Malware Protection (Armor Anywhere)

This topic only applies to **Armor Anywhere** users.

To fully use this screen, you must add the following permission to your account:

- Read AVAM
- Writer Trend Manual Scan
- Read Trend Manual Scan

View malware events

The **Total Malware Events** table displays detected malware events from the past 30 days. You can click the widget to filter the data in the table below the widgets.

The Malware Protection subagent detects the following malware types:

- TROJAN (TROJ)
- WORM
- EICAR (VIRUS)
- VIRTUS
- RANSOM (RANSOMWARE)
- SPYWARE
- ADWARE
- COINMINER (COIN_MINER)

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Malware Protection**.
3. Review the widgets for malware events.

Widget	Description
Clean	This widget indicates that the infected file was cleaned.
Pass	This widget indicates that no action was taken on the infected file.
Quarantine	This widget indicates that the file was renamed, and then moved to a temporary location.
Delete	This widget indicates that an infected file was deleted.
DenyAccess	This widget indicates that an infected file has restrictive access. As a result, no action was taken.
Other	This widget indicates all other possible actions performed on the infected file, such as renaming the file.

4. (Optional) Click a widget to filter the table.

Column	Description
Name	This column displays the name of the virtual machine or instance.
Malware Name	This column displays the name of the malware detected in your virtual machine or instance.
File Name	This column displays the location of the malware detected in your virtual machine or instance.

Action Taken	This column displays the action that took place in the file where the malware was detected: • Cleaned • Passed • Quarantined • Deleted • Denied Access • Other
Date	This column displays the date when the malware was detected.

View service health data for Malware Protection

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Malware Protection**.
3. Navigate to the **Malware Protection Service** table.
4. The status icons above the **Malware Protection Service** table indicate the overall Malware Protection status for all of your instances. There are three status types:
    - **OK** (in green) indicates that your server's agent has communicated (hearbeated) with Armor.
    - **Warning** (in yellow) indicates that your server's agent appears to be reporting behind its expected timelines.
    - **Needs Attention** (in red) indicates that your server's agent has not properly communicated (heartbeated) with Armor.

Column	Description
Name	For Armor Complete, the name of the virtual machine you created in AMP. For Armor Anywhere, the name of the instance that contains the installed Anywhere agent, which includes the Malware Protection subagent.
Provider	For Armor Complete, the entry will display **Armor**. For Armor Anywhere, the name of the public cloud provider for the instance will appear.
Last Communication Date	The date and time that the Malware Protection subagent last communicated with Armor. • **Never** displays if your server's agent has not run a Malware scan.
Last Scan	The date and time of the last Malware scan. • **Never** indicates that your server's agent has not run a Malware scan. • **Persistent** indicates that your server's agent has real-time scanning enabled.
Scan	The **Scan** button will display if your subagent has heartbeated within the last four hours, AND a scan is not already in progress for the virtual machine or instance. The **Scan** button will NOT display if an initial Malware scan has not been run, nor if your sub-agent has not heartbeated for that particular virtual machine or instance within the last four hours. ⚠ The Scan button will be disabled if there are five active scans running on your account.

⚠ The number of active scans will display in the top right corner of the table.

⚠ To learn how the overall Malware Protection status is determined, see Understand service health data for Malware Protection.

Understand service health data for Malware Protection

In the **Malware Protection** screen, the **Malware Protection Service** table displays the various malware protection statuses of your virtual machines or instances:

- **Green** indicates a virtual machine in a **Secured** Malware Protection status.

- **Yellow** indicates a virtual machine in a **Warning** Malware Protection status.
- **Red** indicates a virtual machine in a **Critical** Malware Protection status.

The **Malware Protection** status can change based on the following two conditions:

- The date of your last scan (**Last Scan**)
- The date that Armor last received your data (**Last Communication Date**)

> ⚠ The overall status of your virtual machine is based on the individual status of your virtual machine's subcomponents (subagents), including Malware Protection.

Condition 1 - Date of last scan

If the last scan for **Malware Protection** took place between 7 to 13 days ago, then the **Malware Protection** status changes from **Secured** to **Warning**.

If the last scan for **Malware Protection** took place 14 days ago or more, then the **Malware Protection** status changes from **Warning** to **Critical**.

Date of last scan	Security status
7 to 13 days ago	Warning
14 days or more	Critical

Condition 2 - Date that Armor last received your data

If Armor last received data between 24 to 48 hours ago, then the **Malware Protection** status changes from **Secured** to **Warning**.

