

Microsoft Defender

Microsoft Defender as a comprehensive security solution that safeguards your computer or network from malicious software, viruses, and other cyber threats. It continuously monitors your system, scans for potential risks, and takes action to mitigate those risks.

Microsoft Defender, recommendations refer to suggested actions or best practices provided by the security solution to enhance the security posture of your system. These recommendations are based on the analysis of security data and potential vulnerabilities observed in your environment.

Components of Microsoft Defender:

1. **Microsoft Defender Antivirus**: It protects your computer from viruses and other harmful software that can damage your files and compromise your security.
2. **Microsoft Defender SmartScreen**: It warns you about potentially dangerous websites and files, helping you avoid phishing attempts and downloads that may harm your computer.
3. **Microsoft Defender Firewall**: It acts as a barrier between your computer and the internet, monitoring incoming and outgoing network traffic to prevent unauthorized access and block malicious attacks.
4. **Microsoft Defender Exploit Guard**: It protects your computer from common attack techniques by implementing security measures that make it harder for attackers to exploit vulnerabilities in your system.
5. **Microsoft Defender Application Guard**: It isolates your web browser in a secure container, preventing potentially harmful websites and downloads from affecting your computer and compromising your data.
6. **Microsoft Defender for Endpoint**: It detects and responds to advanced threats that target your computer, using advanced technologies to identify suspicious activities and take action to protect your system.
7. **Microsoft Defender for Identity**: It detects and investigates attacks that target user identities, such as unauthorized access attempts, helping protect your accounts and sensitive information.
8. **Microsoft Defender for Office 365**: It provides advanced protection for your Microsoft 365 services like email, file sharing, and collaboration tools, helping prevent malicious attachments, URLs, and phishing attacks from compromising your data.

It includes :

Security Posture : (security status of enterprise network or system. It'll tell the percentage of our system means upto what percentage it is secure.)

Regulatory compliance: (regulatory compliance in Azure means following the rules and guidelines set by authorities to protect sensitive data and ensure the privacy and security of information stored or processed in the Azure cloud.)

Suppose we create a storage on public link so it'll tell us to create it in private. But we can't directly make the changes we have to ask for the permission from resource group owner.

Workload Protection : (Detect and respond to attacks in real time to protect your multicloud, hybrid, and on-premises workloads.). It'll give details how many attack happen in our system and does it successful or not.

What is recommendation in Microsoft defender:

Microsoft Defender continuously monitors your system and analyzes various security indicators, such as configuration settings, installed software, and user behavior, to identify potential security risks. Based on this analysis, it provides recommendations tailored to your specific environment.

These recommendations typically aim to address security vulnerabilities, improve system configurations, and enhance overall protection against known and emerging threats.

1. **Enable security features**: Microsoft Defender may suggest turning on specific settings that make your computer safer. It's like activating extra guards to keep out any potential threats.
2. **Install software updates**: Recommendations may advise you to regularly update your computer's programs. This is important because updates often fix security problems and make it harder for attackers to harm your computer.

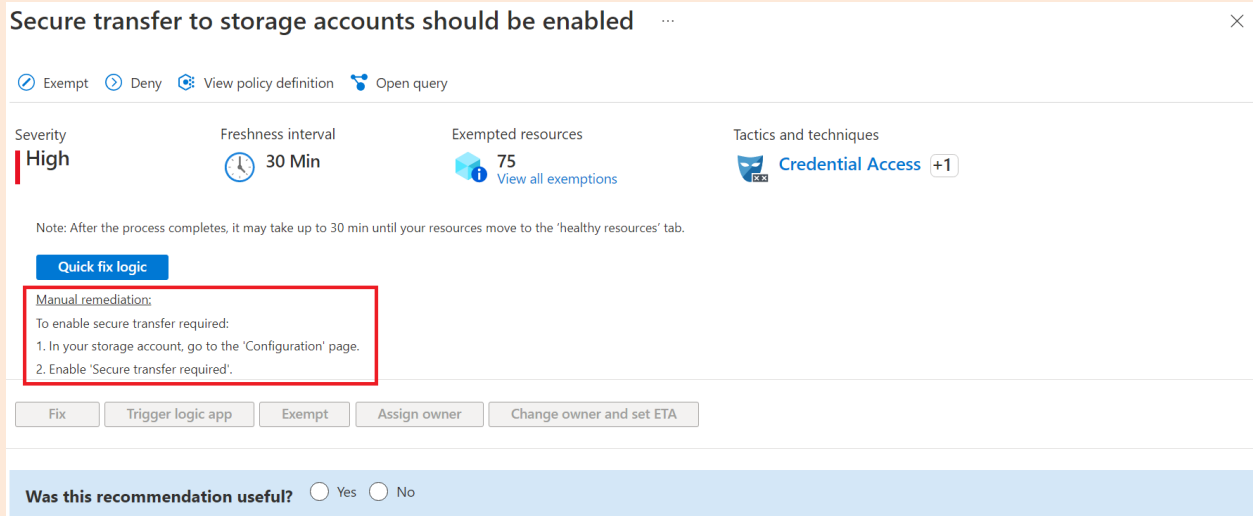
3. **Review security settings**: Microsoft Defender may suggest checking your computer's security options to ensure they are set up correctly. It's like double-checking the locks on your doors and windows to keep intruders out.
4. **Conduct security assessments**: Recommendations might suggest scanning your computer for any vulnerabilities or weaknesses. This is similar to having a security expert check your home for any potential entry points for burglars.
5. **Educate users**: Microsoft Defender may provide suggestions for learning about common security threats and how to stay safe online. It's like getting tips on how to recognize scams or avoid dangerous websites.

