TM1951 VirtualMachines-005Apply Latest OS Patches

Risk Level: Medium
Rule ID: VirtualMachines-005

Ensure that the latest OS patches (critical security and system updates) are being applied to all your Microsoft Azure virtual machines (Windows and Linux) in order to improve the operating system (OS) general stability, address a specific bug or flaw, or fix a security vulnerability.

Azure Security Center retrieves a list of available security and critical updates from Windows Update or Windows Server Update Services (WSUS), depending on the service configured on your virtual machines (VMs). The Security Center service also checks for the latest updates within Linux systems. If one of your virtual machines is missing a system update, Azure Security Center will recommend updating the VM's operating system. Cloud Conformity strongly recommends applying the latest system updates/OS patches as soon as these become available, in order to improve your VM's security, functionality, and performance.

Audit

To determine if your Azure VMs have the latest system updates installed, perform the following actions:

Note: Checking your Microsoft Azure virtual machines to find out if they have the latest system updates installed using Azure Command Line Interface (CLI) is not currently supported.

Using Azure Console

01Sign in to Azure Management Console.

02Navigate to Azure Security Center blade at https://portal.azure.com/#blade/Microsoft_Azure_Security/SecurityMenuBlade/.

03In the navigation panel, under **RESOURCE SECURITY HYGIENE**, choose **Recommendations** to view the recommendations made available by the Azure Security Center for the cloud resources available in the current subscription. A recommendation represents an action for you to take in order to secure your Azure resources. Each Security Center recommendation consists of 1) a short description of what is being recommended, 2) the steps required to implement the recommendation, 3) the affected resource(s) that require the recommended actions and 4) the secure score impact if the recommendation is implemented.

04On the **Recommendations** page, search for the **Missing system updates** recommendation entry. If there is no **Missing system updates** recommendation, the Security Center did not find any virtual machines that require the latest OS patches to be installed. If **Missing system updates** are available as recommendation, one or more Microsoft Azure virtual machines (Windows and/or Linux), provisioned within the current subscription, are missing the latest system updates (i.e. OS patches).

05Repeat steps no. 2 – 4 for each Microsoft Azure subscription available in your account.

Azure Official Documentation

- Apply system updates in Azure Security Center
- Remediate recommendations in Azure Security Center
- CIS Microsoft Azure Foundations