# Malware Protection

## Knowledge Base

## Feedback

**Have a suggestion for the Armor Knowledge Base?**

Send a message to **kb@armor.com**.

⚠ 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 **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:<br>• Cleaned<br>• Passed<br>• Quarantined<br>• Deleted<br>• Denied Access<br>• Other |
| **Date** | This column displays the date when the malware was detected. |

## 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:<br>• Quarantine<br>• Clean<br>• Rename<br>• Pass<br>• Deny Access |
| **Date** | The date when the malware was detected. |

## 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<br><br>Vm Provider<br><br>Os<br><br>Last Agent Communication Date<br><br>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. |

### Troubleshooting

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

## Related Documentation

- Malware Protection
- Malware Scans
- Patching
- Service Health Data