![ThreatDown — Powered by Malwarebytes]

ThreatDown Endpoint Detection & Response (EDR)

Simple, Effective Prevention, Detection, and Remediation

Overview

Organizations today face a grim reality: the prospects of a breach is no longer a question of "if" but when. Compounding this reality is the global and sustained shortage of cybersecurity professionals, which leaves security teams short on staff, pressed for time, and beset with a disparity of skill levels.

ThreatDown EDR was designed with this grim reality in mind. It delivers effective protection—from prevention through identification to response actions—that users with emerging cybersecurity acumen can learn and use with ease. But this simplicity belies its underlying sophistication: ThreatDown EDR includes high-powered tools and customizable options that users can embrace as their skill level grows and the organization's security needs change. By deploying our readily accessible cloud-based security platform, organizations of all sizes gain powerful detection and remediation while freeing their security teams to spend time on other more pressing projects.

ThreatDown EDR Advantages

Ease-of-Use

ThreatDown EDR offers organizations the assurance of powerful protection and trouble-free management. Easy to learn and use, our cloud-native console opens to an intuitive dashboard displaying visual cues that immediately convey which endpoint and servers need attention and why.

High-quality Alerts Without the "Noise"

We deliver alerts with insights. Detected threats trigger alerts that contain information with a high-level of contextual detail to help users to quickly make informed decisions about how to respond appropriately.
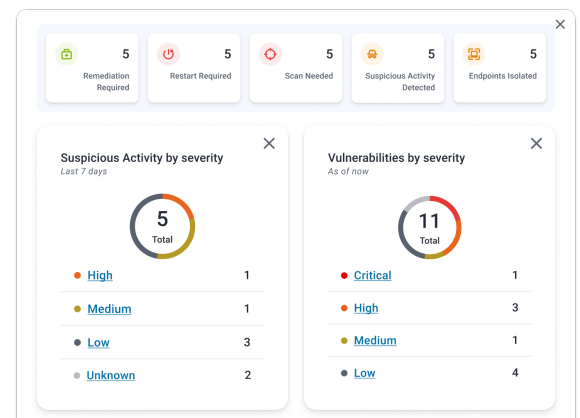
Expanded Remediation

With a few clicks from within our Nebula cloud-based management console, you can remotely remediate an infected endpoint. Our proprietary Linking Engine is designed to identify and remove residual malware-related artifacts and infection-induced changes to help ensure thorough remediation.

Accelerated Deployment

tWe designed ThreatDown EDR with ease in mind to simplify use and accelerate deployment. Our lightweight agent for Windows, macOS, and Linux deploys within minutes.

Challenges

- **Attacks are evolving** - 71% of companies were impacted my ransomware last year[1]

- **Complexity from agent sprawl** - 55 average number of cybersecurity tools deployed at a company[2]

- **Lack of budget and resources** - 80% of security alerts ignored[3]

[1]Malwarebytes State of Malware Report. [2]Anomali's Cybersecurity Insights Report 2021. [3]ThreatDown Research

Platform Expansion

As your security needs change, ThreatDown EDR expands to meet them. EDR is a key component of our bundles that enable your team to reinforce prevention in key threat vectors such as software vulnerabilities, patch management, tand DNS filtering.

How Does it Work?

ThreatDown EDR helps prevent cyber threats—including malware, brute force attacks, and zero-day exploits—from reaching your environment. To do so, it continuously searches for known malware using rules-based threat detection while proactively hunting for unknown malware using AI-based (also known as "behavioral-based") detection designed to detect and analyze anomalous files and programs to mitigate risk. Whether known or unknown, detected threats trigger alerts that include the details users need to respond quickly and appropriately.

ThreatDown EDR also detects, alerts users of, and automatically removes Potentially Unwanted Programs (PUPs) and Potentially Unwanted Modifications (PUMs) that, while not malicious, commonly diminish end users' experience. Our MITRE-evaluated platform also automates analysis of zero-day threats and empowers users with the ability to isolate suspicious code per machine, user and/or process; containing questionable code allows for investigation without risk of further exposure and spread. ThreatDown EDR includes a cloud sandbox that users can use to investigate dubious executable binaries; users can also use the sandbox to remotely and securely detonate malware.

When infections creep into your digital environment, ThreatDown's award-winning detection and remediation can help you effectively remove malware. Our advanced remediation technology is designed to ensure that all residual traces of malware are eradicated and any malware-induced configuration changes are undone. For complete recovery from ransomware, ThreatDown EDR comes with our 7-day Ransomware Rollback (for Windows only); this capability helps you return to a pre-ransomware state without the time-consuming task of reimaging machines or re-creating encrypted files.

Industry Accolades

Consistent top ranking of Level 1 certification in MRG Effitas 360 degree testing and #1 Endpoint Security Suite by G2 validate ThreatDown's effective and easy-to-use solution.

Keep Threat Levels Down

Protect your organization's workstations, servers and more with award-winning prevention, detection and response

- **Detect Accurately** - Identify malicious and suspicious threats

- **Respond Immediately -** Isolate users, endpoints, and networks to stop breaches

- **Remediate Fully -** Return endpoints to healthy state and prevent reinfection

---

MRG Effitas CERTIFIED — 360° ASSESSMENT

MRG Effitas CERTIFIED — RANSOMWARE

Request a Quote

To request a custom quote visit
threatdown.com/custom-quote/endpoint-detection-and-response/

ThreatDown™
Powered by **Malwarebytes**

www.threatdown.com/edr

corporate-sales@malwarebytes.com

1.800.520.2796