SOLUTION BRIEF

Malwarebytes

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 compliment other endpoint security solutions, including Microsoft Defender. We've won high customer loyalty and praise because we're non-disruptive, 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, PUPs, 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

Malwarebytes applies powerful threat intelligence to our sandbox to provide for deep analysis of unknown threats to increase the precision of threat detection and ensure prepackaged analysis of actionable IOCs. Potentially harmful malware can be detonated within the sandbox for evaluation and analysis, including remote investigation of suspicious code that won't disrupt end user productivity.

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 endpoint threat information for analysis and investigation to enable organizations to search for indicators of compromise (IOCs) and go from infection to recovery within seconds.

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. Data storage is minimized by using proprietary dynamic exclusion technology.

CONTINUOUS MONITORING

The Flight Recorder search feature in Malwarebytes EDR provides continuous monitoring and visibility into Windows, Mac, and Linux workstations for powerful insights. Included are search capabilities for MD5 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.

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 uniquely 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.

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

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.