

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
8. **EDR vs. Antivirus: What's the Difference?**
- What is antivirus?
- What is EDR?
- EDR vs. antivirus: The key differences
- When to use EDR vs. antivirus
- Pros and cons: Breaking it down
- Why antivirus is not enough
- Can EDR replace antivirus?
- Final verdict: What's the right choice for your business?
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    

EDR vs. Antivirus: What's the Difference?

Published: May 23, 2025

By:  **Brenda Buckman**

Key Takeaways:

- Antivirus is like a security guard checking IDs. It works, but only for known threats.
- Endpoint detection and response (EDR) is your full security team. It monitors, analyzes, and responds to threats in real time.
- Modern cyber threats need modern defense. If you're serious about security, EDR is the way forward.

In the ultimate cybersecurity showdown, it's not old-school antivirus (AV) vs. next-gen EDR, it's antivirus and EDR working together.

When it comes to EDR vs AV detection, think of it as the difference between a metal detector at the door and a high-tech surveillance system. AV spots known threats and is good at detecting what it's seen before. Meanwhile, [EDR](#) goes further. It monitors behavior, identifies suspicious activity, and fights back.

The battle of antivirus vs endpoint protection has evolved. It's no longer just about catching viruses; it's about a comprehensive digital defense where AV provides hygiene and EDR fills the critical gaps. Together, they form an Endpoint Protection Platform (EPP) that hunts the unknown.

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

What is antivirus?

Antivirus is the OG of cybersecurity—good, but best when used with EDR to fill in the gaps. It works like a bouncer at a club, checking IDs (signatures) against a list of known bad guys ([malware](#)). If it doesn't see a match, it lets them in.

What antivirus brings to the table:

- ✓ Signature-based detection (aka "Hey, I've seen this virus before!")
- ✓ Real-time scanning for known threats
- ✓ Minimal behavioral analysis—if it walks like a duck but doesn't quack, antivirus might miss it

The problem? The volume, velocity, and variety of malware are huge. Cybercriminals create a ton of malware variants and rely on [living-off-the-land attacks](#) (aka LOLBins) that blow right past traditional antivirus.

What is EDR?

EDR not only looks for known threats, but it watches how programs behave, too, spotting the weird moves hackers make before they strike. Think of it like a security camera that not only records but also predicts when someone's about to break in and calls the cops before they do.

Why EDR is stronger and smarter

- ✓ Real-time monitoring: Always watching, with machine intelligence and human expertise working together to catch threats as they emerge
- ✓ Behavioral analysis: Detects threats by what they do, not just what they are
- ✓ Threat intelligence: Knows the latest about attackers and threats
- ✓ Automated response: Isolates threats before they wreak havoc
- ✓ Forensics and threat hunting: Helps when investigating attacks and strengthening defenses

EDR vs. antivirus: The key differences

So, what is the difference between EDR and antivirus when cybercriminals are using stealth tactics, zero-day exploits, and fileless attacks? Is a simple bouncer enough to protect your business, or do you need a full-blown security squad? Which one should you rely on? Let's break it down.

Feature	Traditional AV	EDR
Detection	Signature-based (known threats)	Behavior-based (unknown and advanced threats)
Response	Quarantines/deletes files	Isolates endpoints, kills processes, and rolls back damage
Visibility	Limited	Full system activity visibility
Threat Hunting	No	Yes
Zero-Day Attacks	Struggles	Designed to detect and help stop more effectively

When to use EDR vs. antivirus

Knowing when to use EDR vs antivirus shouldn't be about picking one over the other. It's about recognizing that antivirus alone can't cover it all. That means, in today's world, it's not AV or EDR, it's both. And for many organizations, [Managed EDR](#) takes it a step further by combining tech with human expertise for 24/7 threat monitoring and response.

Pros and cons: Breaking it down

The global average cost of a data breach reached [\\$4.45 million in 2023](#), marking a 15% increase over the previous three years. When it comes to EDR vs antivirus pros and cons, it's not even a fair fight. But still, let's highlight some of the pros and cons of each:

AV pros:

✓ Affordable and easy to install

- ✓ Affordable and easy to install
- ✓ Low resource usage
- ✓ Good for basic protection

AV cons:

- ✗ Struggles against advanced threats
- ✗ Limited visibility into attacks
- ✗ Reactive instead of proactive

EDR pros:

- ✓ Catches threats before they do damage
- ✓ Full attack visibility and forensics
- ✓ Integrates with other security solutions

EDR cons:

- ✗ More expensive upfront
- ✗ Requires skilled security personnel to manage
- ✗ Can generate alert fatigue if not tuned properly

Why antivirus is not enough

Hackers aren't just throwing viruses at your system anymore. They're slipping in through backdoors, hiding in legit-looking software, and using your own tools against you. Here's why antivirus alone doesn't work anymore:

- ✓ Zero-day exploits: Zero-day exploits are unknown and can sneak past AV undetected.
- ✓ Fileless malware attacks: Threat actors use legitimate, existing tools to target victims, rather than malicious files.
- ✓ Lateral movement: Once inside, attackers move around undetected. AV won't spot this.

Can EDR replace antivirus?

Short answer: not exactly. You still need strong malware protection.

Most modern EDR solutions bundle in antivirus-like features, covering both signature-based detection and advanced behavior analysis. That means you get the best of both worlds—traditional malware protection plus next-level threat detection and response.

However, it's important to note that many compliance standards, like PCI DSS v4.0 still require antivirus or anti-malware protection as part of a complete endpoint security program.

Bottom line: EDR doesn't replace antivirus, but builds on it.

Final verdict: What's the right choice for your business?

If your business just needs basic protection and the budget is tight, antivirus will get the job done—until it doesn't. But if you're serious about security and want a defense system that can catch modern threats and attacks, EDR is the way to go.

Threats can seem overwhelming, but with our in-depth understanding of how threat actors think

threats can become overwhelming, get more in-depth understanding of how threat detection works, 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. If you're ready to move beyond basic protection, [book a demo](#) with Huntress.



Brenda Buckman

[Read More >](#)

[Continue Reading](#)

Essential EDR Features: What to Look for in a Solution >

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

