



Endpoint Detection & Response (EDR)

Evaluation Guide



Contents

<u>Introduction</u>	3
<u>The Purpose and Value of EDR</u>	4
<u>Essential EDR Capabilities</u>	6
<u>The Five Qualities of a Great EDR</u>	7
<u>Considerations for Selecting the Ideal EDR Vendor</u>	8
<u>The ThreatDown Approach to Modern EDR</u>	10
<u>EDR Evaluation Checklist</u>	12
<u>Born from Malwarebytes. Built for Business.</u>	14

Introduction

In today's hyperconnected world, your endpoints — laptops, servers, and mobile devices — are the critical frontlines where cyberattacks unfold. That's because they're treasure troves of coveted sensitive data and business IP. Cybercriminals know this, and they've evolved their tactics far beyond classic malware to gain persistent access without detection. Attacks are stealthier, smarter, and more relentless.

Modern threats evade detection by blending into normal activity: hijacking legitimate tools, exploiting trusted credentials, or operating entirely in memory without leaving a trace on disk. In fact, 37% of ransomware attacks now use fileless techniques, which renders traditional malware detection ineffective.¹ At the same time, AI-powered hacking tools and malware-as-a-service are lowering the barrier to entry, putting sophisticated attacks into the hands of even low-skilled adversaries.

This shift underscores the need for modern endpoint security—solutions designed to detect and respond to today's fast-moving, evasive threats.

Endpoint Detection and Response (EDR) delivers exactly that.

Operating where attacks unfold on the endpoint — EDR provides deep visibility, correlates suspicious behavior, and enables rapid investigation, containment, and remediation. It goes far beyond traditional tools by layering behavioral analysis, threat intelligence, and real-time response to address the full spectrum of modern cyberthreats.

But when you're searching for a solution, the differences between EDR platforms really start to matter. Capabilities can vary widely — from the depth of detection to the speed and ease of response. This guide gives you the evaluation blueprint for selecting a robust EDR that fits your organization's unique needs.

Use this guide to:

- Understand the role and value of EDR
- Learn about its key capabilities
- Drive your evaluation efforts

Not all EDRs are built the same.

Visibility, detection capabilities, and response speed can make or break your defense.

Know what to look for before you buy.

¹ ThreatDown 2024 State of Ransomware Report

The Purpose and Value EDR

EDR was built for a new era of threats — one where malware is just the tip of the spear. As attackers shift to fileless techniques, stolen credentials, and living-off-the-land tactics, organizations need more than basic endpoint protection. They need visibility into what's really happening on endpoints and the ability to act fast.

EDR is a security control made up of two core components: a centralized management console and lightweight software agents installed on endpoints — including desktops, laptops, and servers. The agents continuously monitor system activity and report critical events, while the management console provides centralized visibility, analysis, and control across your entire fleet of endpoints.

The main functions of EDR are:

- **Detect** malicious or suspicious activity by monitoring real-time data such as process launches, network calls, file changes, and memory injections.
- **Protect** endpoints with enforcement measures such as blocking suspicious binaries and isolating hosts to contain threats.
- **Respond** by orchestrating rapid incident actions such as killing malicious processes, quarantining files, resetting credentials, and executing playbooks.
- **Remediate** the effects of an incident by rolling back encryption, restoring settings, cleaning up artifacts, and creating a timeline for root-cause analysis.

EDR is recognized as a standard for meeting the monitoring objectives of ISO 27001:2022 Annex A Control 8.16, and plays a key role across multiple NIST Cybersecurity Framework functions—particularly in the Detect and Respond functions through continuous endpoint monitoring and automated threat response capabilities.

Antivirus vs. EPP vs. EDR: What's the difference?

You'll often hear the terms antivirus, Endpoint Protection Platform (EPP), and EDR tossed around — sometimes even used interchangeably. But while they all contribute to endpoint security, they each serve distinct purposes.

Traditional antivirus and EPP are primarily prevention focused. They're designed to stop known threats from executing using methods

like signature matching, machine learning, and heuristic analysis. These tools form the first layer of defense, blocking many common threats before they can take hold.

