Malwarebytes

SOLUTION BRIEF

Malwarebytes **Endpoint Protection & Response**

Integrating multiple protection layers with detection and response capabilities

How Limited Visibility Led to Complexity

When it comes to protecting your business endpoints against threats, the reality is that 100 percent protection is a myth. A common misperception among organizations is that 98 percent of their endpoints are protected.

Figure 1: Real-time global threat remediation map

www.malwarebytes.com/remediationmap

In reality, customer environments have demonstrated that closer to 60 percent of endpoints are harboring hidden threats—30% of which are critical threats (e.g., Trojans, rootkits, backdoors). These threats lead to a common business pain involving the cost and time for re-imaging their endpoints with costs ranging from $500 USD to more than 100 hours per endpoint.

Businesses need better visibility and insights to understand how attacks are getting in and answer the questions of "who-what-where-when-why." This has led some organizations to turn to Endpoint Detection and Response (EDR) solutions to address the hidden threats being missed by their real-time protection and "next-gen" security solutions. EDR solutions originally came to market to help businesses address their growing need for continuous protection from hidden and advanced threats. These solutions naturally extended from finding known bad, or malicious, files to start finding files that deemed to be suspicious.

ENDPOINT PROTECTION & RESPONSE

KEY BENEFITS

- Protect against all stages of an attack (pre- and post-execution)
- Gain powerful insights into endpoints and threats
- Reduce mean time to respond (MTTR)
- Rapidly detect and isolate to prevent lateral movement across environments
- Avoid the need to hire, train, and retain a dedicated EDR specialist
- Save time and cost associated with re-imaging endpoints
- Roll back up to 72 hours of damage caused by ransomware attacks
- Simple to deploy and easy to manage

Unfortunately, EDR solutions currently on the market generate large volumes of data and customers find them complex and overwhelming. While the IT industry continues to face a human InfoSec skills shortage, these complex EDR solutions demand highly skilled, dedicated security experts for the organization to realize a full return on those investments. Many EDR customers find that they are unable to derive all the benefits from their EDR solution without either hiring an EDR specialist or investing in a managed service. Despite the complexity, these EDR solutions don't remediate infections.

HERE'S WHAT BUSINESSES TELL US

Problems

- "Threats keep getting through."
- "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."

Challenges

- "I have too many tools, and the ones I have are not always the right tool."
- "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."

"MALWAREBYTES SAVES US FROM CHASING DOWN FALSE THREATS THAT MIGHT BE OUT THERE. IT GIVES US AN ACCURATE REAL VIEW OF AN EVENT, AND LEADS US TO THE PRECISE LOCATION OF THE PROBLEM. IT'S A HUGE TIME-SAVER."

AARON GOODWIN
CHIEF INFORMATION OFFICER, WUNDERLICH

An Easier Way

As threats and attack methods continue to evolve, gaining increased visibility of the threat landscape will help you better prepare for the inevitable. In the case of a breach, you need the right tools in order to quickly provide insights across your endpoints. They must be intuitive and easy to use—after all, you're likely already in crisis mode.

Businesses need a solution that protects endpoints against threats and eliminates the complexity of dedicated EDR offerings. Requirements for an easy-to-use EDR include:

- Scalable solution
- Deployment via a single endpoint agent
- One console to centrally manage everything
- Intuitive user interface that enables you to assess situation in less than 5 seconds
- Ability to leverage your existing staff instead of needing to hire dedicated resources or purchase additional managed services

We Don't Just Alert, We Fix It

Malwarebytes Endpoint Protection and Response integrates Multi-Vector Protection with detection and response capabilities via a single agent that eliminates EDR complexity. By leveraging Malwarebytes best-informed remediation threat intelligence, you can confidently defend against all attack vectors and techniques with:

- Seven layers of static and dynamic detection technologies that protect you across every stage of an attack
- Continuous visibility into endpoints to help reduce the dwell-time of zero-day threats
- Three modes of endpoint isolation to rapidly stop the spread of an attack
- Response options beyond just alerts, to fix the problem—including proprietary Linking Engine remediation and Ransomware Rollback capabilities

