DATA SHEET

ThreatDown™
Powered by Malwarebytes

THREATDOWN ENDPOINT PROTECTION

Powerful malware protection for the endpoint.
Built for any size organization.

Today, even basic malware campaigns are automated—enabling cybercriminals with few resources to launch sophisticated attacks against organizations of all sizes. To fight back, businesses deployed multiple layered, yet siloed, endpoint security solutions, which threat actors soon defeated by exploiting the gaps in between. These synergistic trends mean there has never been a greater need for a unified, comprehensive approach to endpoint protection that's strong enough to thwart advanced attacks, but agile enough to adapt to the threat landscape.

Enter ThreatDown Endpoint Protection, a complete malware protection and remediation solution with predictive threat detection, proactive threat blocking, and integrated end-to-end protection. Driven from the cloud through a single pane of glass, ThreatDown Endpoint Protection provides flexible management and speed for organizations of all sizes.

Comprehensive protection built for speed

Quickly deploy, improve end user productivity

Precision detection at the point of attack

Innovative advanced endpoint protection

Scales to combat growing threats

Simple to use protection from a single pane of glass

EXPLORE THE ADVANTAGES

COMPREHENSIVE PROTECTION BUILT FOR SPEED

Agent architected for performance
Many endpoint security platforms stuff endpoints with an ever-increasing store of malware signatures and slow performance with brute-force scanning algorithms. In contrast, ThreatDown, powered by Malwarebytes, uses a single, low footprint agent that quickly pinpoints and blocks malicious code from running without impacting performance on your Windows, Mac, or Linux machines.

Comprehensive web protection
Our web protection technology proactively prevents users from accessing malicious sites, malvertising, scammer networks, and suspect URLs, as well as downloading potentially unwanted programs and potentially unwanted modifications.

Hardened devices and apps
ThreatDown, powered by Malwarebytes, hardens your devices by blocking exploits, stopping remote code execution, and breaking communication with hostile malware servers to dramatically reduce your organization's attack surface.

Behavioral-based blocking
Our behavior-based analysis provides near real-time identification of behavior that is undeniably hostile and automatically blocks the threat, delivering the most proactive protection on the market today.

Zero-day prevention
ThreatDown, powered by Malwarebytes, applies signatureless payload analysis and anomaly detection to proactively identify and block malware, vulnerability exploits, and infections from USB peripherals from harming your environment.

PRECISION DETECTION AT THE POINT OF ATTACK

The right type of machine learning
Instead of training on malware, the ThreatDown, powered by Malwarebytes, model is trained to recognize goodware—properly-signed code from known vendors. The result is a predictive malware verdict that becomes increasingly faster and incrementally more precise. We also test for malicious code and bad behavior at all stages, including remote investigation of suspicious code that won't disrupt end user productivity.

Fastest threat intelligence on the market
Benefit from ThreatDown detection and remediation intelligence collected from millions of corporate and consumer-protected endpoints. Even brand-new, unidentified malware is typically eliminated before it can impact your endpoints.

Unified detection funnel catches more threats
ThreatDown, powered by Malwarebytes, applies behavioral monitoring and machine learning to profile threats across web, memory, application, and files. Successive learnings along the detection funnel provide increasingly higher detection rates with lower false positives.

Traces the infection, maps the removal
The ThreatDown Linking Engine traces every installation, modification, and process instantiation—including in-memory executables that other anti-malware packages miss—mapping a complete picture of the threat that enables full remediation.

Lethal "one-and-done" remediation
Applying in-depth insights from the Linking Engine, ThreatDown thoroughly and permanently removes both the infection and any artifacts, delivering lethal "one-and-done" remediation.

SCALES TO COMBAT GROWING THREATS

Complete endpoint security solution driven by a single pane of glass
A full suite of endpoint security functionality and automation capabilities driven from the ThreatDown Nebula cloud platform and accessed from an intuitive UI make fighting malware a matter of clicks, not scripts.

Prioritizes security team productivity
Your security team can traverse from the global dashboard down to identified threats and quarantined devices in just a few clicks. Scanning and remediation is automated across a single department or thousands of devices at a time.

Analyzes the impact so you don't have to
ThreatDown, powered by Malwarebytes, provides extensive threat analysis background along with assessment of its potential impact. Your CISO can save time and effectively communicate potential impacts to executive leadership.

Scalable to the largest enterprise
Our solution applies the power of the cloud to scale to even the largest organization's needs, efficiently detecting advanced threats, and providing a globally consistent and speedy response.

REQUEST A TRIAL

To request a free trial, visit: malwarebytes.com/business/request_trial