



Malwarebytes Nebula Quick Start Guide

2020



Table of Contents

- [Introduction](#)
- [Minimum specifications](#)
- [External access requirements](#)
- [Anti-Virus and firewall exclusions](#)
- [Deploy your endpoints](#)
- [Understanding Nebula subscriptions](#)
- [Subscription comparison](#)
- [What's an Endpoint Policy](#)
- [Configure policy options](#)
- [Incident Response policy considerations](#)
- [Endpoint Protection policy considerations](#)
- [Endpoint Detection and Response policy considerations](#)
- [Server policy considerations](#)
- [Groups overview](#)
- [Understand endpoints' status](#)
- [Scan types](#)
- [Generate reports](#)
- [Malwarebytes Support Tool and Excel Add-in](#)
- [Malwarebytes resources](#)

Introduction to Malwarebytes Nebula

Nebula cloud console:

- Web-based centralized management tool that is responsible for discovery, deployment, management and administration of Malwarebytes agents on your company's endpoints.

Endpoint Agent:

- Intermediary software component in charge of direct communication between the Malwarebytes cloud console and installed Malwarebytes products.

Unmanaged remediation products:

- These products are designed to protect and remediate Windows/Mac endpoint from malware and adware. These extra options can be found within the Malwarebytes Nebula Downloads page.

Minimum specifications

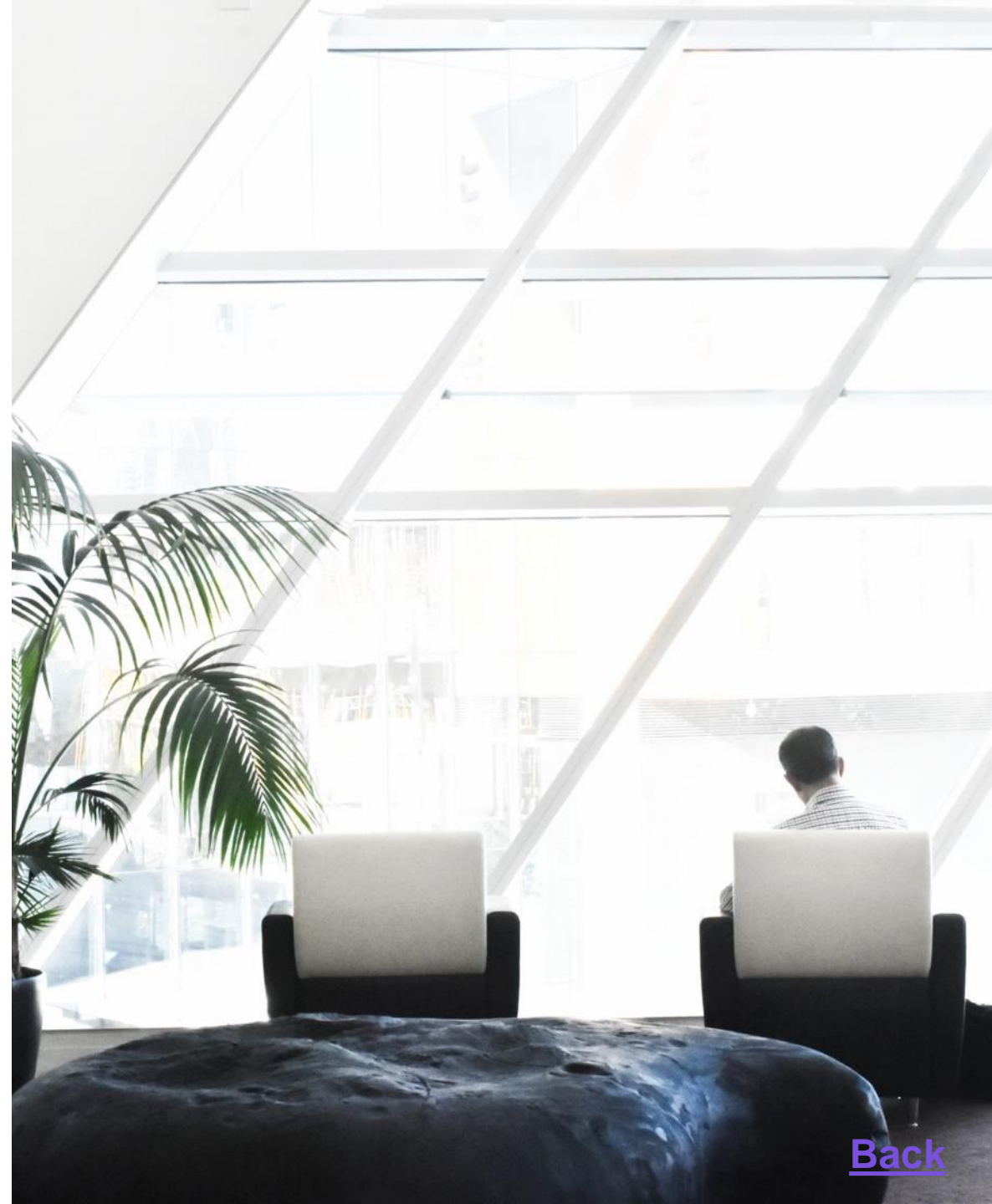
Prior to installing the Malwarebytes Endpoint Agent, confirm that endpoints meet our minimum specifications.

