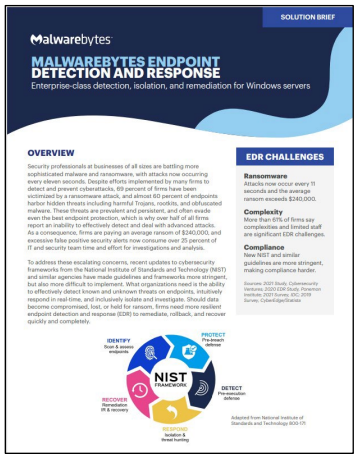


Malwarebytes Endpoint Detection and Response

Enterprise-class detection, isolation, and remediation for Windows servers

Thank you for downloading this Malwarebytes solution brief. Carahsoft is the master government aggregator and distributor for Malwarebytes' Cybersecurity solutions available via MAS, ILTPP, MHEC, and other contract vehicles.

To learn how to take the next step toward acquiring Malwarebytes' solutions, please check out the following resources and information:

For additional resources:
carah.io/MalwarebytesResources

For upcoming events:
carah.io/MalwarebytesEvents

For additional Malwarebytes solutions:
carah.io/MalwarebytesSolutions

For additional CyberSecurity solutions:
carah.io/CyberSecuritySolutions

To set up a meeting:
Malwarebytes@carahsoft.com
844-214-4790

To purchase, check out the contract vehicles available for procurement:
carah.io/MalwarebytesContracts

For more information, contact Carahsoft or our reseller partners:
Malwarebytes@carahsoftcom | 844-214-4790

SOLUTION BRIEF

Malwarebytes

MALWAREBYTES ENDPOINT DETECTION AND RESPONSE

Enterprise-class detection, isolation, and remediation for Windows servers

OVERVIEW

Security professionals at businesses of all sizes are battling more sophisticated malware and ransomware, with attacks now occurring every eleven seconds. Despite efforts implemented by many firms to detect and prevent cyberattacks, 69 percent of firms have been victimized by a ransomware attack, and almost 60 percent of endpoints harbor hidden threats including harmful Trojans, rootkits, and obfuscated malware. These threats are prevalent and persistent, and often evade even the best endpoint protection, which is why over half of all firms report an inability to effectively detect and deal with advanced attacks. As a consequence, firms are paying an average ransom of $240,000, and excessive false positive security alerts now consume over 25 percent of IT and security team time and effort for investigations and analysis.

To address these escalating concerns, recent updates to cybersecurity frameworks from the National Institute of Standards and Technology (NIST) and similar agencies have made guidelines and frameworks more stringent, but also more difficult to implement. What organizations need is the ability to effectively detect known and unknown threats on endpoints, intuitively respond in real-time, and inclusively isolate and investigate. Should data become compromised, lost, or held for ransom, firms need more *resilient* endpoint detection and response (EDR) to remediate, rollback, and recover quickly and completely.

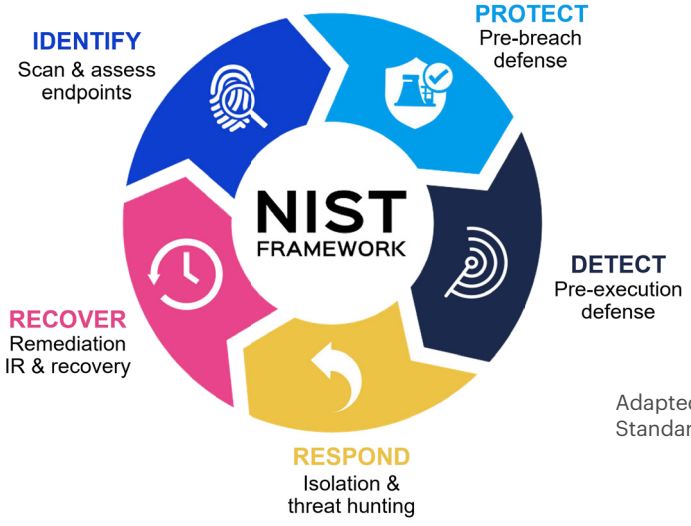
EDR CHALLENGES

Ransomware
Attacks now occur every 11 seconds and the average ransom exceeds $240,000.

