Malwarebytes cyberprotection

ACCELERATE AND SIMPLIFY YOUR INCIDENT RESPONSE WITH AUTOMATED REMEDIATION

How 4 enterprises use Malwarebytes to reduce dwell time and advance their security posture

Introduction

Strong cybersecurity is an essential component of a company's success. Unfortunately, traditional practices of manually remediating endpoints increases the cost and complexity of incident response, not to mention increasing risk exposure.

In fact, more than 40 percent of enterprises require days to weeks to remediate an incident.[1] Getting ahead of this requires a move to automated endpoint remediation in the face of limited resources and continuous attacks.

A key factor in improving incident response processes is lowering mean-time-to-response (MTTR) or dwell time. The goal is to meet the **1-10-60 rule:** 1 minute to detect, 10 minutes to investigate, and 60 minutes to remediate.

That means organizations should **set a benchmark to remove malware and other threats from the environment in under an hour** to effectively mitigate any damage and reduce impact on productivity.

This eBook illustrates how four organizations are accelerating their remediation efforts with the help of Malwarebytes Incident Response.

[1] Computing Research. Best practice makes perfect: malware response in the new normal. 2020.

Why Malwarebytes for your malware remediation?

Even with multi-layered security in place, no organization can prevent every endpoint attack. Investing in a solution that automates remediation and works around-the-clock to eradicate threats will advance your security practices and remediate threats in minutes.

Solution overview

Malwarebytes Incident Response (IR) makes it easy to **quickly and proactively respond to security alerts and incidents** with an automated, remote remediation solution. Unlike others that only remove malicious executables, Malwarebytes IR removes artifacts and changes that can lead to reinfection, allowing you to implement “zero trust for zero day” as advised by NIST.

Flexible options let you deploy the way you want

Our flexible implementation options let you deploy according to your endpoint strategy.

Malwarebytes Remediation for CrowdStrike®

Dissolvable agent

Works seamlessly with your CrowdStrike Falcon to provide automated remediation that thoroughly removes malware.

Malwarebytes Incident Response

Persistent agent

Lightweight agent that runs scheduled endpoint scans and removes detected threats on proactively scheduled time intervals.

Malwareytes Incident Response

Dissolvable agent

Deploy the agent when you have a detected threat to eradicate. After remediation is complete, you can harvest the logs for reporting and dissolve the agent and files.

Delivering important benefits

Compress response time

Automated malware remediation that lets you eradicate threats with fast response time and thorough removal.

Drive greater operational efficiency

Accelerates security operations, saves security analyst resource time, and preserves user productivity.

Automate orchestration

Our API makes it easy to integration across your security stack to drive further automation and orchestration of your security processes.

---

*CrowdStrike" and "CrowdStrike Falcon" are registered trademarks of CrowdStrike, Inc. Malwarebytes Remediation for CrowdStrike is not associated with, or endorsed by, CrowdStrike Holdings, Inc. or its affiliates.

University of Illinois gains fast, effective endpoint remediation

Challenges

Keeping students and staff devices free from malware is a priority for maintaining day-to-day learning and campus operations. Yet, when the university's CrowdStrike* endpoint protection would detect a malicious threat, the follow on remediation process was time consuming for the university's large, decentralized IT team, often relying on

- ✓ **Time-consuming machine reimaging to clean up infections.**
- ✓ **Non-uniform incident response processes for endpoint eradication.**
- ✓ **Lacking fast, effective remediation solution for campus IT professionals.**

Solution

- ✓ **Malwarebytes Remediation for CrowdStrike**
- ✓ **Endpoints: 26,000**

"Malwarebytes has a strong reputation as the remediation. To have leading remediation that integrates with our CrowdStrike product made it very compelling to select Malwarebytes."

- ✓ **Leading remediation that integrates directly with incumbent endpoint protection solution.**
- ✓ **Automated and through malware removal that accelerates, simplifies incident response.**
- ✓ **Powerful scan engine that provides a security layer to detect Potentially Unwanted Programs (PUPs), Potentially Unwanted Modifications (PUMs), and other threats.**

Results

Since deploying Malwarebytes Remediation for CrowdStrike, keeping the university's 26,000 student and staff endpoints malware-free has been a simple, turnkey process.

