Malwarebytes for Business

SOLUTION BRIEF

MALWAREBYTES ENDPOINT DETECTION & RESPONSE

Solution for Advanced Prevention

Breaches are unavoidable—and nearly 70% originate at endpoints.[1] Given this grim not-if-but-when reality, organizations are turning toward Endpoint Detection and Response (EDR). The best EDR offers both advanced prevention *and* mitigation—to detect, investigate and remediate threats that evade prevention. Unfortunately, when resource-constrained organizations search for EDR, they often find products that are prohibitively costly and complex. Short staffed, pressed for time, and beset with skill-level disparities, small security teams need *accessible* EDR that works, right out of the box.

Malwarebytes EDR is designed to provide the prevention and mitigation capabilities you need—with the ease-of-use and expandability you demand. In this brief, you'll learn more about the advanced *prevention* capabilities that our single lightweight Malwarebytes EDR endpoint agent provides for Windows and macOS desktops and laptops and for optionally-licensed Windows and Linux servers. Malwarebytes EDR identifies and prevents both known and unknown threats. We back our advanced proactive threat prevention with our renowned remediation, designed to not only eradicate malware but remove what it leaves behind and thereby prevent re-infection.

CLOUD MANAGEMENT CONSOLE

Our cloud-based Nebula console is **designed to deliver trouble-free management**. Easy to learn and use, our console opens to an intuitive dashboard that immediately conveys how many endpoints need attention and why. Users can see at a glance what actions to take (e.g., check endpoint status, run scan, isolate malicious activity, remediate threat). All actions are executable with simple clicks from within the console.

ADVANCED PREVENTION

Signature-based detection

Malwarebytes EDR provides signature-based protection to **stop *known* malware using very few resources with minimal end-user impact and very few false positives**. This essential security foundation guards against cyberthreats by searching endpoints for unique identifiers that have been associated with specific threats.

EDR FOR ALL

Challenge

Resource-constrained organizations need EDR as much (or more) than large organizations. Yet, too many EDR solutions are too costly and complex to meet their needs.

Solution

Malwarebytes EDR was designed to provide advanced prevention and mitigation without complexity; it is effective and easy to deploy, learn, and manage out of the box. Malwarebytes EDR grows alongside your organization as its needs change and your team's acumen matures.

Benefits

- Easy-to-understand cloud management console guides point-and-click action
- Signature- and behavior-based detection designed to prevent known and unknown threats
- Proprietary Linking Engine provides deep remediation to prevent re-infection
- Cloud-based platform and single lightweight endpoint agent ease deployment and expansion
- MITRE ATT&CK 2022 evaluation results[2] validate our Visibility and Protection capabilities

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

[2] https://attackevals.mitre-engenuity.org/enterprise/participants/malwarebytes?view=overview&adversary=wizard-spider-sandworm

Behavior-based detection

Built on machine learning (ML) and behavioral analysis techniques, our behavior-based detection, is designed to thwart unknown threats, which account for 80% of successful breaches.[3]

Our ML technology collects and analyzes data from groups of endpoints, gleaning insights it uses to update algorithms that essentially "train" machines to recognize and classify new threats; by design, ML detection improves with time and more data, steadily increasing the speed and efficiency with which it detects unknown threats. Our behavior-based detection collects and analyses user and application behavior, searching for anomalous patterns that might indicate malicious intent.

Brute-force attack protection

Malwarebytes EDR is also designed to prevent brute-force attacks, which accounted for 51% of all breaches in 2022 Q1.[4] It does so by tracking repeated failed login attempts to selectively block potentially malicious Host IPs, thereby thwarting attempts to drop infectious payloads.

REMEDIATION

Effective remediation begins with effective detection: the earlier an attack is detected, the better. Malwarebytes EDR is designed to detect attacks as early as possible; once detected, **our EDR enables *thorough* remediation with the click of a button**.

Most EDR products eliminate only *active* malware components, which is a good place to start but does not protect against re-infection. To prevent re-infection, **our proprietary Linking Engine begins by eradicating active malware components; then it seeks out and removes detected artifacts and config changes, which malware commonly leaves in its wake**.

LIGHTWEIGHT AND EXPANDABLE

Malwarebytes EDR is built on our Nebula cloud-based platform and powered by our single lightweight endpoint agent. We designed these components to facilitate and accelerate deployment. **Our customers deploy EDR within hours**[5] **—and complete their initial scan and remediation within minutes of deployment**.[6]

In addition to being easy to deploy, learn and manage, Malwarebytes EDR's Nebula platform allows for easy expansion. **Our click-to-add threat-vector modules enable your team to scan, discover, and prioritize security vulnerabilities in software and operating systems, as well as web sites and content**.

MITRE ATT&CK EVALUATION

Results from the MITRE ATT&CK 2022 evaluations[7] validate Malwarebytes EDR Visibility and Protection capabilities on Windows. For these evaluations, MITRE professionals assaulted EDR products with emulated attacks wrought by active and particularly noxious cybercriminals. Malwarebytes EDR scored a 92% in Visibility, indicating that we captured relevant data for 83 out of 90 attack sub-steps. Arguably more important, **Malwarebytes EDR earned 100% in Protection**: we blocked eight out of eight attacks.

[3] Ponemon Institute LLC. (Jan 2020). "The Third Annual Study on the State of Endpoint Security Risk." (An independently conducted research report.)
[4] Kapko, Matt. (12 July 2022). "Threat actors favor brute force attacks to hit cloud services." Cybersecurity Dive.
[5] University of Texas System
[6] Holyoke Public Schools
[7] https://attackevals.mitre-engenuity.org/enterprise/participants/malwarebytes?view=overview&adversary=wizard-spider-sandworm

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.