

Topics

1. What Is Endpoint Detection and Response (EDR)?
2. What Is the Difference Between EDR vs. MDR?
3. What Are the Key Benefits of Managed EDR for a Business?
4. How to Evaluate and Choose a Managed EDR Provider for Your Business
5. Essential EDR Features: What to Look for in a Solution
6. What is Endpoint Security?
7. What is Managed EDR? Why Your Business Needs It
 - The Managed EDR definition
 - How does Managed EDR work?
 - How does managed EDR work to detect threats?
 - EDR vs. managed EDR: What's the difference?
 - How Managed EDR improves security?
 - Is Managed EDR right for your business?
 - Managed EDR—The defense you need against modern cyber threats
8. EDR vs. Antivirus: What's the Difference?
9. Essential EDR Features: What to Look for in a Solution
10. Top Managed EDR Solutions
11. Endpoint Security for Linux: What You Need to Know
12. Endpoint Security for Mac: What You Need to Know
13. What is Mobile Endpoint Security?

Share [f](#) [X](#) [in](#) [share](#)

What is Managed EDR? Why Your Business Needs It

Published: May 23, 2025

By:  [Brenda Buckman](#)

Key Takeaways:

- Huntress Managed EDR is a complete cybersecurity solution, combining purpose-built endpoint detection and response (EDR) technology with human expertise to protect endpoints in real time.
- Faster detection & response = fewer breaches. Around-the-clock monitoring and expert analysis make sure threats are detected, investigated, and stopped before they become serious.
- Outsmart cyber threats before they strike. Managed EDR continuously adapts to new hacker tactics and techniques to help keep businesses safe.

Today, threat actors lurk everywhere, ready to pounce on unprotected systems. If you're relying on traditional antivirus alone to monitor for threats and attacks, that's like bringing a paper shield to a sword fight. Enter Managed EDR. But what is [Huntress Managed EDR](#), and why should you care? And how does Managed EDR detect threats?

By continuously monitoring and analyzing endpoint behavior, the combination of tech and human expertise uncovers anomalies to stop cyberattacks before they can cause damage. Read on to get the big picture.

[Try Huntress for Free](#)
[Get a Free Demo](#)

The Managed EDR definition

Let's start with a quick [EDR](#) definition. Imagine having an elite team dedicated to cyber threats—always watching, always ready. [Managed EDR](#) combines advanced EDR software with human experts who monitor, analyze, and respond to cyber threats 24/7.

Unlike old-school security that only detects known malware, Managed EDR sniffs out shady behavior, analyzes it, and acts fast to shut it down before it becomes a disaster.

Here's the breakdown:

- ✓ EDR software collects real-time data from every endpoint (laptops, servers). It's like having security cameras everywhere.
- ✓ Advanced threat detection spots suspicious activity on endpoints, not just known malware signatures. But it also takes human expertise (see next bullet) to analyze complex threats and separate real dangers from false alarms.
- ✓ Human analysts from the [Huntress SOC](#) step in to investigate and eliminate false alarms, ensuring real threats get immediate action.
- ✓ Rapid containment actions stop attacks from spreading before they can do damage

How does Managed EDR work?

Threat actors don't take weekends off, and neither should your security. Managed EDR operates continuously to detect, analyze, respond, and improve. Here's how it works:

1. **Deployment and monitoring:** Lightweight agents are deployed on all endpoints, gathering real-time telemetry on user activity, system processes, and network connections.
2. **Advanced threat detection:** Constant monitoring flags anything suspicious, like fileless malware, privilege escalation, or unusual lateral movement.
3. **Expert investigation:** Security pros in Huntress's 24/7 SOC review alerts, intervene in real threats, and surface the ones that matter.
4. **Rapid containment:** If a threat is real, infected endpoints get quarantined, stopping the attack in its tracks.
5. **Remediation and hardening:** Once the threat is contained, the security team investigates what happened, cleans up the environment, patches vulnerabilities, and strengthens defenses.
6. **Continuous learning:** Every detected attack feeds into future defenses, making your security posture smarter over time.