- ✓ **Effective remediation across the university's 26,000 endpoints.**
- ✓ **Additional endpoint protection with Malwarebytes detecting threats that are active and inactive.**
- ✓ **Fast endpoint eradication that eliminates time consuming machine reimaging.**
- ✓ **Automated endpoint remediation that removes manual remediation efforts and saves IT resources.**

> Malwarebytes gives us an effective and streamlined process for endpoint remediation that doesn't introduce another agent. We can do entire system-wide scan with Malwarebytes to detect what's on the machine, in addition to whatever CrowdStrike detects, and then automatically remediate all as one step. With Malwarebytes, we have confidence in the healthy state of our endpoints.
>
> **- Mark Wenneborg, IT Specialist**
> **University of Illinois**

Kraft Heinz scales and automates global endpoint incident response

Challenges

Acting on endpoint malware detections and remediating the issue was presenting several challenges. One of the biggest hurdles was identifying which employee endpoint was infected.

For detections that said a user had introduced malware from a malicious site, the company's web security solution was only providing the IP address of the infected endpoint. By the time the information was sent to the team, the endpoint had gone off the network. Tracking down the right machine after it reconnected with a new IP address was a manual and time-consuming effort.

Solution

- ✓ **Malwarebytes Incident Response (dissolvable agent)**
- ✓ **Endpoints: 38,000**

"As we started our investigation for a solution, we really liked that we could simply download Malwarebytes and do a free proof of concept. From that firsthand experience we knew, with confidence, that it worked. That positive trial experience led us to select Malwarebytes."

Results

"The integration between Malwarebytes and our SIEM allows our security team to orchestrate a fast and effective process from detection to remediation that's fully automated and consistent across the globe."

> With Malwarebytes automating remediation, we can see it's working well. Job done. Endpoint remediation doesn't require any tickets or any of our security team resources. An incident response process that was previously taking us a lot of effort is now down to minutes.
>
> **- Chris Leonard, Senior Manager**
> **European IT Security and Global Compliance**
> **Kraft Heinz**

Fast, effective remediation for a best-practice SOC process

Challenges

In defining requirements for incident response processes, the SOC team wanted a solution that would:

- ✓ **Accelerate processes for endpoint remediation that reduces dwell time.**
- ✓ **Support multi-layered security strategy with a solution that works well with the security stack.**
- ✓ **Provide effective detection and eradication of endpoint threats to keep systems secure and operational.**

Solution

- ✓ **Malwarebytes Incident Response (persistent agent)**
- ✓ **Endpoints: 25,000**

"Malwarebytes has a strong reputation for its effective remediation capabilities, so it was our solution of choice."

Results

- ✓ **Accelerated processes: Gained a strong foundation for endpoint remediation, improving the organization's security posture.**
- ✓ **Effective incident response: Remediation effectively cleans up the endpoints from PUPs, PUMs, spyware, and unwanted toolbar add-ins.**
- ✓ **Resource savings: SOC resource time savings with automated remediation across all 25,000 global endpoints.**

> Malwarebytes Incident Response is fabulous, and we've had great success with it. It's effective at thoroughly cleaning an infection, including PUPs and PUMs so that we don't have to worry about a possible re-infection. Also, it's really easy to use and works collaboratively with our other security tools.
>
> **- Bob Chadwick, SOC Manager**
> **Fidelity National Financial**

Entrust scores win against disruptive malware

Challenges

Until the team could manually remediate the system, suspicious items represented a risk that could result in damage. When the team received an alert, they would call the end user.

"This created a tremendous impact to our users. An employee doesn't need someone calling and taking an hour out of their day to fix a suspicious item on their system. We needed a faster, less intrusive way to remediate systems."

Solution

- ✓ **Malwarebytes Incident Response (persistent agent)**
- ✓ **Endpoints: 2,500**

"The cloud-based architecture made Malwarebytes Incident Response a no-brainer for us. It enhanced our layers of defense and was an easy sell."

Results

"We love the thoroughness of Malwarebytes Incident Response. In just the past 90 days it cleaned up 14,000 PUPs. It not only fixes what we have identified as a threat, it also remediates secondary and tertiary infections and artifacts."

> For every malware alert we receive, we clean it up with Malwarebytes, without affecting the end use. It's a win for us, the SOC team, and the company.
>
> **- Brian Withrow Senior Manager, Security Operations Center Entrust**

Conclusion

Incident response requires speed. Analysts need the right technology that helps them scale.

These four enterprises are proof that you can achieve fast malware removal in minutes. With Malwarebytes you can streamline and enhance your security posture across your environments with automated remediation.

Choose Malwarebytes Remediation for CrowdStrike, Malwarebytes Incident Response with a persistent agent, or Malwarebytes Incident Response with a dissolvable agent—the choice is yours.

To learn more visit:

https://www.malwarebytes.com/business/incident-response