ConductorOne

Implementing Just-in-Time Access for VMs in Microsoft Azure

With the rising frequency and sophistication of cyberattacks specifically targeting cloud infrastructure, safeguarding cloud resources has become critical for businesses. Just-in-time (JIT) access, a practice of allowing temporary and tightly controlled access to specific resources only when necessary, offers a solid solution to this challenge. This security practice shrinks your system's attack surface, reduces exposure time to vulnerabilities, and bolsters overall security.

JIT access reduces the attack surface by limiting the entry points into your cloud environment. Instead of having open ports and continuous access, it allows entry on a need-to-know basis, thus reducing the potential avenues for attackers. Moreover, access is granted for a predefined and limited period. By minimizing the access duration, JIT shortens the window during which your resources are vulnerable. Unauthorized users face a significantly more complex challenge when exploiting security gaps.

JIT also empowers organizations to define the ports and resources that can be accessed. This level of granularity provides fine-grained control over who can connect to your virtual machines (VMs) or services. The access request process is also streamlined, thanks to JIT's structured process for requesting and granting access. Administrators can scrutinize and approve access requests based on genuine need, adding an extra layer of security.

In the event of a security incident, JIT access enables swift response. This is possible because JIT maintains detailed audit records of access requests and approvals. These audit logs help security teams maintain a clear record of who accessed which resources and when.
By combining all these benefits from JIT's tight control over access permissions and strict adherence to time limits, you get a proactive security approach that strengthens your overall security posture, making it considerably more challenging for attackers to infiltrate your systems.

This article explores JIT access and shows how to implement it as a security method for your virtual machines (VMs). Whether you are responsible for managing cloud security or just beginning to explore the intricacies of securing cloud resources, this guide will equip you with the knowledge and practical steps needed to bolster your security practices.

How to Implement Just-in-Time Access in Microsoft Azure

This section provides a step-by-step guide for implementing just-in-time (JIT) access in Microsoft Azure.

Prerequisites

Before you begin, ensure you have an active Azure account and the necessary permissions to configure security settings. You'll need to log in with an account that has Global Administrator privileges to configure JIT access.

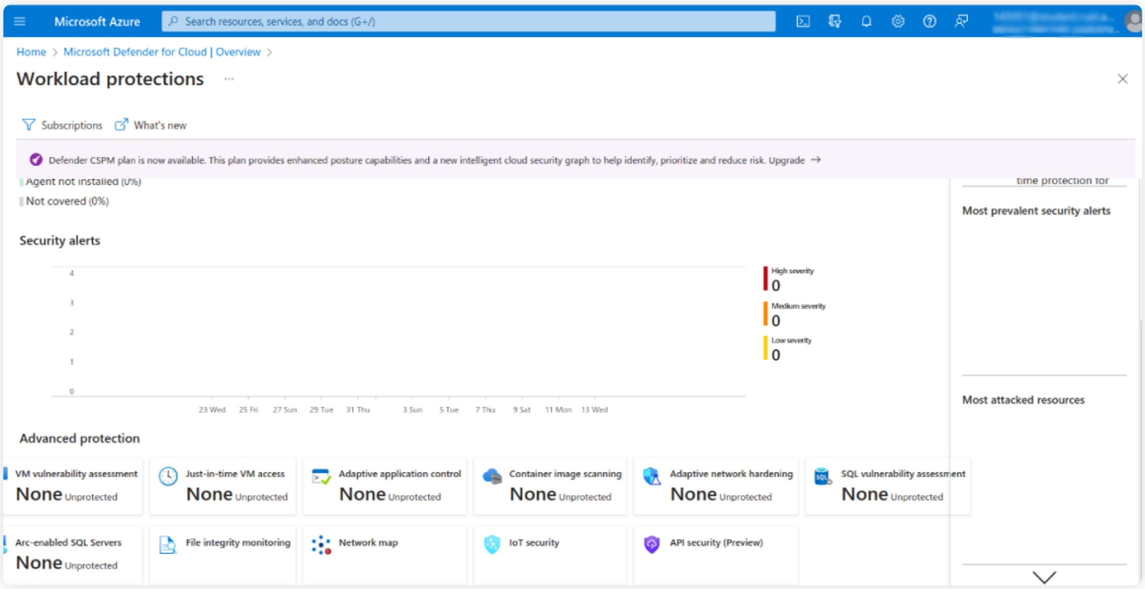
Logging In to the Azure Portal

Open your web browser and navigate to the Azure portal, then sign in using your Azure account credentials. Make sure to use a Global Administrator account since you can't update JIT settings using a standard user account.

