Malwarebytes

SOLUTION BRIEF

Advancing SOC endpoint incident response practices

Why it's time to start automating endpoint remediation

Even with a comprehensive multi-layered protection solution in place, no organization can prevent every endpoint attack. When an attack occurs, security operations center (SOC) teams need fast, effective response actions to mitigate the damage from a breach. A key factor in improving incident response processes is lowering mean-time-to-response (MTTR) or dwell time.

Experts recommend aiming to meet the **1-10-60 rule**: 1 minute to detect, 10 minutes to investigate, and 60 minutes to remediate.

That means the cyber-prepared enterprise should aim to eradicate cyberthreats from the environment in under an hour to effectively combat sophisticated attacks and avoid the damage a successful breach can inflict on an organization's reputation and bottom line.

KEY BENEFITS

Automated and complete remediation
Enables security analysts to eliminate manual efforts to remediate attacks

Visibility of remediation status across the fleet of endpoints
Malwarebytes IR makes it easy to manage response actions across distributed locations and dispersed workforces

Interoperability to orchestrate automation across security investments
Malwarebytes API Provides integration opportunities across your security stack

A look at the current incident response trends

With the goal of remediating in an hour, how are enterprises doing?

Looking into the near future, 75 percent of organizations assume they are likely to experience a breach within the next one to three years.[1] Yet only 17 percent are very confident in their enterprise's ability to recover quickly from a malware attack.[2] So, how long does it take to recover from these attacks? According to Malwarebytes sponsored research, 43 percent of enterprises require days to weeks to remediate an incident.[3]

Factors impeding fast remediation

There are several factors and market trends that slow down endpoint incident response processes.

Dispersed workforce
With nearly 40 percent of enterprises moving 81 – 100 percent of their employees to a work-from-home model in response to COVID-19, they've created a business environment where they now operate across vast regional locations.[4] The resulting architectural complexity from distributed locations and a dispersed workforce has added challenges for SOC teams to manage enterprise incident response processes.

With endpoint systems that no longer sit within a brick and mortar corporate headquarters, enterprises are consistently facing long response times. The simple act of accessing an endpoint to perform remediation can be a manual, slow, and tedious effort.

Manual remediation processes
Reimaging an infected endpoint is fraught with time inefficiencies and inherent risks as shown in Figure 1. 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.

The other approach is traditional remediation. A typical malware infection performs between 70 to 80 changes on an endpoint. These can include disabling existing security software, modifying registry values, and system file changes. However, traditional remediation solutions only remove the active malware components or payload, which doesn't provide complete remediation.

Once the machine is running again, the uncleaned artifacts can rapidly re-infect the machine and move laterally to other systems.

The reality is manual remediation doesn't provide the speed or completeness enterprises need to ensure all infection points are restored with minimal resource impact to a dispersed workforce and resource strained SOC team.

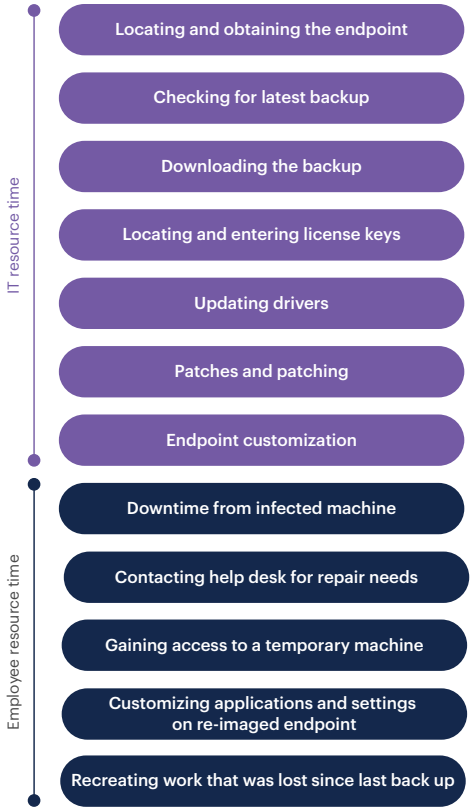


Figure 1. Traditional reimaging approach

A modern remediation approach

According to research by the Ponemon Institute, there are three, common factors that improve incident response:

1. Automation
2. Visibility
3. Interoperability

In particular, 42 percent of enterprises find that investing in automation increases cyber resilience.[5] When security teams adopt a solution that allows them to automatically remediate malware across remote devices, they greatly improve operational efficiencies and relieve constrained SOC team resources.

Most notably, automated endpoint incident response allows SOC teams to reach the 60-minute benchmark of the 1-10-60 rule.

Malwarebytes Incident Response: The trusted standard in automated remediation

Now more than ever, enterprises need to shift from reactive to automated incident response processes. With constrained SOC resources and a constant barrage of advanced threats, an automated remediation approach can advance SOC practices to create a high performing cyber resilient organization.

Malwarebytes Incident Response (Malwarebytes IR) is the trusted standard in automated endpoint remediation that bolsters your enterprise cyber resilience by compressing your response times with fast and complete remediation. With our automated approach, Malwarebytes IR saves analyst resource time, preserves user productivity, and improves your enterprise security posture.

Our proprietary technology uniquely supports the three factors mentioned above that arm SOC teams with a highly efficient and effective incident response practice: automation, visibility, and interoperability.

Automated and complete remediation
Our automated approach enables your security analysts to eliminate manual efforts to remediate attacks, freeing up valuable resource time so your analysts can focus on revenue-generating initiatives. Automated tasks take place in less time with greater accuracy and compress your response time.

