Malwarebytes

SOLUTION BRIEF

Malwarebytes Endpoint Detection & Response (EDR)

Endpoint Detection and Response built to respond at the speed of an attack

A simple security response for complicated attacks

Technology allows us to digitally engage with colleagues and partners. Great technology allows us to do the same, but securely. In a post-perimeter world, secure technology means resilient endpoints that can act as the first line of defense against a cyberattack. But research tells us that close to 60 percent of endpoints harbor hidden threats—30 percent of which are critical Trojans, rootkits, and backdoors. These threats are sophisticated, persistent, and often evade even the best protection measures.

Compromised endpoints mean lost productivity. Today, organizations respond by re-imaging infected machines, frequently at a cost greater than the device itself—and they may still lose the data. Alternatively, they deploy complicated endpoint response solutions that require a team of engineers to deploy and a larger team of PhDs to operate.

Neither of these options enables a resilient endpoint security posture. What organizations require is the ability to actively respond to a threat while it is happening, allowing them to isolate, investigate, remediate and recover the data—putting endpoints back into operation.

The case for resilience

The endpoint and the valuable data residing on it is at the heart of workforce productivity. Security teams struggle to secure endpoints against automated threats that adapt techniques to target vulnerable users, applications, and devices. Organizations that rely on single-point-of-failure, signature-based detections succeed in protecting corporate endpoints against viruses of the past but fail to predict and protect against the threats of the future.

For security professionals, failing to protect the endpoint can result in a catastrophic disruption of operations. But this business need comes at a time when security teams are fatigued by

What prevents an active response approach?

"Threats keep getting through my existing protection."

"Multiple vendor protection agents are slowing down users' machines."

"I don't know who is attacking my systems. I don't know how long they've been there, and I don't know how they got there."

"I don't have the tools or experienced staff to run them."

"I have installed an EDR but can't get the most out of it without an EDR expert onsite."

"My endpoint response solution allows me to study the last attack. I need a tool that allows me to prevent the next attack."

high volumes of alert triage and manual endpoint remediation tasks. Organizations need a cost-effective approach to endpoint resilience that allows them to prepare for and actively respond to the inevitable attack.

When suspicious activity occurs, security professionals need to actively respond in mere minutes, immediately stopping potential threats from propagating, while determining if the behavior is indeed malicious. Endpoint response solutions need to be quick and easy to deploy, rapidly protecting organizational assets and shortening the time to respond. Integrated threat detection allows for progressive enrichment of threat detection insights across an attack chain. And a cloud-based platform that guides administrators through investigation, response, and recovery gives them the tools and intelligence needed to respond.

Active response in minutes

In the event of a breach, security teams don't have time to spend training models. When threats strike, the focus needs to be on taking action, instead of allowing paralysis by analysis while the threat propagates.

Malwarebytes enables security professionals to immediately respond across all endpoints with a solution that is intuitive and doesn't require a steep learning curve.

When remediation is required, a single, unified agent eliminates the complexity and costs associated with deploying multiple solutions, along with system conflicts that negatively impact performance. Malwarebytes protects without sacrificing endpoint performance, enabling organizations to go from infection to recovery in seconds.

Simple deployment minimizes response time

Malwarebytes is simple to deploy via a single endpoint agent and provides the visibility needed into endpoints and hidden threats. The Malwarebytes Nebula Console centrally manages everything, and an intuitive user interface enables security teams to assess the situation in less than five seconds.

Linking engine for complete remediation

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. For other security vendors

What is active threat response?

- **Active response** that can quickly be deployed in just a few minutes
- **Progressive threat detection** that catches threats and ensures immediate response capabilities against attacks
- **Guided threat response platform** that provides the intelligence needed to minimize mean time to respond (MTTR)

Key benefits

- **Built to be effective, yet simple** to deploy and manage by security professionals of all abilities
- **Complete and thorough remediation** to return endpoints to a truly healthy state
- **Continuous cloud-based endpoint monitoring** of suspicious activity
- **Integrated threat detection** that stops a threat regardless of attack vector
- **Progressive threat detection enrichment intelligence** that enables rapid investigation of a successful attack
- **Guided threat response** to isolate, remediate and recover compromised endpoints
- **An extensible cloud-based Malwarebytes Nebula platform** that orchestrates a cross enterprise attack response

to thoroughly remove these artifacts, they must create database rules, or signatures, targeting and remediating each separate component of the threat. This cumbersome approach slows down endpoint performance down to a crawl.

Malwarebytes is trusted by incident response teams around the globe thanks in part to the effectiveness of its Linking Engine technology, which identifies and removes all artifacts associated with the primary threat payload.

