OneView BEST PRACTICES

This Malwarebytes OneView best practices guide covers the recommended settings for your OneView console. It is intended to provide a general guidance on configuring your OneView console.

Our OneView solutions build on each other, so as you move forward with Endpoint Protection or Endpoint Detection and Response recommendations below, ensure that suggestions for Incident Response are followed as well.

		INCIDENT RESPONSE (IR)	ENDPOINT PROTECTION (EP)	ENDPOINT DETECTION & RESPONSE (EDR)
SCHEDULES	GENERAL CONSIDERATIONS	Create a Daily Software Inventory Scan, Daily Threat Scan and Weekly Custom Scan under Schedules in OneView. For more information, see Set scheduled scans in OneView. If you create additional groups in OneView and assign endpoints to them, revisit your schedules to include those groups in the scans. Scheduled scans run using the endpoint's locally configured time.	For servers, we recommend creating separate scans that run during the evening or low utilization periods.	
	DAILY SOFTWARE INVENTORY SCAN	The daily software inventory scan keeps the console updated with asset information like hardware, startup programs, and installed software programs and versions. Make the following selections: • **Type**: Software Inventory scan • **Frequency**: Daily		
	DAILY THREAT SCAN	A daily threat scan is important for regularly checking for any threats on your endpoints. Select and enable the following options: • **Type**: Detections scan. • **Quarantine threats automatically**: Allow Malwarebytes to remove threats without additional user action. • **Scan method**: Threat Scan. • **Run missed schedules as soon as possible**: Scheduled scans will run when the endpoint is online If it was offline during the configured time. • **Frequency**: Daily		
	WEEKLY FULL SCAN	A weekly full scan is the most thorough scan and utilizes the most resources. Select and enable the following options: • **Type**: Detections scan. • **Quarantine threats automatically**: Allow Malwarebytes to remove threats without additional user action. • **Scan method**: Custom Scan. • **Treat Potentially Unwanted Programs (PUPs) as malware**: Detect and clean PUPs. • **Treat Potentially Unwanted Modifications (PUMs) as malware**: Detect and clean PUMs. • **Scan all local drives on endpoints**: Includes all connected drives and removable storage devices. • **Frequency**: Weekly		

		INCIDENT RESPONSE (IR)	ENDPOINT PROTECTION (EP)	ENDPOINT DETECTION & RESPONSE (EDR)
EXCLUSIONS	GENERAL CONSIDERATIONS	Exclude your software applications from being flagged or monitored by Malwarebytes with the Exclusions page. For more information, see Create and edit exclusions in OneView. We recommend toggling on **Exclude GPO PUMs**. This setting prevents Malwarebytes from flagging intentional Group Policy registry modifications. For a list of keys included in this toggle, see Group Policy registry keys detected as PUMs in Endpoint Protection.		
POLICIES	SCAN SETTINGS	This section covers settings for scans like the types of files detected and if potentially unwanted programs and potentially unwanted modifications should be treated as malware. For more information, see Configure Scan settings in OneView. We recommend keeping everything enabled here except for **Scan for rootkits**, as enabling this will prolong scans and is not necessary for identifying threats.		
	TAMPER PROTECTION	Tamper Protection adds an additional layer of protection to Malwarebytes, should a malicious actor enter your environment. For more information, see Configure Tamper protection options in OneView. • **Uninstall Protection**: Requires additional authentication to uninstall Malwarebytes from the endpoint. Use a different password than any OneView administrator password in case of account compromise. • **Service and Process Protection**: Prevents all users and admins from tampering with Malwarebytes services.		

	ENDPOINT AGENT	Endpoint agent settings control how the Malwarebytes Endpoint Agent software interfaces with the endpoint. For more information, see Configure Endpoint agent settings in OneView.
		
		• **Endpoint agent updates:** Control when endpoints receive Malwarebytes software updates.
		  ○ **Automatically download and install Malwarebytes application updates**: This option only applies to Protection Service updates. Component Package updates are always automatic!
		  ○ If needed, use **Pause Software Updates** to prevent updates from installing for up to 31 days. After 31 days, endpoints resume receiving software updates.
		• **Reboot settings:** Automatically reboot endpoints when required for installation, updates, uninstallation, and detection removal.
		• **Inactive endpoints**: Keep your endpoints list accurate by automatically removes endpoints not seen after a set number of days.
		• **Startup options**: Ensure Malwarebytes Services can start by providing all services with additional time to start.
		• **Health monitoring**: Launches a secondary service on Windows endpoints via Service Control Manager (SCM) designed to monitor the Endpoint Agent service and restart it if it is an unhealthy state.
			For servers, we recommend changing a few endpoint agent settings. For more information, see Configure Protection settings in OneView.
			
