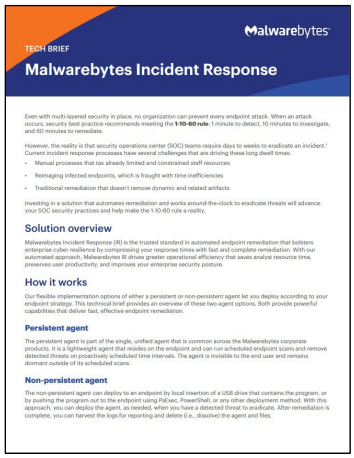


Malwarebytes Incident Response

Thank you for downloading this Malwarebytes tech brief. Carahsoft is the master government aggregator and distributor for Malwarebytes' Cybersecurity solutions available via MAS, ILTPP, MHEC, and other contract vehicles.

To learn how to take the next step toward acquiring Malwarebytes' solutions, please check out the following resources and information:

For additional resources:
carah.io/MalwarebytesResources

For upcoming events:
carah.io/MalwarebytesEvents

For additional Malwarebytes solutions:
carah.io/MalwarebytesSolutions

For additional CyberSecurity solutions:
carah.io/CyberSecuritySolutions

To set up a meeting:
Malwarebytes@carahsoft.com
844-214-4790

To purchase, check out the contract vehicles available for procurement:
carah.io/MalwarebytesContracts

For more information, contact Carahsoft or our reseller partners:
Malwarebytes@carahsoftcom | 844-214-4790

TECH BRIEF

Malwarebytes Incident Response

Even with multi-layered security in place, no organization can prevent every endpoint attack. When an attack occurs, security best practice recommends meeting the **1-10-60 rule**: 1 minute to detect, 10 minutes to investigate, and 60 minutes to remediate.

However, the reality is that security operations center (SOC) teams require days to weeks to eradicate an incident.[1] Current incident response processes have several challenges that are driving these long dwell times:

- Manual processes that tax already limited and constrained staff resources
- Reimaging infected endpoints, which is fraught with time inefficiencies
- Traditional remediation that doesn't remove dynamic and related artifacts

Investing in a solution that automates remediation and works around-the-clock to eradicate threats will advance your SOC security practices and help make the 1-10-60 rule a reality.

Solution overview

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

How it works

Our flexible implementation options of either a persistent or non-persistent agent let you deploy according to your endpoint strategy. This technical brief provides an overview of these two agent options. Both provide powerful capabilities that deliver fast, effective endpoint remediation.

Persistent agent

The persistent agent is part of the single, unified agent that is common across the Malwarebytes corporate products. It is a lightweight agent that resides on the endpoint and can run scheduled endpoint scans and remove detected threats on proactively scheduled time intervals. The agent is invisible to the end user and remains dormant outside of its scheduled scans.

Non-persistent agent

The non-persistent agent can deploy to an endpoint by local insertion of a USB drive that contains the program, or by pushing the program out to the endpoint using PsExec, PowerShell, or any other deployment method. With this approach, you can deploy the agent, as needed, when you have a detected threat to eradicate. After remediation is complete, you can harvest the logs for reporting and delete (i.e., dissolve) the agent and files.

Managing the solution

Malwarebytes IR automates the process of eradicating endpoint threats and provides powerful, complete remediation. Our automated approach enables your security analysts to eliminate manual efforts to remediate attacks, freeing up valuable resource time. Automated tasks take place in less time with greater accuracy and compress your response time.

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

Powerful scan capabilities

When managing your remediation approach, you can choose from multiple scan types:

- **Hyper Scan:** focuses on memory objects and startup objects to determine if malware is actively running on the endpoint.
- **Threat Scan:** includes all items in the Hyper Scan and adds scans for registry objects and file system objects. The scan focuses on common paths that infections target to install.
- **Full Scan:** includes all items in Threat Scan and adds scans for rootkits, PUPs and PUMs, and custom root folders for local drives. The Full Scan focuses on all of the device's drives and includes all scanning capabilities the solution has to offer.

The product also provides the flexibility for you to decide the action you want Malwarebytes IR to take following a scan. You can choose to report the findings, quarantine malicious files, or remove any detected malware, PUPs, PUMs, and other threats found during the scan.

Supported environments

Malwarebytes IR supports your workstations and servers, making it easy to automate remediation across your enterprise-wide environment.

PERSISTENT AGENT

Windows
Windows 10, 8.1, 8, 7, and Vista
Windows XP® with SP3
Windows Server 2019, 2016, 2012, 2011, and 2008

Mac
OS X 10.11 El Capitan
macOS 10.12 Sierra
macOS 10.13 High Sierra
macOS 10.14 Mojave
macOS 10.15 Catalina
macOS 11.0 Big Sur

Linux
Linux servers: Debien-based distros, RPM-based distros

NON-PERSISTENT AGENT

Windows
Windows 10, 8.1, 8, and 7
Windows Server 2012, 2012 R2
Windows Small Business Server 2011
Windows Server 2008 R2

