Malwarebytes

SOLUTION BRIEF

A Modern Approach to Endpoint Remediation

Why it's time to stop reimaging your endpoints

Even with a comprehensive multi-layered protection solution in place, no organization can prevent every endpoint attack. An effective solution needs to include three critical components – protection, detection, and response (see Figure 1.) A key factor in improving incident response processes is lowering Mean Time To Response (MTTR) or dwell time.

What are the current Incident Response (IR) Trends?

According to Incident Response teams, malware is the root cause of 68 percent of the incidents they investigate[1]. Nearly 15 percent of US security budgets go to remediating active compromises. So, how long does it take to recover from these attacks? In 2017, 28% of IR teams reported the time from detection to remediation was 6 to 24 hours and 23% required a minimum of 1 to 5 hours to recover.[2]

According to Osterman's "The True Costs of Cybercrime" report the average cost for remediating just a single major security event is approximately US$290K for a 2,500 employee organization. In the US, the average cost escalates to over US$429K.

Traditional Reimaging Approach

Reimaging an infected endpoint has a long legacy as the de facto standard. However this approach is also fraught with time inefficiencies and inherent risks as shown in Figure 2. This can add up to hours of restoring data and settings, lost work between the last backup and time of infection, as well as lost employee productivity.

Traditional Remediation Approach

A typical malware infection performs between 70 to 80 changes on an endpoint. These can include disabling existing security software, modifying registry values, system file changes etc. Most traditional remediation solutions only remediate the active malware components or payload—this doesn't provide complete remediation. When infection changes on the endpoint are not completely reversed, such as leaving a port open, it leaves endpoints vulnerable to rapid reinfection or new attacks focused on that specific vulnerability.

Figure 1. Componenets of an effective EDR solution

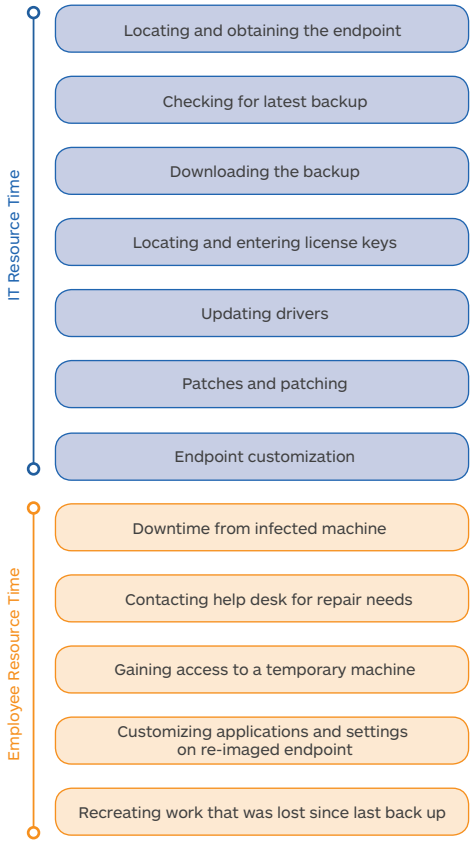


Figure 2. Traditional reimaging approach

A Modern Remediation Approach

Linking Engine Remediation

Unlike traditional remediation approaches, proprietary Malwarebytes Linking Engine Remediation maps all changes associated with an infection. It detects all related infection artifacts and is then able to completely remove dynamic and related artifacts to return endpoints to a truly healthy state while minimizing the impact to the end-user.

Three Modes of Endpoint Isolation

Fast remediation prevents lateral movement across the endpoint estate preventing malware from phoning home and remote attackers are locked-out. You can safely keep a system online for detailed analysis via the Malwarebytes Management Console. Malwarebytes Endpoint Protection and Response (EPR) is the first product to offer three ways to isolate an endpoint.

1. Network isolation to restrict which processes can communicate.
2. Process isolation to restrict which processed can run.
3. Desktop isolation to alert the end users and halt interaction.

