Malware Protection

This topic only applies to **Armor Complete** 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 **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.

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
Cleaned	This widget indicates that the infected file was cleaned.
Passed	This widget indicates that no action was taken on the infected file.
Quarantined	This widget indicates that the file was renamed, and then moved to a temporary location.
Deleted	This widget indicates that an infected file was deleted.
Denied Access	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).
Filename	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
Scan 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 Service Health** table.

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. The status of this column helps to determine the overall Malware Protection status for the instance. There are three status types: • Secured (in green) • Warning (in yellow) • Critical (in red)
Last Scan	The results from the last scan provided by Trend Micro. The status of this column helps to determine the overall Malware Protection status for the instance. There are three status types: • Secured (in green) • Warning (in yellow) • Critical (in red)

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 Service Health** 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. 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.

Column	Description
Malware Name	The name of the malware detected in your virtual machine (or instance).
Filename	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
Scan Date	The date when the malware was detected.

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), at the bottom, click **New**.
2. Click **Ticket**.
3. In **Ticket Subject,** enter a descriptive name.
4. In **Add Recipien**t, enter the email address of additional users who should receive support updates.
5. In **Ticket Explanation**, enter useful details that can help Armor troubleshoot the problem quickly, especially the name of the server.
6. Click **Attach File** to add relevant images of your issue, such as the code or error message.
7. Click **Create Ticket**.
8. To view the status of your ticket, in the left-side navigation, click **Support**, and then click **Tickets + Notifications**.

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 (Armor Complete).

Review API calls

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

Related documentation

- Page:Malware Protection
- Page:Patching
