SOLUTION BRIEF

Malwarebytes

# THE MSP ESSENTIAL EDR TOOLKIT FOR MALWARE REMEDIATION

Time is a valuable asset for managed service providers (MSPs). When your customer has an endpoint infection, you need the right tools that let you respond quickly and efficiently.

How fast is fast? Well, the golden rule is to **remediate within 60 minutes**, which is an important benchmark to measure your organization's cyber readiness to mitigate lateral spread and withstand today's sophisticated threats. **To make this possible, your vendor's endpoint detection and response (EDR) solution must provide these essential capabilities:**

### Automated isolation

Isolation-based capabilities create an air gap between the compromised endpoint and the other systems within your customer's organization. Helping your customers achieve endpoint resilience requires the means to contain the infection through **network, device, and process isolation.**

These containment mechanisms will also impede the malware from phoning home to receive command-and-control communication, which restricts it from doing further damage. Automation here is essential. A key factor in improving incident response processes is lowering mean time to respond (MTTR) or dwell time, and automated isolation methods will significantly aid in this area.

### Thorough remediation

Your EDR's remediation must be thorough. It's not simply enough to delete the primary payload and call it a day. When remnants and secondary payloads are left behind, it provides attackers with coveted dwell time and increases the odds that it will become a major infection. When your customers get re-infected from the original malware artifacts that were left behind, this starts your remediation efforts all over again.

## A LOOK AT INCOMPLETE REMEDIATION CAPABILITIES

Enabling swift response actions for your customers, requires an EDR solution that thoroughly eradicates malware. Many EDR solutions fall short on this requirement. They commonly provide capabilities to quarantine an infection, which prevents it from harming the machine, but the malware removal feature often only deletes the active malware files.

This leaves behind artifacts that can reinfect the machine and wreak havoc on your customer's environment. Just how much havoc? Considering ransomware is notorious for leaving behind artifacts on the endpoint, a re-infection of this nature could halt your customer's operations and require your team's time restoring their system from back-ups—or paying the extortion cost.

# MALWAREBYTES: MULTI-MODE ISOLATION AND REMEDIATION DELIVERS THE GOLD STANDARD IN EDR

With Malwarebytes, MSPs get a leading EDR solution that lets you swiftly respond to any endpoint issues and provide your customers with peace of mind about their security posture.

### Granular, automated attack isolation

Our granular isolation capabilities prevent lateral movement of an attack by allowing you to segment individual machines, subnets, or groups and continue your active response activities with breathing room. Rather than simply quarantining a file, suspicious files can be isolated in three ways to ensure they are completely restricted from doing harm:

1. **Network isolation** limits device communications so attackers are locked out and malware can't "phone home."
2. **Process isolation** restricts which operations can run, halting malware while still allowing end users to work away.
3. **Desktop isolation** alerts the end user of the threat, temporarily blocks their access while keeping their device online for analysis.

### Thorough remediation

Endpoint remediations are thorough and complete with our Linking Engine technology that maps system changes associated with the malware to detect and remove dynamic and related artifacts and return your customer's endpoints to a truly healthy state. This ensures no artifacts are left behind to wreak havoc on your customer's environment.

## SUMMARY

Malware infections are inevitable. For MSPs, that means providing customers with efficient, resilient endpoint incident response is just as important as providing powerful endpoint protection. When that future event occurs, your vendor EDR solution must provide you with the modern capabilities to perform expertly to meet the benchmark of remediating within 60 minutes.

Malwarebytes equips MSPs with the gold standard in EDR to effectively protect and expertly remediate customer endpoints. Granular isolation capabilities along with thorough remediation of all malware artifacts is the true EDR standard to provide your customers.

## LEARN MORE

To learn more about the Malwarebytes isolation and remediation capabilities available within our MSP Partner Program, visit: malwarebytes.com/msp.

malwarebytes.com/business | msp@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 remediations, 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.