Malwarebytes

DATA SHEET

Malwarebytes Endpoint Detection and Response

Keep devices working with integrated detection, protection, and response.

Overview

Organizations of all sizes are pinned between increasingly sophisticated malware that attacks deeper and broader than ever before and having a mishmash of security approaches – antivirus, system monitors, and more. However, malware has evolved to finding the gaps between these silos of defense.

Malwarebytes Endpoint Detection and Response (EDR) is a full suite malware detection, protection, and remediation product that enables Operational EDR to keep devices working. It provides extended detection along the attack chain and enables fast, effective operations. Driven from the cloud via a single pane of glass for organizations of all sizes, Malwarebytes EDR provides sophisticated detection able to pinpoint even zero-day exploits, intuitive investigation without requiring a PhD, and recovery even from ransomware that has already triggered.

HIGHLIGHTS

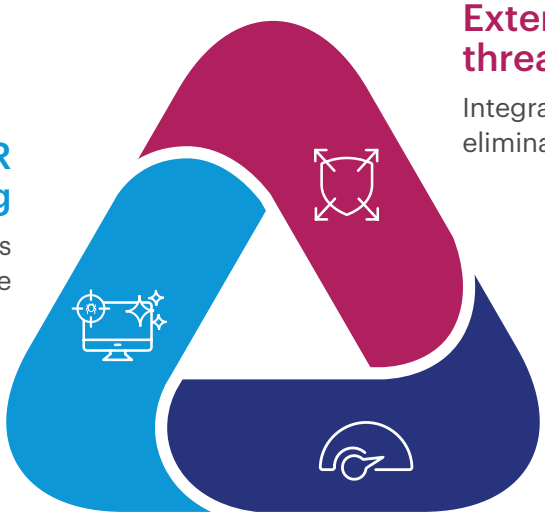
Full suite
A single pane of glass handles all operational endpoint security needs.

Ransomware rollback
Rolls the device back to a known healthy state even after ransomware has triggered.

Efficient yet transparent
Optimizes the security pros efficiency yet is transparent to the end user.

Operational EDR keeps devices working

Unique focus on keeping endpoints online and end users productive



Extend your threat protection

Integrated detection and analysis eliminate silos of defense

Deploy fast, manage efficiently

Deploy, manage, and tune endpoint security with speed and efficiency

Experience the advantages

Operational EDR keeps devices online.

You need to get compromised endpoints back online quickly. Our product enables you to isolate, investigate, and remediate, including ransomware rollback, in just a few clicks. Plus, our insightful threat hunting capabilities empower you to investigate and either whitelist approved software or drill down into suspicious behavior.

Guided investigation
Our guided threat hunting provides severity-prioritized Indicators of Compromise (IoCs), so you can quickly assess the extent and urgency of a threat. Integrated incident response enables you to isolate and remediate all traces of a threat or exclude activity that you deem is benign—all with clicks, not scripts. Flexibility is maximized by allowing exclusions to be global or per policy.

Granular attack isolation
Our product prevents lateral movement of an attack by allowing isolation of a network segment, of a single device, or of a process on the device. This capability provides breathing room for the right active response while minimizing impact on the end user.

Thorough remediation
The Malwarebytes proprietary Linking Engine technology maps system changes associated with the malware, thoroughly removes the infection, and returns the endpoints to a truly healthy state.

Flight Recorder search
Flight Recorder captures file, process, network domain, and IP address changes and activities over time for both endpoints and servers. Flight Recorder Search enables freeform threat hunting across the entire device pool managed by Malwarebytes EDR. It provides advanced search capabilities of MD5 hashes, filenames, network domains, IP addresses, and more. This feature provides the capability to search for specific IoCs that can be mapped to MITRE ATT&CK techniques.

Ransomware rollback
Malwarebytes stores changes to files on the system in a local cache over a 72-hour period. With one click, you can reverse the damage caused by ransomware and restore the device to a healthy, productive state.

Extend your threat protection.

Malwarebytes integrates protection with detection, securing endpoints and providing full visibility and control across the attack chain.

Global threat intelligence
Threat intelligence provides global insights into behavioral heuristics, IoCs, and attack techniques, allowing for constant adaptation of detection and remediation capabilities to address new threats.

Integrated endpoint protection
Our product integrates automated, adaptive detection techniques (including a cloud sandbox) that learn along each stage of the threat detection funnel, providing continual situational awareness of suspicious activity until a final verdict can be made with precision.

Suspicious activity monitoring
Malwarebytes monitors endpoints, creating a "haystack of data" in the cloud where a combination of behavioral analysis and machine learning pinpoints any IoC "needles."

Cloud sandbox
We apply powerful threat intelligence to the cloud sandbox's deep analysis of unknown threats to increase the precision of threat detection, providing you with prepackaged analysis of actionable IOCs.

Deploy fast, manage efficiently.

Malwarebytes was built for speed—from deployment to management to ongoing maintenance. Organizations with scarce security resources achieve active response and a strong security posture in minutes.

Cloud-native where it matters
Leveraging the power of the Malwarebytes Nebula cloud platform, endpoint detection and response capabilities evolve at the speed of attack innovation. And, our low footprint agent taps the power of the cloud to efficiently detect advanced threats based on behavior.

Management built for endpoints
Our product lets you effectively manage security on endpoints at enterprise scale, and with just a few clicks, go from a global dashboard to a highlighted threat to prioritized remediation of groups of devices or locations.

Automated operations and tracking
Baseline security tasks such as scans and remediations are launched with a few clicks. Plus, tracking is automated so that endpoints that have not executed a scan or an incomplete remediation are flagged for action. These capabilities free you for more strategic security work.

Benefits

Maximizes device availability
EDR provides powerful capabilities—from investigation to recovery of a device with ransomware that has triggered—that keep devices humming.

Threat hunt without a PhD
Malwarebytes leverages patented, market-leading techniques to provide security pros with current global intelligence tailored to their environment so they don't have to have a PhD in analytics.

Handle more devices with less effort
Automation and tracking of key tasks, such as scans and remediations, enable security pros to manage more devices with less effort.

LEARN MORE

To learn more, please contact your account team or your authorized channel partner. Or, to communicate with a local sales expert, visit: malwarebytes.com/business/contact-us/

malwarebytes.com/business corporate-sales@malwarebytes.com 1.800.520.2796

Malwarebytes is a cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against malicious threats, including ransomware, that traditional antivirus solutions miss. The company's flagship product uses signature-less technologies to detect and stop a cyberattack before damage occurs. Learn more at www.malwarebytes.com.