			• **User interface options:** Controls the Endpoint Agent interface settings on an endpoint.
			  ○ **Allow only Administrator level users to interact with the Malwarebytes Tray:** Prevents the tray icon from loading on standard level user accounts. This is helpful for multi-user environments such as Microsoft Terminal Services.
			• **Endpoint agent updates**
			  ○ **Automatically download and install Malwarebytes application updates**: Disable this to prevent servers from automatically updating. Manually update servers during your scheduled maintenance windows.
			• **Reboot settings:** Disable this to prevent servers from automatically rebooting after an installing an update or quarantining a threat.	

	INCIDENT RESPONSE (IR)	ENDPOINT PROTECTION (EP)	ENDPOINT DETECTION & RESPONSE (EDR)

PROTECTION SETTINGS		This section covers how Malwarebytes protects your devices from threats. For more information, see Configure Protection settings in OneView.
		• **Real Time Protection**: These settings control which protection layers are enabled to protect your devices in real-time. It is recommended to keep these enabled. For servers, see Configure Windows server roles for Nebula.
		  ○ **Web Protection**: Blocks access to and from known or suspicious Internet addresses.
		  ○ **Exploit Protection**: Guards against vulnerability exploits for installed applications. When applications launch, Exploit Protection shields them.
		  ○ **Malware Protection**: Protects against malicious content that tries to execute on your endpoints.
		  ○ **Behavior Protection**: Safeguards against both known and unknown ransomware. Ransomware often remains undetected until it activates. Behavior Protection is not supported on endpoints with Windows XP or Windows Vista.
		  ○ **Block untrusted applications (Mac only)**: Prevents applications published by known bad developers from being executed on your endpoints.
		• **Additional Protection**: Other protection methods available with Malwarebytes that focus on other threat vectors.
		  ○ **Self-Protection**: Prevents malicious control of Malwarebytes software.
		  ○ **Device Control**: Controls the ability to use USB storage devices on Windows endpoints. Support for macOS is targeted for release later this year. For more information, see Device Control in OneView.
		  ▪ **Read only access to the device**: Allow copying files from the device and block modifying or copying files to the device.
		  ▪ **Block access to the device**: Block modifying and copying files to the device.	

BRUTE FORCE PROTECTION		Enabling Brute Force Protection (BFP) on your console protects Windows endpoints from suspicious connections via remote devices. For more information, see Configure Brute Force Protection in OneView. • **Windows and server protocols**: Enable this setting and enter your designated RDP port. If no port is set, Malwarebytes will automatically detect which port is used for RDP. ○ **Note:** When BFP is configured to **Block**, Windows Firewall is required and automatically enabled. If you are unable or unwilling to have Windows Firewall enabled, you can still configure BFP to **Monitor and detect**. Once enabled by block mode, Windows Firewall must be manually turned off as	

		INCIDENT RESPONSE (IR)	ENDPOINT PROTECTION (EP)	ENDPOINT DETECTION & RESPONSE (EDR)
			disabling BFP or switching to **Monitor and detect** will not turn the Windows Firewall off. For servers, enable and configure each **server-only protocol** as it applies to your environment.	

ENDPOINT DETECTION & RESPONSE				This section covers all the settings available for EDR. For more information, see Configure Endpoint Detection and Response options in OneView.
				
				• **Suspicious Activity Monitoring**: Allows behavioral monitoring for suspicious activity on endpoints.
				  ○ Advanced settings
				  ▪ **Collect networking events to include in searching**: Enable to allow searching for contacted domains and IPs in flight recorder.
				• **Ransomware Rollback**: Allows for rollback of files modified by any Suspicious Activity. Set the rollback timeframe to 72 hours for maximum coverage. Suspicious Activity Monitoring must be enabled to use this feature.
				• **Enable Endpoint Isolation:** Allows locking and unlocking of endpoints to prevent further distribution of threats and provides additional time to investigate malicious threats within your organization. Customize the isolation title, message, and image as needed.
				
				For servers, you must check **Enable server operating system monitoring for suspicious activity** under advanced settings to utilize EDR for Servers.

FLIGHT RECORDER	FLIGHT RECORDER SEARCH			On the Flight Recorder page, click the settings button in the top right and toggle on **Enable Flight Recorder Search** to enable endpoint data indexing for threat investigation. For more information, see Flight Recorder in OneView.