SOLUTION BRIEF

Malwarebytes | CONNECTWISE

MALWAREBYTES ENDPOINT DETECTION AND RESPONSE

Enterprise-class detection, isolation, and remediation for Windows, Mac, and Linux

OVERVIEW

In a recent research report from Ponemon Institute, 68 percent of respondents reported one or more damaging endpoint attacks that compromised valuable information or infrastructure. Similar research shows that almost 60 percent of endpoints harbor hidden threats, including harmful Trojans, rootkits, and backdoors. These threats are sophisticated, 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.

Equally concerning are recent changes to compliance mandates requiring more stringent protection of Personally Identifiable Information (PII). The New York Department of Financial Services (NYDFS) guidelines and California Consumer Privacy Act (AB 375) are among the more stringent, but most U.S. States now have stricter guidelines. If security teams can't prove that "false positive" alerts are not positive threats or attacks, their firms could be fined, forced to make public announcements, and sued by Attorneys General or private parties. Internationally, new General Data Protection Regulation (GDPR) and Payment Services Directive 2.0 (PSD2) regulations are also creating challenges.

What organizations need is the ability to immediately detect known and unknown threats, actively respond in real-time, and thoroughly isolate and investigate. Should data be lost or held for ransom, firms need to remediate, rollback, and recover quickly and completely.

EDR CHALLENGES

Attacks have doubled
Over 68% of firms suffered recent attacks and 80% were new "zero-day" threats.

High false positives
Almost 60% of firms need zero-day detection, but high false positives are a primary concern.

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

Source: 2020 EDR Study, Ponemon Institute

Deploy quickly and manage with ease

Deploy within minutes and manage with an intuitive cloud-native console

Detect, isolate, and remediate threats

Reduce risks and false positives; stop threats with multiple isolation modes

Threat hunt and rollback ransomware

Guided threat hunting and Windows ransomware rollback

EASY

Malwarebytes Endpoint Detection and Response (EDR) for Windows, Mac, and Linux can easily replace or complement other endpoint security solutions, including Microsoft Defender. We've won high customer loyalty and praise because we're nondisruptive, straightforward, and economical to deploy via one endpoint agent, and offer robust integrations and compatibilities.

- Non-disruptive, deploy within minutes
- One endpoint agent, simple integration
- Intuitive cloud-native management console

EFFECTIVE

Malwarebytes EDR uses unique anomaly detection machine learning to proactively detect web-based attacks, zero-day malware, ransomware, potentially unwanted programs or modifications (PUPs and PUMs), and infections from USB peripherals. Malwarebytes EDR boasts higher accuracy, which is why we have one of the industry's lowest false positive rates. Our granular isolation capabilities prevent lateral movement of an attack by allowing you to contain individual machines, subnets, or groups, and continue active response activities.

- Detects "zero-day" threats with low false positives
- Granular isolation for processes, networks, and Windows desktops
- Removes executables, artifacts, and changes

EFFICIENT

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 some other solutions.

- Single lightweight agent, no performance impact
- 72-hour ransomware rollback for Windows
- Low total cost of ownership (TCO)

INTEGRATED PROACTIVE ENDPOINT PROTECTION

Malwarebytes EDR includes integrated endpoint protection and automated adaptive detection techniques that learn along each stage of the threat detection funnel. Unlike more reactive signature-based solutions that allow malware to execute before working, our endpoint protection finds and blocks threats before devices are infected. Malwarebytes EDR proactively and accurately recognizes and prevents both hostile code and suspicious behavior.

OPERATING SYSTEM-SPECIFIC ISOLATION MODES

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.

AUTOMATED AND THOROUGH REMEDIATION

Our automated approach enables IT and security analysts to eliminate 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 in an organization's network. Most solutions only remediate active malware components, such as executables, which exposes systems to reinfection.

Malwarebytes' proprietary Linking Engine detects and removes dynamic and related artifacts, changes, and process alterations. Our engine applies associated sequencing to ensure thorough disinfection of malware persistence mechanisms.

CLOUD SANDBOX

To increase the precision of our threat detection, Malwarebytes utilizes a cloud "sandbox," a virtual cellblock for isolating and detonating potentially harmful malware for evaluation and analysis.

The sandbox allows you to investigate suspicious code—even remotely—without disrupting end user productivity. Post analysis, Malwarebytes delivers a comprehensive report, so you can respond appropriately to incidents of compromise (IoCs).

