Malwarebytes

DATA SHEET

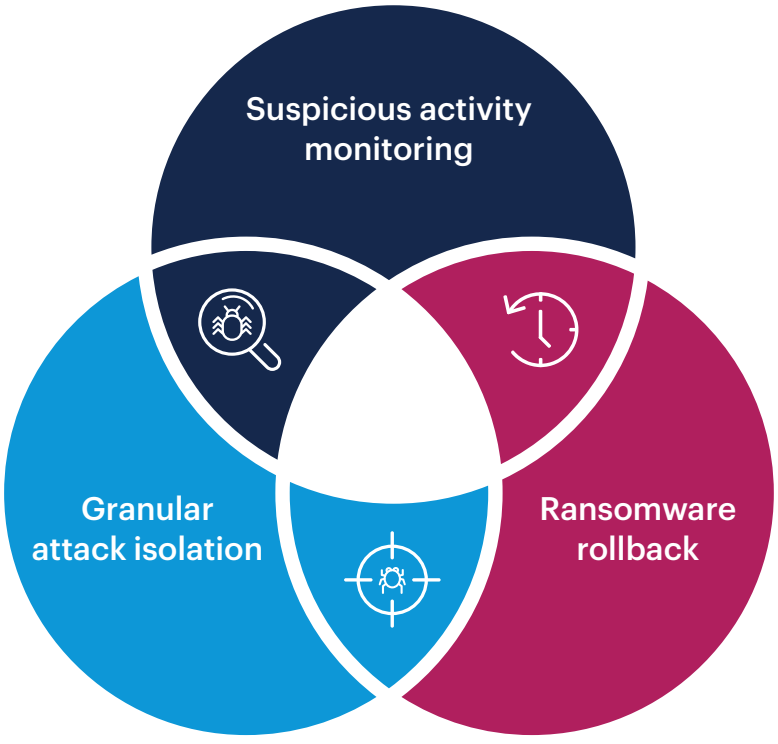
Malwarebytes Endpoint Detection and Response for Servers

Integrated protection, detection, and response. Built for ease and speed.

Overview

Corporate servers and the data that resides on them are the backbone of modern business operations. One successful cyberattack can take a critical system offline and bring productivity to a standstill. Because servers are at the core of all organizational activity, they require comprehensive security that makes them resilient against any attack.

Malwarebytes Endpoint Detection and Response for Servers is fast, lightweight, and purpose-built to protect your most valuable data. The solution delivers integrated, proactive protection and "one-and-done" remediation that is laser-focused on keeping your server infrastructure online and operational. And its Ransomware Rollback feature returns impacted servers to a truly healthy state—without costly re-imaging, lost productivity, or having to pay the ransom.



KEY BENEFITS

Comprehensive visibility
Centralized, cloud-based management provides comprehensive visibility into your security posture.

Efficiency
Delivers continuous detection of and response to advanced security threats for unprecedented operational efficiency.

Precise verdicts
Integrated detection across the attack chain returns a verdict with precision.

Platform needs
From servers to workstations, Malwarebytes delivers advanced protection for your organizational platform needs.

PLATFORMS

Windows servers

Features

Deploy fast. Manage simply.

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

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 server footprint taps the power of the cloud to efficiently detect advanced threats based on behavior.

Management built for endpoints
Our solution lets you effectively manage server security at enterprise scale, and, with just a few clicks, gain broad visibility from the global dashboard down to individual indicators of compromise (IoCs) discovered on a server.

Extend your threat protection.

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

Integrated proactive protection
Automated threat detection and protection across web, memory, application, and files applies adaptive detection techniques, including behavioral monitoring and cloud-based machine learning.

Suspicious activity monitoring
Continuously analyzes endpoint processes, registry, file system, and network activity in the cloud using behavioral analysis and machine learning to pinpoint potential suspicious activity.

Cloud sandbox
Deep analysis of unknown threats is done safely in the cloud, providing highly precise detection through threat intelligence, delivering actionable IoCs.

Flight Recorder search
Flight Recorder captures file, process, network domain, and IP address changes over time. This enables freeform threat hunting for specific IoCs such as MD5 hashes, filenames, network domains, and IP addresses.

Investigate, isolate, and recover.

Malwarebytes Endpoint Detection and Response for Servers gives security professionals the ability to quickly investigate, isolate, thoroughly remediate, and recover from threats in a matter of minutes.

Granular attack isolation
Now, it's easy to halt malware from spreading if a server is attacked. Malwarebytes Endpoint Detection and Response for Servers maximizes IT response capabilities, drawing from three modes of device isolation:

1. Network isolation limits device communications so attackers are locked out and malware can't "phone home." In addition, network isolation limits the malware's lateral movement.
2. Process isolation restricts malware from spawning new processes, limiting its impact. Users are also restricted from initiating new applications that may complicate a response effort.
3. Sever isolation allows administrators to lock out the machine while the IT staff manages triage. In addition, the server isolation can be leveraged to prevent insider threats.

With multiple modes of server isolation, security teams are able to take actionable steps to respond to threats.

Thorough remediation
A true "one-and-done" solution, Malwarebytes' remediation maps the correct path to permanently remove all malware. Traditional approaches focus on removing only the active executable and ignore residual changes, which leads to re-infection.

Malwarebytes' proprietary Linking Engine tracks every artifact, change, and process alteration, including memory executables others miss.

Ransomware Rollback
Our Ransomware Rollback technology works in sync with suspicious activity monitoring to catch ransomware behaviors. If ransomware behaviors are detected, Malwarebytes activates the file backups process by encrypting and relocating the data for later restoration.

The file backup process limits backup copies to just-in-time encrypted files. With one click, incident response teams can reverse ransomware damage by rolling back affected files to their pre-attack state up to 72 hours before their compromise.

Benefits

Comprehensive protection for your most valuable assets

Gain innovative, advanced protection for the organization's most valuable assets. With the solution's suspicious activity monitoring, granular attack isolation, and Ransomware Rollback, organizations can keep their systems up and running, even under the most lethal cyberattack.

Lightweight server security built for scale

Malwarebytes Endpoint Detection and Response for Servers provides the perfect balance between protection and performance. Quickly deploy endpoint protection for your servers without impacting system processing power.

Granular visibility, driven from a central cloud console

Our central cloud console provides broad visibility into your security posture. Through one pane of glass with an intuitive UI, gain visibility into all activity across your entire organization—from servers to workstations.

Summary

Corporate servers are constantly under attack. Providing services, applications, and other resources that are essential to keep business operations running, servers require nothing less than the best in protection.

From protection to detection and response, Malwarebytes Endpoint Detection and Response for Servers safeguards an organization's most valuable data. Built for organizations of all sizes that value efficiency, Malwarebytes Endpoint Detection and Response for Servers is designed from the ground up integrating and communicating across the detection funnel—all from a single agent and management console—to uniquely allow organizations to manage server security with speed, scale, and ease.

REQUEST A TRIAL

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

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.