Protect your Azure customer: Increase the Azure environment security posture

As a cloud service provider, it is your responsibility to monitor and increase the security posture of Azure environments that belong to your customers. This helps your customers to be more resilient to attacks and to adopt the correct security best practices.

According to the annual Microsoft Digital Defense Report the number of attacks is increasing, and the attackers are targeting all industries and both small and large customers.

The first edition of our Cyber Signals quarterly report, shows many attacks are targeting the user identity because the attackers find it quite convenient to steal the credentials using simple techniques like phishing that allows them to easily “log in” instead of “break in” using complex attacks. Usage of Multi Factor Authentication can prevent 99.9% of identity attacks.

Thanks to Conditional Access, it is possible to enforce company access policies based on signals that are collected and elaborated in real time.

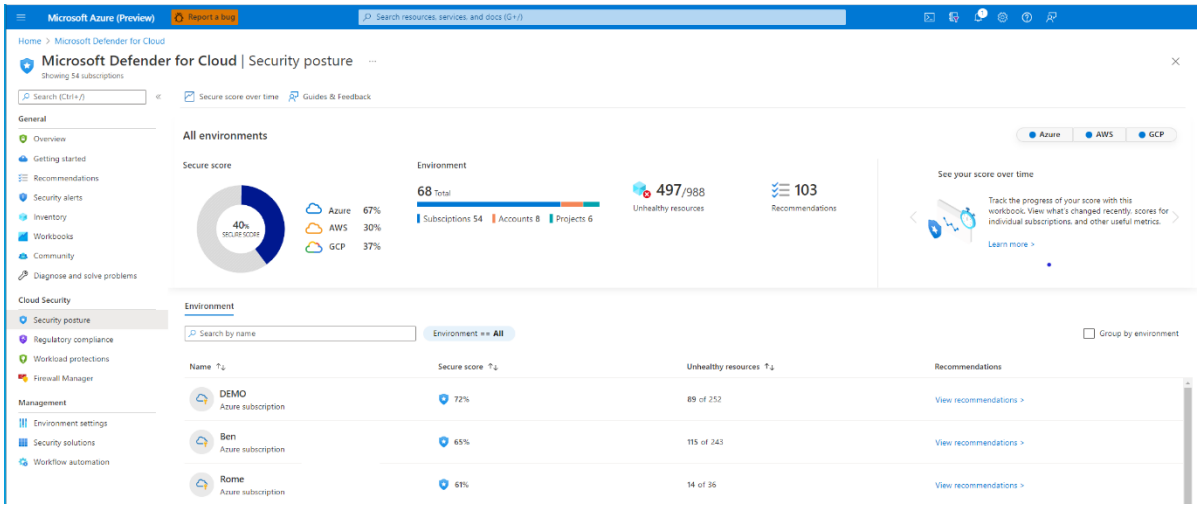
This allows to minimise the impact for the user that is asked to perform additional steps like Multi Factor Authentication only under specific conditions like a login from an unmanaged device or from a risky IP.

Even if protecting the identity is protecting an Azure environment, other misconfigurations can result in a poor security posture.

For example, exposing server ports directly on the internet can increase the risk of attacks like RDP brute force while the lack of encryption of at rest or in transit can expose sensible data that can be easily stolen.

Microsoft Defender for Cloud security Posture can help to asset and remediate the weakness inside an Azure, AWS or Google Cloud environment that a partner is managing.

Using the free mode of Microsoft Defender, you can get the secure score from your customers Azure Environment and its related features: security policy, continuous security assessment, and actionable security recommendations to help you protect your Azure resources.



How to check and increase your customer security posture

You can check your customer security posture using Microsoft Defender for Cloud:

1. Sign in to the Azure Portal and search for Microsoft Defender for Cloud.
2. Select in the blade **"Security Posture."**
3. Select a customer environment and check the **"Secure Score."**
4. Select **"View Recommendations."**
5. Review the recommendations for the selected environment.
6. Notice that all recommendations can **"trigger a logic app for automation."**
7. Selected recommendations can also trigger a **"fix"** button, a pre-built automation created and maintained by Microsoft that implement the recommendation.

Increase your customer workload protection

Microsoft Defender for Cloud allows to actively protect your customer workloads:

1. Sign in to the Azure Portal and search for Microsoft Defender for Cloud.
2. Select in the blade **"Environment settings."**
3. Select a subscription.
4. Select the workload that you want to protect (example: **"Servers")** and turn the status **"On."**
5. Select "X" in the upper right corner to go back to Microsoft Defender for Cloud.
6. Select in the blade **"Security Alerts"** to check alert events

NOTE: if the customer environment is not visible from the partner tenant, it is possible to set up a delegation using Azure Lighthouse.

Interesting articles:

- What is Microsoft Defender for Cloud?

Relevant Links:

Identity Multifactor Authentication Setup Guide

Microsoft Defender for Cloud - an introduction | Microsoft Docs

Getting Started with Microsoft Defender for Cloud - YouTube
Microsoft Secure Score | Microsoft Docs

Azure Secure Score vs. Microsoft Secure Score

Comprehensive Security for Business | Microsoft Security