Enabling Just-in-Time (JIT) VM Access

You need to enable JIT access to your VMs in Microsoft Defender for Cloud (formerly Azure Security Center), which unifies security management for Azure cloud, multicloud, and hybrid cloud setups.

You can access Defender for Cloud through the **Azure services** list or by finding it using the search bar. Once there, navigate to **Cloud Security > Workload protections**, then click the **Advanced protection > Just-in-time VM access** option:



Home > Microsoft Defender for Cloud | Overview >

Workload protections

Defender CSPM plan is now available. This plan provides enhanced posture capabilities and a new intelligent cloud security graph to help identify, prioritize and reduce risk. Upgrade →

Agent not installed (0%)

Not covered (0%)

time protection for

Most prevalent security alerts

Security alerts

High severity 0

Medium severity 0

Low severity 0

Most attacked resources

Advanced protection

VM vulnerability assessment None Unprotected

Just-in-time VM access None Unprotected

Adaptive application control None Unprotected

Container image scanning None Unprotected

Adaptive network hardening None Unprotected

SQL vulnerability assessment None Unprotected

Arc-enabled SQL Servers None Unprotected

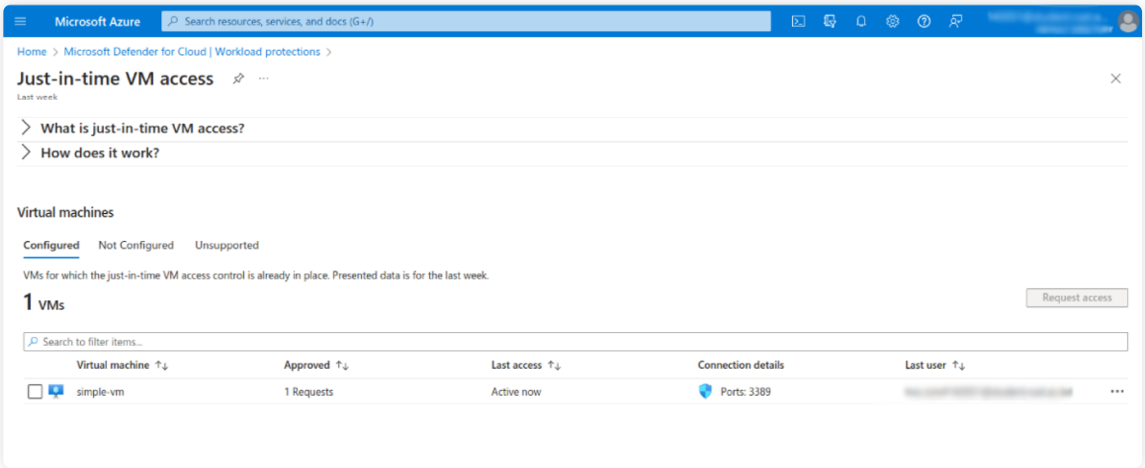
File integrity monitoring

Network map

IoT security

API security (Preview)

This page displays all your VMs in three groups:


Microsoft Azure
Search resources, services, and docs (G+/)
Request access
Search to filter items...

Home > Microsoft Defender for Cloud | Workload protections >

Just-in-time VM access

Last week

> What is just-in-time VM access?

> How does it work?

Virtual machines

Configured | Not Configured | Unsupported

VMs for which the just-in-time VM access control is already in place. Presented data is for the last week.

