Securing Azure with PIM: A Just-in-Time Access Study

Author: Dustin Bourgois, bourgois@gmail.com
Advisor: *Russell Eubanks*

Accepted: May 15th, 2025

Abstract

Misconfigured privileges in Azure environments present serious risks to organizations, including privilege escalation, data breaches, and financial losses, especially as cloud adoption increases. This study assesses Azure Privileged Identity Management (PIM) and its Just-in-Time access model within a controlled Azure environment, simulating enterprise scenarios across Azure Subscription Roles. Findings show that PIM's time-bound privileges significantly reduce the attack surface by limiting unauthorized access outside approved periods. These insights provide organizations with actionable strategies to strengthen cloud security amid evolving cyber threats.

1. Introduction

Security breaches in cloud environments often result from stolen credentials, privilege misuse, and exploited vulnerabilities. The 2025 Verizon Data Breach Investigations Report indicates that credential misuse was involved in 22% of breaches. Breaches involving third parties, such as supply chain partners and vendors, have doubled from the previous year. Including third-party breach data accounts for nearly 30% of all incidents, enabling external access to sensitive information (Verizon, 2025).

Despite these indicators, many organizations continue to assign persistent administrative privileges to users, expanding the attack surface and increasing the likelihood of misconfiguration, insider threats, and lateral movement by external actors. Persistent administrative access introduces long-lived credentials and unrestricted role assignments, which conflict with modern Zero Trust security principles. In cases of account compromise, attackers may gain wide-ranging, unimpeded access to cloud resources.

Azure Privileged Identity Management (PIM) addresses this vulnerability through a Just-in-Time access model. PIM enforces time-bound privilege elevation and requires justification and multi-factor authentication (MFA) for administrative actions. By reducing the duration and scope of privileged access, PIM limits opportunities for abuse and strengthens an organization's security posture. Microsoft reports that organizations using Azure PIM’s Just-in-Time access reduced privilege-related security incidents by 75% within six months (Microsoft, 2023).

Prior studies emphasize the risks of continuous administrative access in cloud environments. Ahmadi (2024) conducted a systematic review identifying cloud security threats and emphasized least privilege access controls as a critical mitigation strategy for credential misuse and unauthorized access. The Center for Internet Security (2021) recommends minimizing privilege duration and applying role-based controls to defend against insider threats and external actors. While these frameworks support time-bound access, few studies have tested how Azure PIM performs across real-world role types.

Author Name, email@address

This research addresses that gap by examining how PIM handles privilege escalation attempts under simulated threat scenarios.

This study evaluates the impact of PIM's Just-in-Time enforcement by testing the Owner, Contributor, and Reader roles within Azure subscriptions. Each scenario replicates administrative tasks and simulates misuse to assess how time-limited access affects identity governance and risk exposure. The testing results demonstrate that PIM strengthens privilege management by enforcing time-bound access and reducing the likelihood of unauthorized privilege use.

Azure PIM's integration with Zero Trust architecture through least privilege enforcement, MFA, and audit logging positions it as a critical control in securing modern cloud environments. As organizations deepen their reliance on cloud services, adopting PIM becomes necessary for enterprise cybersecurity strategies.

Zero Trust is a security model that assumes no implicit trust, even inside the network perimeter. It requires continuous verification of identity, strict access controls, and minimal privilege allocation. Instead of assuming users or devices are trustworthy based on network location or previous authentication. Azure PIM directly supports these principles by enforcing time-bound access, MFA, and role-specific justifications for elevation.

2. Research Method

This study examines how Azure PIM's Just-in-Time access model reduces privilege escalation risks and limits the attack surface in cloud environments. The central research question guiding this analysis is: To what extent does Just-in-Time privilege enforcement in Azure PIM mitigate security threats associated with persistent administrative access?

A test Azure environment simulates legitimate administrative actions and potential misuse to address the research method question. The test scenarios use the Owner, Contributor, and Reader roles. Each Just-in-Time activation policy assigns a time window to each role based on its risk level.

Author Name, email@address

The evaluation focuses on two measurable outcomes: (1) whether PIM blocks unauthorized actions outside approved elevation periods and (2) whether users can successfully execute tasks during active, time-limited sessions. Azure Monitor logs, sign-in activity reports, and observable system responses during access attempts provide the basis for assessment.

The evaluation measures how Azure PIM's Just-in-Time access controls improve security compared to traditional always-on role assignments. Always-on roles leave privileged access continuously available, which increases the risk of misuse, insider threats, and post-compromise escalation. PIM restricts access by requiring users to request elevation, provide justification, and complete MFA. These controls ensure privileges remain active only when needed and authorized. PIM supports Zero Trust principles such as least privilege, identity verification, and time-bound access by enforcing short-lived, auditable access.

2.1. Azure Test Environment Configuration

A dedicated Microsoft Entra ID tenant and Azure subscription are the test environments to evaluate Azure PIM's Just-in-Time access controls. The setup uses Microsoft 365 E5 licenses, which include Entra ID P2 features required for PIM, such as Just-in-Time role elevation, MFA, Conditional Access, and Azure logging.

Administrative tasks take place on a Windows 11 workstation using Microsoft Edge and PowerShell, with a mobile device used for MFA prompts during elevation. Multiple test accounts with varied access roles simulate common enterprise scenarios. Azure Monitor and Entra ID sign-in logs capture events related to role activation, policy enforcement, and access attempts.

2.1.1 User Accounts and Roles

Test accounts are created in the Microsoft Entra ID tenant to simulate standard privilege levels within the Azure environment. Each account is assigned one or more

Azure subscription roles to replicate administrative scenarios. These roles follow Microsoft's standard definitions (Microsoft, 2023):

- **Owner**: Grants complete control over the subscription, including the ability to assign permissions.
- **Contributor**: Allows resource management but restricts permission changes.
- **Reader**: Provides view-only access to resources.

One user account (ftowner@pimkota.com) holds permanent Owner privileges to represent a traditional administrative model. All other accounts require PIM-based elevation to perform tasks. This role contrast highlights the difference between persistent access and time-bound privilege models.

Table 1 lists the test user accounts and the roles assigned to each, simulating persistent and Just-in-Time privilege access scenarios.

Name	Email ID	Roles
PIM SysAdmin	pim_sysadmin@pimkota.com	Contributor, Owner, Reader
PIM Owner	owner@pimkota.com	Owner
Full-Time Owner	ftowner@pimkota.com	Owner
PIM Reader	reader@pimkota.com	Reader
PIM Contributor	contributor@pimkota.com	Contributor
PIM Terraform	pim_terraform@pimkota.com	Contributor

Table 1: Test User Accounts and Roles

Activation durations and MFA requirements are set based on each role's operational risk. Higher-risk roles receive shorter elevation windows and stricter controls. Due to its authority, the Owner role has the shortest elevation period, which is limited to one hour, to reduce exposure and maintain tight oversight during elevated access. The Contributor role receives three hours for resource configuration and deployment. At the same time, the Azure PIM grants the Reader role an eight-hour window to observe logs and resource states without interruption.

All roles require an MFA to elevate and reduce unauthorized access due to credential theft. Tested configurations summarized in Table 2 enforce Zero Trust

principles by granting temporary access only to verified identities under controlled conditions.