If Armor last received data over 48 hours ago, then the **Malware Protection** status changes from **Warning** to **Critical**.

Date of Armor receiving your data	Security status
24 to 48 hours ago	Warning
Over 48 hours	Critical

Armor labels the **Malware Protection** status based on the worst status of the two conditions. For example, if the date of your last scan was 9 days ago, but Armor last received your data 72 hours ago, then overall, the **Malware Protection** status is **Critical**.

View detailed Malware Protection data

The **Malware Protection** details screen displays the malware that has been detected in your virtual machine or instance. This screen only shows data for the last 90 days.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Malware Protection**.
3. Locate and select the desired virtual machine or instance.

Column	Description
Malware Name	The name of the malware detected in your virtual machine or instance.
File Name	The location of the malware detected in your virtual machine or instance.
Action Taken	The action taken against the malware: • Quarantine • Clean • Rename • Pass • Deny Access
Date	The date when the malware was detected.

Run a Malware scan

In the **Malware Protection** screen, you can run a manual scan for your virtual machine or instance.

- The **Scan** button will display for a particular virtual machine or instance if the sub-agent has heartbeated within the last four hours, AND a scan is not already in progress for that virtual machine or instance.
- The **Scan** button will NOT display if an initial scan has not been performed by Trend Micro, nor if the sub-agent has not heartbeated for that particular virtual machine or instance within the last four hours.
- The **Scan** button will be disabled if there are five active scans running on the account.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Malware Protection**.
3. Within the **Malware Protection Service** table, locate the desired virtual machine or instance, then click **Scan**.
    a. The **Scan** column will display **Scanning** while the scan is running.

The number of active scans will display in the top right corner of the table.

View Malware scan activity

In the **Malware Protection** screen, on the **Scan Activity** tab, you can view details on current and past scans.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Malware Protection**.
3. Click **Scan Activity**.

The number of active scans will display in the top right corner of the table.

COLUMN	DESCRIPTION
Name	This column displays the name of the virtual machine or instance.
User	This column displays the name of the user who initiated the scan.
Time Started	This column displays the date and time that the scan was initiated.
Last Updated	This column displays the date and time of the last status check for the scan.
Status	This column displays the status of the scan: • **Pending** indicates that the scan is currently in the queue. • **Started** indicates that the scan has been initiated, but is still in-progress. • **Completed** indicates that the scan has run successfully. • **Paused** indicates that the scan has been paused. • **Resumed** indicates that the scan has resumed running (after being paused). • **Failed** indicates that the scan did not run successfully.

Troubleshoot Malware Protection data

Armor troubleshoots servers that contain **Malware Protection** subcomponents in a **Warning** or **Critical** status. To troubleshoot with Armor, you must submit a support ticket.

1. In the Armor Management Portal (AMP), click **Support,** and then click **Tickets**.
2. Click **Create a Ticket**.
3. Select or search for the desired category for your ticket request type.
4. Complete the missing fields.
    a. In **Description**, enter useful details that can help Armor quickly troubleshoot the problem.
5. Click **Create**.

6. To view the status of your ticket, in the left-side navigation, click **Support**, and then click **Tickets**.

Export Malware Protection data

To export the data:

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Malware Protection.**
3. (Optional) Use the filter function to customize the data displayed.
4. Below the table, click **CSV**. You have the option to export all the data (**All**) or only the data that appears on the current screen (**Current Set**).

Function	Data Displayed	Notes
CSV	Vm Name Vm Provider Os Last Agent Communication Date Last Scan	A blank entry indicates that the action has never taken place. For example, if there is a blank entry under **Last Scan**, then a scan has never taken place for that corresponding virtual machine.

Troubleshoot Malware Protection screen

If you do not have any malware events listed, consider that:

- Armor did not detect any malware events on this host in the last 90 days.
    - If a malware event is detected, Armor will contact you based on your notification preferences. To learn how to configure your notification preferences, see Update notification preferences.
- You do not have permissions to view malware events.
    - You must have the **View AVAM** permission enabled to view malware vents. Contact your account administrator to enable this permission. To learn how to update your permissions, see Roles and Permissions.

Review API calls

- Get Anti-Malware Host List
- Get Anti-Malware Account Statistics
- Get Anti-Malware Scan
- Get Overview Security Status