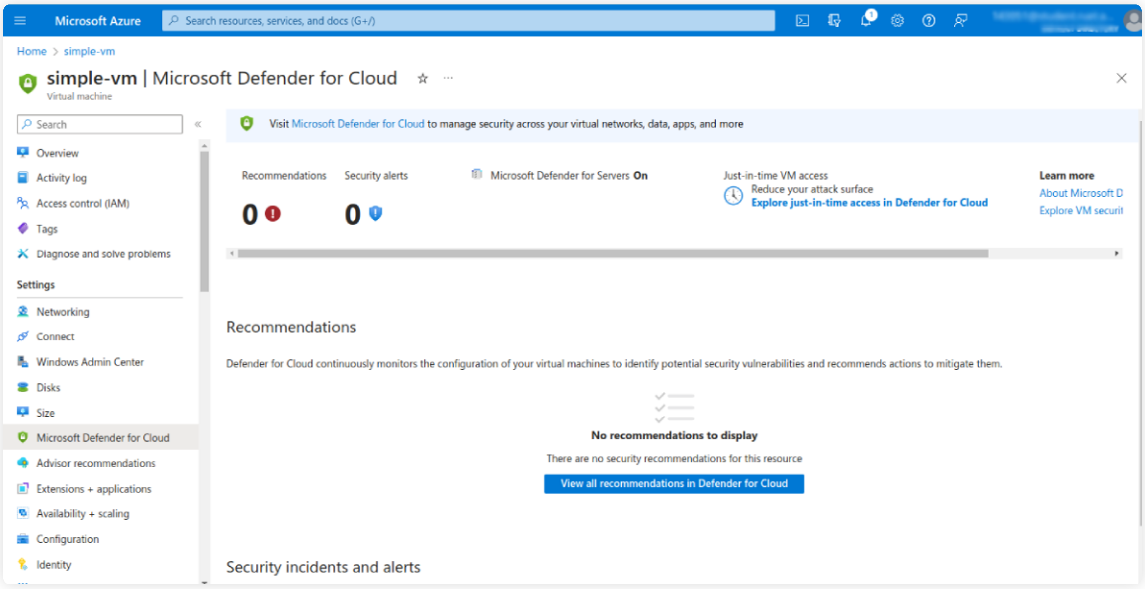
1 VMs

	Virtual machine ↑↓	Approved ↑↓	Last access ↑↓	Connection details	Last user ↑↓
□	simple-vm	1 Requests	Active now	Ports: 3389	[redacted]

Go to the **Not Configured** VM group to find the VMs that don't have JIT access enabled. Select the VMs you want to enable JIT access for, then click **Enable JIT on VM** to save the changes.

Configuring Ports for JIT VM Access

You can configure the ports for which JIT VM access will be allowed. This can be done from the JIT VM access page that opens up after you enable JIT for a VM. You can also navigate to the settings for the virtual machine, then select **Microsoft Defender for Cloud** in the left-hand menu:


Microsoft Azure
Search resources, services, and docs (G+/)
Home > simple-vm
simple-vm | Microsoft Defender for Cloud
Virtual machine
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Networking
Connect
Windows Admin Center
Disks
Size
Microsoft Defender for Cloud
Advisor recommendations
Extensions + applications
Availability + scaling
Configuration
Identity
Recommendations
0
Security alerts
0
Microsoft Defender for Servers On
Just-in-time VM access
Reduce your attack surface
Explore just-in-time access in Defender for Cloud
Learn more
About Microsoft D
Explore VM securit
View all recommendations in Defender for Cloud
Security incidents and alerts

Visit Microsoft Defender for Cloud to manage security across your virtual networks, data, apps, and more

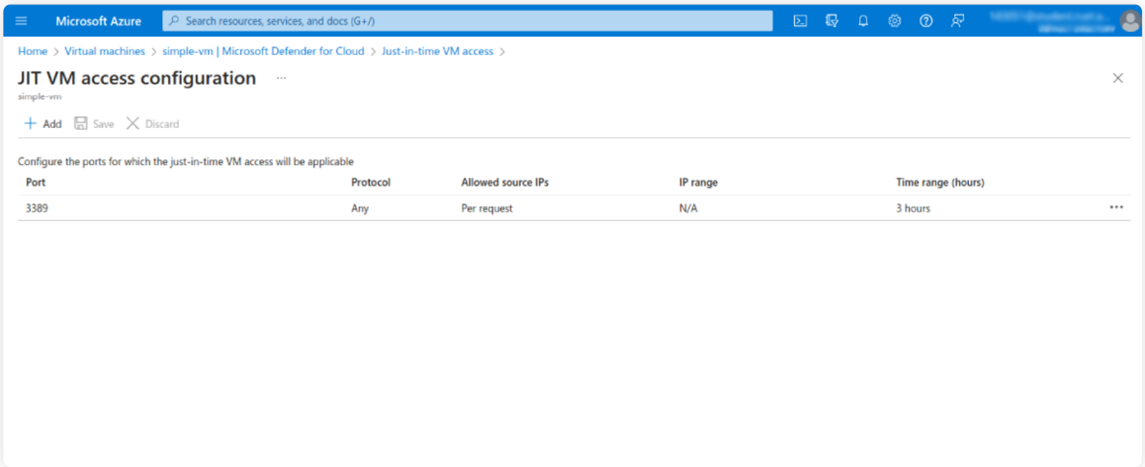
Recommendations

Defender for Cloud continuously monitors the configuration of your virtual machines to identify potential security vulnerabilities and recommends actions to mitigate them.