Role	Activation Duration	Mandatory MFA
Contributor	3 hours	Enabled
Reader	8 hours	Enabled
Owner	1 hour	Enabled

Table 2: Tested PIM Role Configuration Settings

Each role receives a Just-in-Time activation duration based on its privilege level and operational need. The Owner role is limited to a one-hour elevation window to reduce exposure to high-risk actions. The Contributor role is assigned a three-hour window for adequate resource deployment and configuration time. The Reader role is assigned an eight-hour window to support extended monitoring tasks without elevated permissions.

All roles require MFA for activation. This security control adds a critical identity verification step and reduces the likelihood of unauthorized access due to credential compromise. These role-specific configurations, shown in Table 2, reflect Zero Trust principles by enforcing time-bound access for verified users under scoped permissions.

The pim_sysadmin account holds all roles to support flexible system administrator tasks. When read-only observation is needed, the account activates the Reader role. For deployment or system changes, it elevates to Contributor. This approach illustrates PIM's real-world flexibility while reinforcing the principle of least privilege.

2.1.2 Azure PIM Configuration

Azure PIM enforces Just-in-Time access for key roles in the Pimkota Azure subscription. PIM manages role eligibility, assignment conditions, and policy enforcement through a centralized administrative dashboard. Figure 1 illustrates the PIM overview screen used during testing to monitor elevation activity and manage role assignments.

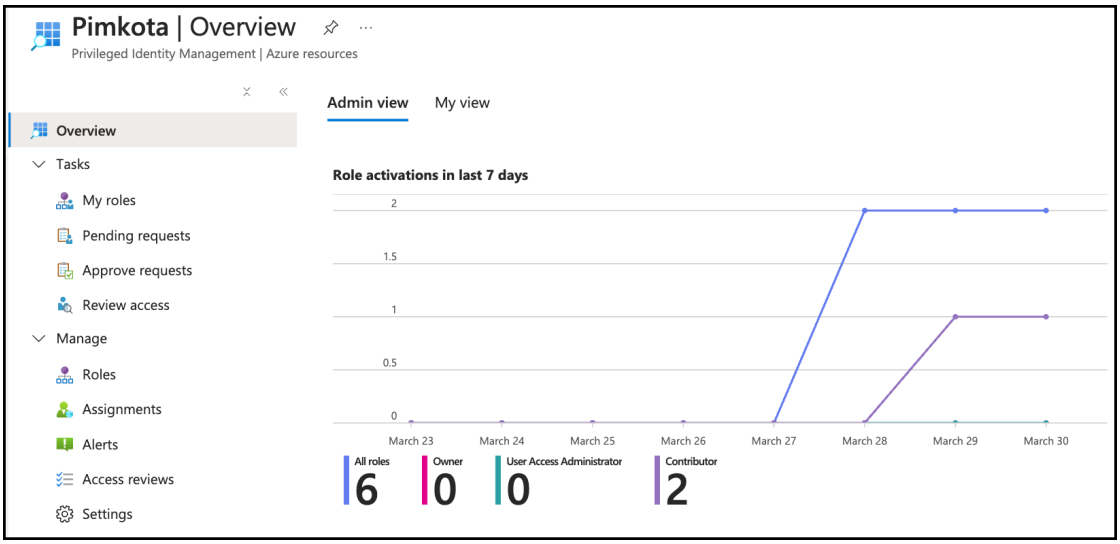


Figure 1: PIM Dashboard

When assigning a role, administrators choose between 'Eligible' and 'Active.' Active roles provide persistent access, similar to legacy models, while Eligible roles require explicit activation and follow custom duration settings. This setup enables PIM to enforce limited access for contractors or task-specific assignments. Figure 2 shows the role assignment interface designating role eligibility and activation scope.

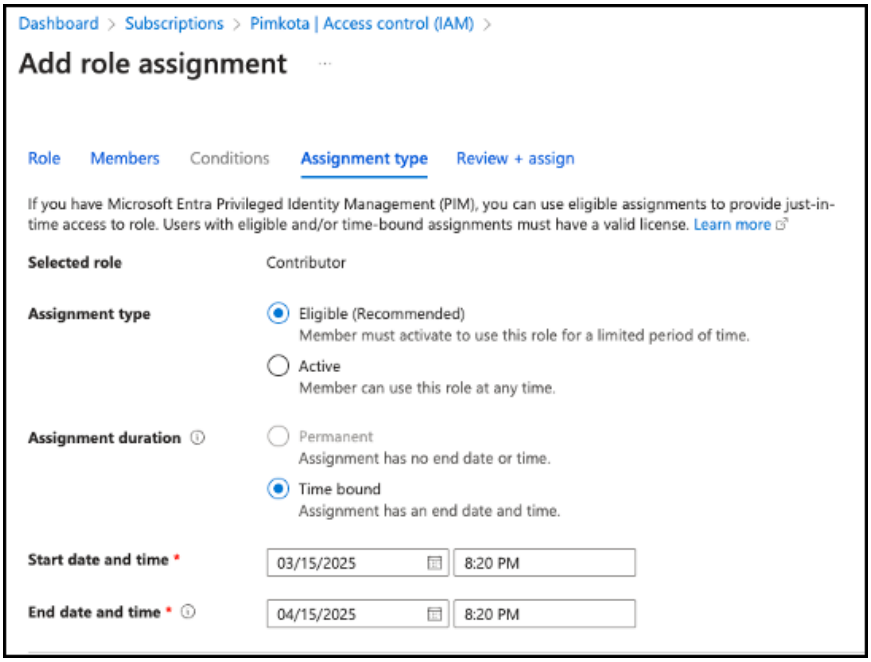


Figure 2: Add PIM Role Assignment

All roles use time-bound access, MFA enforcement, and justification prompts. Every user, internal or external, completes MFA before elevation. These controls support Zero Trust principles by enforcing short-lived, verified access.

The Owner role is assigned a one-hour Just-in-Time activation window and requires an MFA, a justification, and a support ticket reference for elevation. Figure 3 shows the Owner role's PIM policy configuration, which includes an optional approval workflow (not enabled in this study).

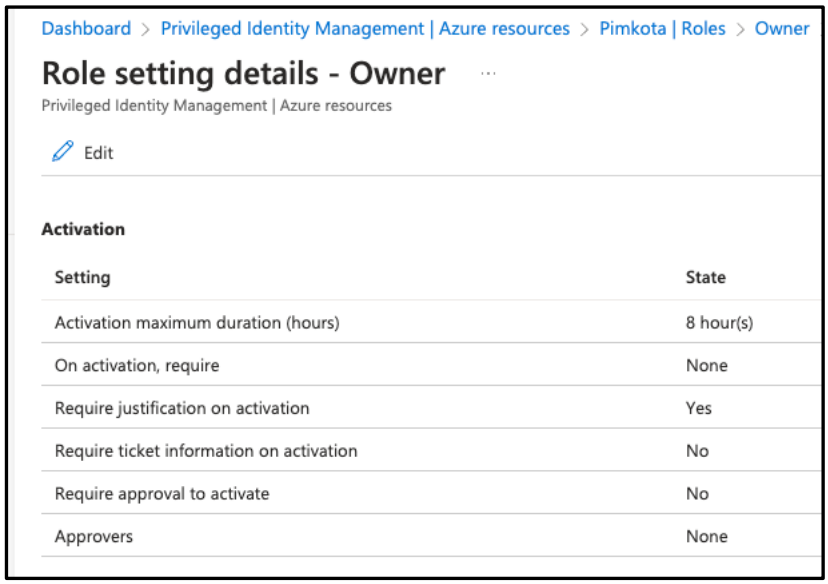


Figure 3: Owner Role Policy Settings

The Contributor role receives a three-hour elevation window to support extended configuration tasks, while the Reader role is limited to eight hours of read-only access. All configurations follow least-privilege principles and are applied using the administrative account pim_sysadmin@pimkota.com.