Flight Recorder for Continuous Visibility

The Flight Recorder feature in Malwarebytes Endpoint Protection and 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
- Drill down into geolocation data
- 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 Protection and Response is the first product to provide three combined modes of endpoint isolation:

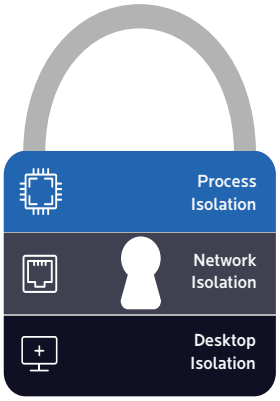

Figure 2: Three modes of Endpoint Isolation

- Network isolation is used to restrict which processes can communicate
- Process isolation acts to restrict which processes can start and run on the endpoint
- Desktop isolation alerts the end user and immediately halts interaction—the system is safely kept online and is only accessible via the Malwarebytes cloud console

Linking Engine for Complete Remediation

Malwarebytes is trusted by incident response teams around the globe thanks in part to the effectiveness of our Linking Engine technology.

Typical malware infections impact multiple components or artifacts, including files, folders, registry keys and registry values. In fact, many malware infections perform changes or modifications to 20, 50, even 100+ artifacts. Depending on the intent of the attack, these infections can propagate to other systems across your network. Trying to thoroughly remove all of these infections requires a security vendor to create database rules, or signatures, that separately target each component of the threat in order to detect and remediate the entire infection. This often slows down the performance of the endpoint and results in lengthy scan times since each rule needs to be checked against all the files, folders, and registry on the system during a scan.

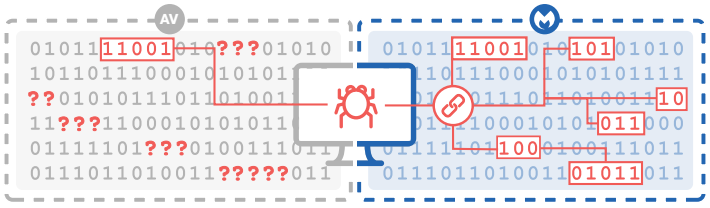

Figure 3: Traditional remediation versus linking engine to linking engine remediation

Malwarebytes Endpoint Protection and Response leverages our proprietary Linking Engine remediation technology along with insights on suspicious activities to remove zero-day, or brand new, malware. 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 you to wind back the clock to negate the impact of ransomware by leveraging just-in-time backups. Malwarebytes Endpoint Protection and Response logs and associates changes with specific processes. Every change made by a process is recorded. If a process does 'bad' things, you can easily roll back those changes and restore files that were encrypted, deleted, or modified in an attack. Data storage is minimized using proprietary dynamic exclusion technology that learns what 'good' applications do. Ransomware Rollback provides you with an additional layer of protection. If an attack impacts your end user's files, you have up to 72 hours to roll back the damage to a healthy state.

Figure 4: Ransomware Rollback

Understanding the Value

Through the integration of multiple protection layers with detection and response capabilities, Malwarebytes and Response helps businesses protect their endpoints against all stages of an attack. Even though Malwarebytes is simple to deploy and provides visibility needed into your endpoints and hidden threats. You can rapidly isolate an endpoint to prevent lateral movement of an attack and roll back any damage caused by ransomware attacks. Malwarebytes makes EDR easy.

Beyond just the security capabilities, you'll be able to reduce mean time to respond (MTTR)—saving you the time and cost associated with re-imaging your endpoints. Choosing Malwarebytes Endpoint Protection and Response can help your IT organization avoid the need to hire, train, and retain dedicated EDR specialists.

AWARDS

A leader in Endpoint Protection, two years running

Malwarebytes named in the top 500 Deloitte's Technology Fast rankings, four years running.

Malwarebytes named in 2018 Security 20 Coolest Endpoint Security Vendors.

Gartner peerinsights™

4.5 Rating for Malwarebytes Endpoint Protection

LEARN MORE

To learn more about Malwarebytes protection, detection, and response capabilities, please contact your Malwarebytes account representative or authorized reseller. To request a free trial, visit: www.malwarebytes.com/business/trial/

malwarebytes.com/epr
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.