Console:

- Browser: Google Chrome

Endpoint Hardware (Windows):

- CPU: 1 GHz
- Disk Space: 100 MB (Program + Logs)
- Ram 1 GM (Client); 2 Gb (Server)



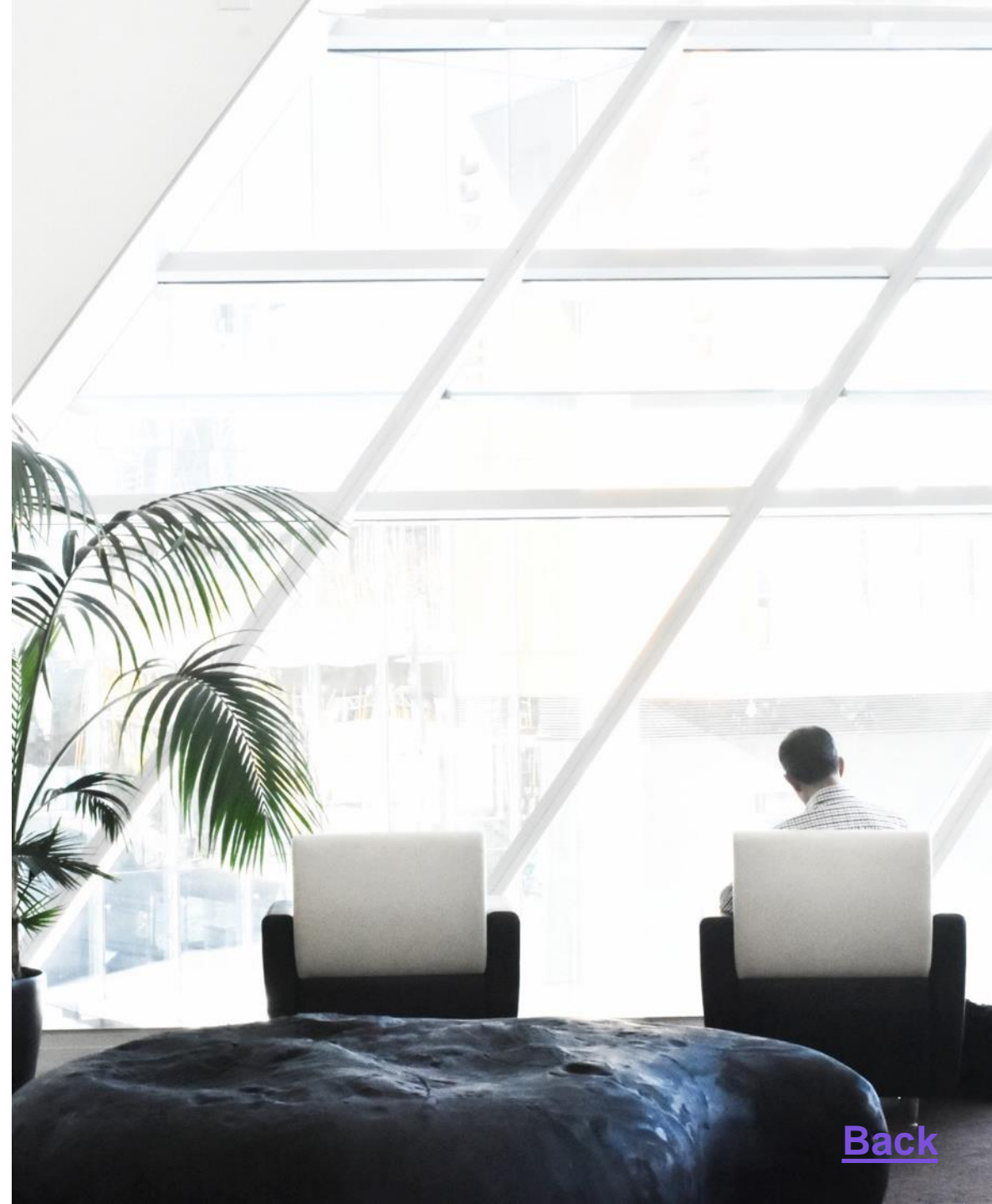
Minimum specifications (continued)

Endpoints Operating System (Windows):

- Windows Server 2016
- Windows Server 2012/2012 R2
- Windows SB Server 2011
- Windows Server 2008/2008 R2
- .Net 4.5.2 or 4.6 installed
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7
- Windows Vista
- Windows XP SP3 (32-bit only)

Endpoints Operating System (Mac):

- Minimum OS X 10.11 El Capitan or macOS 10.12 Sierra



External access requirements

If Internet access is controlled by a firewall or other access-limiting device, grant access for endpoint agents to reach the following Malwarebytes services on port 443 Outbound:

- <https://cloud.malwarebytes.com>
- <https://telemetry.malwarebytes.com>
- <https://detect-remediate.cloud.malwarebytes.com>
- <https://data-cdn-static.mbamupdates.com>
- <https://keystone.mwbsys.com>
- <https://keystone-akamai.mwbsys.com>
- <https://socket.cloud.malwarebytes.com>
- <https://sirius.mwbsys.com>
- <https://hubble.mb-cosmos.com>
- <https://blitz.mb-cosmos.com>
- <https://cdn.mwbsys.com>
- <https://ark.mwbsys.com>
- <https://storage.gra3.cloud.ovh.net>
- <https://nebula-agent-installers-mb-prod.s3.amazonaws.com/>