No recommendations to display

There are no security recommendations for this resource

Once on this page, click **Add**, then specify the desired port, protocol, allowed source IPs, and maximum request time:


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Virtual machines > simple-vm | Microsoft Defender for Cloud > Just-in-time VM access >
JIT VM access configuration
simple-vm
Add
Save
Discard

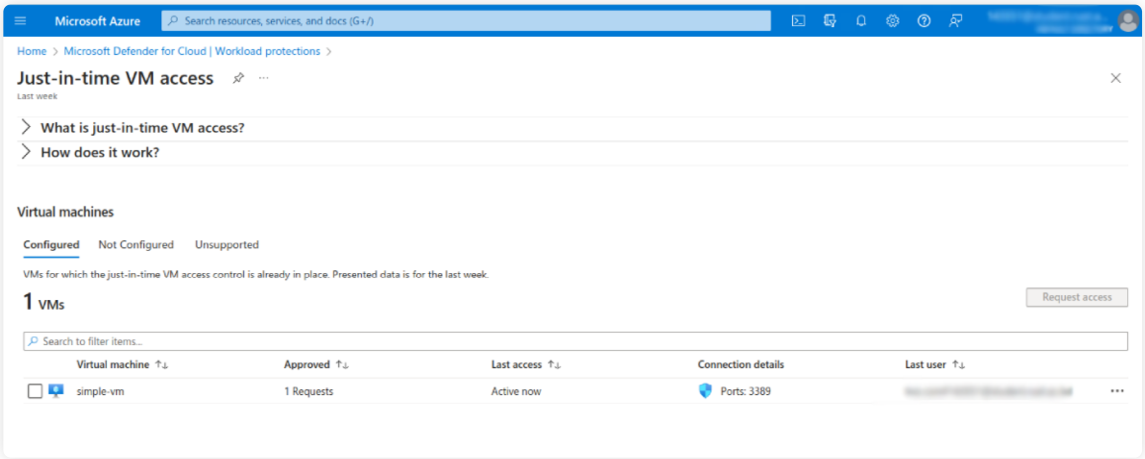
Configure the ports for which the just-in-time VM access will be applicable

Port	Protocol	Allowed source IPs	IP range	Time range (hours)
3389	Any	Per request	N/A	3 hours

Click **OK** to save the changes.

Requesting JIT VM Access

Now that you've enabled JIT access and configured ports for JIT VM access, you can request access to your VM. Back on the **Just-in-time VM access** page, select the desired VM from the **Configured** list to do this. Then, click **Request access:**



Microsoft Azure
Search resources, services, and docs (G+/)

Home > Microsoft Defender for Cloud | Workload protections >

Just-in-time VM access

Last week

> What is just-in-time VM access?

> How does it work?

Virtual machines

Configured | Not Configured | Unsupported

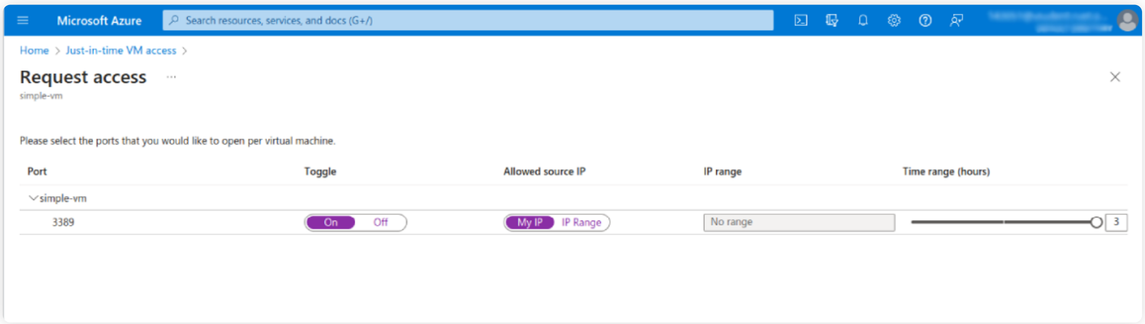
VMs for which the just-in-time VM access control is already in place. Presented data is for the last week.