2.2 PIM Activation Process

Azure PIM enforces Just-in-Time access control by requiring users to explicitly activate roles before accessing resources. This section demonstrates the elevation process and the role-specific enforcement mechanisms used during testing.

Before elevation, users assigned to a role through PIM cannot access Azure subscription resources. This restriction applies even if the user is eligible for a role but has not initiated activation. Figure 4 displays the user's interface before any role is activated (note that no subscription resources are visible).

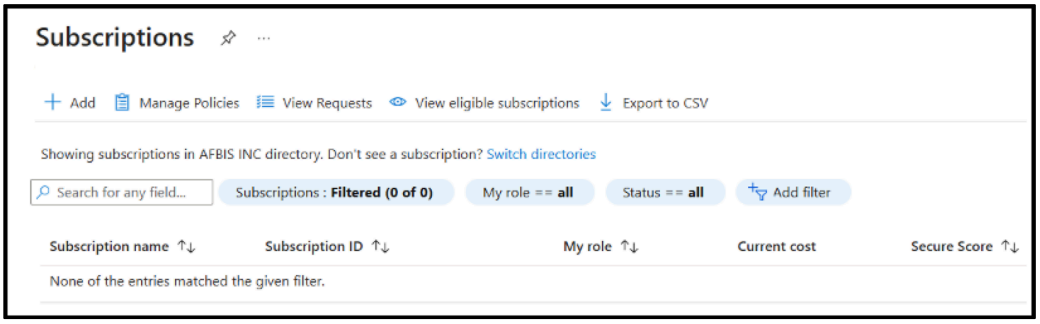


Figure 4: Subscriptions Before Elevation

When a user activates a role, access permissions apply based on the role's assigned scope. For example, elevating to the Reader role grants read-only access to subscription resources. This controlled transition demonstrates PIM's effectiveness in enforcing temporary, least-privilege access. Figure 5 shows the same subscription after elevation.

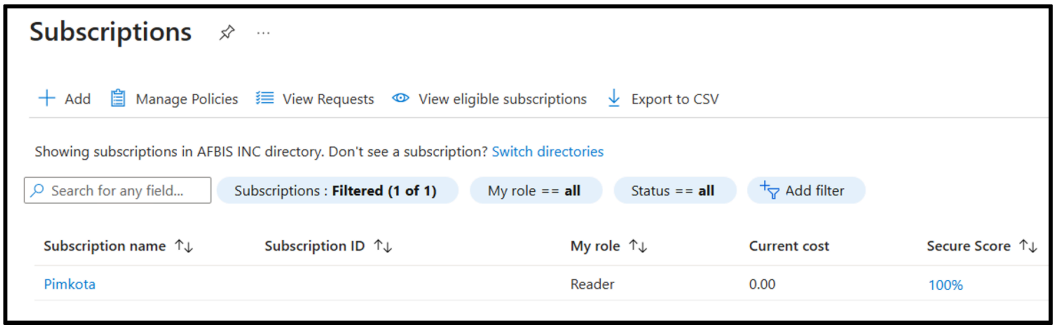


Figure 5: Subscriptions Access After Elevation

Users initiate elevation through the PIM interface, which lists all eligible roles and allows time-bound activation. This interface displays the role type, scope, expiration, and activation controls, as shown in Figure 6.

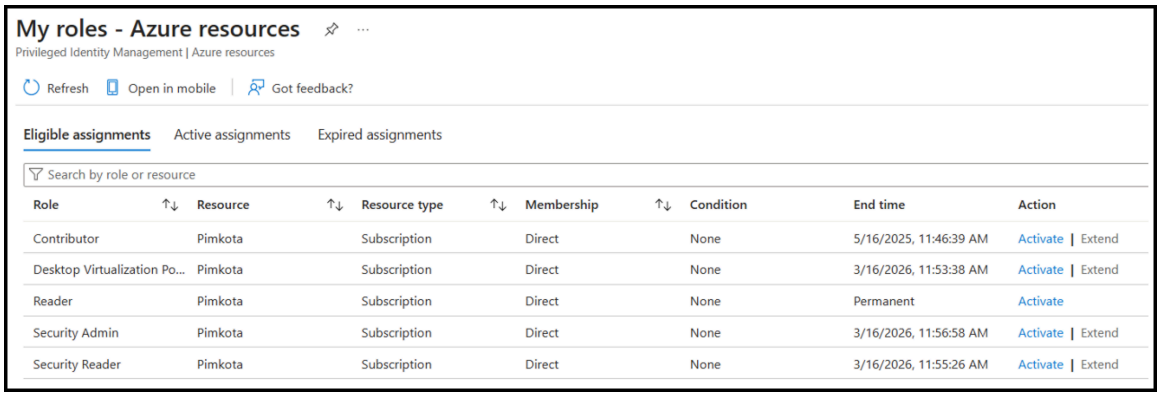


Figure 6: Eligible Role Window

The user initiates role activation through the PIM interface, which lists eligible roles. Each entry includes the role name and an option to activate. The user selects a role and starts the elevation process. Figure 7 shows this interface during elevation to the Reader role.

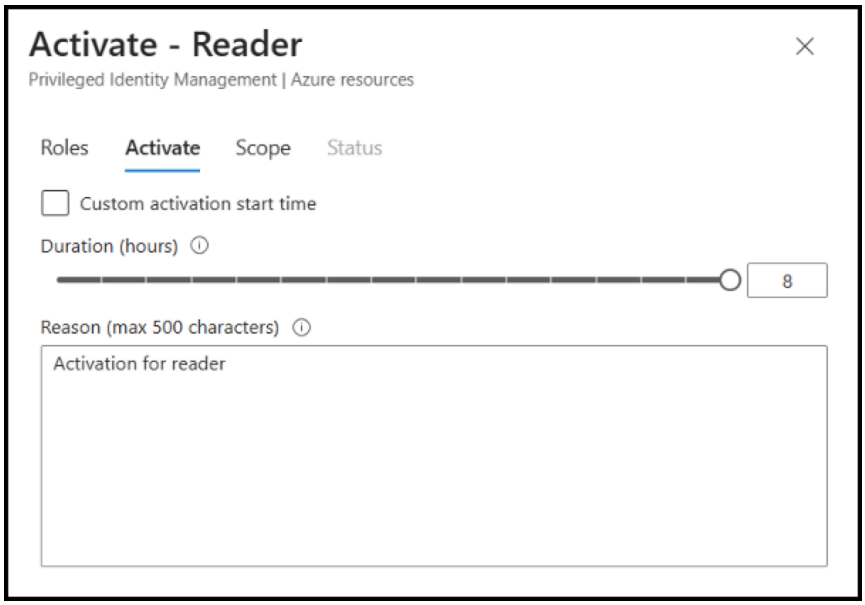


Figure 7: Reader Role Activation Window

Due to its elevated privileges, the Owner role provides full administrative access and uses the strictest enforcement settings. Activation of the Owner role requires the following:

- Completion of MFA.

