

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?](#)
 - Endpoint security, decoded
 - Old-school security won't survive today's threats
 - The three main types of endpoint security
 - Three critical moves to secure your endpoints
 - Every device is a target—What needs protection?
 - Why this is a bigger deal than ever
 - The human factor—Because tools can't do it all
 - How to build an unbreakable endpoint security plan
 - Act before threat actors do
7. [What is Managed EDR? Why Your Business Needs It](#)
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](#) [u](#)

What is Endpoint Security?

Published: **May 23, 2025**

By:  **Brenda Buckman**

Key Takeaways:

- Endpoints are the frontline: Endpoint security is how you protect every device your business relies on against cyber threats.
- Prevention, detection, response, and no weak links: First, harden your defenses. Then, stay paranoid and watch for sneaky threats. When something slips through? Hit back fast.
- Tech isn't a silver bullet: The fanciest security tools in the world won't do you any good if you don't know how to use them. Skilled operators turn good security into great security.

In the wild, wild west of the internet, endpoint security is the armor your business needs to survive. It protects all your devices, from laptops to phones to servers, against cyber threats. It's your first and last line of defense against threat actors looking to cash in on your vulnerabilities for profit. Understanding the importance of endpoint security is crucial because, without it, you're leaving your network wide open for anyone to take a shot at your data.

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

Endpoint security, decoded

Let's break it down. To understand endpoint security, think of it as the practice of protecting every device that connects to your network from malicious threats and attacks. Laptops, desktops, tablets, smartphones, even that fancy smart fridge hooked up to Wi-Fi. Every single one of them is a potential weak spot. And attackers? They're not kicking down your digital front door anymore. They're slipping in through the side windows, the basement, and that Wi-Fi-enabled coffee machine in the breakroom.

While traditional security builds walls, endpoint security sets up a neighborhood watch on every street corner—monitoring, detecting, and shutting down threats before they can make a move.

Old-school security won't survive today's threats

[Antivirus software](#) used to be enough on its own, but those days are long gone. Cybercriminals don't rely on old-school virus files anymore. They use [polymorphic malware](#) that changes its DNA every time it hits a new system, slipping past traditional defenses like a ghost through walls.

On top of that:

- ✓ Remote work blew up the game. Employees are logging in from coffee shops, home offices, and airport lounges. Your "network" now stretches across time zones and personal devices.

zones and personal devices.

- ✓ BYOD (bring-your-own disaster). Employees love using their own devices for work, but guess what? Their security hygiene is nothing compared to what IT enforces in the office.
- ✓ Cloud everything. Your sensitive data is scattered across a dozen cloud services, meaning attackers don't even have to break into your main network anymore. They just go for the weak link.

The three main types of endpoint security

Endpoint security systems are designed to defend against malicious threats targeting the devices connected to your network, ensuring that every potential entry point is secured. So, how do you fight back? Three ways:

1. Endpoint protection platforms (EPP)—Your cyber bodyguard

EPP is your front-door security, scanning for malware, blocking known threats, and keeping out sketchy downloads. It's the classic bodyguard, stopping trouble before it gets through the front door. But let's be real—some cybercriminals are slipping through with fake credentials. That's where the next level comes in.

2. Endpoint detection and response (EDR)—The security camera & SWAT team

EDR blocks threats, but it also watches, learns, and fights back. If something shady gets through, EDR tracks its movements, alerts your security team, and helps you hunt it down before it spreads. It's like a security camera that records crime, calls the cops, and tackles the intruder.

This [EDR explainer](#) breaks down how it keeps cyber threats in check.



3. Extended detection and response (XDR)—The full surveillance grid

XDR takes everything up a notch. Instead of just watching individual devices, it connects the dots across your entire security system—cloud, emails, networks, endpoints, and beyond. It's like upgrading from one security camera to a full-blown CIA surveillance operation, catching threat actors before they even make a move.

Three critical moves to secure your endpoints

Securing your business isn't a one-and-done deal. You need to do it on the daily. Here's how it works:

Step 1: Prevention—Lock it up

Before an attacker can even knock on your door, you want your endpoints locked up. That means:

Before an attacker can even knock on your door, you want your endpoints locked up. That means:

- ✓ Next-gen antivirus (not your old-school, one-size-fits-all antivirus)
- ✓ Application control (so that only trusted programs get to run)
- ✓ Encryption (to scramble your data so it's useless to thieves)
- ✓ Patching and updates (because hackers love exploiting outdated software)

Step 2: Detection—Stay vigilant

Even with the best locks, bad guys still find a way in. That's where real-time detection comes in. You need:

- ✓ Behavior monitoring (watching for weird activity)
- ✓ Threat hunting (looking for sneaky cybercriminals before they attack)
- ✓ Automated alerts (so you know the moment something's off)

Step 3: Response—Act fast or pay the price

When a threat gets through, speed is everything. Your security needs to:

- ✓ Shut down compromised devices before the attack spreads
- ✓ Isolate infected systems like isolating a ticking time bomb
- ✓ Dig into forensic data to figure out what happened
- ✓ Restore systems and lock down vulnerabilities for next time

Every device is a target—What needs protection?

If it connects to your network, it's a target. That includes:

- ✓ Laptops and desktops (your workforce's tech heavyweights)
- ✓ Smartphones and tablets (work doesn't just happen at desks anymore)
- ✓ IoT devices: (security cameras, smart thermostats, industrial sensors)
- ✓ Cloud servers and virtual machines (your data lives here, so attackers do too)

POS systems (even cash registers are a cybercrime jackpot)

Why this is a bigger deal than ever

If you're thinking, "Nah, we're not a target"—consider this. [70% of all breaches start at endpoints, which is why having strong](#) endpoint security systems is a must. Attackers don't discriminate. They're hitting:

- ✓ Small businesses (because they assume you're under-protected)
- ✓ Enterprises (because there's more money to steal)
- ✓ Government agencies (because, well, it's fun for them)

And the damage is expensive:

- ✓ [\\$4.88 million](#)—The average cost of a data breach
- ✓ [62 minutes](#)—How fast attackers move once they're in
- ✓ [11 seconds](#)—How often ransomware attacks happen

The human factor—Because tools can't do it all

Even the best security tools mean nothing if your team doesn't know how to use them. That's where [managed endpoint security](#) comes in. A real security team knows how to filter out false alarms so you're not chasing ghosts. They proactively hunt for threats, rather than sitting back and waiting for an attack. And they respond 24/7, because hackers don't exactly keep business hours.

How to build an unbreakable endpoint security plan

1. Inventory every device: Know what's connecting to your network
2. Assess your weak spots: Find security gaps before attackers do
3. Deploy the right tools: EPP, [EDR](#), or XDR based on your risk level
4. Build your defenses in layers: No single tool is enough
5. Monitor everything, always: Cyber threats don't take vacations
6. Have a response plan: If an attack happens, what's your move?
7. Consider managed security: If you don't have in-house experts, get pros who do

Act before threat actors do

The digital battlefield is unforgiving, and your endpoints are ground zero. Threats can seem overwhelming, but with our in-depth understanding of how threat actors think, we know what to look for. Huntress gives you fully [managed endpoint detection and response \(EDR\)](#), so you've got 24/7 support from security experts ready to respond to threats.

Read more in our in-depth guide on [what EDR is and how it works](#).



Brenda Buckman

[Read More >](#)

[Continue Reading](#)

What is Managed EDR? Why Your Business Needs It >

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](#)