Malwarebytes™ for Business

SOLUTION BRIEF

MALWAREBYTES ENDPOINT DETECTION & RESPONSE

Solution for Threat Mitigation

OVERVIEW

Most organizations know that even advanced prevention is not 100% effective: today's complex threats sneak past preventative measures and often linger undetected for days—or even weeks. In fact, recent research shows that in 2021, smaller companies were unable to detect attackers in their systems for a mean time of 51 days (nearly double the 28 days that larger companies experienced).[1] Given this grim reality, organizations are turning toward Endpoint Detection and Response (EDR), which empowers teams to detect, isolate, investigate, and respond to threats that evade prevention. Unfortunately, when resource-constrained organizations search for EDR, they often find products that are prohibitively costly and complex; what they need is accessible EDR that works, right out of the box.

Malwarebytes EDR is designed to provide the prevention, detection, and response capabilities you need—with the ease-of-use and expandability you demand. In this brief, you'll learn more about the threat mitigation 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 continually monitors all of your endpoints, searching for threats lurking undetected on your network. By stopping these threats in the earliest stages of an attack, Malwarebytes EDR helps preclude their ability to do harm.

ENABLES POINT-AND-CLICK ACTION

Our cloud-based EDR platform is **designed to deliver trouble-free management** that aligns with MITRE ATT&CK© workflows. Easy to learn and use, our console opens to an intuitive dashboard that immediately conveys how many endpoints need attention and why. A quick glance at the red-, yellow-, and green icons guides point-and-click action (e.g., run scan, isolate malicious activity, remediate threat).

EDR FOR ALL

Challenge

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

Solution

Malwarebytes EDR offers detection, isolation, investigation, and remediation technologies that are designed with ease-of-use foremost in mind, empowering *all* security teams—from the still-maturing to the highly-experienced.

Benefits

- Easy-to-understand cloud management console guides point-and-click action
- Suspicious activity monitoring thwarts zero-day attacks
- Integrated cloud sandbox expedites suspicious activity analysis and detonation
- Granular threat isolation facilitates risk-free triage
- Detail-dense alert notification enables prompt response
- Ransomware Rollback facilitates return to pre-attack state

[1] Shier, John. (7 June 2022). "The Active Adversary Playbook 2022." *Sophos News*. In this report, "smaller" refers to organizations with 1 to 250 employees, and "larger" to organizations with 500 to 3000.

THWARTS ZERO-DAY ATTACKS

Zero-day threats account for 80% of successful breaches.[2] **Malwarebytes EDR helps uncover unknown (zero-day) threats** by monitoring process, registry, file system, and network activity on endpoints then applying machine-learning models and cloud-based analysis. Our console's Suspicious Activity page provides context for each resulting detection to facilitate assessment and action.

EXPEDITES THREAT ANALYSIS

Our integrated cloud sandbox **safely analyzes potential threats and, for validated malicious activity, helps teams take appropriate action**. When teams upload a suspicious activity to the sandbox, the console returns a comprehensive report within minutes, plainly confirming whether or not the activity is malicious.

FACILITATES RISK-FREE TRIAGE

Malwarebytes EDR **empowers your team to isolate and triage threats without risking further harm**. Our granular isolation modes—per network segment, process, or endpoint—lock out remote attackers, stop malware from spawning new processes, and prevent users from initiating applications that might complicate response.

DELIVERS CONTEXT-DENSE ALERTS

Malwarebytes EDR is **designed to deliver alerts with the details your team needs for prompt and appropriate threat response**. The MITRE ATT&CK 2022[3] evaluation results validate our claims on this front, indicating that we provided the highest-quality alerts for 82 out of our 83 detections. Also, during these evaluations, **we blocked eight out of eight attacks before they could do harm, earning a 100% in Protection**.

FACILITATES RANSOMWARE RECOVERY

Since 2017, breaches resulting from ransomware attacks have increased by a total of 25%.[4] Worse still, ransomware attacks were costlier than other breach types, costing organizations an average of US $4.62M in 2021.[5] Malwarebytes EDR **helps protect you from the cost of a ransomware breach by continually monitoring endpoints for evidence of ransomware behaviors**. When such behavior is detected, Malwarebytes EDR activates our file backup process, encrypting and relocating data for later restoration. With one click, teams can reverse ransomware damage by rolling back affected files to their pre-attack state up to 72 hours before their compromise.

AV TEST av-test.org 12/2021 CERTIFIED WINDOWS TOP PRODUCT

AV TEST av-test.org 10/2021 CERTIFIED WINDOWS ADVANCED

ADVANCED IN-THE-WILD MALWARE TEST AVLAB CYBERSECURITY FOUNDATION 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

[2] Ponemon Institute LLC. (Jan 2020). "The Third Annual Study on the State of Endpoint Security Risk." (An independently conducted research report.)
[3] https://attackevals.mitre-engenuity.org/enterprise/participants/malwarebytes?view=overview&adversary=wizard-spider-sandworm
[4] G. Bassett, C. D. Hylender, P. Langlois, A. Pinto and S. Widdup. (2021). "2021 Data Breach Investigations Report." Verizon.
[5] IBM Security and Ponemon Institute. (2021). "Cost of a Data Breach 2021."

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.