Implement security recommendations in Microsoft Defender for Cloud

Remediation steps:

After reviewing all the recommendations, decide which one to remediate first. We recommend that you prioritize the security controls with the highest potential to increase your secure score.

1. From the list, select a recommendation.
2. Each recommendation has its own set of instructions. The following screenshot shows remediation steps for configuring applications to only allow traffic over HTTPS.

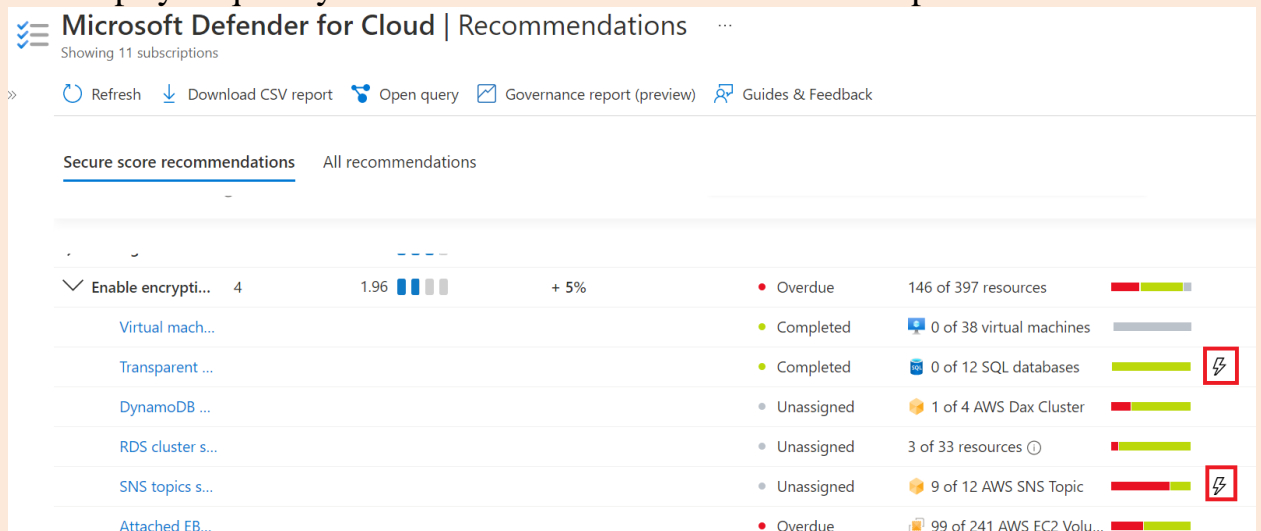


Once completed, a notification appears informing you whether the issue is resolved.

Fix button

To simplify remediation and improve your environment's security (and increase your secure score), many recommendations include a **Fix** option.



1. **Fix** helps you quickly remediate a recommendation on multiple resources




2. From the **Unhealthy resources** tab, select the resources that you want to implement the recommendation on, and select **Fix**.


3. In the confirmation box, read the remediation details and implications.





CloudFront distributions should require encryption in transit ...

 Exempt  Open query

Severity
Medium

Freshness interval
 6 Hours

Tactics and techniques
 **Discovery** +2

<input type="checkbox"/>	Name	↑↓	AWS Account	Connector name	Region	Resource type
<input checked="" type="checkbox"/>	 EADHFPDYLP SGI		102614528198	securityConnector	global	AWS CloudFront dist...
<input type="checkbox"/>	 E1HOYFML2L HS1D		102614528198	securityConnector	global	AWS CloudFront dist...
<input type="checkbox"/>	 E1CRCDWYB E4DE		102614528198	securityConnector	global	AWS CloudFront dist...
<input type="checkbox"/>	 E13VNP7E A1C0YB		102614528198	securityConnector	global	AWS CloudFront dist...


Fix

Trigger logic app

Exempt

Assign owner

Change owner and set ETA



Was this recommendation useful? ☐ Yes ☐ No

Insert the relevant parameters if necessary, and approve the remediation

Note: It can take several minutes after remediation completes to see the resources in the **Healthy resources** tab. To view the remediation actions, check the [activity log](#).

Once completed, a notification appears informing you if the remediation succeeded.

Fix actions logged to the activity log

The remediation operation uses a template deployment or REST API `PATCH` request to apply the configuration on the resource. These operations are logged in [Azure activity log](#).

Security Alerts In Microsoft Defender

Security alerts in Microsoft Defender are like warning signals that tell you when there might be something wrong with the security of your computer. They are generated by the security software when it detects potential threats or suspicious activities that could harm your system.

1. **Detecting threats**: Microsoft Defender is always watching your computer for signs of danger, like viruses or malicious programs. When it detects something suspicious, it sends out a security alert to get your attention.
2. **Notifying you**: The security alert appears as a message or notification on your screen, letting you know that there's a possible security issue. It provides details about what the threat is, which files or parts of your system are affected, and how serious the problem is.
3. **Taking action**: When you see the security alert, it's important to do something about it. The alert will suggest actions you can take to deal with the threat, such as running a scan, removing the threat, or isolating the affected files.
4. **Investigating and responding**: You can investigate further to understand the nature of the threat and its potential impact. Based on that, you can decide how to respond and take appropriate steps to protect your computer and your data.
5. **Resolving and preventing**: By following the recommended actions and addressing the security alert, you can resolve the threat and prevent further harm. This might involve removing the malicious software, fixing vulnerabilities, or changing your security settings to avoid similar issues in the future.