Anti-Virus and firewall exclusions

To prevent conflicts with our Malwarebytes Endpoint Agent, we recommend you exclude the following Malwarebytes folders and files in your firewall and other Anti-Virus programs:

- **For Windows endpoints:**

- %ProgramFiles%\Malwarebytes Endpoint Agent
- %ProgramData%\Malwarebytes Endpoint Agent
- %ProgramFiles%\Malwarebytes\Anti-malware
- %ProgramData%\Malwarebytes\MBAMService
- %ProgramFiles%\Malwarebytes Endpoint Agent\Plugins\Incident Response\Logs
- %SystemRoot%\system32\drivers\ESProtectionDriver.sys
- %SystemRoot%\system32\drivers\farflt.sys
- %SystemRoot%\system32\drivers\mbae.sys (mbae64.sys on an x64 system)
- %SystemRoot%\system32\drivers\mbam.sys
- %SystemRoot%\system32\drivers\MBAMChameleon.sys
- %SystemRoot%\system32\drivers\MBAMSwissArmy.sys
- %SystemRoot%\system32\drivers\mwac.sys
- %SystemRoot%\system32\drivers\flightrecorder.sys

- **For Mac endpoints:**

- /Library/Application Support/Malwarebytes/Malwarebytes Endpoint Agent
- /Library/Application Support/Malwarebytes/Malwarebytes Endpoint Agent/UserAgent.app
- /Library/LaunchDaemons/com.malwarebytes.EndpointAgent.plist





Deploy your Endpoints

Manual installation:

- This is a completely manual option and requires the user of each endpoint to first download the executable file directly onto the endpoint. (Remote, USB, File Share).

Third-party deployment tool:

- For use when you have your own deployment tool (SCCM, PDQ). Larger companies who already have a third-party tool for deploying licenses across their networks may choose to use our MSI installer.

Malwarebytes Discovery and Deployment Tool:

- Tool provided by Malwarebytes to deploy to endpoints. Can utilize Active Directory or IP Address.

Understanding Nebula subscriptions

Each Malwarebytes Nebula subscription serves a different purpose and must be configured in the Policy settings to provide proper functionality for your installed endpoints.

Incident Response (IR):

- Provides scheduled scanning of your endpoints based on your specifications, and on-demand scanning of areas where most malware hides. If a threat is detected, it is quarantined for later remediation.

Endpoint Protection (EP):

- Provides all functionality that IR offers, including our multi-layered Real-Time Protection modules (**Anti-Malware, Anti-Exploits, Behavioral Protection, and Malicious Web Control**).

Endpoint Detection and Response (EDR):

- Provides all functionality that IR and EP offers, including Suspicious Activity Monitoring and Flight Recorder search.

Subscription comparison

Endpoint Agent Features (Nebula) For more on features, Click Here	Incident Response (IR)	Endpoint Protection (EP)	Endpoint Detection and Response (EDR)
On-Demand Scans: Scans areas of your endpoints where malware usually resides.	●	●	●
Scheduled Scans: Automatically scans your endpoint based on specified schedules.	●	●	●
Quarantine: Isolates detected threats for later remediation.	●	●	●
Asset Management: See what software your endpoints have installed.	●	●	●
Real-Time Protection: Anti- Malware, Anti-Exploit, Web Protection, Anti-Ransomware protection layers actively stop threats.		●	●
Suspicious Activity Monitoring: Continuous monitoring and visibility of endpoint file system events, network connections, process events, and registry activity.			●
Ransomware Rollback: Up to 72 hours of protection for files encrypted, deleted, or modified by a ransomware attack.			●
Endpoint Isolation: Network, process, and desktop isolation stops malware from spreading to the rest of your environment from a compromised endpoint.			●
Aggressive Mode: Observes behaviors and actions of suspicious files, validating local Anomaly Detection Machine Learning verdicts.			●
Flight Recorder: Search event data captured from your managed endpoints to investigate and identify indicators of compromise.			●

What's an endpoint policy?

Each policy must be configured to provide proper functionality of the Malwarebytes Endpoint Agent on your endpoints.

Policy:

- A policy defines *Malwarebytes* behavior when running a scheduled scan, using Real-Time Protection, or monitoring Suspicious Activity. Initially there is a single policy, called the Default Policy. We recommend first time users assign endpoints to the Default Policy.

Note:

- While you can apply multiple groups to the same policy, you cannot apply multiple policies to the same group.
- You cannot delete the Default Policy.

Configure General, Settings, and Endpoint Interface options for your policy

General options:

General options include rebooting endpoints, applications that launch at startup, asset events, and protection updates.

Support article:

- [Configure General options in Malwarebytes Nebula platform](#)

Settings options:

Includes options for scans, Real-Time Protection and additional protection options, the Windows Action Center, and Malwarebytes Endpoint Detection and Response.