EDR incorporates EPP capabilities and extends them with powerful detection and response that's focused on catching and stopping threats that slip through. By continuously monitoring for suspicious or anomalous behavior, EDR identifies threats that have bypassed preventive defenses. It equips security teams to investigate incidents in depth, respond quickly, and preserve forensic evidence for remediation, compliance, and future readiness.

The bottom line: EDR and EPP aren't interchangeable — they're complementary. Together, they form a layered defense that strengthens your endpoint security posture.

The Purpose and Value of EDR (continued)

Benefits to organizations

Modern EDR helps organizations stay resilient in the face of constant, evolving attacks. By delivering visibility, control, and faster response at the endpoint, EDR strengthens both your security posture and your team's effectiveness.

Business benefits

- **Reduce breach risk and business disruption.** EDR improves threat detection and speeds up response, which helps prevent breaches that can lead to data loss, legal exposure, and reputational harm.
- **Maintain continuity.** By stopping ransomware, malware, and lateral movement early, EDR helps you maintain continuity of operations and employee productivity.
- **Support compliance and audit readiness.** EDR solutions provide detailed event logs, threat reports, and attack timelines that support regulatory reporting and internal audits.
- **Protect company IP and sensitive data.** Endpoints often house valuable data. EDR prevents attackers from stealing or destroying these critical assets.

Team benefits

- **Reduce alert fatigue.** Behavioral detection and threat correlation help teams focus on high-confidence alerts, rather than getting buried in noise.
- **Speed up investigations.** Built-in forensics and historical telemetry allow analysts to quickly understand what happened, when, and how.
- **Streamline containment and remediation.** Many EDR tools automate isolation and rollback, reducing the manual effort required to contain damage.
- **Amplify impact.** EDR equips your analysts with the visibility, context, and automation they need to work faster and more effectively. This helps you stay ahead of threats, even with a limited headcount.

Essential EDR Capabilities

An effective EDR provides a suite of features that monitor endpoints; identify, classify and prioritize suspicious activity; expose attack chains; enable fast threat hunting across an entire suite of endpoints; and provide a comprehensive range of automated and manual countermeasures to contain threats.

When selecting an EDR, ensure it has the following attributes:

✓ **Real-time monitoring**

Endpoint activity data, such as process launches, network connections, registry changes, file system changes, and user logons, are monitored and stored to provide raw data for other functionality, and a complete audit trail of events on every endpoint.

✓ **Advanced threat detection**

Behavioral analytics and machine learning identify deviations from normal behavior, such as suspicious process injections, living-off-the-land techniques, lateral-movement, and privilege escalation.

✓ **Alerting and triage**

Raw events are contextualized, prioritized by risk, and mapped to the MITRE ATT&CK framework to focus attention on the most significant incidents.

✓ **Investigation and root cause analysis**

Suspicious activity is contextualized with timelines, process trees, and threat intelligence so analysts can investigate attack chains and determine the scope and severity of incidents.

✓ **Threat hunting**

Historical data from endpoints can be queried and correlated with threat intelligence feeds to expose nascent threat actor activity.

✓ **Response and containment**

Countermeasures such as isolating hosts, killing processes, and quarantining files give analysts a range of instruments for containing and neutralizing threats.

✓ **Remediation and rollback**

Encrypted files, modified registry entries, and persistence artifacts are cleaned or rolled back to restore endpoints to a known good state.

✓ **Reporting and compliance**

Dashboards, timelines, and reports prove due diligence for frameworks such as ISO 27001, PCI-DSS, and NIS2.

✓ **Cloud native management**

A cloud-native console provides alert prioritization, threat hunting, and countermeasures across an organization's entire suite of endpoints.

✓ **Tamper protection**

Self-defense mechanisms prevent malicious actors from disabling, modifying, or bypassing the EDR agent and its security controls, ensuring continuous protection even during sophisticated attacks that attempt to evade detection.

The Five Qualities of a Great EDR

Beyond the essential capabilities, buyers should also focus on these five essential qualities:

1. Unified platform

Modern EDR should be part of a unified platform — not a standalone tool. Look for solutions that consolidate key controls, such as vulnerability management, application blocking, and DNS protection into a single, centrally managed system. A central console and platform reduces complexity, eliminates security silos, and improves your team's ability to manage security.

