Malwarebytes

DATA SHEET

Malwarebytes Incident Response

Centralized threat detection and remediation

TECHNICAL FEATURES

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

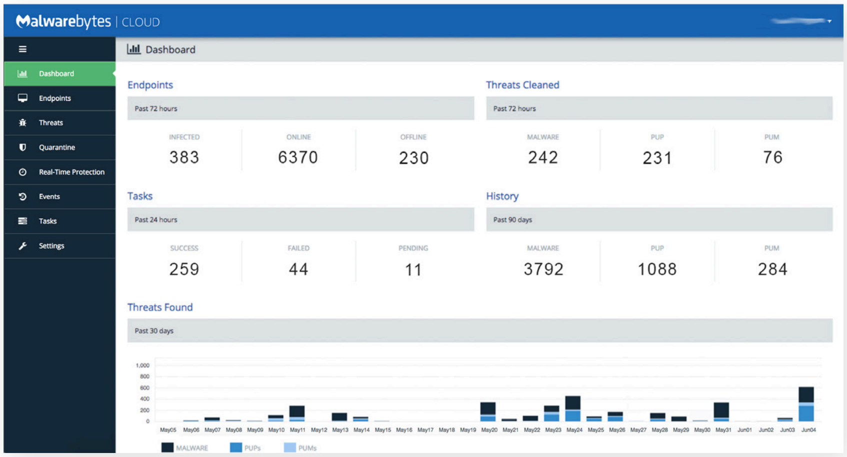
Supplies convenient endpoint system details, including memory objects, installed software, startup programs, and more

Forensic Timeliner

Gathers and arranges Windows log events in a single chronological view

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[1] 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[2]. 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
≡
Dashboard
Endpoints
Threats
Quarantine
Real-Time Protection
Events
Tasks
Settings
Dashboard
1,000
800
600
400
200
0
May05 May06 May07 May08 May09 May10 May11 May12 May13 May14 May15 May16 May17 May18 May19 May20 May21 May22 May23 May24 May25 May26 May27 May28 May29 May30 May31 Jun01 Jun02 Jun03 Jun04
MALWARE
PUPs
PUMs

Endpoints

Past 72 hours

INFECTED	ONLINE	OFFLINE
383	6370	230

Threats Cleaned

Past 72 hours

MALWARE	PUP	PUM
242	231	76

Tasks

Past 24 hours

SUCCESS	FAILED	PENDING
259	44	11

History

Past 90 days

MALWARE	PUP	PUM
3792	1088	284

Threats Found

Past 30 days

Malwarebytes cloud console dashboard

References

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

[2] Source: Ponemon Institute, 2016 Cost of Data Breach Study, June 2016.

Key benefits

Automation

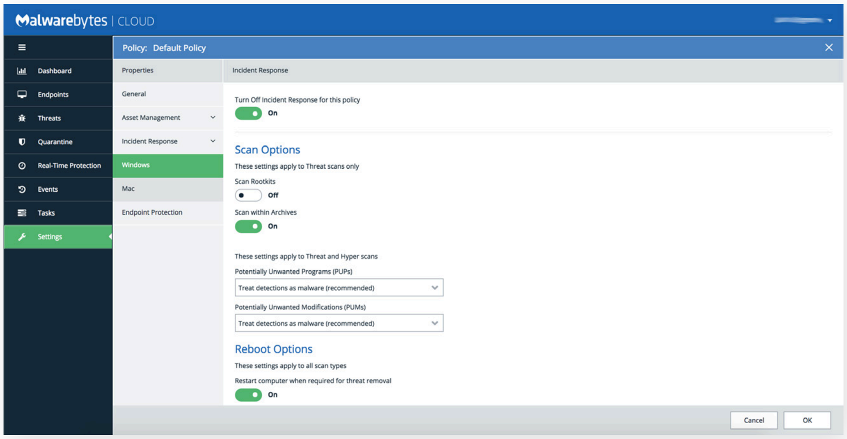
You can pre-deploy Malwarebytes Incident Response on your endpoints to have advanced threat detection and remediation ready at the click of a button. It also integrates with your existing endpoint management, SIEM, and threat detection tools to automatically respond to incident alerts. By automating 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.



Policy: Default Policy

Incident Response

Turn Off Incident Response for this policy
On

Scan Options

These settings apply to Threat scans only

Scan Rootkits
Off

Scan within Archives
On

These settings apply to Threat and Hyper scans

Potentially Unwanted Programs (PUPs)
Treat detections as malware (recommended)

Potentially Unwanted Modifications (PUMs)
Treat detections as malware (recommended)

Reboot Options

These settings apply to all scan types

Restart computer when required for threat removal
On

Malwarebytes Incident Response security policy settings

SYSTEM REQUIREMENTS

Included Components

- Malwarebytes cloud platform
- Malwarebytes Incident Response (persistent Windows and Mac OS X agents)
- Breach Remediation (non-persistent Windows CLI, Mac GUI, Mac CLI agents)
- Forensic Timeliner (Windows)
- Email and phone support

Hardware Requirements

Windows
CPU: 1 GHz
RAM: 1 GB (clients); 2 GB (servers)
Disk space: 100 MB (program + logs)
Active Internet connection

Mac
Any Apple Mac device that supports
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)
Mac OS X (10.10 or newer)

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.*

malwarebytes.com   corporate-sales@malwarebytes.com   1.800.520.2796

Malwarebytes is the next-gen cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against dangerous threats such as malware, ransomware, and exploits that escape detection by traditional antivirus solutions. The company's flagship product combines advanced heuristic threat detection with signature-less technologies to detect and stop a cyberattack before damage occurs. More than 10,000 businesses worldwide use, trust, and recommend Malwarebytes. Founded in 2008, the company is headquartered in California, with offices in Europe and Asia, and a global team of threat researchers and security experts.

Copyright © 2017, 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.