Malwarebytes Endpoint Detection & Response leverages this proprietary approach, along with insights on suspicious activities to quickly remove zero-day, or brand new, malware and return endpoints to a truly healthy state while minimizing the impact to end-users. Linking Engine technology:

- Uniquely maps and removes all traces and artifacts of an infection—not just the primary threat payload
- Saves time normally spent wiping and re-imaging endpoints

Up to 72 hours of Ransomware Rollback

Ransomware Rollback technology allows organizations to wind back the clock and rapidly get back to a healthy state. If an attack impacts end user files, Malwarebytes Endpoint Detection & Response easily rolls back these changes to restore files that were encrypted, deleted, or modified in a ransomware attack. Plus, organizations have up to 72 hours to undo the damage.

- Wind back the clock to negate the impact of ransomware by leveraging just-in-time backups.
- Easily roll back changes and restore files that were encrypted, deleted, or modified in an attack.
- Data storage is minimized using proprietary dynamic exclusion technology.

Progressive Threat Detection

Malwarebytes Endpoint Detection & Response's multi-layered protection catches threats and provides the intelligence required to investigate, isolate, and remediate cyberattacks.

Malwarebytes finds and remediates 3 million infections every day. Our unique telemetry provides insight into the threats and techniques that are succeeding in the wild and offers a better understanding of what makes these attacks effective and how to best counter them.

Flight recorder for suspicious activity monitoring

The Flight Recorder feature in Malwarebytes Endpoint Detection & Response provides continuous monitoring and visibility into Windows desktops for powerful insights. It allows you to:

- Easily track file system events, network connections, process events, and registry activity
- View full command line details of executed processes
- Store events in the cloud for a rolling 72-hour period
- Automatically display suspicious activity

Endpoint isolation

When an endpoint is compromised, Malwarebytes stops the bleeding by isolating the endpoint. Combining this isolation with fast remediation prevents lateral movement of the infection. Malware is stopped from phoning home, and remote attackers are locked out. Endpoint Detection & Response is the first product to provide three combined modes of endpoint isolation:

- **Network isolation** restricts all endpoint-initiated processes from communicating.
- **Process isolation** prevents new processes from starting up on the endpoint.
- **Desktop isolation** immediately stops further interaction—the system is safely kept online and is only accessible via the Nebula Console.

Guided threat response

Malwarebytes delivers on guided threat response with an easy-to-use platform of simplified tools built for security professionals of all abilities to conduct proactive and cost-effective investigations. For organizations both large and small to achieve endpoint resilience, they must have access to intelligent tools with the ability to investigate and provide the right guidance for response to an attack. These tools and their platform must be extensible in order to guide a cohesive and consistent response across existing SIEM, ITSM, and network management tools. Finally, guided threat response must support agile data exploration with visual data maps that allow IR teams to identify impacted endpoints, data, and users, as well as any potential threat actor details.

Guided threat response capabilities include:

- On-demand and scheduled endpoint scanning for custom IOC threat hunting
- User-initiated remediation scans enabled through integrations with your existing IT systems management tools
- Continuous monitoring for suspicious files and process events, network connections, and registry activity
- Asset management that collects and displays endpoint details (e.g., installed software, updates, and startup programs)
- Visual graphs to investigate processes spawned by a threat and where it moved laterally

The value of enterprise resilience

Malwarebytes Endpoint Detection & Response provides enterprises with the resilience needed to protect employees, endpoints, and the sensitive, proprietary data they store. When breaches occur, a solution featuring active threat response puts a quick stop to the spread of infection through an organization's network, minimizing its impact and putting devices, data, and employees back to work. Progressive threat detection prevents as many breaches as possible while providing the necessary intelligence and tools to investigate, isolate, and remediate any successful attacks. And finally, our guided threat response platform is not only easy-to-use, but also agile and extensible, bridging technology and security silos to provide security teams with a cohesive and consistent response plan.

Malwarebytes Endpoint Detection & Response embraces all three approaches—active threat response, progressive threat detection, and guided threat response—while offering innovative remediation technology in an elegant, easy-to-use interface. Put these together, and now you not only have resilient endpoints, but a resilient organization, ready to bounce back from any cyberattack and get back to work.

malwarebytes.com/healthcare corporate-sales@malwarebytes.com 1.800.520.2796

Malwarebytes is a cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against malicious threats, including ransomware, that traditional antivirus solutions miss. The company's flagship product uses signature-less technologies to detect and stop a cyberattack before damage occurs. Learn more at www.malwarebytes.com.