Figure 3. Traditional AV Remediation versus Malwarebytes Linking Engine Remediation

Up to 72 Hour Ransomware Rollback

Malwarebytes uniquely offers the ability to rollback ransomware for up to 72 hours to ensure coverage over a long weekend or for unique customer environments.

Ransomware Rollback technology allows you to wind back the clock to negate the impact of ransomware by leveraging just-in-time backups. Malwarebytes 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 to restore files that were encrypted, deleted, or modified. Data storage is minimized using proprietary dynamic exclusion technology that learns what 'good' applications do.

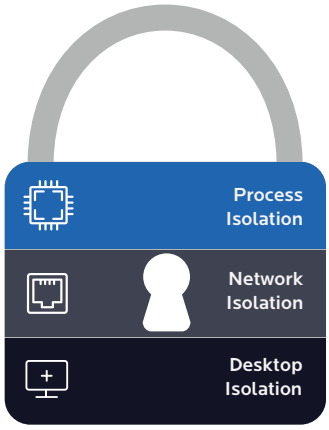


Figure 4. Modes of endpoint isolation

Automated Remediation

Now more than ever organizations need to shift from reactive to automated incident response processes. In the face of limited resources and constant barrage of advanced threats an automated remediation approach can advance your security model and bridge operational silos.

The integration between Malwarebytes and various Enterprise-grade visibility and orchestration platforms allows for rich automated response workflows to trigger remediation even before a human as acknowledged the incident, strongly reducing the mean time to recovery (MTTR).

This prevents lateral movement, data exfiltration and leaves zero chance to the attackers.

Figure 5. Ransomware rollback process

The Malwarebytes integration with ServiceNow provides automation and orchestration to reduce MTTR. The integration enables organizations to:

- Generate Security Incidents based on malware detections and other Malwarebytes real-time protection events.
- Analyze threats and malware detections directly within ServiceNow
- Initiate Malwarebytes scans and remediation on demand with a single click
- Automatically respond to Security Incidents with Zero-Touch remediation.
- Easily Integrate Malwarebytes Remediation in complex Incident Response workflows using an activity pack.

Pro-Active Malware Hunting

Malwarebytes empowers your IR team to run scheduled scans that proactively hunt for recently reported Indicators of Compromise (IOCs) across the company. The integrated solution makes it easy to adopt an assume-the-compromise process to ensure your remediation includes searches for lateral movement and disinfection of all impacted endpoints.

This transforms any threat intelligence you have, from inside (eg: sandboxing) or outside your organization (eg: subscribed feeds).

It allows your incident responder to extend the scope of Malwarebytes detections to their need while still benefiting from its industry-leading remediation engine.

> "MALWAREBYTES IS A CRITICAL PART OF THE LAYERED SECURITY NEEDED IN TODAY'S ENVIRONMENTS. IT'S DOING A GREAT JOB PROTECTING US."
>
> JOHN MAJOR
> IT Operations Manager, Sun Products

Malwarebytes integration with ForeScout provides:

- Pro-Active Hunting of IOCs from any third-party source
- Rapid Threat Detection and Remediation
  - Allow, deny, or limit network access based on detected threats and remediation response stage
  - Assess high-risk endpoints and remediate threats instantly
- Automated Threat Response
  - Automate incident response workflows beyond just quarantine actions

The Malwarebytes integration with Splunk provides:

- Representation and visualizations of endpoints, detections, quarantine with real-time and historical reporting
- Easy workflow drilldown from high level to low level
- Pre-built dashboard panels for easy custom dashboard creation by the user
- Custom alert action to execute remediation based upon various triggers
- Pro-active Malware hunting with MBBR and third party-IOC

Malwarebytes Endpoint Protection and Response

With 500 thousand downloads and 4 million remediation events per day, Malwarebytes is the industry's most trusted remediation vendor. Unlike other Endpoint Detection and Response solutions on the market, Malwarebytes Endpoint Protection and Response doesn't just generate alerts, it fixes the problem. It provides immediate response capabilities in the event an infection occurs. Proprietary Linking Engine remediation provides complete and thorough remediation. Endpoint Isolation rapidly stops the bleeding, and rollback technology allows you to wind back the clock to negate the impact of ransomware.