- Submission of an access justification.
- Entry of a support ticket reference.

These controls grant access only to verified users with a legitimate need to elevate. PIM logs each activation, capturing both successful elevations and related activity. Figure 8 depicts the Owner role elevation windows, which include optional settings such as requiring the ticket system, ticket number, and reason for elevation. These requirements ensure elevated access remains justified, time-bound, and fully auditable.

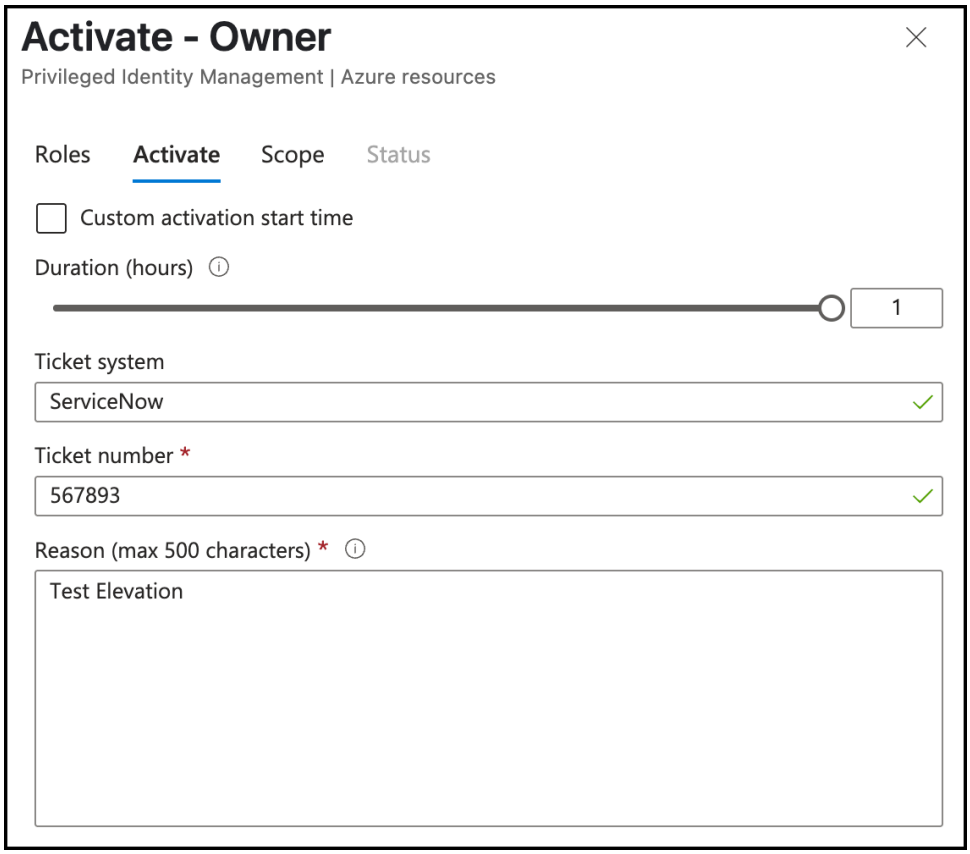


Figure 8: Owner Role Activation Window

PIM activation mechanics enforce privileges based on user roles, time limits, and predefined elevation conditions. Access is granted after identity verification and justification.

2.3 PIM Access Evaluation

The evaluation simulates realistic administrative scenarios in the Pimkota Azure environment to assess how effectively Azure PIM enforces Just-in-Time access controls. Everyday tasks such as adding resource tags, modifying configuration settings, and assigning user permissions occur under varied privilege levels, determining whether access is granted or denied based on elevation status.

Each scenario tests one of four roles: no elevation, Reader, Contributor, or Owner. The role-based tests operate under Just-in-Time conditions assigned to each role. Users must activate their assigned role to gain access. The system denies access when the elevation window expires or the user fails to meet requirements such as MFA or justification. The denials trigger immediate browser-based errors, providing feedback on policy enforcement. If users elevate to the same role, PIM generates automated email alerts to promote transparency and coordination among team members.

Azure sign-in logs support this evaluation by capturing authentication details for each access attempt. Log entries include user identity, authentication method, elevation status, location, and conditional access result. The following access controls are confirmed:

- **MFA enforcement**: All successful elevations require MFA.
- **Conditional Access enforcement**: Denied attempts indicate failure to meet policy conditions.
- **Failure and interruption tracking**: Logs highlight attempts blocked due to incomplete authentication or expired activation windows.

PIM restricts elevated access to verified users. It enforces identity verification and time-bound access controls to eliminate persistent administrative permissions. The Contributor, Owner, and Reader roles each receive tailored Just-in-Time durations based on their risk profiles. The Contributor role has a three-hour window to complete configuration tasks without requiring long-term access. The Owner role is limited to one hour because it can assign roles and create or delete resources. The Reader role receives eight hours of viewing privileges.

The evaluation also reveals limitations in Azure PIM's monitoring and identity enforcement. Azure Monitor records role activations and successful logins but does not capture every unsuccessful access attempt when elevation does not occur. This gap in visibility reduces the detection of privilege escalation attempts and may hinder incident response. Microsoft documentation acknowledges this limitation and recommends pairing PIM with Azure Sentinel or providing extended diagnostic logging for improved oversight (Microsoft, 2023)

The assessment supports that Azure PIM effectively enforces role-based, time-bound access and prevents unauthorized privilege escalation. Scenario-based testing highlights strengths, including enforcement, real-time blocking, and audit logging. It also identifies current limitations, such as gaps in failed access logging.

2.4 Task Simulation and Evaluation Criteria

Simulated tasks use Just-in-Time access configurations to evaluate the effectiveness of Azure PIM. These tasks span the Owner, Contributor, and Reader roles and a 'No Elevation' scenario to verify PIM's ability to enforce role-based access controls and time-bound privilege elevation. Users perform tasks through the Azure portal and, where applicable, use Terraform to simulate typical administrative actions and potential misuse cases.

Table 3 summarizes the simulated tasks assigned to each role and the expected enforcement outcomes based on PIM’s Just-in-Time model. Tasks under the Owner, Contributor, and Reader roles execute after elevation. The "No Elevation" scenario tested access without any active role assignment.

Role	Simulated Tasks	Expected Outcome
Owner	Assign Contributor role, modify access policies, deploy resources	All actions allowed when elevated
Contributor	Add resource tags, attempt permission assignment	Deployment and tagging allowed; role assignment denied
Reader	View resource configuration, attempt to tag/edit resources	Viewing allowed; modifications denied
No Elevation	Attempt all actions without activating a role	All actions denied

Table 3: Simulated Azure Subscription Tasks

All observed outcomes aligned with expected PIM behavior. The evaluation confirms that, when implemented correctly, PIM enforces role-based access controls, time-bound elevation, and least-privilege principles.

