Malwarebytes

DATA SHEET

Malwarebytes **Endpoint Protection & Response**

We don't just alert, we fix it

The reality of today's threat landscape is that no vendor provides 100 percent protection: www.malwarebytes.com\remediationmap.

Breaches are inevitable. Remediation is essential.

Today's organizations are seeking ways to address incidents not handled adequately by their existing defenses. When attackers bypass defenses, they often go unnoticed for weeks or months. In a 2017 global study conducted by Ponemon Institute, the mean time to identify (MTTI) a breach was 191 days.

Endpoint Detection and Response (EDR) capabilities aim to accelerate threat detection and reduce dwell time. The faster a data breach can be identified and contained, the lower the cost. Current EDR solutions identify a threat that has bypassed traditional protection, and a response is typically generated in the form of logs, alerts, and emails. A threat analyst then uses tools to evaluate the code, and the infected machines are reimaged.

Malwarebytes Endpoint Protection and Response takes a different approach. By leveraging proprietary Linking Engine remediation and Ransomware Rollback, Malwarebytes goes beyond alerts and reimaging to fix the damage. With Endpoint Protection and Response, you don't need to make a trade-off between cost and complexity.

TECHNICAL FEATURES

Web Protection
Prevents access to malicious websites, ad networks, scammer networks, and bad neighborhoods

Application Hardening
Reduces vulnerability exploit surface and proactively detects fingerprinting attempts used by advanced attacks

Exploit Mitigation
Proactively detects and blocks attempts to abuse vulnerabilities and remotely execute code on the endpoint

Application Behavior Protection
Prevents applications from being leveraged to infect the endpoint

Anomaly Detection Machine Learning
Proactively identifies viruses and malware through machine learning techniques

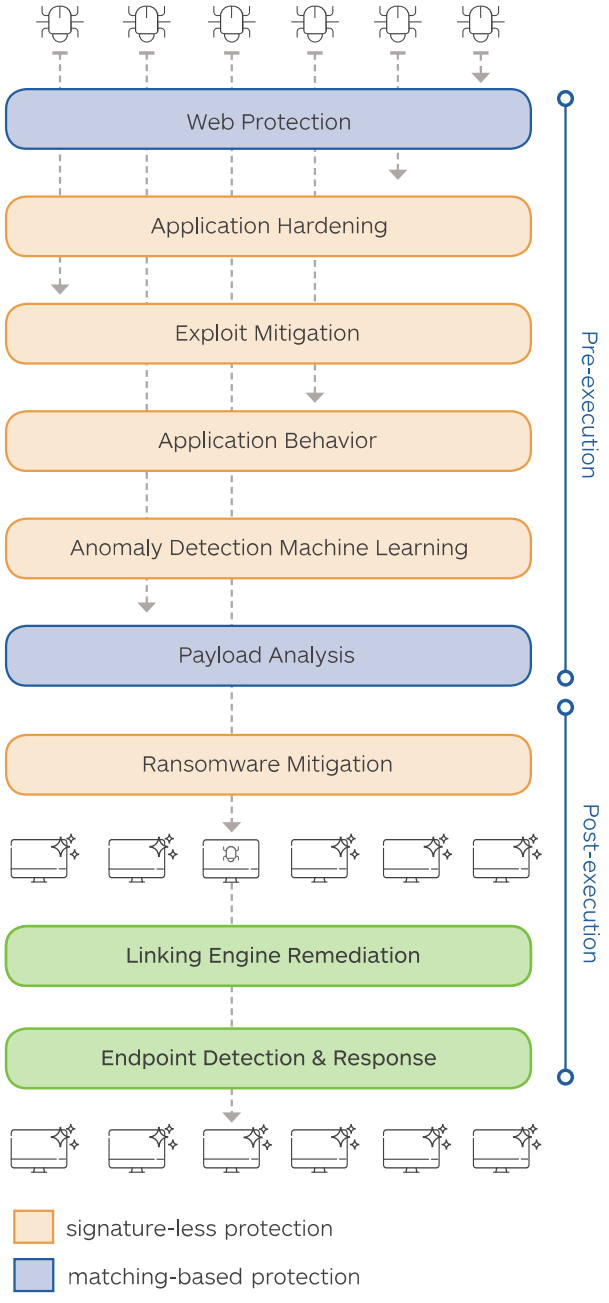
Payload Analysis
Identifies entire families of known and relevant malware with heuristic and behavioral rules

Ransomware Mitigation
Detects and blocks ransomware via behavioral monitoring technology

Linking Engine and Remediation
Provides complete and thorough remediation to return the endpoint to a truly healthy state while minimizing the impact to the end-user

Endpoint Detection and Response (EDR)
Visibility into endpoints for continuous behavioral analysis and forensics. Reduces the dwell-time of zero-day threats. Provides response options beyond alerts

ENDPOINT PROTECTION & RESPONSE



Key Benefits

Multi-layered protection

Malwarebytes Multi-Vector Protection (MVP) uses a seven layered approach, including both static and dynamic detection techniques, to protect against all stages of an attack. This approach provides protection against all types of threats from traditional viruses to tomorrow's advanced threats.

Visibility into endpoints for continuous monitoring

Flight Recorder provides continuous monitoring and visibility into Windows desktops for powerful insights. You can easily track file system activity, network activity, process activity, and registry activity. Flight Recorder events are stored both locally and in the cloud.

Three modes of endpoint isolation

When an endpoint is compromised, Malwarebytes stops the bleeding by isolating the endpoint. Fast remediation prevents lateral movement. Malware is stopped from phoning home, and remote attackers are locked-out. Endpoint Protection and Response is the first product to offer three ways to isolate an endpoint. Network Isolation to restrict which processes can communicate. Process Isolation to restrict which processes can run. Desktop Isolation to alert the end user and halt interaction. Safely keeps the system online for detailed analysis.

Complete and thorough remediation

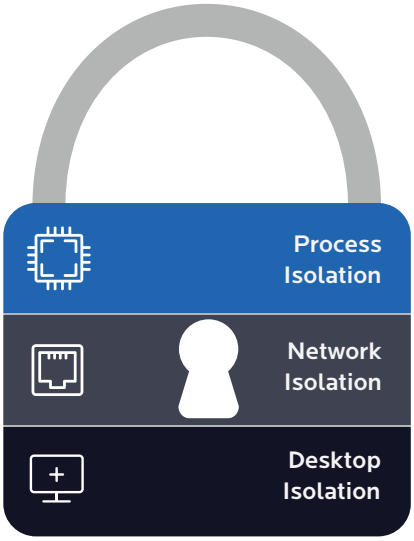
Malwarebytes delivers the industry's most trusted remediation, as evidenced by 500,000 downloads and remediation of 3 million infections per day around the globe. Malwarebytes Endpoint Protection and Response leverages proprietary Linking Engine technology to remove all traces of infections and related artifacts—not just the primary threat payload. This approach saves time normally spent wiping and re-imaging endpoints.

Ransomware Rollback

Ransomware Rollback technology allows you to wind back the clock to negate the impact of ransomware by leveraging just-in-time backups. Malwarebytes logs and associates changes with specific processes. Every change made by a process is recorded. If a process does 'bad' things you can easily roll back those changes to restore files that were encrypted, deleted, or modified. Data storage is minimized using proprietary dynamic exclusion technology that learns what 'good' applications do.

Centralized cloud-based management

This reduces complexity, making it easy to deploy and manage, regardless of the number of endpoints. Additionally eliminates the need to acquire and maintain on-premises hardware.



logo 50X70 | My site is great | 777.77.7777

Here is my text.

malwarebytes.com/business | 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.