Malwarebytes Endpoint Detection and Response

A simple security response for complicated cyberattacks

Technology allows us to digitally engage with colleagues andpartners. 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 in operation.

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.

Key business benefits

- Improve protection against cyberattacks at every point of the attack chain
- Gain visibility into potential endpoint problems and investigate user helpdesk tickets via consolidated endpoint information
- Manage security policies painlessly across all of your Windows and Mac endpoints
- Save money eliminating console hardware, software, and database management costs
- Reach support quickly with included phone technical support
- Reduce agent footprint and decrease deployment complexity

Enpoint 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

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.

Key security 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

Learn more

Discover how your organization can protect its endpoints with N8 Solutions and Malwarebytes. Get in touch with us today to protect against unknown cyberthreats:

Phone: 262-288-1501
Email: info@n8its.com