- Users successfully executed tasks within their assigned Just-in-Time windows and were blocked immediately after expiration, validating proper access revocation.
- Azure Monitor consistently captured successful task executions during active elevations. Failed actions were not reliably logged, particularly for the Reader role. This inconsistent logging reveals a logging gap in Azure's activity tracking for unauthorized attempts.

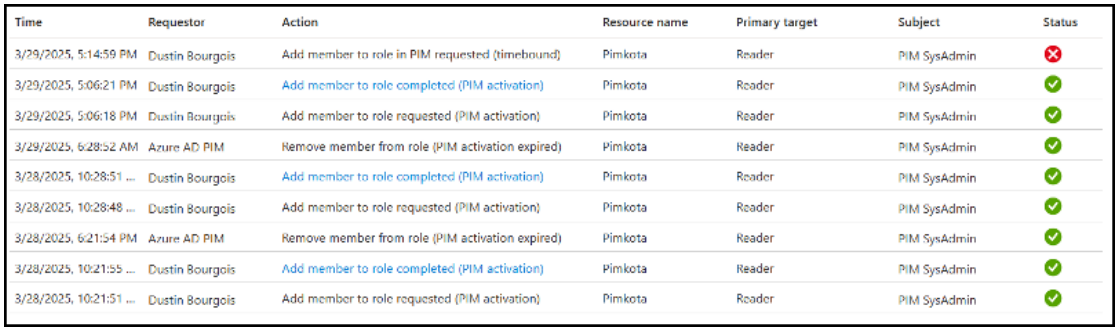
These results support that PIM effectively enforces Zero Trust and least-privilege models, offering a repeatable framework for testing privilege escalation controls in Azure environments.

3. Privileged Identity Management Results

Scenario-based testing confirms that Azure's Just-in-Time model effectively enforces time-bound role activation, prevents unauthorized access, and supports the principle of least privilege in the Pimkota Azure environment.

The evaluation simulated administrative behavior across different privilege levels and directly measured how policies enforced access. For example, the system denied a user's attempt to modify a resource group when they failed to elevate to the Contributor role. Upon elevation, with justification and MFA completed, the same action succeeded, demonstrating that PIM correctly enforced conditional access and time-scoped permissions.

The evaluation also confirmed that expired elevation sessions automatically revoked access, as expected. In one instance, the system denies access to a user who fails to complete MFA within the activation window and marks the attempt as 'Interrupted' in the sign-in log in Figure 9.



Time	Requestor	Action	Resource name	Primary target	Subject	Status
3/29/2025, 5:14:59 PM	Dustin Bourgois	Add member to role in PIM requested (timebound)	Pimkota	Reader	PIM SysAdmin	✗
3/29/2025, 5:06:21 PM	Dustin Bourgois	Add member to role completed (PIM activation)	Pimkota	Reader	PIM SysAdmin	✓
3/29/2025, 5:06:18 PM	Dustin Bourgois	Add member to role requested (PIM activation)	Pimkota	Reader	PIM SysAdmin	✓
3/29/2025, 6:28:52 AM	Azure AD PIM	Remove member from role (PIM activation expired)	Pimkota	Reader	PIM SysAdmin	✓
3/28/2025, 10:28:51 ...	Dustin Bourgois	Add member to role completed (PIM activation)	Pimkota	Reader	PIM SysAdmin	✓
3/28/2025, 10:28:48 ...	Dustin Bourgois	Add member to role requested (PIM activation)	Pimkota	Reader	PIM SysAdmin	✓
3/28/2025, 6:21:54 PM	Azure AD PIM	Remove member from role (PIM activation expired)	Pimkota	Reader	PIM SysAdmin	✓
3/28/2025, 10:21:55 ...	Dustin Bourgois	Add member to role completed (PIM activation)	Pimkota	Reader	PIM SysAdmin	✓
3/28/2025, 10:21:51 ...	Dustin Bourgois	Add member to role requested (PIM activation)	Pimkota	Reader	PIM SysAdmin	✓

Figure 9: Activity showing Elevations

These controlled tests demonstrate that PIM reliably enforces time-based access and blocks privilege escalation attempts. PIM strengthens role-based access governance by replacing permanent permissions with temporary, elevated access based on specific tasks and timeframes, reducing the attack surface associated with administrative privileges.

3.1 PIM Evaluation Results

The evaluation of Azure PIM demonstrates consistent enforcement of Just-in-Time access controls during role activation scenarios. Table 4 shows that PIM reliably blocked every unauthorized attempt to perform privileged actions outside defined

activation windows while successfully permitting intended actions during valid Just-in-Time sessions.

Test Scenario	Role	Outcome	User Tested
Activate Owner Role Without MFA	Owner	Blocked	Sys_admin
Add Permissions as Contributor	Contributor	Blocked	Sys_admin
Add Permissions as Owner	Contributor	Allowed	Sys_admin
Add Resources as Owner	Owner	Allowed	Sys_admin
Add Resources as Contributor	Contributor	Allowed	Sys_admin
Add Resources as Reader	Reader	Blocked	Sys_admin
Add Tag to Resource	Contributor	Allowed	Sys_admin
Add Tag to Resource	Reader	Blocked	Sys_admin
Outside Window Access	All Roles Eligible	Blocked	All PIM Roles
Modify Resources as Reader	Reader	Blocked	Sys_admin

Table 4: Test Results for Azure PIM Access Enforcement

All denied actions occurred outside an active Just-in-Time window or failed to meet elevation requirements, such as MFA failure. Test accounts encountered no failures when performing valid operations within the configured Just-in-Time access period. The result confirms that PIM enforces access according to role-based policies and time-based restrictions.

These results confirm that:

- **The Owner role** correctly denied access when users attempted to activate without completing MFA.
- **The Contributor role** was permitted to create and manage resources but blocked from assigning permissions, an operation reserved for the Owner role.
- **The Reader role** was appropriately restricted to view-only actions. Attempts to modify or tag resources were blocked.

Each outcome aligns with the assigned role's capabilities and confirms that the system enforces access strictly according to policy. The portal displays immediate errors for denied attempts, while Azure Monitor logs successful role activations and actions. Figure 9 shows activity logs capturing success and a few failure outcomes across different scenarios.

Role activation in PIM also generates an email alert to all users assigned to that role, improving visibility and accountability. As shown in Figure 10, the elevation process requires a justification before proceeding. Figure 11 displays a sample alert triggered after the Reader role was activated.