2. Ease of deployment

EDR rollouts that require complex configurations, extensive testing phases, manual installations, and extensive troubleshooting place a heavy burden on IT staff and budgets, create security gaps, and delay critical protection. EDR deployment should be easy, regardless of existing security tools, a remote workforce, or a mixed operating-system estate.

3. Ease of management

Solutions that are overly complex, unintuitive, split across multiple consoles, or require specialized expertise to operate end up delivering less security in practice than on paper. The best EDR platforms provide intuitive interfaces that allow analysts to focus on genuine threats rather than wrestling with the tool itself.

4. Low false positive rates

High false positive rates make it harder to identify genuine threats, waste analysts' time, lower an organization's trust in the EDR solution, and lead to alert fatigue, ultimately compromising security. EDR solutions should minimize false positives while maintaining high detection rates for real threats.

5. Minimal system performance impact

Security should not come at the cost of productivity. EDR agents that consume excessive CPU, memory, disk I/O, or network resources can slow business applications and create resistance to necessary cybersecurity measures. EDR solutions should use lightweight agents that provide comprehensive protection without a noticeable impact on performance.



Considerations for Selecting the Ideal EDR Vendor

With dozens of EDR vendors in the market, you'll have no shortage of choices when selecting one as your service provider. Finding an EDR provider is easy, but how do you find a good one? Ultimately, this will be a long-lasting relationship, so you'll want to ask questions that let you evaluate a vendor from multiple angles to ensure they'll provide the most value to your business.

Investigative questions across the following criteria will help you identify your preferred EDR vendor:

✓ Trusted brand

Choose a vendor with a proven track record in innovation, reliability, and customer focus. A recognizable name helps, but reputation is earned through consistent delivery, transparent practices, and strong customer outcomes.

1. How long has the vendor been in the cybersecurity space, and how have they evolved their EDR offering?
2. Are they known for reliability, transparency, and customer-centric development?
3. Are there strong customer success stories or references in your industry or size segment?

✓ Vendor support

Look for a vendor that not only provides a strong product but also backs it with the right level of support, enablement, and partnership.

1. What support options are available (e.g., 24/7, business hours, severity-based SLAs)?
2. How responsive is their support team during real-world incidents?
3. Are self-service resources available, such as a knowledge base, documentation, and community forums?
4. Do they provide onboarding tools like quick start guides, deployment checklists, or step-by-step setup tutorials?

✓ Pricing and licensing

EDR pricing models can vary widely. Understanding the total cost of ownership is key to selecting a sustainable solution.

1. Is the pricing model transparent and easy to forecast across devices or users?
2. What capabilities are included in the core license, and which, if any, require additional fees or modules?
3. How scalable is the licensing model as your environment changes?
4. Are costs for support, updates, or integrations built into the license, or charged separately?

Considerations for Selecting the Ideal EDR Vendor (continued)

Product vision & roadmap alignment

An effective EDR solution should evolve alongside your business and the threat landscape. A clear, forward-looking product roadmap shows the vendor's commitment to long-term security innovation.

1. How frequently does the vendor deliver product updates or new capabilities?
2. Are they expanding support for emerging threats (e.g., fileless attacks, identity misuse) or technologies like AI-driven detection?
3. Does their roadmap address trends relevant to your organization — like cloud migration, hybrid work, or automation?
4. How does customer feedback influence product development and prioritization?



The ThreatDown Approach to Modern EDR

ThreatDown EDR delivers advanced protection, detection, and response that combines powerful security with worry-free management in a cloud-native, single-tenant platform that covers your entire endpoint security stack.

With AI/ML-driven analytics and real-time behavioral analysis, ThreatDown EDR equips you to stop threats early and respond fast — delivering the superior defense today's threats demand. Its lightweight agent deploys in minutes across Windows, macOS, and Linux endpoints, while the intuitive console surfaces meaningful alerts — without flooding your team with noise.

