SOLUTION BRIEF

Malwarebytes

MALWAREBYTES ENDPOINT PROTECTION

Enterprise-class detection, prevention, and remediation for Windows and Mac endpoints

OVERVIEW

IT professionals at small to medium businesses (SMBs) are struggling to meet escalating demands and avoid malware and ransomware attacks, which now occur every eleven seconds. Traditional anti-virus (AV) solutions and endpoint protection platforms (EPP) have proven ineffective at detecting and preventing cyberattacks, which is why almost 60 percent of endpoints harbor hidden threats, including harmful Trojans, rootkits, and obfuscated malware that can execute ransomware.

Given these challenges, 69 percent of firms have been victimized by a ransomware attack, and 77 percent report an inability to effectively detect and deal with advanced threats. As a result, even small firms are paying an average ransom of $240,000, and a majority say solution complexities and limited staff are significant challenges. To address these escalating threats, numerous compliance and security mandates have become more stringent, but also more difficult to meet. What SMBs need is the ability to effectively detect known and unknown threats on endpoints, intuitively manage endpoint security with ease, and inclusively isolate and investigate threats.

EDR CHALLENGES

Ransomware
Attacks now occur every 11 seconds and the average ransom exceeds $240,000.

Complexity
More than 61% of firms say complexities and limited staff are significant challenges.

Compliance
New compliance mandates are more stringent, making compliance harder.

Sources: 2021 Study, Cybersecurity Ventures; 2020 EDR Study, Ponemon Institute; 2021 Survey, IDC; 2019 Survey, CyberEdge/Statista

Deploy quickly and manage with ease

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

Detect and prevent zero-day cyberattacks

Reduce risks and false positives; prevent threats with seven layers of defense

Remediate attacks and prevent reinfection

Clean up executables, changes, and alterations to eliminate reinfection

EFFECTIVE

Malwarebytes uses powerful Anomaly Detection machine learning to detect known and unknown "zero-day" threats. Our web protection technology proactively prevents users from accessing malicious sites, malvertising, scammer networks, and suspect URLs, as well as downloading potentially unwanted programs and modifications. We harden your devices by blocking exploits, stopping remote code execution, and breaking communication with hostile malware servers to dramatically reduce attack surfaces.

- Detects "zero-day" threats with low false positives
- Web protection, hardened devices and apps
- Blocks exploits, stops remote code execution

INTUITIVE

Malwarebytes Endpoint Protection (EP) can easily replace legacy anti-virus (AV) or compliment other endpoint security solutions. Unlike others that use signatures or brute-force scanning, we employ a single, lightweight agent that quickly pinpoints and blocks malicious code from running without impacting device performance. We also offer robust integrations with SIEM, SOAR, and ITSM* solutions.

- Non-disruptive, deploys within minutes vs. days
- Lightweight deployment, simple integration
- Intuitive Nebula cloud-native management console

INCLUSIVE

Malwarebytes offers industry-leading fast and thorough remediation. Our proprietary Linking Engine traces every installation, modification, and process, including in-memory executables that others miss, to ensure thorough remediation, prevent reinfection, and reduce costs and efforts.

- Linking Engine ensures complete remediation
- Removes executables, changes, and artifacts
- Lowers total cost of ownership (TCO)

*SIEM: Security Information and Event Management
SOAR: Security Orchestration, Automation and Response
ITSM: IT Service Management

NEBULA CLOUD MANAGEMENT

A full suite of endpoint security functionality andautomation is easily managed within the Malwarebytes Nebula cloud platform, an intuitive "single pane of glass" that lets you vanquish malware with a few clicks, not a dozen scripts. Your security team can quickly nnavigate from the global dashboard down to identified threats and quarantined devices within seconds. Scanning and remediation is automated across a single department or thousands of devices.

SEVEN LAYERS OF DEFENSE

Malwarebytes applies behavioral monitoring and machine learning to profile threats across web, memory, application, and files. Multiple layers of defense ensure higher detection rates with lower false positives. Unlike more reactive signature-based solutions that may allow malware to execute, we find and block threats, including obfuscated malware.