Support article:

- [Configure policy Settings options in Malwarebytes Nebula platform](#)

Endpoint Interface options:

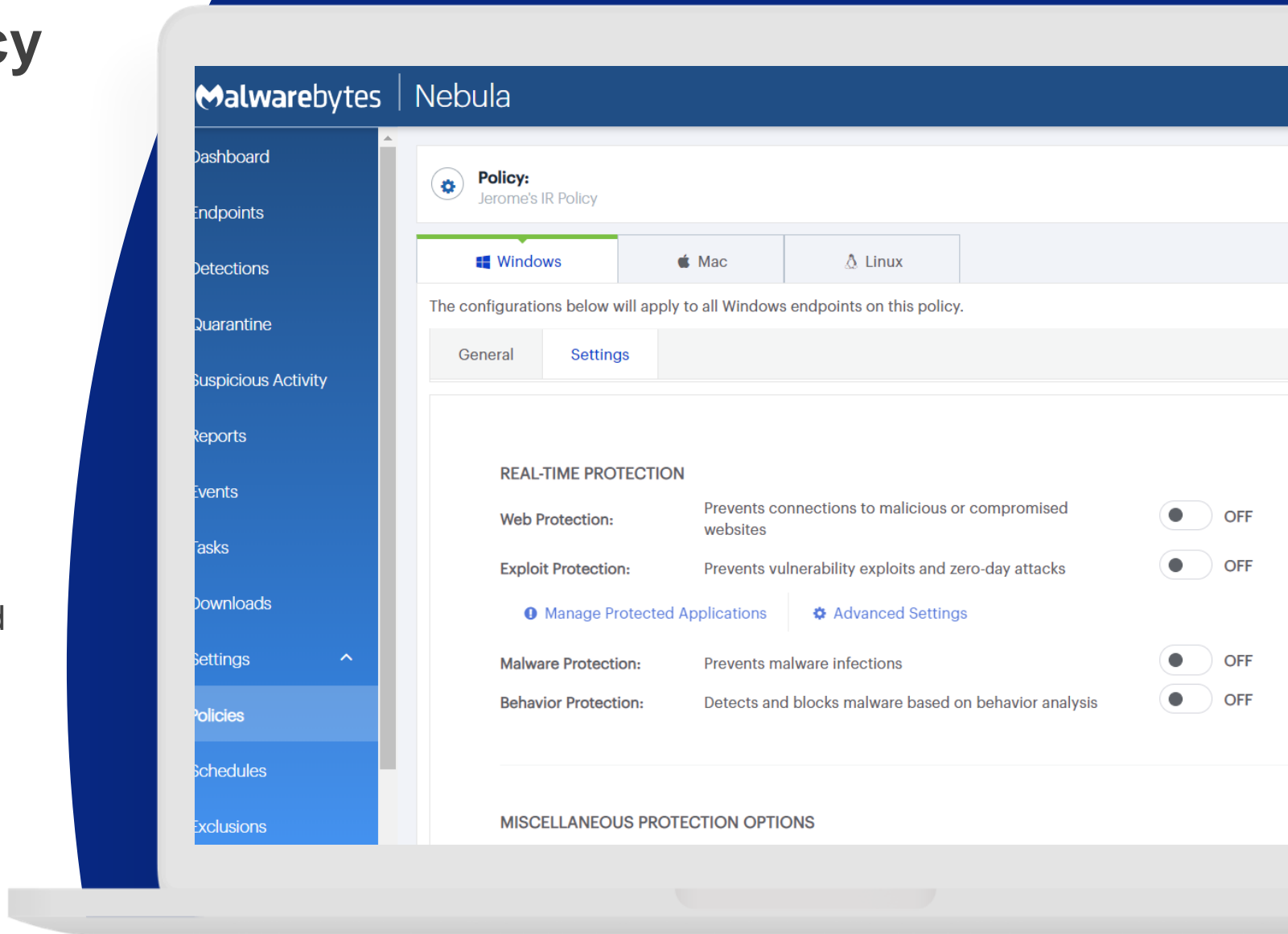
Endpoint Interface options enables you to customize how endpoint users interact with the Malwarebytes interface. These policy settings are applied to all endpoints in the group. Below this section you can set additional options that only apply to specific operating systems.

Support article:

- [Configure Endpoint Interface options in Malwarebytes Nebula platform](#)