As part of the ThreatDown Nebula platform, you can consolidate key security controls — including vulnerability assessment, patch management, application blocking, and DNS protection — into a single, unified platform. By eliminating silos and simplifying operations, ThreatDown gives you complete visibility and control from the same Nebula console you use to manage endpoint protection.

Leading capabilities that transform your endpoint security

ThreatDown EDR delivers advanced capabilities that empower you to proactively reduce your endpoint attack surface:

- **Security Advisor**
An AI-powered dashboard that makes it easy to understand and optimize your security posture. It delivers a clear headline security score, real-time insights into your environment, alerts for emerging risks, and an "easy button" to make the changes needed to enhance your security posture.
- **Flight Recorder**
Provides full endpoint telemetry history with fast, intuitive filters—no complex query languages needed—so your team can hunt threats efficiently and accurately.
- **Attack Isolation**
Delivers an unmatched array of tools for containing threats, including process, desktop, and network isolation. Isolation can be triggered automatically during critical events or manually with a single click. Analysts retain full access and control over isolated endpoints through a secure command-line interface.
- **Thorough Remediation**
Automatically and remotely remediate infected endpoints with just a few clicks from the Nebula console — no need for hands-on intervention or reimaging.
 - Patented Linking Engine** automatically identifies and removes residual malware artifacts, reversing configuration, registry, and system changes to restore the endpoint to its pre-infection state.
 - Ransomware Rollback** from ransomware attacks by rolling back any file changes up to seven days, without relying on Microsoft VSS.
- **Lightweight agent**
A single, lightweight agent deploys easily without rebooting, reduces system impact, and lowers operational costs.

The ThreatDown Approach to Modern EDR (continued)

ThreatDown: A security partner you can count on

✓ Trusted brand

More than 15,000 organizations rely on ThreatDown to protect millions of endpoints—and we're rated 4.6 stars by real-world users.

✓ Proven performance

Name AVLab's Product of the Year for the third consecutive year, and earn the highest Level 1 certification for MRG Effitas' real-world threat tests every single quarter since Q3 2021.

✓ Innovation that delivers

We continually evolve our platform—adding new capabilities and expanding coverage—to stay ahead of modern threats.

✓ High value, low overhead

Deployment is quick, scaling is seamless, and ROI is unmatched—maximum protection without the complexity or cost.

✓ Customer-first support

Our dedicated support team is known for fast, expert service that ensures you get expert help when you need it.



ThreatDown's EPP+EDR combination is an Info-Tech Software Reviews and AV Labs Gold Award winner, beating Sophos and Bitdefender.

ThreatDown detected 12 out of 12 simulated real-world attacks providing complete visibility of every attack in its console.



"Simple and powerful"

"Excellent cybersecurity product"

"I love this platform"

"Amazing experience"

"Wonderful product, terrific support"

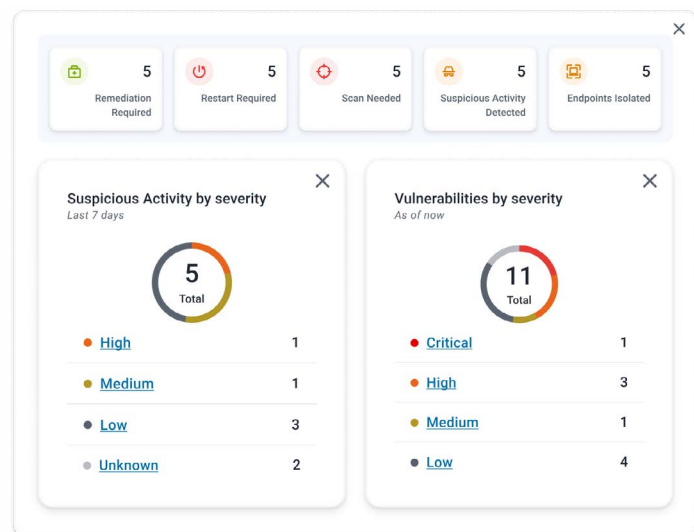
EDR Evaluation Checklist

Choosing the right EDR solution starts with knowing what to look for. Use this checklist as a practical tool to compare vendors side by side. It summarizes the essential capabilities, platform qualities, and vendor traits outlined in this guide so you can make an informed, confident decision.