GUIDED THREAT HUNTING

The friendly visualization interface presents a summary Kanban board that automatically classifies the combination of actions into MITRE ATT&CK Framework, quickly giving you the "why" our machine learning algorithm has identified the Suspicious Activity worthy of your attention. In addition, we offer a detailed view for the forensic analyst that requires the blow-by-blow steps utilizing a linked chain of actions and commands issued to provide you with the necessary IOCs. Moreover, the visualization interface can launch into our Flight Recorder Search (FRS) child window without losing your place. FRS is a guided user interface that systematically walks you through searching for breadcrumbs/clues (indicators) across every managed endpoint across your enterprise for early signs of a threat actor that is moving laterally.

WINDOWS 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. If an attack impacts user files, Malwarebytes can easily roll back these changes to restore files that were encrypted, deleted, or modified in a ransomware attack. And don't worry: our proprietary data storage technology minimizes the space needed to backup your data.

CONTINUOUS MONITORING

The Flight Recorder search feature in Malwarebytes EDR provides continuous monitoring and visibility into Windows and Mac for powerful insights. Included are search capabilities for filenames, network domains, IP addresses, MD5 hashes, 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.

VULNERABILITY AND PATCH MANAGEMENT

Our Vulnerability Assessment module seamlessly plugs into and builds upon the visibility and prevention tools afforded you by our EDR solution, helping you shore up your defenses from within the same cloud-based security platform. Using an up-to-date inventory of your software, drivers, and operating systems (OSes), our Vulnerability Assessment module identifies known software vulnerabilities – areas that threat actors could use to gain network access. It then prioritizes recommended actions based on the degree of risk posed by each identified vulnerability. Malwarebytes' Patch Management module assumes control of the software patching process. Combined with our Vulnerability Assessment module, the Patch Management module accelerates the identification, deployment, installation, and verification of revisions to Windows endpoint and server OSes as well as a wide range of third-party applications.

DNS FILTERING

Malwarebytes' Domain Name System (DNS) Filtering module helps prevent onsite and remote users alike from accessing inappropriate web content or nefarious websites, and helps you enforce your organizations Code of Conduct policies. Furthermore, our DNS Filtering module encrypts all domain name requests to help mitigate the means by which threat actors exploit websites and web-based applications. To further reduce risk, our DNS Filtering is backed by Malwarebytes' real-time protection against malicious downloads.

MANAGED DETECTION AND RESPONSE

Malwarebytes also offers Managed Detection and Response (MDR) for companies of all sizes with constrained cybersecurity resources. With Malwarebytes MDR, your environment is protected by Malwarebytes EDR and our team of cybersecurity professionals with decades of experience monitors your environment 24/7 to investigate the alerts that Malwarebytes EDR generates in real time. In addition,, our Malwarebytes MDR team remediates threats or provides remediation guidance to your team, freeing up time for your IT and security teams to pursue other more pressing projects.

HIGH ROI, LOW TCO

With our cloud-native solution, Malwarebytes EDR easily scales to meet future requirements. Our cyber intelligence expertise in remediation provides you with a solution that's powered by threat intelligence from millions of Malwarebytes-protected endpoints, both business and consumer. The Malwarebytes API makes it simple to integrate with SIEM, SOAR, ITSM, etc. to further drive automation and compatibility. Malwarebytes EDR 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 enterprise-class Endpoint Detection and Response for Windows, Mac, and Linux platforms effectively and efficiently detects suspicious activity, isolates attacks, investigates threats, and remediates damage.

Other solutions can be difficult to deploy and manage and are usually not compatible with other security software like Microsoft Defender. Most other EDR solutions only remove executables and don't provide multiple layers of isolation to stop threats before they can cause harm. They are also designed to alert on almost every threat, which is why they have high false positive alerts.

Malwarebytes EDR seamlessly integrates with and is compatible with most other endpoint security solutions, including Microsoft Defender. We're easy to deploy and manage through our Nebula cloud-based console and we effectively detect suspicious activity and isolate processes and networks to mitigate damage. Desktop isolation is also available for Windows workstations. Malwarebytes' proprietary Linking Engine removes artifacts, changes, and process alterations while providing unique 72-hour ransomware rollback for Windows workstations. Malwarebytes EDR for Windows, Mac, and Linux uses a single lightweight agent that does not impact performance.

Don't wait until it's too late. Malwarebytes is your safest choice for Windows, Mac, and Linux EDR. We've won high customer loyalty and praise for enterprise-class EDR that's easy, effective, and efficient.

CONNECTWISE