Patching (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 OS Packages

View Patching data

Every four hours, the Patching subagent compares available patch updates to the instance's installed software.

Each instance's patching status is displayed in the Armor Management Portal (AMP), along with the number of patches available.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Patching**.

Column	Details
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 Patching subagent.
Provider	For Armor Complete, the entry will display **Armor**. For Armor Anywhere, the name of the public cloud provider for the instance.
Pending Updates	The number of patches available.
Security Updates	The number of security patches available, with a colored indicator.
Reboot Required	If the server requires a reboot to apply a patch.

To learn how the overall Patching status is determined, see Understand OS Patching data.

Understand Patching data

In the **Patching** screen, the dashboard displays the various patching statuses of your virtual machines (or hosts):

- **Green** indicates a virtual machine in a **Secured** patching status.
- **Yellow** indicates a virtual machine in a **Warning** patching status.
- **Red** indicates a virtual machine in a **Critical** patching status.

Not Available indicates that Armor does not have patching information available. In short, Armor is not sure if a patch is available because the patching information is not available.

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

- The date of the last reboot
- The date of the last applied security patch

> The overall status of your virtual machine is based on the individual status of your virtual machine's subcomponents, including **Patching**.

Condition 1 - Date of last reboot

If the date of the last reboot was between 7 to 40 days ago, then the **Patching** status changes from **Secured** to **Warning**.

If the date of your last reboot was 40 days ago or more, then the **Patching** status changes from **Warning** to **Critical**.

Date of last reboot	Security status	Color
7 to 40 days ago	Warning	Yellow
Over 40 days	Critical	Red

Condition 2 - Date of last applied security patch

If the date of your last applied security patch was between 60 to 89 days, then the **Patching** status changes from **Secured** to **Warning**.

If the date of your last applied security patch was 90 days or more, then the **Patching** status changes from **Warning** to **Critical**.

Date of last applied security patch	Security status	Color
60 - 90 days	Warning	Yellow
Over 90 days	Critical	Red

Analysis of patching data

Armor labels the **Patching** status based on the worst status. For example, if the date of your last reboot was 9 days ago, but the date of the last applied security patch was over 90 days, then overall, the **Patching** status is **Critical**.

Troubleshoot patching data

To troubleshoot virtual machines that contain **Patching** subcomponents in a **Warning** or **Critical** status, search for and apply the latest vendor-supplied security patches.

You can always contact Armor support for assistance.

View Patching details

The **Patching** details screen displays information about available patches for your server's operating system.

> Armor recommends that you use this information to download and install patches from the operating system's website. Patches are not available in the Armor Management Portal (AMP).

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Patching**.
3. Locate and select the desired server.
    - If patching details is not available for a particular server, then the operating system does not have a patch available.
    - Linux users will see the following information:

Column	Detail
Update Name	The name of the patch.
Update Version	The version number of the patch.
Type	The type of patch, such as **update** or **security**. **Update** patches are optional; **security** patches are highly recommended.
Date Patch Became Available	The date the patch became available from the operating system.

    - Windows users will see the following information:

Column	Detail
Update Name	The name of the patch.
Type	The type of patch, such as **update** or **security**. **Update** patches are optional; **security** patches are highly recommended.
Date Patch Became Available	The date the patch became available from the operating system.

4. (For Linux users) Note the **Update Name** and **Update Version**.
5. In a web browser, search for the patch on the operating system's site to download and install.

Export Patching data

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Patching.**
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	• Name • Provider • Os • Pending Updates • Security Updates • Reboot Required	A blank entry indicates that the action has never taken place. For example, if there is a blank entry under **Last Patched**, then a patch has never taken place for that corresponding virtual machine.

Review API calls

- Get Packages Status
- Get Packages
- Get Overview Security Status