Fill in the blanks as you explore your options and use the criteria to drive deeper conversations with vendors during demos, trials, and stakeholder reviews.

			Vendor 2	Vendor 3
Core Capabilities	Real-time monitoring of endpoint activity	✓		
	Behavioral threat detection (incl. fileless attacks)	✓		
	Alerting and triage mapped to MITRE ATT&CK	✓		
	Built-in investigation tools (process trees, timelines, etc.)	✓		
	Threat hunting with historical telemetry	✓		
	Automated response (isolation, kill process, etc.)	✓		
	Ransomware rollback	✓		
	Automated, deep remediation (e.g., Linking Engine)	✓		
	Compliance-ready reporting and dashboards	✓		
	Tamper protection	✓		
Platform Qualities	Unified platform with additional controls (DNS, app block, vuln)	✓		
	Lightweight agent with minimal system impact	✓		
	Cloud-native management console	✓		
	Easy deployment and onboarding	✓		
	Intuitive UI and low learning curve	✓		
	Low false positive rate	✓		
Vendor	Strong industry reputation	✓		
	Support availability and responsiveness	✓		
	Access to documentation, training resources, quick-start tools	✓		
	Transparent, scalable pricing and licensing	✓		
	Clear product vision and roadmap aligned with your needs	✓		

Put ThreatDown EDR on Your Shortlist



“Ransomware rollback is one that we mention a lot. It’s one of the features that really appealed to us having gone into environments that have been attacked”

Simon Bough,
Founder, ICT North

Learn more about how ThreatDown EDR can help your business.

Speak to an EDR expert



threatdown.com/edr



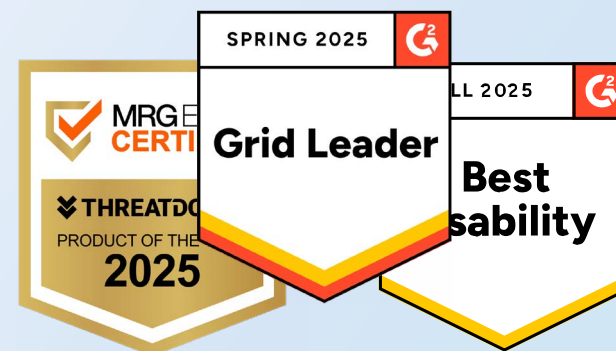
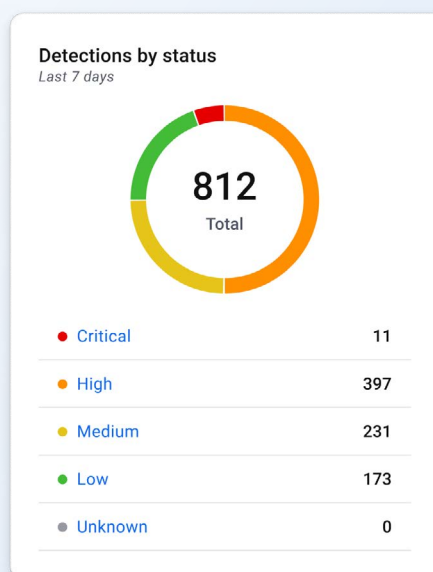
sales@threatdown.com

Born from Malwarebytes. Built for Business.

Formerly known as Malwarebytes for Business, ThreatDown delivers cybersecurity for businesses.

Built on Malwarebytes' expertise in malware detection and remediation, ThreatDown's comprehensive suite of solutions is designed for IT-constrained teams that need advanced protection, without the complexity.

Improve your security posture with one easy-to-manage platform that combines EDR, MDR, Patch Management, 7-day Ransomware Rollback, and AI-driven insights— deployed with a single, lightweight agent. No extra headcount or complex setup required.



IT teams trust us to deliver enterprise-grade protection that's easy to deploy and manage. From award-winning tools to top ratings on Gartner Peer Insights™ and G2, security professionals choose ThreatDown for ease-of-use, fast deployment, and responsive support.

Spend less time managing threats and more time powering your business.

Visit threatdown.com/explore-portfolio