Figure 10: Activate Reader Role

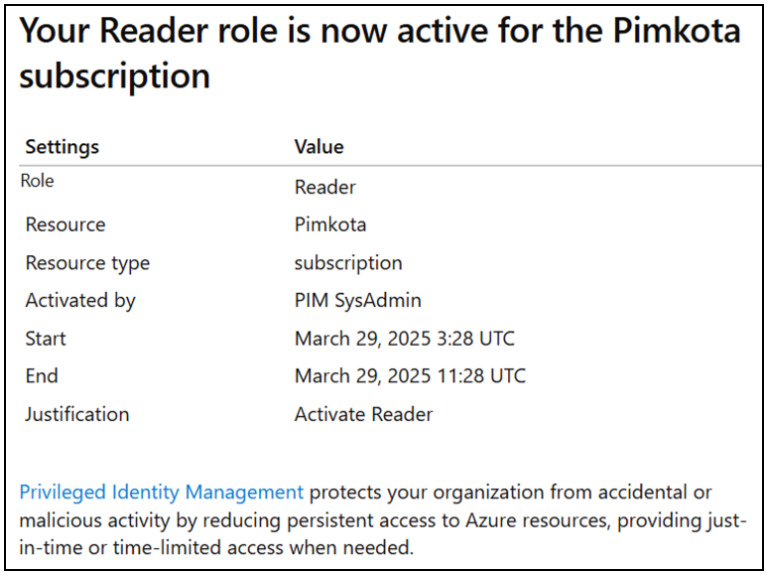


Figure 11: PIM Activation Alert

Messages confirm who elevates access, why the elevation occurs, and when the session begins and ends, reinforcing operational transparency. Azure Monitor captures the successful permission and role assignments for the owner role. The system blocks the

Contributor role from performing access control changes, aligning with Azure's role-based access model. Due to current logging limitations, Azure Monitor does not record denied attempts.

The Reader role cannot modify resources, and the system denies all modification attempts. Although the browser displays the blocks, Azure Monitor does not log the corresponding events.

Microsoft documentation notes that Azure Activity Logs typically capture create, update, or delete actions but not read-only or failed operations. As a result, when users with the Reader role attempt unauthorized actions, the activity is blocked in the portal but may not generate a corresponding log entry. This limitation constrains visibility into misuse attempts and reduces the monitoring trail during investigations (Microsoft, 2025).

Table 4 and the associated figures demonstrate that PIM's elevation rules function as expected, enforcing identity and time-bound access. The results reinforce PIM's role in reducing always-on privileges, strengthening identity governance, and improving operational security in Azure environments.

3.2 Comparative Analysis Results: PIM vs. Baseline

The analysis between baseline and PIM-enabled configurations reveals how privilege management impacts security outcomes in Azure environments. In the baseline configuration, administrative roles like the Owner role give account ftowner@pimkota.com always-on unrestricted access. These roles allow complete control over all subscription resources without requiring elevation. Privilege management practices where users retain elevated permissions indefinitely pose a risk to Azure environments. The always-on approach simplifies day-to-day administrative tasks such as resource deployment and configuration management but introduces significant risks. Attackers who compromise the Owner's account through phishing or credential theft gain continuous access to the subscription. They can create, modify, or delete resources with that access, which may lead to data exfiltration or service outages. A malicious insider

can exploit persistent access without triggering immediate detection. This unchecked access increases the potential for severe damage.

The PIM-enabled configuration transforms by enforcing a Just-in-Time access framework. The Owner role is restricted to a one-hour activation window, requiring multi-factor authentication and a documented justification for each elevation. The time-bound approach drastically reduces the exposure window. The baseline setup allowed all privileged actions, including resource modifications, to execute without restriction during testing. All unauthorized attempts made after the Just-in-Time window expired were blocked and given a "No Access" message, as shown in Figure 12.

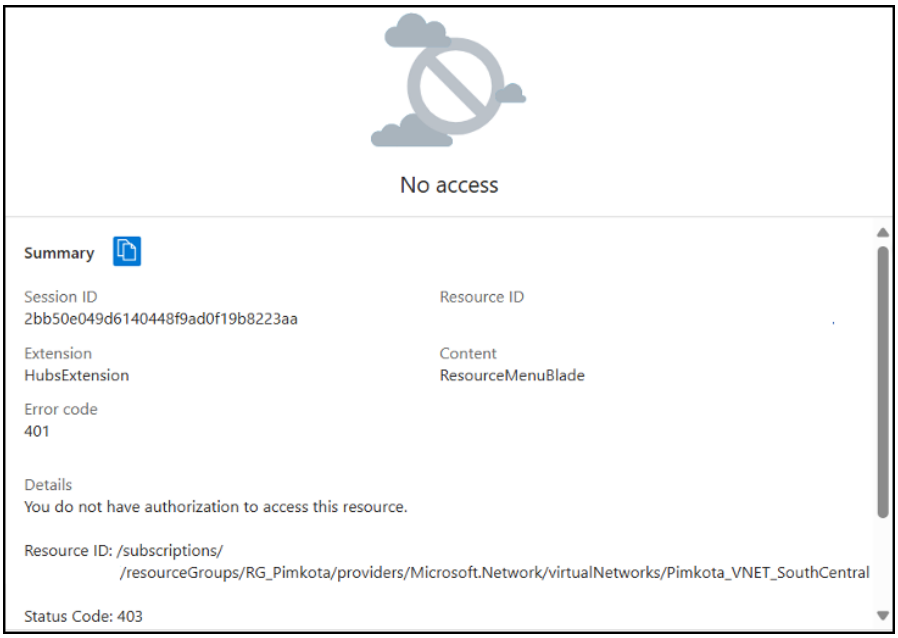


Figure 12: User Access Denied Resource Access After PIM expiration

Attackers who steal credentials can only operate during the short window when elevated access remains active. This limited timeframe restricts the potential damage. Organizations can reduce the attack surface by applying conditional access policies if attackers compromise systems or credentials.

PIM offers monitoring capabilities through its role-based logging. Audit logs capture successful role assignments and activation events in the baseline configuration.

Failures, such as MFA denials, timeout expirations, or configuration errors, are logged during activation. The system does not record unsuccessful attempts to access resources outside a Just-in-Time window. The logging gap means unauthorized access attempts without a valid elevation period may go undetected in standard PIM audit logs (Microsoft, 2023).

Testing with the Owner, Reader, and Contributor roles included creating a tag, deleting a virtual network, adding a resource, and removing a resource. Azure Monitor did not log any of these actions when attempted without the necessary permissions, particularly under the Reader role. Azure Monitor logs every successful change made within the subscription. Figure 13 shows an example of a test tag applied to an Azure virtual network.

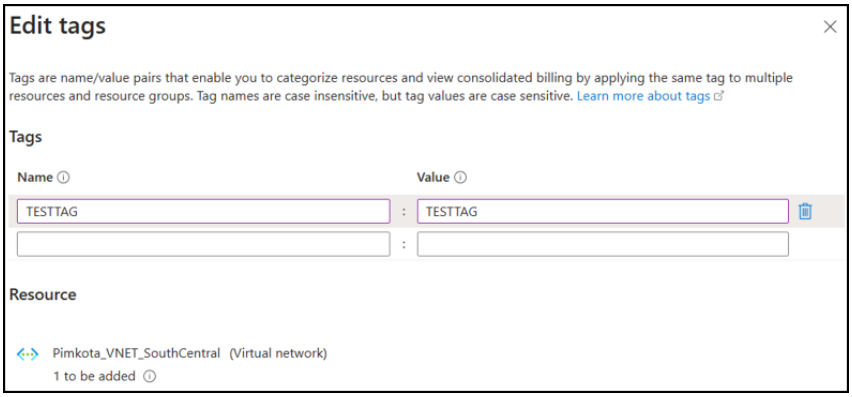


Figure 13: Apply Test Tag

All other active elevations for the Owner and Contributor had no problem adding, editing, or deleting the tag. Azure Monitor successfully displays the logs. The Reader role received an error message after the test tag was applied. The error message on the browser at the top right displayed "Failed to assign tags," as shown in Figure 14.

