Malwarebytes™ for Business

DATA SHEET

MALWAREBYTES ENDPOINT DETECTION AND RESPONSE (EDR)

Simple, Effective Detection, Remediation and Recovery

Organizations today face a grim reality: the prospects of a breach is no longer a question of "if" but "when," and nearly 70% of those breaches originate at endpoints.[1] Compounding this reality is the global and sustained shortage of cybersecurity professionals, which leaves security teams short on staff, pressed for time, and beset with a disparity of skill levels.

Malwarebytes EDR was designed with this grim reality in mind. It delivers effective protection—from prevention through identification to response actions—that users with emerging cybersecurity acumen can learn and use with ease. But this simplicity belies its underlying sophistication: Malwarebytes EDR includes high-powered tools and customizable options that users can embrace as their skill level grows and the organization's security needs change. By deploying our readily accessible cloud-based security platform, organizations of all sizes gain powerful detection and remediation while freeing their security teams to spend time on other more pressing projects.

AT A GLANCE

WHAT IS IN IT FOR YOU?

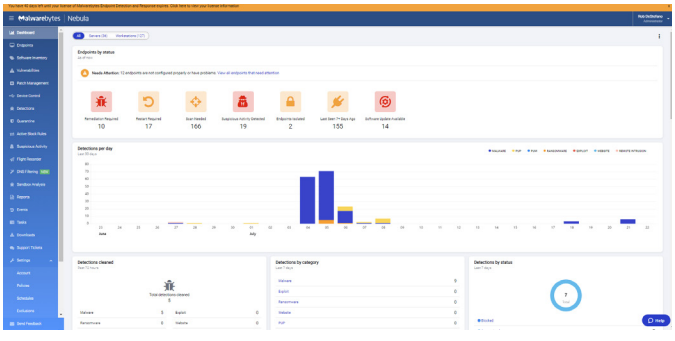
- EDR that bridges the cybersecurity skills gap
- Alerts with details about what, where, and how threats occurred
- Powerful prevention and remediation
- 72-hour Ransomware Rollback
- Alignment with common cybersecurity frameworks, including NIST, ENISA and MITRE

What does Malwarebytes EDR offer that others don't?

EASE OF USE: Malwarebytes EDR offers organizations the assurance of powerful protection and trouble-free management. Easy to learn and use, our cloud-native console opens to an intuitive dashboard displaying visual cues that immediately convey which endpoints need attention and why.

HIGH-QUALITY ALERTS WITHOUT THE "NOISE": We deliver alerts with insights. Detected threats trigger alerts that contain information with a high-level of contextual detail to help users to quickly make informed decisions about how to respond appropriately.

EXPANDED REMEDIATION: With a few clicks from within our Nebula cloud-based management console, you can remotely remediate an infected endpoint. Our proprietary Linking Engine is designed to identify and remove residual malware-related artifacts and infection-induced changes to help ensure thorough remediation.



ACCELERATED DEPLOYMENT: We designed Malwarebytes EDR with ease in mind to simplify use and accelerate deployment. Our lightweight agent for Windows and Mac operating systems (OSes) deploys within hours.

PLATFORM EXPANSION: As your security needs change, Malwarebytes EDR expands to meet them. Our click-to-add platform modules enable your team to reinforce prevention in key threat vectors such as software vulnerabilities, patch management, and DNS filtering.

[1] (3 Nov 2020). "Why a culture change program is key to effective cybersecurity." EY.

How does it work?

Malwarebytes EDR helps prevent cyber threats—including malware, brute force attacks, and zero-day exploits—from reaching your environment. To do so, it continuously searches for known malware using rules-based threat detection while proactively hunting for unknown malware using AI-based (also known as "behavioral-based") detection designed to detect and analyze anomalous files and programs to mitigate risk. Whether known or unknown, detected threats trigger alerts that include the details users need to respond quickly and appropriately.

Malwarebytes EDR also detects, alerts users of, and automatically removes Potentially Unwanted Programs (PUPs) and Potentially Unwanted Modifications (PUMs) that, while not malicious, commonly diminish end users' experience. Our MITRE-evaluated platform also automates analysis of zero-day threats and empowers users with the ability to isolate suspicious code per machine, user and/or process; containing questionable code allows for investigation without risk of further exposure and spread. Malwarebytes EDR includes a cloud sandbox that users can use to investigate dubious executable binaries; users can also use the sandbox to remotely and securely detonate malware.

When infections creep into your digital environment, Malwarebytes' award-winning detection and remediation can help you effectively remove malware. Our advanced remediation technology is designed to ensure that all residual traces of malware are eradicated and any malware-induced configuration changes are undone. For complete recovery from ransomware, Malwarebytes EDR comes with our 72-hour Ransomware Rollback (for Windows only); this capability helps you return to a pre-ransomware state without the time-consuming task of reimaging machines or re-creating encrypted files.

You don't have to take our word for it

The MITRE ATT&CK 2022 evaluations support the claim that Malwarebytes EDR provides superior visibility and analytic coverage without config changes or delayed detections while also providing excellent threat protection.

BUSINESS OUTCOMES

- **Discover 40% more threats** than traditional antivirus products
- **Reduce infections by as much as 90%** and completely prevent PUPs and PUMs
- Complete scan and remediation processes on **1,000+ endpoints in 15 minutes**
- **Minimize time** from threat detection to complete remediation and recovery
- **Avoid up to 30 days downtime** remediating cryptocurrency malware
- **Reduce helpdesk tickets** related to malware by +25%
- **Remotely isolate and remediate infection**—ideal for remote end users
- **Forensic analysis capabilities** to detect and guide thorough malware eradication

AV-TEST TOP PRODUCT CERTIFIED WINDOWS · AV-TEST ADVANCED CERTIFIED WINDOWS · AV-LAB EXCELLENT MARCH 2022 · MRG Effitas CERTIFIED 360° ASSESSMENT Q1 2022 · MRG Effitas CERTIFIED EXPLOIT Q1 2022 · MRG Effitas CERTIFIED ONLINE BANKING Q1 2022 · MRG Effitas CERTIFIED RANSOMWARE Q1 2022 · MITRE ENGENUITY ATT&CK® EVALUATIONS Enterprise WIZARD SPIDER & SANDWORM PARTICIPANT 2022