Complexity
More than 61% of firms say complexities and limited staff are significant EDR challenges.

Compliance
New NIST and similar guidelines are more stringent, making compliance harder.

Sources: 2021 Study, Cybersecurity Ventures; 2020 EDR Study, Ponemon Institute; 2021 Survey, IDC; 2019 Survey, CyberEdge/Statista



Adapted from National Institute of Standards and Technology 800-171

EFFECTIVE

Malwarebytes Endpoint Detection and Response uses unique Anomaly Detection machine learning to not only detect known threats, but also find unknown threats. Malwarebytes EDR boasts higher accuracy, which is why we have one of the industry's lowest false positive rates. Our granular isolation and resilient remediation capabilities help prevent lateral malware movement that can eventually execute ransomware.

- Granular isolation prevents lateral movement to contain individual servers, subnets, or groups
- MITRE ATT&CK mapping with low false positive alert rates
- Resilient remediation Linking Engine removes executables, artifacts, and changes

INTUITIVE

Malwarebytes EDR is non-disruptive and deploys within minutes via one lightweight endpoint agent. Our Nebula cloud console ensures simple and intuitive management.

- Intuitive Nebula cloud-native management console reduces IT time, cost, and effort
- Non-disruptive, role-based access and a lightweight agent
- Robust SIEM, SOAR, ITSM* integrations automate support tickets, scans, and remediation

INCLUSIVE

Malwarebytes EDR offers ransomware rollback for Windows, and to avoid performance impacts, uses a lightweight agent that only requires three background processes as compared to an order of magnitude more for many other solutions.

- Guided threat hunting and safe cloud sandbox threat analysis
- 72-hour Windows ransomware rollback for Windows servers
- Includes protection for Brute Force attacks via Remote Desktop Protocol (RDP)

INTEGRATED ENDPOINT PROTECTION

Malwarebytes EDR machine learning not only detects known threats, but finds unknown "zero-day" threats, obfuscated malware, rootkits, and suspicious behaviors often missed by others. Suspicious activity detection alerts on threats and provides actionable insights. Unlike more reactive signature-based solutions that may allow malware to execute, our advanced protection finds and blocks threats before servers are infected. The intuitive Malwarebytes Nebula cloud-native management console lets you vanquish malware with a few clicks, not a dozen scripts. Your security team can quickly navigate from the global dashboard down to identified threats and quarantined devices within seconds.

MULTI-MODE ISOLATION

Malwarebytes EDR is the first solution to provide multiple combined modes of endpoint isolation. If an endpoint is attacked, you can easily halt malware from spreading and causing harm and mitigate IT and user disruption during attacks.

- **Network isolation** limits device communications to ensure that attackers are locked out and malware can't "phone home."
- **Process isolation** restricts which operations can run, halting malware while still allowing users to remain productive.
- **Desktop isolation** for Windows workstations alerts users to threats and temporarily blocks access while keeping the device online for analysis.

*SIEM: Security Information and Event Management
SOAR: Security Orchestration, Automation and Response
ITSM: IT Service Management

BRUTE FORCE PROTECTION

Remote work has expanded remote desktop protocol (RDP) usage, which is one of the primary ransomware attack vectors. Malwarebytes brute force protection for RDP is easy to configure, up and running in minutes, prevents RDP intrusion, improves detection, blocks malicious logins, and protects against exploits such as packaged/polymorphic malware.

AUTOMATED REMEDIATION

Our automated approach eliminates manual efforts to remediate attacks, freeing up valuable resource time. Typical malware infections can leave behind more than 100 artifacts, including files, folders, and registry keys that can propagate to other systems on your network. Most solutions only remediate active malware components, such as executables, which exposes systems to reinfection including Potentially Unwanted Programs or Modifications (PUPs or PUMs). Malwarebytes' proprietary Linking Engine detects and removes dynamic and related artifacts, changes, and process alterations. Our engine applies associated sequencing to ensure thorough eradication of malware.