- **Predictive machine learning** recognizes goodware—properly signed code from known vendors—to predict malware verdicts faster and better.
- **Global threat intelligence** from millions of corporate and consumer endpoints ensures detection and prevention of unknown strains.
- **Behavioral-based blocking** provides near real-time identification of hostile behavior and automatically blocks threats to deliver proactive protection.

SCALABLE AND RELIABLE

Malwarebytes applies the power of the cloud to scale from the smallest to the largest organizations, and offers proven reliability and consistently high return on investment (ROI).

ANOMALY DETECTION

Most endpoint security technologies use machine learning classification detection models. These are trained to recognize malware by using known malware samples. While this approach may help ensure higher test lab results, it unfortunately can lower detection accuracy for unknown "zero-day" malware. Malwarebytes employs a groundbreaking new approach that uses anomaly detection. Instead of training on known malware, our model uses "goodware" to determine classifications. This makes us far more robust, accurate, and long-lived. Our model has been shown to be more effective at identifying "sneaky" attacks, including obfuscated and fileless malware. This is why Malwarebytes often receives top ratings and awards from industry experts.

THREAT ANALYSIS

Malwarebytes Endpoint Protection provides extensive threat analysis background along with assessment of potential impacts. Your security team can now save time and effectively communicate potential impacts to executive leadership.

BRUTE FORCE RDP PROTECTION

Remote work has expanded remote desktop protocol (RDP) usage, which is the primary ransomware attack vector. Malwarebytes brute force protection for RDP is easy to configure, up and running in minutes, prevents RDP intrusion, improves detection, blocks malicious logins, and protects against exploits such as packaged/polymorphic malware.

AUTOMATED REMEDIATION

Our automated and thorough approach eliminates manual efforts to remediate attacks, freeing up valuable resources and t me. Typical malware infections can leave behind more than 100 artifacts, including files, folders, and registry keys that can propagate to other systems on your network. Most solutions only remediate active malware components, such as executables, which exposes systems to reinfection such as Potentially Unwanted Programs or Modifications (PUPs or PUMs). 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. Automation of IT support ticket creation and resolution is also provided by seamless integration with SIEM, SOAR, and ITSM.

ROOTKIT REMEDIATION

Malwarebytes uses a combination of kernel-level Direct Disk Access (DDA) and delete-on-reboot (DOR) technology to remove any malware we detect. Malwarebytes remediation contains a dedicated module to detect and remediate rootkits (system-level malware that corrupts the "eyes and ears" functionality of an operating system). Although rootkits are less common than other types of malware, they can cause severe damage and are traditionally far more difficult for other security products to detect and remediate. By comparing high-level and low-level views of the filesystem and registry, Malwarebytes Anti-Rootkit is signatureless and able to detect most rootkits generically.

INDUSTRY-LEADING TECHNOLOGY

Malwarebytes was issued some of the earliest patents for ransomware detection, including one for file comparison and three for behavior-based detection. We leverage years of security expertise in remediation to provide you with threat intelligence from millions of Malwarebytes-protected endpoints, both business and consumer. Malwarebytes Endpoint Protection, managed within our cloud-native Nebula console, easily scales to meet future requirements. Malwarebytes 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

Malwarebytes Endpoint Protection effectively and efficiently detects suspicious activity, prevents attacks, and remediates damage. Other solutions can be difficult to deploy and manage, and only remove executables. They use less effective classification machine learning models, which is why most have high false positive alerts that can burden analysts and security teams and prevent accurate detection. By offering more effective detection and industry-lower false positive alerts, Malwarebytes has won numerous industry awards and accolades.

Malwarebytes Endpoint Protection is easy to deploy with a single lightweight agent that uses an order of magnitude fewer resources than many other products. Our intuitive Nebula cloud-native console simplifies management and reduces IT time and effort. Unlike others, Malwarebytes Endpoint Protection offers a proprietary Linking Engine that thoroughly removes executables, artifacts, changes, and process alterations. Brute force protection for remote desktop protocol (RDP) is included to protect remote workers.

Don't wait until it's too late. Malwarebytes Endpoint Protection is your safest and smartest choice. We've won high customer loyalty and praise for enterprise-class security products that are effective, intuitive, and inclusive.

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

Is your current security strategy optimized for the best ROI? Click here to instantly see the value that this product can create for your organization.

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.