloud, email, applications
Monitoring	Tool-based, requires internal staff	24/7 by external analysts	Tool-based, requires internal staff
Threat Hunting	Manual, team-dependent	Proactive, included in service	Automated correlation, manual follow-up
Response Type	Automated + manual	Expert-guided or fully managed	Automated across security stack
Alert Management	High volume, requires triage	Prioritized and validated by analysts	Consolidated, correlated alerts

Resource Requirements

	EDR	MDR	XDR
Team Size	2-3 dedicated security staff	Minimal (service handles heavy lifting)	3-5 security staff with cross-domain knowledge
Skill Level Required	Intermediate to advanced	Basic (for internal IT team augmentation)	Advanced (multi-tool expertise)
Time Investment	Medium to high (daily alert triage)	Low (analysts handle investigation)	High (initial integration, ongoing tuning, alert triage)
Infrastructure Complexity	Single layer (endpoints)	Single to moderate	High (multiple integrated tools)
Total Cost Consideration	License + internal staff costs	Service fee (predictable)	License + integration + internal staff costs

THREATDOWN™

Making the Decision: Which Solution Fits Your Organization?

Choosing the right detection and response approach depends on your operational reality. Many organizations do not have the time, staff, or expertise to interpret large volumes of alerts and perform hands-on investigations. A clear understanding of your constraints and strengths helps you determine which technology aligns with your environment.

The following framework simplifies that process. Answer the five questions below, then review the scoring guide to see which option fits your current needs.

The 5-Question Decision Framework

Answer each question, then use the scoring guide below to identify your best-fit solution.

1. **How many endpoints does your organization manage?**

   A. Fewer than 50
   B. 50-500
   C. 500+

2. **What is your current security team size?**

   A. 0-1 dedicated security staff
   B. 2-3 security personnel
   C. 4+ security team members

3. **How would you rate your team's cybersecurity skill level?**

   A. Basic (can manage malware, patches, basic configs)
   B. Intermediate (can interpret some alerts, perform investigations)
   C. Advanced (expertise in threat hunting, forensics, incident response)

4. **How many security tools are currently in your stack?**

   A. 1-3 tools (antivirus, firewall, basic protection)
   B. 4-6 tools (adding email security, SIEM, etc.)
   C. 7+ tools (complex, multilayered architecture)

5. **What is your biggest security challenge right now?**

   A. Limited visibility into endpoint threats
   B. Too many alerts, not enough time or expertise to respond
   C. Siloed security tools that don't communicate

Mixed responses?

If your answers span multiple letters, focus on question #5 (your biggest challenge). Addressing that pain point should drive your decision.

THREATDOWN™

Making the Decision: Which Solution Fits Your Organization? (continued)

Scoring Guide

Add up which letter you selected most often. Your pattern reveals the approach that fits your current capacity and operational maturity.

Mostly A's: Start with EDR

You need stronger endpoint visibility and a reliable way to detect malicious activity. EDR helps you understand what is happening on your devices and supports structured response workflows. As your environment grows in size or complexity, consider adding MDR to absorb the workload that comes with higher alert volume.

Mostly B's: MDR Fits Your Team

Your team does not have the time or specialized skills to manage the volume of EDR alerts. MDR provides continuous monitoring and response handled by trained analysts. This empowers your organization to focus on strategic priorities while experienced responders manage threats.

Mostly C's: XDR (Often Paired with MDR)

You're managing a complex security environment with multiple tools generating disconnected alerts. XDR consolidates this data and provides unified visibility. However, XDR still requires significant expertise, so consider pairing it with MDR service to handle the investigation and response workload.

THREATDOWN™

The Maturity Model: When to Adopt Each Solution

Security needs shift as organizations grow and their environments become more complex. The three stages below show how detection and response technologies align with operational maturity and the capacity of your team.

Stage 1: Foundation

Characteristics

- Small team (0 to 2 security staff)
- Limited budget and time
- Endpoints are the primary attack surface
- Reliance on antivirus and basic protections

Recommended Solution: EDR

Organizations at this stage need reliable visibility into endpoint activity. EDR establishes the starting point for structured detection and response. It gives you centralized monitoring, threat detection, automated response actions such as isolating compromised endpoints, and forensic data that antivirus tools cannot supply.