CLOUD SANDBOX

Malwarebytes applies powerful threat intelligence to our cloud sandbox to provide for deep analysis of unknown threats to increase the precision of threat detection and ensure prepackaged analysis of actionable Indicators of Compromise (IOCs). Potentially harmful malware can be detonated within the cloud sandbox for evaluation and analysis.

GUIDED THREAT HUNTING

Threat hunting allows for on-demand and scheduled endpoint scanning for custom IOC threat investigation; user-initiated remediation scans through integrations with existing IT system management tools; and continuous monitoring for suspicious files and process events, network connections, and registry activity. Asset management capabilities collect and display endpoint details including installed software, updates, and startup programs.

Visual graphs help you investigate processes spawned by a threat and determine where they moved laterally. Integrated incident response enables you to isolate and remediate all traces of a threat or globally exclude non-threatening activity—all with a few simple clicks rather than complex scripts. Malwarebytes EDR collects detailed server threat information and provides MITRE ATT&CK mapping for analysis and investigation to enable organizations to implement a Zero Trust Architecture (ZTA) for endpoints.

RANSOMWARE ROLLBACK

For Windows platforms, Malwarebytes EDR includes unique 72-hour ransomware rollback technology that can wind back the clock and rapidly return your firm to a healthy state. Unlike less effective file backup strategies, if an attack impacts user files, Malwarebytes can easily roll back all changes to restore files that were encrypted, deleted, or modified in a ransomware attack. Data storage is minimized by using proprietary dynamic exclusion technology.

CONTINUOUS MONITORING

The Flight Recorder advanced search feature in Malwarebytes EDR provides continuous monitoring and visibility into Windows and Mac workstations for powerful insights. Included are search capabilities for MD5 (message digest) hashes, filenames, network domains, IP addresses, and file/process paths or names. You can also automatically display suspicious activity, view full command line details of executed processes, and store thirty days of rolling data in the cloud.

INDUSTRY-LEADING TECHNOLOGY

Malwarebytes was issued some of the earliest patents for ransomware detection, including one for file comparison and three for behavior-based detection. We leverage years of security expertise in remediation to provide you with threat intelligence from millions of Malwarebytes-protected endpoints, both business and consumer. Malwarebytes Endpoint Detection and Response for Windows and Mac, managed within our Nebula cloud-native management console, easily scales to meet future requirements. Malwarebytes ensures a high Return on Investment (ROI) and low Total Cost of Ownership (TCO), and we're also known for our superior service and support.

YOUR SAFEST CHOICE FOR EDR

Malwarebytes EDR effectively and efficiently detects suspicious activity, isolates attacks, investigates threats, and remediates damage. Many solutions can be difficult to deploy and manage and are often not compatible with other security software. Most other EDR solutions are less resilient and only remediate executables. They don't provide multiple layers of isolation to stop threats before they can cause harm, and they are designed to alert on almost every threat, which results in high false positive alert rates. By offering more effective detection and industry-lower false positive alerts, Malwarebytes won the CISO Choice Award for EDR.

Malwarebytes EDR for Windows and Mac uses a single lightweight agent that does not impact performance. Malwarebytes EDR is also more resilient and easy to manage through our Nebula cloud-native console. We uniquely detect suspicious activity and isolate processes and networks to mitigate ransomware. Desktop isolation is available for Windows workstations, and our proprietary Linking Engine removes artifacts, changes, and process alterations. Finally, unique 72-hour Windows ransomware rollback restores endpoints to pre-attack states.

Don't wait until it's too late. Malwarebytes EDR is your safest choice for a more *resilient* Windows and Mac EDR. We've won high customer loyalty and praise for enterprise-class EDR that's effective, intuitive, and inclusive.

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

Is your current security strategy optimized for the best ROI? Click here to instantly see the value that this product can create for your organization.

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

Malwarebytes believes that when people and organizations are free from threats, they are free to thrive. Much more than malware remediation, the company provides cyberprotection, privacy, and prevention to tens of thousands of consumers and organizations every day. For more information, visit https://www.malwarebytes.com.