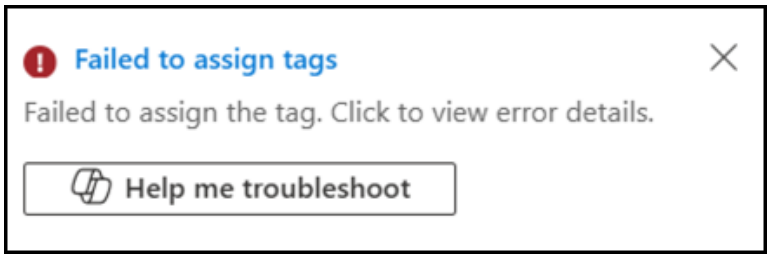


Figure 14 - Failed Test Tag

Limited logging weakens incident response because Azure Monitor does not record failed resource modification attempts. An example would be the Reader trying to change anything in the Azure subscription. Azure Monitor captures successful role activations and denied elevation requests but fails to log blocked actions after login. Employees with permanent Owner access in the baseline setup could modify critical resources without elevation alerts. Administrators can configure Azure Sentinel or Log Analytics alerts to notify users of subscription changes in always-on scenarios.

By enforcing Just-in-Time access, the narrow window of elevated access and audit logs during activation will help trace suspicious behavior when incidents arise. The comparison demonstrates how PIM enhances accountability and lowers risk exposure. An employee attempting to escalate privileges after hours would cause PIM's Just-in-Time restrictions and log alerts in a real-world insider threat scenario. The baseline scenario configuration has no protections to identify or prevent such behavior. Logs will still be captured in Azure Monitor but require more investigative work.

PIM requires justification before allowing access and enforces MFA. These controls aid in enforcing security policies and deter casual misuse. An email alert is also generated and emailed to everyone else with the same role.

Organizations that value simplicity may select the baseline configuration. The baseline organization is exposed to more risk in the current threat landscape because it has no time-based access limits. PIM adopts a more controlled and proactive strategy. It produces gains in risk mitigation and operational supervision and is consistent with contemporary security procedures.

Author Name, email@address

3.3 Terraform Testing

Testing explores how Azure PIM integrates with Terraform during automated provisioning in Azure. A user account named pim_terraform@pimkota.com receives the Contributor role with a three-hour Just-in-Time activation window. While the Just-in-Time role remains active, Terraform successfully authenticates and deploys all resources. The test confirms that PIM-enforced elevation supports Terraform workflows when a human user initiates the session.

Once the three-hour Just-in-Time window expires, Terraform operations fail. Results confirm that PIM correctly enforced time-bound access and blocked further privileged actions.

A key limitation appears when assigning Just-in-Time access to a Terraform service principal. Figure 15 shows that the Azure interface only allows permanent "Active" assignments for service principals and does not support the "Eligible" designation required for Just-in-Time activation. Without native PIM integration, service principals retain continuous access by default, which conflicts with least-privilege practices in infrastructure-as-code environments.

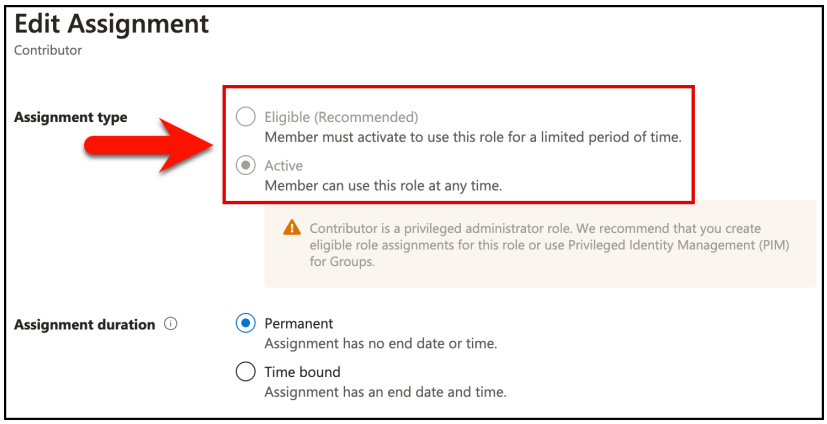


Figure 15: Assigning PIM to Terraform Service Principal

To reduce this risk, organizations apply Conditional Access policies to service principals. These controls restrict access based on IP range, sign-in risk, device

compliance, or workload identity federation. While Conditional Access does not replicate Just-in-Time behavior, it is a compensating safeguard that reduces automation account exposure.

Organizations consider replacing service principals with Azure-managed identities for longer-term solutions, especially when automating deployments from trusted Azure resources. Managed identities eliminate credential management, support role-based access control, and offer tighter scoping than traditional service principals. Azure-managed identities currently do not support native Just-in-Time elevation, which limits their use in scenarios requiring temporary privilege escalation.

3.4 Summary of Key Findings

The evaluation confirms that Azure PIM's Just-in-Time access model significantly reduces privilege escalation risks within Azure environments by minimizing persistent administrative privileges. Testing scenarios include manual elevation attempts, automated Terraform deployments, and comparisons against baseline Microsoft Entra ID Security Defaults.

PIM consistently enforces MFA and strict time-bound access requirements in all test cases. Unauthorized elevation attempts, both manual and automated, are effectively blocked. Terraform operations succeed only when executed with valid Just-in-Time elevation, reaffirming that PIM strengthens security by ensuring elevated privileges are granted only when required and within a tightly controlled time window.

The evaluation also reveals several important limitations. One notable concern is vulnerability to MFA fatigue, where attackers send repeated MFA prompts to overwhelm users into approving unauthorized access. Microsoft acknowledges this issue and recommends controls like number matching in MFA prompts to reduce this risk. Microsoft's security team documents large-scale MFA fatigue attacks targeting Entra ID, underscoring the importance of enforcing elevation through PIM and Just-in-Time to reduce unnecessary privilege exposure and require identity re-verification at the time of access (Microsoft Security, 2022).

The evaluation identifies further limitations in how service principals in automated workflows interact with PIM. Non-human identities cannot directly leverage PIM's Just-in-Time functionality and require manual configuration and elevation. Manual handling increases administrative overhead and raises the risk of misconfiguration, emphasizing the need for improved automation support.

Recent incidents reinforce the necessity of stringent access control frameworks. In July 2023, Microsoft investigated a breach involving threat actor Storm-0558, which exploits weaknesses in token issuance and access control within Microsoft's cloud environments. The Storm-0558 incident highlights the critical importance of short-lived tokens, robust identity verification, and granular visibility into privilege use core elements of Azure PIM (Microsoft Security, 2023).

