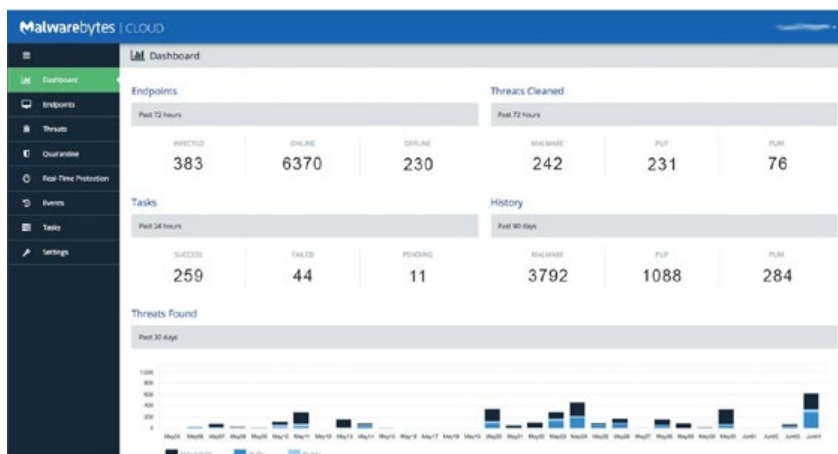


# Malwarebytes Incident Response

Centralized threat detection and remediation

Modern attackers are increasingly sophisticated in how they target and gain intelligence on their victims, and execute their cyberattacks. Malicious threats continue to penetrate network and endpoint defenses even though businesses, schools, and government agencies have spent billions on bolstering their security stacks. The time and effort required to respond to these incidents<sup>1</sup> are lengthy, often taking 6-8 hours just to remediate or re-image a single endpoint. According to Ponemon Institute research, malicious or criminal attacks take an average of 229 days to identify and 82 days to contain<sup>2</sup>. Businesses need to arm their security teams with the most informed telemetry and the best remediation.

Malwarebytes Incident Response is a threat detection and remediation tool built on a highly scalable, cloud-based management platform. It scans networked endpoints for advanced threats including malware, PUPs, and adware and thoroughly removes them. Malwarebytes Incident Response improves your threat detection and the time it takes to respond to an attack with the added benefits of scalability, flexibility, and automation.



Malwarebytes cloud console dashboard

## References

<sup>1</sup>Incident response generally refers to the tools, processes, and talent that organizations use to address and mitigate a cyberattack once it's identified.

<sup>2</sup>Source: Ponemon Institute, 2016 Cost of Data Breach Study, June 2016.

## TECHNICAL FEATURES

### INCIDENT RESPONSE

#### Incident Response engine

Fast, extremely effective threat scanning with on-demand, scheduled, and automated options

#### Multiple scan modes

Hyper, Threat, and Custom scan modes won't interrupt end users

#### Linking Engine

Signature-less technology identifies and thoroughly removes threat artifacts linked with the primary threat payload

#### Malwarebytes cloud platform

Cloud-based management console provides easy, centralized security policy management, deployments, and threat reporting

#### Asset Management

Supplies convenient endpoint system details, including memory objects, installed software, startup programs, and more

#### Forensic Timeliner

Gathers and arranges Windows log events in a single chronological view

## Key benefits

### Automation

You can pre-deploy Malwarebytes Incident Response on your endpoints to have advanced threat detection and remediation ready at the click of a button. It also integrates with your existing endpoint management, SIEM, and threat detection tools to automatically respond to incident alerts. By automating threat responses, businesses can accelerate their incident response workflows while reducing attack dwell times.

### Flexibility

Malwarebytes Incident Response uses a unified persistent agent and also includes non-persistent agent options (Breach Remediation). This provides flexible deployment options for varying business IT environments. Malwarebytes easily integrates into your existing security stack while meeting your operating system (Windows and Mac OS X) and infrastructure requirements.

### Scalability

Malwarebytes Incident Response is delivered via our new Malwarebytes cloud-based endpoint management platform. The Malwarebytes cloud platform reduces complexity, making it easy to deploy and manage Malwarebytes Incident Response and other Malwarebytes solutions, regardless if you have one or 1 million endpoints. This centralized cloud console eliminates the need to acquire and maintain on-premises hardware.

<sup>1</sup>Persistent Windows and Mac OS X agents

<sup>2</sup>Non-persistent Windows CLI, Mac GUI, Mac CLI agents

## SYSTEM REQUIREMENTS

### Included Components

Malwarebytes cloud platform  
Malwarebytes Incident Response<sup>1</sup>  
Breach Remediation<sup>2</sup>  
Forensic Timeliner (Windows)  
Email and phone support

### Hardware Requirements

#### Windows

CPU: 1 GHz, RAM: 1 GB (clients); 2 GB (servers) Disk space: 100 MB  
Active Internet connection

#### Mac

Mac OS X (10.10 or newer)  
Active Internet connection

### Supported Operating Systems

Windows 10® (32-bit, 64-bit)  
Windows 8.1® (32-bit, 64-bit)  
Windows 8® (32-bit, 64-bit)  
Windows 7® (32-bit, 64-bit)  
Windows Vista® (32-bit, 64-bit)  
Windows XP® with SP3 (32-bit only)  
Windows Server 2016® (32-bit, 64-bit)  
Windows Server 2012/2012R2® (32-bit, 64-bit)  
Windows Small Business Server 2011  
Windows Server 2008/2008R2® (32-bit, 64-bit)  
Windows Server 2003® (32-bit only)  
macOS 10.13 (High Sierra)  
macOS 10.12 (Sierra)  
macOS 10.11 (El Capitan)  
macOS 10.10 (Yosemite)

*Please note that Windows servers using the Server Core installation process are specifically excluded.*

*Windows Action Center integration not supported for Windows Server operating systems.*

## REQUEST A TRIAL

Visit

[malwarebytes.com/business/trial/](https://malwarebytes.com/business/trial/)



[malwarebytes.com/business](https://malwarebytes.com/business)



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](https://www.malwarebytes.com).

Copyright © 2018, Malwarebytes. All rights reserved. Malwarebytes and the Malwarebytes logo are trademarks of Malwarebytes. Other marks and brands may be claimed as the property of others. All descriptions and specifications herein are subject to change without notice and are provided without warranty of any kind.