1 VMs

Request access
Search to filter items...

	Virtual machine ↑↓	Approved ↑↓	Last access ↑↓	Connection details	Last user ↑↓
□	simple-vm	1 Requests	Active now	Ports: 3389	[redacted]

In the new window, select the ports you want to open for accessing this VM, then click **Open ports:**



Home > Just-in-time VM access >

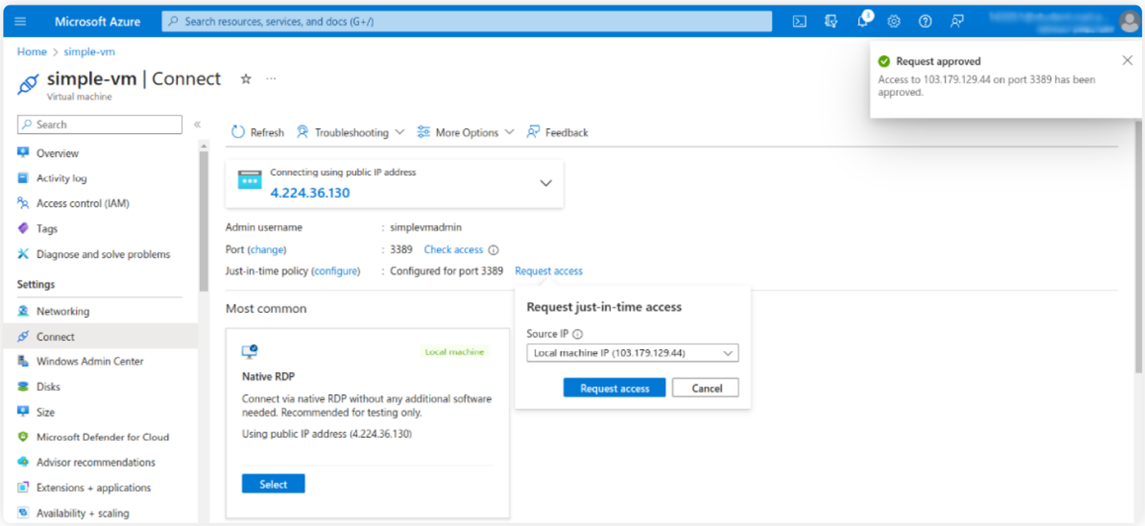
Request access

simple-vm

Please select the ports that you would like to open per virtual machine.

Port	Toggle	Allowed source IP	IP range	Time range (hours)
simple-vm				
3389	On / Off	My IP / IP Range	No range	3

You can do the same in the settings for your virtual machine. Click **Connect** in the left-hand menu for your VM, then use the **Request access** option to request just-in-time access:



Home > simple-vm

simple-vm | Connect

Virtual machine

Request approved

Access to 103.179.129.44 on port 3389 has been approved.

Connecting using public IP address

4.224.36.130

Admin username : simplevmadmin

Port (change) : 3389 Check access

Just-in-time policy (configure) : Configured for port 3389 Request access

Most common

Local machine

Native RDP

Connect via native RDP without any additional software needed. Recommended for testing only.

Using public IP address (4.224.36.130)

Request just-in-time access

Source IP: Local machine IP (103.179.129.44)

Request access | Cancel

Tips to Optimize Access Security in Azure

Implementing JIT access is only one part of a much bigger picture when it comes to securing access in Azure. By combining JIT access with the following strategies, you can ensure your access security is fully optimized.

Implement Multifactor Authentication (MFA)

One of the simplest and most effective ways to enhance security in Azure is to implement multifactor authentication (MFA). It's a login process that requires multistep verification, usually a combination of something you know (like a password), something you possess (such as a security token or phone), or something unique to you (like a fingerprint or voice recognition). It even offers adaptive authentication, which uses factors like location and device type to confirm user identity. Azure's system-preferred MFA feature prompts users to sign in using the most secure method they registered, which discourages less secure sign-in methods like SMS. Overall, MFA ensures that even if a password is compromised, malicious actors can't easily gain access to your systems.