In Summary

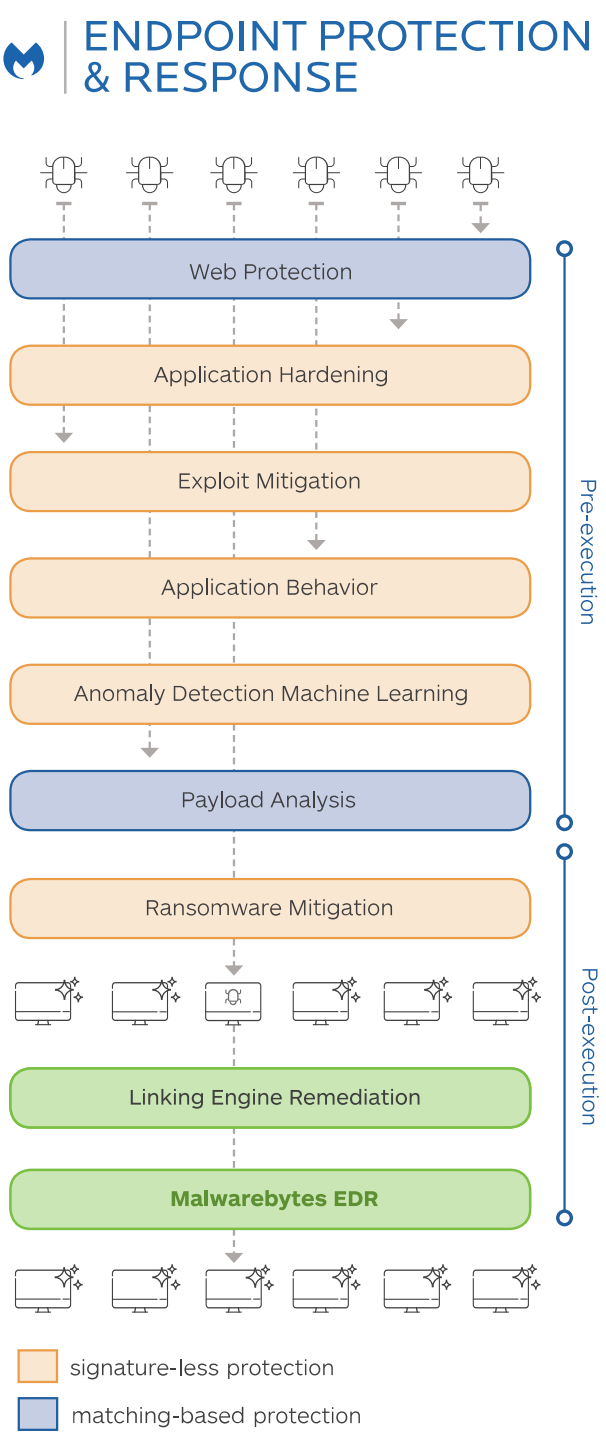
IR teams can benefit from adopting an automated endpoint remediation that effectively rips malware out by the roots. To deliver benefits beyond reimaging, remediation needs to be fast, thorough, and seamlessly restore endpoints to their healthy pre-infection state. The advantages of automated remediation over reimaging:

- Delivers automated, accurate, and thorough remediation
- Bridges operational silos
- Greatly increases response time efficiency
- Reduces malware dwell time
- Closes gap in personnel and skills shortage
- Lowers cost and complexity of managing incident response
- Minimizes workstation and employee downtime
- Restores all employee work

LEARN MORE

To learn more about Malwarebytes Endpoint Protection and Response visit:
malwarebytes.com/business/endpointprotectionandresponse/

To learn more about Malwarebytes technology integrations visit:
malwarebytes.com/integrations/



REFERENCES

[1, 2] *SANS Institute "The 2017 SANS Incident Response Survey" June 2017*

malwarebytes.com/business 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.