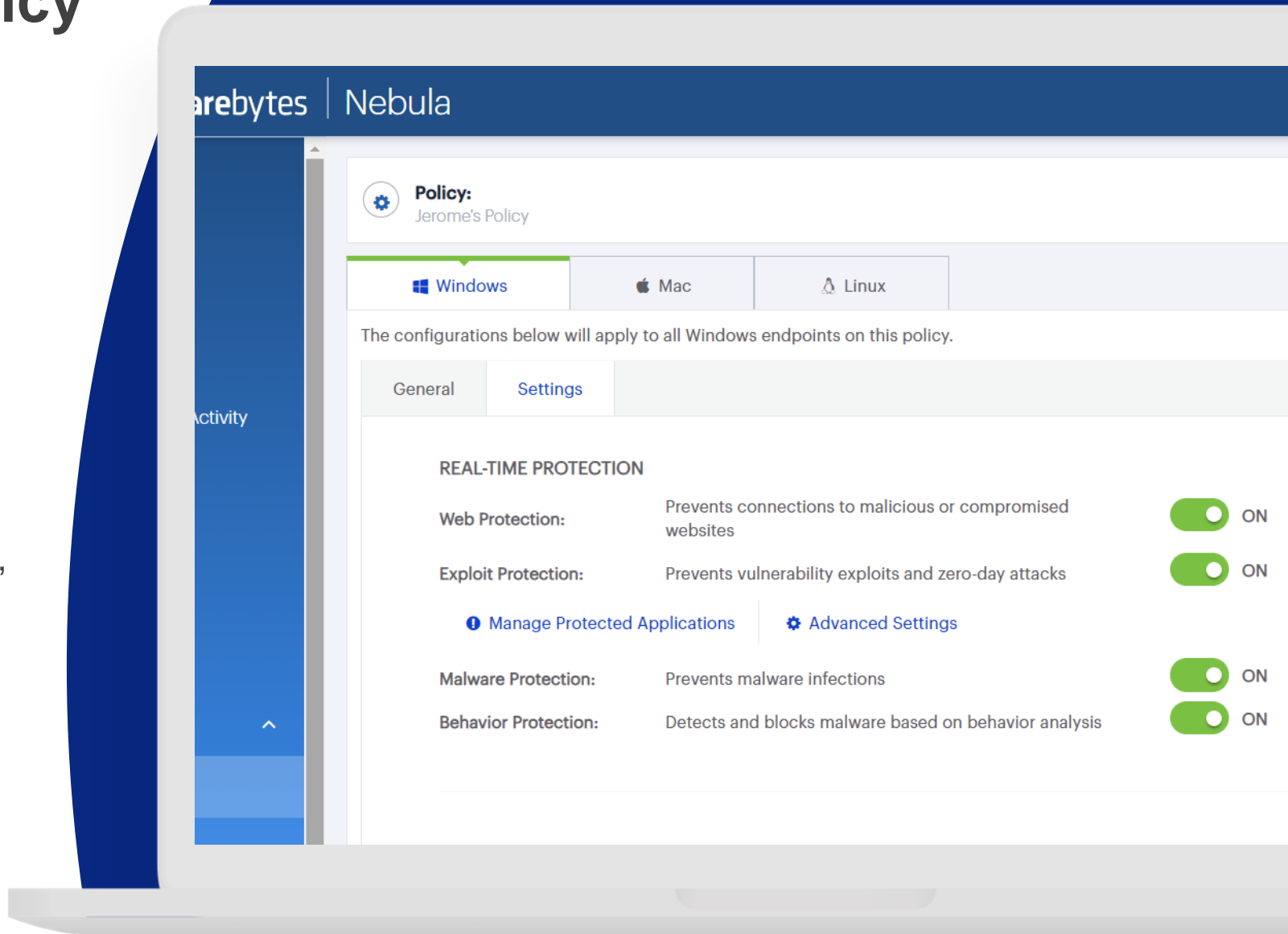
Incident Response policy considerations

- Malwarebytes Incident Response subscription does **not** include Real-Time Protection.
- For Incident Response subscriptions, the Real-Time Protection options are disabled and unable to turn on.



Endpoint Protection policy considerations

- By default, Real-Time Protection is turned on for EP and EDR subscriptions.
- For information on supported server roles, [click here](#).



Endpoint Detection and Response policy considerations

- By default, Suspicious Activity Monitoring is turned off unless enabled by a Super Admin.
- Suspicious Activity Monitoring is only available for endpoints running minimum Windows 7 operating systems.
- Suspicious Activity Monitoring and Rollback is not available on Server operating systems, but you may enable Endpoint Isolation on servers using Server 2008 R2, 2012 R2, or Server 2016.
- For more information on Malwarebytes Endpoint and Response, [click here](#).

The configurations below will apply to all Windows endpoints on this policy.

General Settings

Endpoint Detection and Response (EDR) Settings

SUSPICIOUS ACTIVITY MONITORING (EDR)

Suspicious Activity Monitoring: Allow Behavioral Monitoring for Suspicious Activity on endpoints ON

Aggressive Mode: Enables a very aggressive detection mode; this will result in additional file uploads to the Malwarebytes sandbox for deep analysis where needed OFF

RANSOMWARE ROLLBACK (EDR)

Enable/Disable Rollback: Allow for Rollback of files modified by any Suspicious Activity ON

Rollback Timeframe: Rollback (Rolling time to store changes) 24 Hours 72 Hours Max 72 Hours

Rollback File Size: Maximum size for individual file backups 1 MB 100 MB Max 100 MB

ENDPOINT ISOLATION (EDR)

Lock/Unlock Endpoints: Allow for Locking/Unlocking of Endpoints ENABLED

Isolation Title: Maximum 80 Characters

Isolation Message: Message to display to end-users when an endpoint is isolated
Maximum 255 Characters

Custom Icon Image: Icon to display on the custom message screen

Server policy considerations

Servers may encounter performance or network related issues when using a policy with Real-Time Protection features enabled. As an example, DNS/DHCP/DC servers may be unable to resolve hostnames when Web Protection is enabled.

Support articles:

- [Configure Malwarebytes Endpoint Protection Windows server roles](#)
- [Disable real-time protection to avoid server conflicts](#)

The screenshot displays the Malwarebytes Nebula management console. The left sidebar contains navigation options: Dashboard, Endpoints, Detections, Quarantine, Suspicious Activity, Reports, Events, Tasks, Downloads, Settings, Policies, Schedules, Exclusions, and Groups. The main content area shows the configuration for a policy named 'Jerome (server)' for Windows endpoints. The 'Settings' tab is selected, showing the following configuration:

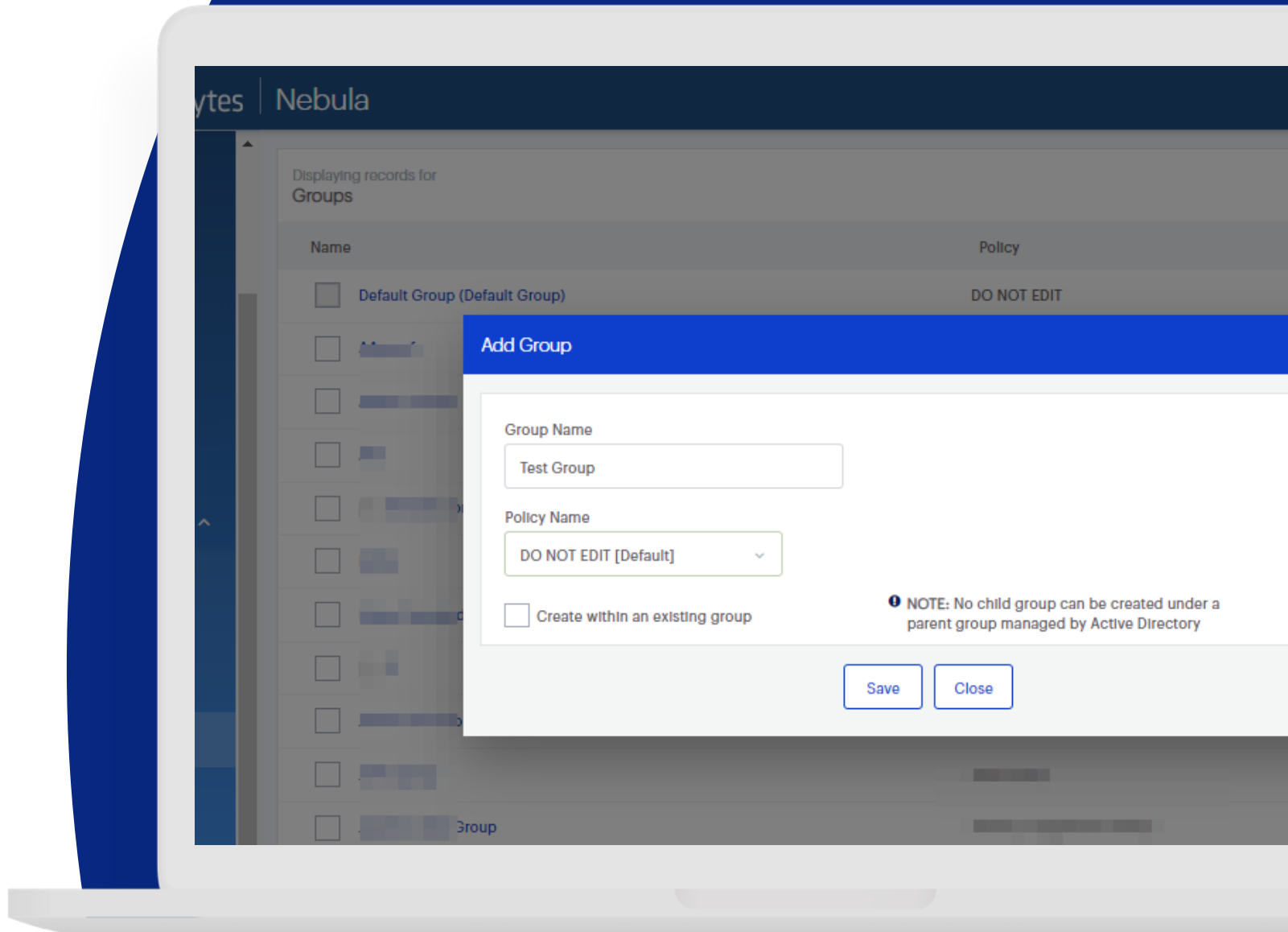
Setting	Description	Status
REAL-TIME PROTECTION		
Web Protection:	Prevents connections to malicious or compromised websites	OFF
Exploit Protection:	Prevents vulnerability exploits and zero-day attacks	ON
Manage Protected Applications Advanced Settings		
Malware Protection:	Prevents malware infections	ON
Behavior Protection:	Detects and blocks malware based on behavior analysis	OFF
MISCELLANEOUS PROTECTION OPTIONS		
Delay Real-Time Protection:	Delay Real-Time Protection when Malwarebytes starts	
Delay protection for:	Adjust the Real-Time protection delay	
Enable Self-Protection Module:	Protect Malwarebytes from targeted threats	

What's an endpoint group?

- Groups are used to join several endpoints into one functional area, allowing you to manage them simultaneously with one policy.
- You can create and customize groups to fit your environment's needs.
- You can move endpoints from one group to another.
- Groups cannot share endpoints.
- For more information, see [Manage groups in Malwarebytes Nebula](#).












Note:

- Each policy must have a unique name. You can rename a policy at any time by editing the Policy Name field.
- While you can apply multiple groups to the same policy, you cannot apply multiple policies to the same group.
- For more information, see [Overview of groups in Malwarebytes Nebula](#).



Understanding the status of your endpoints

- In the Endpoints page, the Status column shows icons to help quickly identify endpoints that need attention. The table on the right shows the different status icons that you may see while using the Nebula console, along with a brief description.

ICON	STATUS
	The endpoint has not run a <i>Malwarebytes</i> scan for a long period of time. A scan should be run to check for threats.
	A scan is pending on the endpoint.
	A scan is currently running on the endpoint.
	The endpoint has threats that were detected during a scan that need to be remediated.
	Remediation of threats is pending on the endpoint.
	The endpoint is actively undergoing remediation.
	The endpoint should be restarted to completely quarantine items found during a scan.
	A restart command was issued to the endpoint and is currently pending.
	The endpoint is restarting and the console is waiting for it to reconnect.
	Suspicious activity was detected on the endpoint. This is only available to <i>Endpoint Protection and Response</i> customers.
	The endpoint is currently isolated. This is only available to <i>Endpoint Protection and Response</i> customers.