What this looks like

You deploy EDR across all endpoints, train your team on alert triage, and begin building security processes around endpoint monitoring. You'll handle most response activities internally, understanding that some threats may require longer investigation times while processes mature. Automated actions such as endpoint isolation strengthen containment while your team investigates incidents.

Stage 2: Scaling Security

Characteristics

- Growing endpoint count (50-500 devices)
- 2-3 security staff members
- Experiencing alert fatigue
- Longer investigation times affecting response speed
- Need for 24/7 coverage but can't staff it

Recommended Solution: EDR + MDR

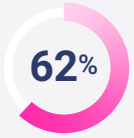
Your EDR deployment now produces more alerts than your team can analyze. MDR adds a dedicated response function that strengthens your coverage. Analysts monitor your environment around the clock, investigate threats, and take action when needed. You retain ownership of strategy and tool management while MDR absorbs the operational load.

What this looks like

EDR continues collecting telemetry. MDR analysts triage alerts, investigate threats, and provide clear guidance for remediation or execute response actions on your behalf. Organizations without a security team rely on MDR as their primary detection and response function. Organizations with a small team shift internal effort toward strategic priorities instead of constant alert review.

The Maturity Model: When to Adopt Each Solution (continued)

3,832 alerts daily
Average volume security teams must manage[3]



Go uninvestigated[4]

MDR solves this – by having experts handle the volume and focus on what truly matters.

Stage 3: Advanced Security Architecture

Characteristics

- Large, distributed environment
- Multiple security tools (SIEM, email security, network monitoring, cloud security)
- Alerts coming from many siloed sources
- Difficulty correlating data across security stack
- Advanced threats that move laterally across systems

Recommended Solution: XDR or XDR + MDR

Your environment produces high volumes of telemetry across many domains. XDR unifies that data and correlates events to identify threats that cross endpoint, network, email, or cloud boundaries. It centralizes detection and supports coordinated response across your infrastructure, including automated actions such as restricting compromised accounts.

What this looks like

XDR aggregates telemetry from all major security layers. When suspicious activity appears, XDR links related events, flags lateral movement, and can trigger automated containment across multiple systems. If your team lacks deep expertise, pairing XDR with MDR ensures that both technology and investigation capability advance together.

XDR Without Expertise = Missed Value

XDR is powerful, but only if someone knows how to tune it, interpret cross-domain alerts, and execute coordinated responses. If your team lacks this depth, XDR + MDR is the more effective combination.

[3] Cyber Sierra, What Is Alert Fatigue and How to Combat It in Your SOC
[4] Ibid

How ThreatDown Approaches Detection and Response

ThreatDown recognizes that businesses need flexibility, not one-size-fits-all solutions. Our approach combines best-in-class EDR technology with MDR services, allowing you to match your security stack to your current resources and maturity level.

What sets ThreatDown apart:

Unified Platform, Flexible Delivery

Whether you manage detection and response internally or rely on our 24/7 security team, you work from the same platform. This means you can start with ThreatDown EDR and seamlessly add ThreatDown MDR service without switching tools or losing visibility.

Threat Intelligence Integration

Our detection engine uses real-time threat intelligence from multiple reputable sources, including MITRE and others. This enriches alerts with context that helps identify known tactics, techniques, and indicators faster.

24x7x365 Monitoring

We monitor endpoints and perform expert investigations day and night, weekdays, weekends, and holidays. We're always watching.

Expert-Level Response, On Demand

Our MDR service includes guided response (we tell you exactly what to do) or fully managed response (we handle it for you). You choose the level of involvement that fits your team's bandwidth.

Active Threat Hunting

Our MDR Team hunts unseen threats based on past indicators of compromise (IOCs) and suspicious activity observed on endpoints.

You shouldn't have to choose between strong security and team burnout. ThreatDown scales with you.

Next Steps: Getting Started

Choosing the right detection and response solution starts with a clear picture of where your organization stands today. An honest assessment of your capacity, visibility gaps, and operational challenges will guide the right path forward.

If you are ready to move ahead:

1. Review your current state using the 5-question decision framework.
2. Identify your primary challenge, whether it relates to visibility, limited expertise, or tool sprawl.
3. Select the solution that directly addresses that challenge. For many businesses, EDR or EDR+MDR is the most effective starting point.
4. Build for growth. Security needs shift as environments expand, so choose a solution that lets you add capabilities when you need them.

Want protection that fits your resources and environment?

Get a demo

THREATDOWN™ | threatdown.com | sales@threatdown.com