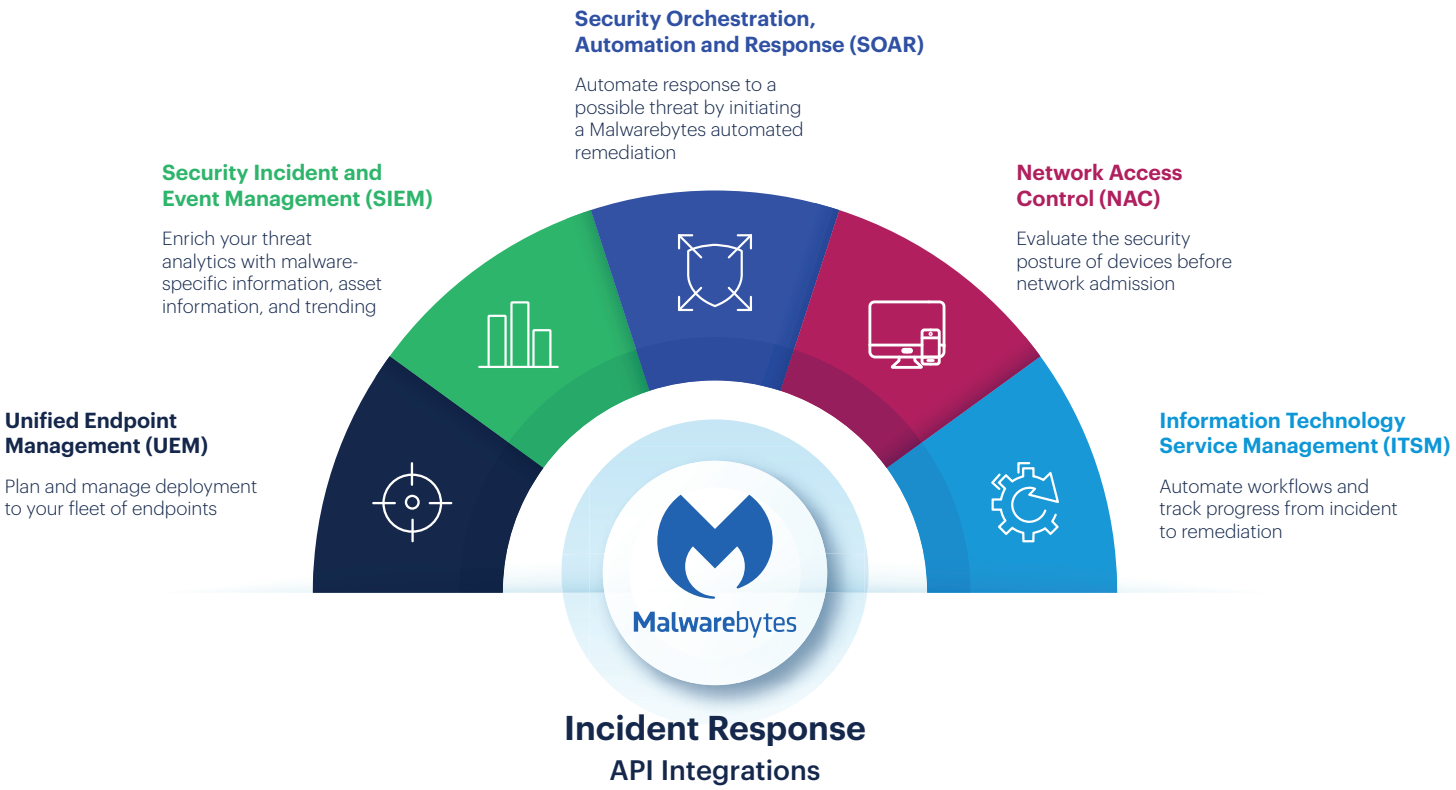
Most solutions only remediate active malware components—this doesn't provide complete remediation. Malwarebytes Linking Engine applies a propriety approach that also detects and removes dynamic and related artifacts. Our engine applies associated sequencing to ensure disinfection of malware persistence mechanisms.

Visibility of remediation status across the fleet of endpoints
Driven from the cloud, Malwarebytes IR makes it easy to manage response actions across your distributed locations and dispersed workforce. The solution's centralized dashboards provide a single pane of glass that lets your security analysts quickly view and understand your attack response footprint and remediation status.

Traditional AV Remediation versus Malwarebytes Linking Engine Remediation

Interoperability to orchestrate automation across security investments

The Malwarebytes API provides integration opportunities across your security stack, such as your SIEM, SOAR, and ITSM to drive further automation and orchestration of your security processes. This delivers enterprise cyber resilience that is nimble with faster actions that protect and respond to attacks as they occur.



Summary

SOC teams can significantly benefit from adopting an automated endpoint remediation that effectively rips malware out by the roots. To compress response times and eradicate threats from the environment in under an hour, remediation needs to be fast, thorough, and seamlessly restore endpoints to their healthy pre-infection state.

Malwarebytes Incident Response is the enterprise go-to, trusted solution for automated remediation. Malwarebytes IR relieves enterprises from the challenges stemming from architectural complexity, manual processes, and constrained resources to deliver fast response times and complete remediation. With Malwarebytes IR, you can effectively combat sophisticated cyberthreats and avoid the damage a successful breach could inflict on your organization's reputation and bottom line.

---

[1] Malwarebytes. How to Become Cyber Resilient. 2019.
[2] Computing Research. Best practice makes perfect: malware response in the new normal. 2020
[3] Ibid.
[4] Malwarebytes. Enduring from home: COVID-19' impact on busines security. 2020.
[5] Ponemon Institute. Cyber Resilient Organization Report. 2020.

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.