Scan types

Threat Scan:

- Memory Objects
- Startup Objects
- Registry Objects
- File System Objects
- Heuristic Analysis

Hyper Scan:

- Memory Object
- Startup Object

Support articles:

- [Set scan schedules in Malwarebytes Cloud Platform](#)
- [Types of Malwarebytes Cloud Platform scans](#)

Custom Scan:

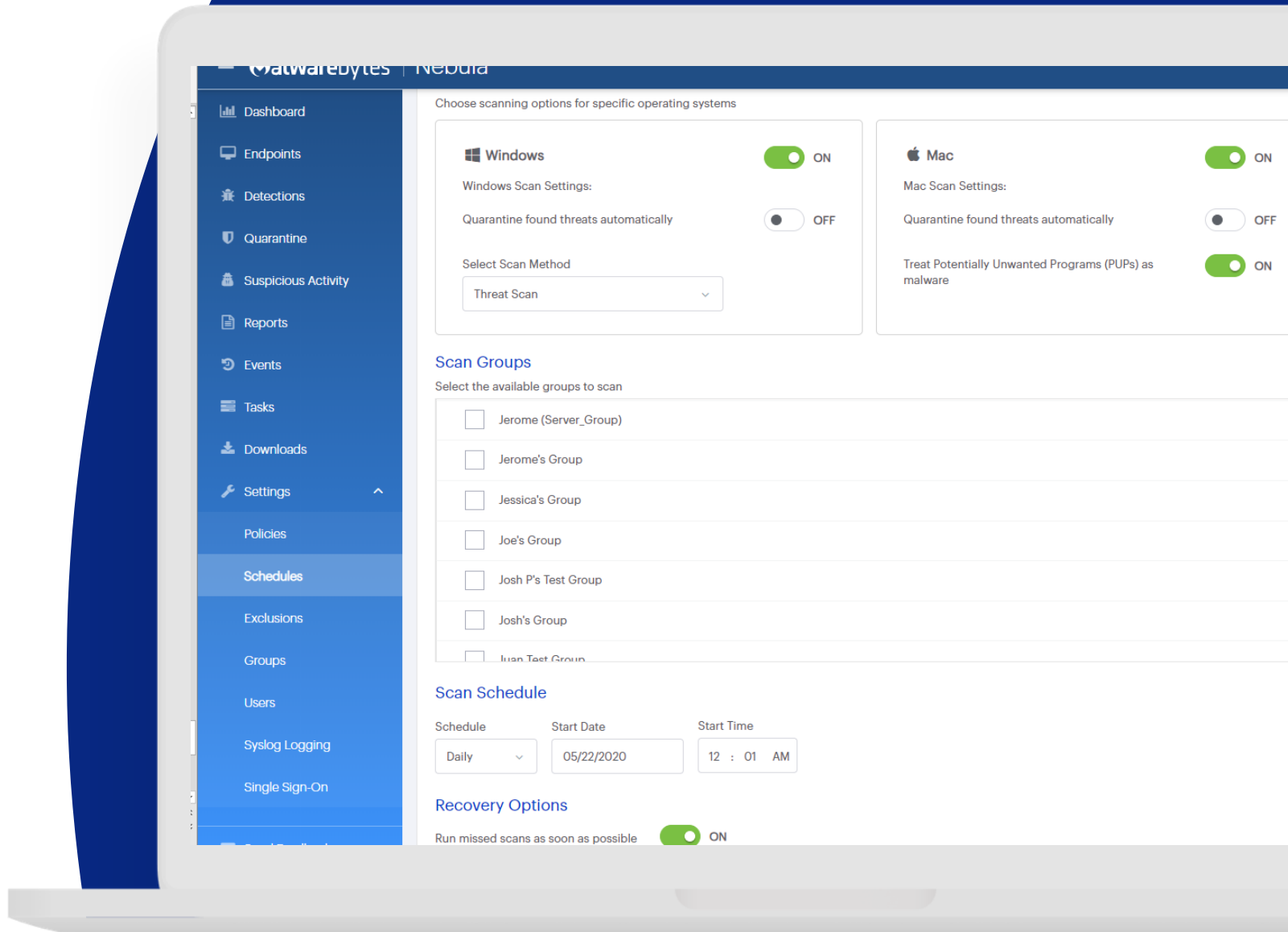
- Quarantine found threats automatically
- Scans memory objects
- Scans startup and Registry
- Rootkits

Recovery options:

- Runs missed scans on next check in

Note:

- Options defined in Schedules will override scan options defined in Policy Settings.