Mac
macOS version 10.9.5 or later

Managing workflows and reporting

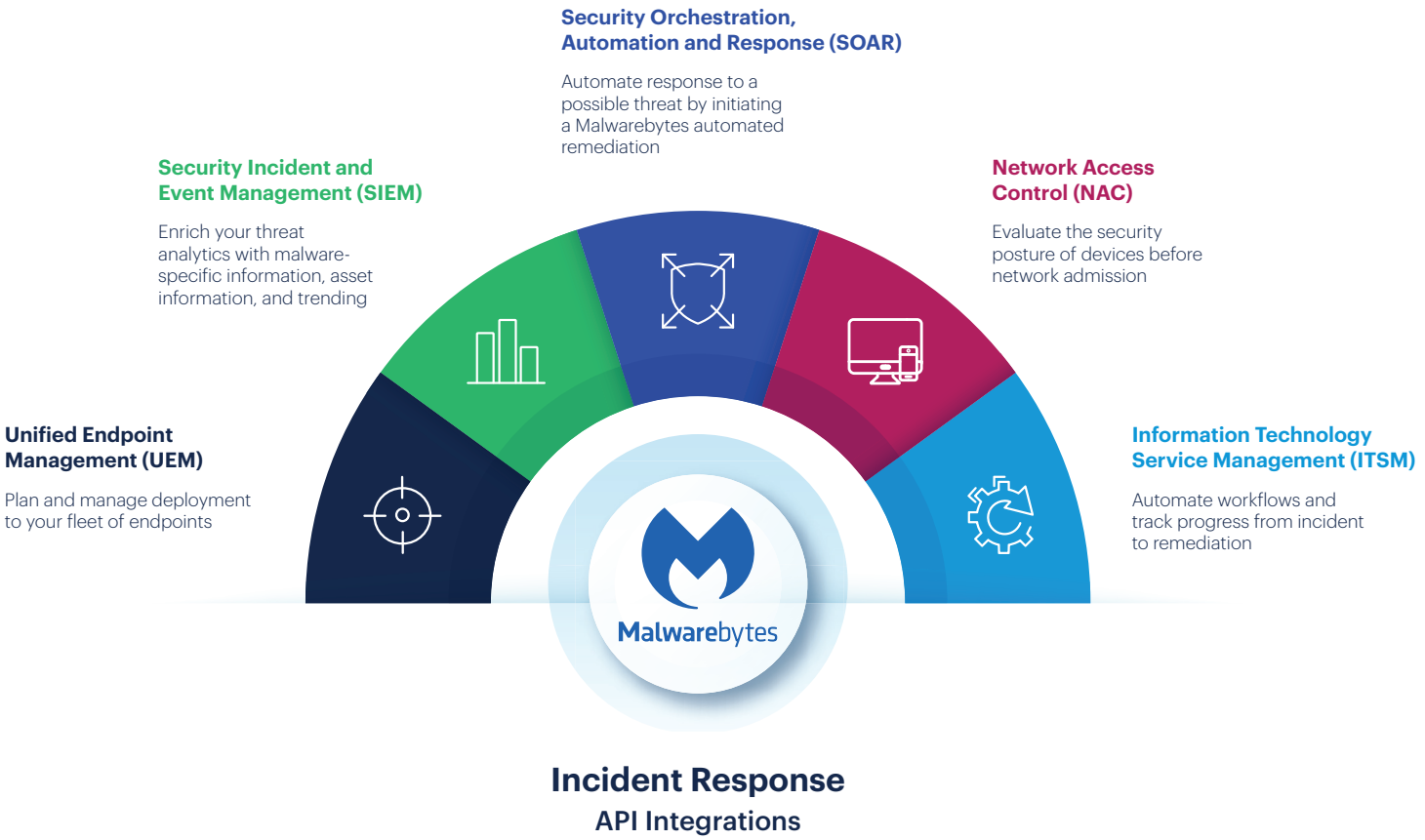
With the two deployment options, there are variances in the user interface workflows and reporting approaches.

The persistent agent is managed through the cloud-based Malwarebytes Nebula platform that allows you to centrally manage all Malwarebytes products under a single pane of glass. The Nebula platform augments them with a guided user interface and API integration capabilities that maximize your security investments across your enterprise.

The non-persistent agent is driven through a command line structure and supports a variety of command line parameters, which can be used from a command prompt, batch file, or script. After each scan, the solution creates a ScanSummary.txt file along with ScanResults.json. These provide your SOC team with a high-level overview on the scan results including the number of items detected and remediated. This data can easily be fed into your information technology service management (ITSM) solution to gain a single pane of glass for your incident response tracking and workflow.

Security integration opportunities

The Malwarebytes API provides integration opportunities across your security stack, such as your SIEM, SOAR, NAC, 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.



Persistent agent, SIEM, and ITSM integrations use case

For customers who choose the persistent agent approach, you can use the API for bidirectional integration use cases, which provides your SOC team with many scenarios that streamline security processes. Using the Malwarebytes API to integrate with your SIEM, every time Malwarebytes IR runs a scan that detects malware and other threats, the solution can send Malwarebytes Suspicious Activity alerts to your SIEM. This will enrich the SIEM's analytics and can be used by the SOC team to further investigate an event.

Once Malwarebytes IR completes a remediation, the log details can be sent to your integrated ITSM solution. This makes it fast and easy to track event progress from detection to remediation.

Non-persistent agent and SIEM integration use case

For customers who choose the non-persistent agent approach, the Malwarebytes solution can send logs directly to your SIEM's log listener over TCP or UDP.

Your SOC team can also orchestrate automation from detection to eradication between your SIEM and the non-persistent agent. In this scenario, when the SIEM receives new event information indicating that an endpoint was just infected, a fully automated process can push out the Malwarebytes non-persistent agent to the infected endpoint. Malwarebytes IR then performs complete remediation to disinfect the machine, and the agent is removed. Read the Kraft Heinz case study for details on the company that uses this integration scenario across its 30,000 global endpoints.

START YOUR TRIAL

To request a free trial, visit: www.malwarebytes.com/business/request_trial

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