How does managed EDR work to detect threats?

Hackers are slick. Managed EDR is slicker. Unlike old-school security that waits for something bad to happen, [Managed EDR](#) hunts threats before they strike using multiple layers of detection:

- ✓ **Behavioral analysis:** Spots unusual actions, like a regular user suddenly trying to access admin files at 3 AM.
- ✓ **Machine learning:** Learns from past attacks to recognize patterns and anomalies.
- ✓ **Indicators of Attack (IoA):** Tracks hacker tactics, techniques, and procedures (TTPs), rather than just malware signatures.
- ✓ **Memory analysis:** Detects fileless malware running directly in RAM, where traditional antivirus is blind.
- ✓ **Process mapping:** Uncovers hidden attack chains, exposing even the stealthiest cybercriminals.

EDR vs. managed EDR: What's the difference?

You might've heard of EDR, but what sets managed EDR apart?

EDR is software that gives you visibility into activity on endpoints, like laptops and servers. But without the help of an experienced team, you're still on the hook for operating and tuning the software, plus the monitoring, detection, and response to alerts.

Managed EDR, on the other hand, adds experts to the mix. It combines management of the EDR software along with 24/7 human-led monitoring, threat triage, and response. You get all the benefits of EDR but don't need an in-house security team to run it.

How Managed EDR improves security?

Still wondering if Managed EDR is worth it? Here's why it is:

- ✓ **Faster threat detection:** Cuts detection time from months to minutes, stopping threats before they spread.

threats before they spread.

- ✓ Proactive threat hunting: Security pros don't just wait for alerts. They actively hunt cyber threats hiding in your systems.
- ✓ 24/7 protection: Cybercriminals don't sleep, so neither does Managed EDR.

Is Managed EDR right for your business?

If your business:

- ✓ Lacks an in-house security team but still needs round-the-clock protection
- ✓ Can't afford to staff a full-time 24/7 SOC
- ✓ Handles sensitive data (finance, healthcare, legal, etc.)
- ✓ Has a remote workforce that expands your attack surface

Managed EDR solutions are designed for businesses of all sizes, not just large enterprises. Whether you're a growing startup or an established enterprise, we're here to give you the protection you need.

Managed EDR—The defense you need against modern cyber threats

Threats can seem overwhelming, but with Huntress you get [fully managed endpoint detection and response \(EDR\)](#) with purpose-built tech and 24/7 support from security experts ready to find and wreck hackers.

Stay one step ahead with Huntress. [Book a demo](#) today to see how our security experts respond to and mitigate threats.



Brenda Buckman

[Read More >](#)

[Continue Reading](#)

EDR vs. Antivirus: What's the Difference? >

Protect What Matters

Secure endpoints, email, and employees with the power of our 24/7 SOC. Try Huntress for free and deploy in minutes to start fighting threats.

[Try Huntress for Free](#)



Platform

[Huntress Managed Security Platform](#)

[Managed EDR](#)

[Managed EDR for macOS](#)

[Managed ITDR](#)

[Managed SIEM](#)

[Managed Security Awareness Training](#)

[Book A Demo](#)

Solutions

[Phishing](#)

[Compliance](#)

[Business Email Compromise](#)

[Education](#)

[Finance](#)

[Healthcare](#)

[Manufacturing](#)

[State & Local Government](#)

Why Huntress?

[Managed Service Providers](#)

[Value Added Resellers](#)

[Business & IT Teams](#)

[24/7 SOC](#)

[Case Studies](#)

Resources

[Resource Center](#)

[Blog](#)

[Upcoming Events](#)

[Support Documentation](#)

About

[Our Company](#)

[Leadership](#)

[News & Press](#)

[Careers](#)

[Contact Us](#)



© 2025 Huntress All Rights Reserved.
[Privacy Policy](#) | [Cookie Policy](#) | [Terms of Use](#)

[Free Trial](#)