Use a Solution like ConductorOne for Identity and Access Management

ConductorOne is an access control platform that offers solutions to streamline user access management across various platforms. It provides a unified view and allows admins to easily assign, modify, or revoke permissions, thereby enhancing security and simplifying administrative tasks. ConductorOne also enables you to provide just-in-time access to your infrastructure.

A solution like ConductorOne can solidify your security practices and provide access to next-generation identity management.

Use Entra ID Privileged Identity Management (PIM)

Privileged Identity Management (PIM) is a service that makes managing and monitoring access to your sensitive resources easy. PIM is provided through Microsoft Entra ID (formerly, Azure AD).

Note: At time of writing, Microsoft was in the process of rebranding Azure AD as Microsoft Entra ID. While this article uses the updated title, you may still find links and paths that use the old name.

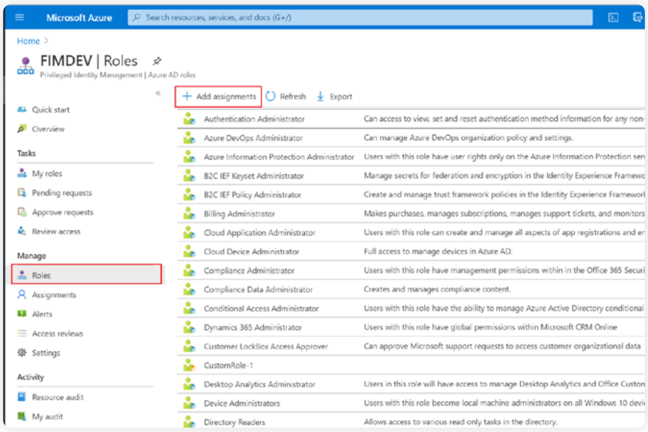
PIM can safeguard Azure cloud resources, Entra ID resources, and other Microsoft online solutions like Intune.

PIM provides just-in-time privileged access, requires a reason for access, and conducts access reviews to ensure that only the right people have access. It minimizes the risk of breaches caused by unnecessary privileged access.

Enable Entra ID PIM for Entra ID Roles

Enabling PIM for Entra ID roles ensures users only have privileged access when they need it and only for a limited time. With PIM enabled, users activate their elevated Entra ID roles using a just-in-time approach when necessary. You can also require approval or multifactor authentication to activate roles, which adds an extra layer of security and verification.

This practice can eliminate the number of elevated roles that are not in use. This reduces the exposure time of Entra ID roles and their potential to be exploited.



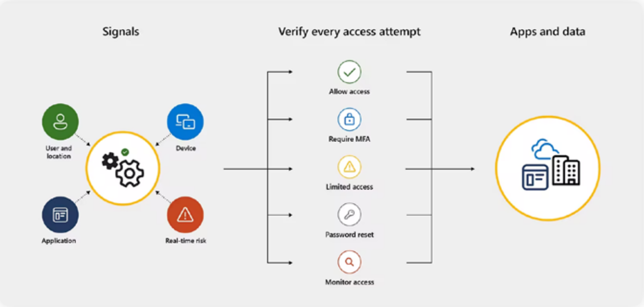
Authentication Administrator	Can access to view, set and reset authentication method information for any non-
Azure DevOps Administrator	Can manage Azure DevOps organization policy and settings.
Azure Information Protection Administrator	Users with this role have user rights only on the Azure Information Protection serv
B2C IEF Keyset Administrator	Manage secrets for federation and encryption in the Identity Experience Framewo
B2C IEF Policy Administrator	Create and manage trust framework policies in the Identity Experience Framework
Billing Administrator	Makes purchases, manages subscriptions, manages support tickets, and monitors
Cloud Application Administrator	Users with this role can create and manage all aspects of app registrations and en
Cloud Device Administrator	Full access to manage devices in Azure AD.
Compliance Administrator	Users with this role have management permissions within in the Office 365 Securi
Compliance Data Administrator	Creates and manages compliance content.
Conditional Access Administrator	Users with this role have the ability to manage Azure Active Directory conditional
Dynamics 365 Administrator	Users with this role have global permissions within Microsoft CRM Online
Customer LockBox Access Approver	Can approve Microsoft support requests to access customer organizational data
CustomRole-1	
Desktop Analytics Administrator	Users in this role will have access to manage Desktop Analytics and Office Custom
Device Administrators	Users with this role become local machine administrators on all Windows 10 devi
Directory Readers	Allows access to various read only tasks in the directory.