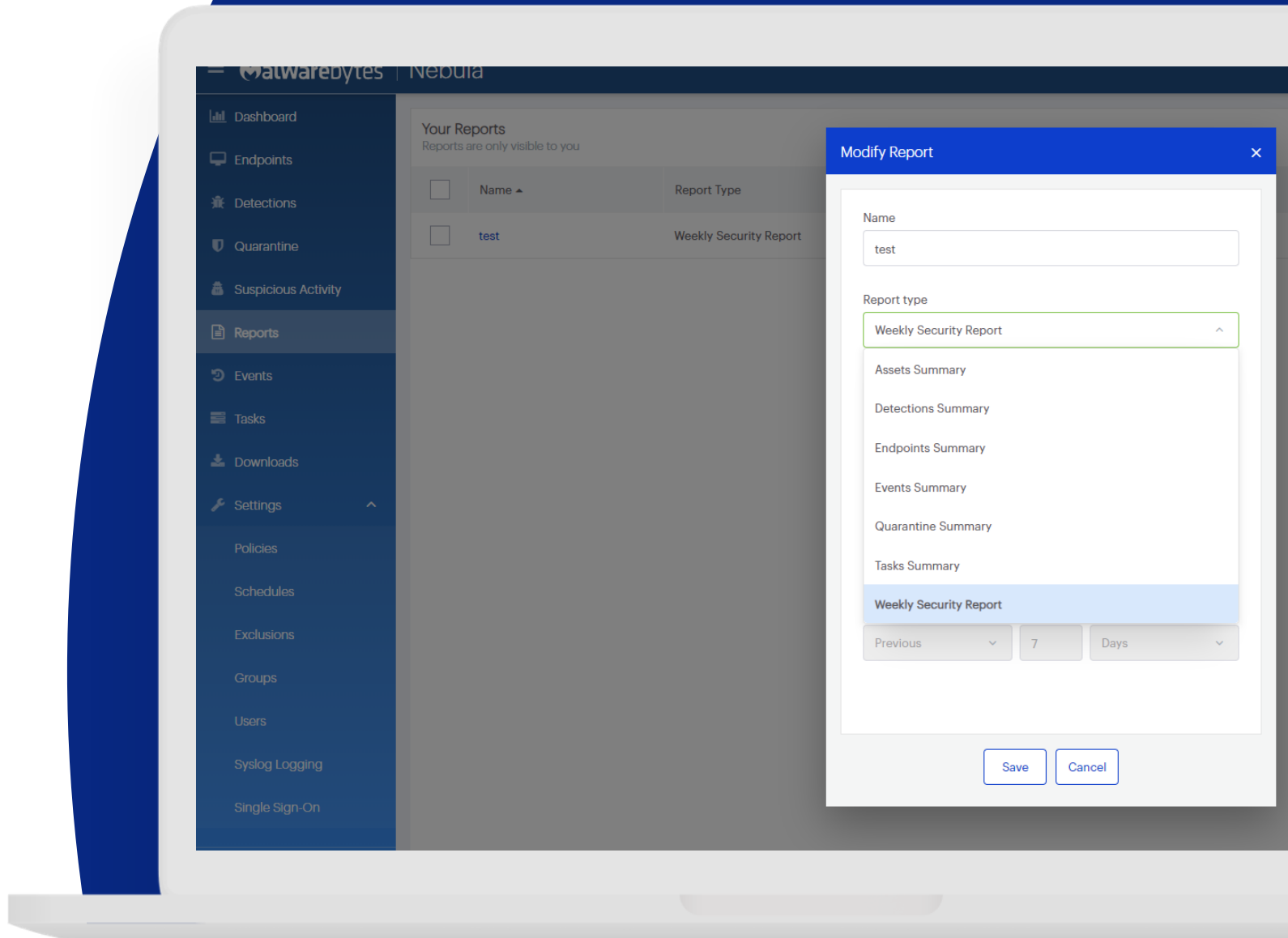
Generate reports

Report types:

- Assets Summary
- Detections Summary
- Endpoints Summary
- Events Summary
- Quarantine Summary
- Task Summary
- Weekly Security Report

Examples of security report metrics:

- Endpoint activity status (current state)
- Protection summary (current state)
- Endpoints needing attention (current state)
- Top five operating systems (current state)
- Detections by category (past week)
- Top five threats (past week)
- Top five at-risk endpoints (past week)



Malwarebytes Support Tool (Uninstaller) and Malwarebytes Excel Add-in Tool

Malwarebytes Support tool:

- The Malwarebytes Support Tool command line version is used to cleanup and remove Malwarebytes products. The Support Tool removes Malwarebytes Endpoint Security and Malwarebytes Endpoint Protection, including their files, settings, and license information. To remove Malwarebytes software from a Windows endpoint, download the Support Tool, then run it from the Command Prompt.
- For more information on Malwarebytes Support Tool, [click here](#)

Malwarebytes Excel Add-in Tool:

- The Malwarebytes Nebula server collects a rich set of information from the endpoints and a common request we get is to turn this data into useful information. Malwarebytes provides a complete set of RESTful APIs for this purpose. The Nebula console uses these same APIs to extract the data. However, it does require some scripting and technical work to make the data useful. To make this easier for you, we have introduced the Malwarebytes Excel Add-in, which provides easy access to import data directly into Microsoft Excel.
- For more information on Malwarebytes Add-in Tool, [click here](#)

Additional Resources

[Back](#)

Contact Support: Reach out to our support team for any additional help.

- Support Ticket: <https://support.malwarebytes.com/hc/en-us/requests/new>
- Phone: 1-888-688-5431

Business Support Portal: To look up Support articles.

- <https://support.malwarebytes.com/>

Malwarebytes Academy: Sign up, and take our free e-learning courses.

- <https://academy.malwarebytes.com/learn>

Malwarebytes Labs: Stay up to date with the latest threats.

- <https://blog.malwarebytes.com/>

Thank You!

Questions?