Malware Protection screen (snippet)

Understand Malware Protection data

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**.

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 Scanned Date	A blank entry indicates that the action has never taken place. For example, if there is a blank entry under **Last Scanned Date**, then a scan has never taken place for that corresponding virtual machine.

View Malware Protection details

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. You will be taken to the **Malware Protection Details** screen.

> ⚠ **Total Events** indicates that the total number of malware detected in the past 90 days.

Column	Detail
Malware Name	The name of the malware detected in your virtual machine.
Filename	The location of the malware detected in your virtual machine.
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 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.