Implement Role-Based Access Control (RBAC)

With role-based access control (RBAC), you can assign predefined or custom roles to users and groups that define their permissions at different scopes, such as subscription, resource group, or resource level. Each role defines a set of actions that the user or group can perform on the resources. This helps ensure that users have just enough access to perform their tasks without unnecessary permissions that malicious actors could exploit. For example, you could assign the “Reader” role to a user at the subscription level, allowing them to view all the resources in the subscription but not make any changes. You could also assign the “Contributor” role to a group at the resource group level, allowing them to manage all the resources in that resource group but not assign roles to others. RBAC enables you to follow the principle of least privilege by granting users only the minimum amount of access to perform their tasks. This way, you can reduce the risk of unauthorized or malicious actions on your Azure resources.

Utilize Entra Conditional Access

Entra Conditional Access provides automated access control decisions for accessing your cloud resources based on predefined conditions. It specifies conditions a user must satisfy (such as their location or device) to access a resource. You can decide whether to grant access, challenge for MFA, or block access. You can also block access based on legacy authentication, risk level, or country/region. Implementing this feature alongside JIT access will boost your cloud security by allowing you to enforce granular and context-aware access policies for your resources.

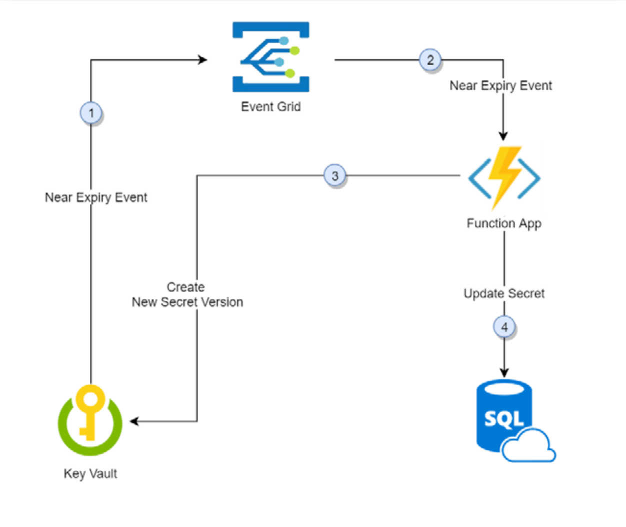


Regularly Review and Update Access Permissions

You should perform periodic and one-time reviews of the access permissions granted to users or groups for resources to ensure that only the necessary people or teams can access specific resources. If any old accounts no longer need some permissions, their access should be revoked. You can use Entra ID to create access reviews that run at specific times and assign actions to be performed in response to the review results, such as removing or extending permissions. These reviews and responses can also be automated. For example, you could set up a process that automatically asks users if they still require access to a particular resource after a specified period and either remove the permission or extend it based on their response. You should also ensure that you have documentation specifying how often access reviews and updates should happen and who is responsible.

Regularly Rotate Access Keys and Secrets

Old or compromised keys and secrets are a security risk. You should regularly rotate these credentials to ensure that any potentially compromised data has a limited lifespan, thereby reducing its value to malicious actors. This practice eradicates lingering problems and contributes to a resilient security posture. Regularly rotating your keys might also be necessary to comply with the security and compliance policies and regulations of your organization or industry. You should also consider automating your key and secret rotations.



Update and Patch Virtual Machines and Services

Like any software, virtual machines and services are susceptible to emerging vulnerabilities. Regularly updating and patching these resources protects you from malicious threats, keeping your Azure infrastructure secure.

There are various ways to ensure that your VMs and services are up-to-date.

Conclusion

Just-in-time access can significantly improve the security of your cloud resources. This article illustrates how JIT access minimizes attack surfaces, reduces vulnerability exposure, and strengthens overall security by allowing controlled and temporary access to specific resources when needed. The article emphasized the significance of implementing robust security practices in the ever-evolving cloud security landscape.

Consider leveraging solutions like ConductorOne for identity and access management (IAM) to further enhance your Azure security practices. ConductorOne offers a streamlined approach to managing user access across diverse platforms, providing you with a unified view and simplifying permission management. By incorporating ConductorOne into your security strategy, you fortify your defenses and seamlessly integrate just-in-time access into your infrastructure, ensuring a more resilient and responsive security posture.