The evaluation demonstrates that Azure PIM's Just-in-Time model enhances security by reducing privilege persistence and enforcing granular access controls. Addressing vulnerabilities such as MFA fatigue and limitations regarding non-human identities through improved automation and stricter MFA policies remains essential for a strong security posture.

4. Recommendations

The evaluation validates that Azure PIM with Just-in-Time access effectively enforces role-based controls, reduces privilege escalation risks, and strengthens identity governance in Azure environments. These outcomes reinforce the value of time-bound privilege enforcement and strong identity verification for managing administrative access.

Organizations should implement phishing-resistant MFA methods like Microsoft Authenticator with number matching. These methods reduce the risk of MFA fatigue attacks, where repeated push notifications attempt to trick users into approving unauthorized access. Administrators require strong MFA for high-impact roles like Owner and Contributor, where elevation grants the ability to configure, assign, or delete critical resources.

Administrators are encouraged to apply Conditional Access policies alongside PIM to restrict access based on device compliance, geographic location, IP ranges, or user risk scores. Using Conditional Access with Just-in-Time elevation improves enforcement and limits privilege exposure by requiring specific conditions before role activation.

Organizations are encouraged to centralize real-time monitoring and role elevation auditing through Azure Monitor or Microsoft Sentinel. While native logging does not capture every failed elevation attempt, successful activations, and anomalous behavior are visible and can be correlated with access timelines for incident response.

Service principals face a challenge in enforcing just-in-time controls. These identities require manual elevation workflows, which introduces risk in automated environments. Applying the same principles of scoping, audit logging, and conditional restrictions used for human accounts can help reduce this gap until native PIM support is available.

Organizations can reduce always-on privileges and strengthen operational resilience in Microsoft Entra ID environments by combining Just-in-Time activation with phishing-resistant MFA, Conditional Access policies, and stronger identity controls for automation.

4.1 Implications for Future Research

Azure PIM with Just-in-Time access shows measurable value in limiting privilege persistence and enforcing policy-driven access control. The evaluation identifies key areas where further research and platform improvement are needed to strengthen these capabilities.

Future studies should continue exploring phishing-resistant MFA and its application across high-impact roles. Research into behavioral prompts, adaptive authentication, and attack resistance techniques such as number matching and continuous

access evaluation may help reduce MFA fatigue, a recurring theme in recent security incidents.

Conditional Access remains a powerful tool for controlling Just-in-Time elevation, but its effectiveness may vary across devices and user environments. Further research is needed to understand how device compliance affects role activation, particularly in bring-your-own-device (BYOD) scenarios where state transitions can lead to unexpected elevation denials or over-permission.

Service principals present another gap in Just-in-Time coverage. These non-human identities require manual configuration for scoped access, limiting their ability to participate in dynamic elevation workflows. Future work should investigate policy-based elevation for workloads, including identity-bound automation accounts with short-lived tokens and enhanced audit trails.

Ongoing research should also evaluate how PIM integrates with broader zero-trust strategies. Understanding how Just-in-Time elevation intersects with workload identity, session risk, and decentralized trust decisions will help organizations scale privileged access controls across hybrid environments as threat models evolve.

5. Conclusion

This study evaluates Azure PIM and its Just-in-Time access model as a method for reducing privilege escalation risks in Microsoft Azure. Testing confirms that PIM enforces time-bound access across critical subscription roles, ensuring that elevated privileges are only active during approved time windows. Unauthorized actions attempted outside those windows are blocked, narrowing the window of opportunity for misuse.

The findings show that PIM enables a shift from permanent administrative access to temporary, auditable elevation. This shift supports zero-trust principles by increasing visibility through logging, limiting standing privileges, and aligning with modern identity

governance expectations. Compared to traditional static role assignments, Just-in-Time elevation reduces the overall attack surface and introduces policy-backed elevation workflows.

MFA fatigue introduces risks when users face repeated prompts. Service principals require manual role assignment and cannot use Just-in-Time functionality natively, creating friction in automation use cases. The inability to log all failed elevation attempts limits complete visibility into potential privilege escalation attempts.

PIM provides a structured and practical approach for enforcing least-privilege access in Azure. Organizations that integrate PIM with Conditional Access, vigorous MFA enforcement, and device compliance policies improve control over privileged operations and reduce exposure to identity-based threats. This evaluation supports PIM with Just-in-Time as a reliable model for securing administrative access in cloud-native environments.

References

Ahmadi, S. (2024). Systematic literature review on cloud computing security: Threats and mitigation strategies. *Journal of Information Security, 15*(2), 148–167. https://doi.org/10.4236/jis.2024.152010

Center for Internet Security. (2021). *CIS critical security controls version 8*. https://www.cisecurity.org/controls/v8/

HashiCorp. (2024). *Terraform Azure Provider Documentation.* HashiCorp. https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs

Microsoft. (2023). *Audit logs in Microsoft Entra Privileged Identity Management*. Microsoft Learn. https://learn.microsoft.com/en-us/entra/identity/monitoring-health/reference-audit-activities

Microsoft Security. (2022, November 2). Defending against token theft and MFA fatigue. *Microsoft Security*. https://www.microsoft.com/en-us/security/blog/2022/11/02/defending-against-token-theft-and-mfa-fatigue/

Microsoft Security. (2023, July 14**).** Summary of Microsoft's investigation into Storm-0558 campaign. *Microsoft Security*. https://www.microsoft.com/en-us/security/blog/2023/07/14/summary-of-microsofts-investigation-into-storm-0558-campaign/

Microsoft. (2023, September 26). *Secure workload identities with Conditional Access*. Microsoft Entra Blog. https://www.microsoft.com/en-us/security/blog/2023/09/26/secure-workload-identities-with-conditional-access/

Microsoft. (2024). *Sign-in logs in Microsoft Entra ID*. Microsoft Learn. https://learn.microsoft.com/en-us/entra/identity/monitoring-health/concept-sign-in-logs

Microsoft. (2023). *Review access to resources using Azure AD access reviews*. Microsoft Learn. https://learn.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

Microsoft. (2023). What is Azure Privileged Identity Management? Microsoft Learn.

Microsoft. (2023). *What is Azure Privileged Identity Management?* Microsoft Learn. https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure

NIST. (2020). *Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5).* National Institute of Standards and Technology.

Author Name, email@address

Verizon. (2025). 2025 Data Breach Investigations Report. Retrieved from https://www.verizon.com/business/resources/reports/dbir/

Appendix A: MITRE ATT&CK Techniques Mitigated by Azure PIM with Just-in-Time

ATT&CK Tactic	**Technique (ID)**	**Mitigation via Azure PIM**
Privilege Escalation	Abuse Elevation Control (T1548)	Time-bound elevation with MFA and justification blocks escalation.
Credential Access	Valid Accounts (T1078)	Just-in-Time elevation and MFA prevent stolen credentials from granting access.
Persistence	Account Manipulation (T1098)	PIM requires elevation and auditing for account changes.
Defense Evasion	Domain Policy Mod (T1484)	Admin actions require elevation, limiting persistence changes.
Privilege Escalation	Create/Modify System Process (T1543)	PIM blocks unauthorized system changes unless elevated.
Credential Access	Brute Force (T1110)	MFA for elevation prevents success even if a password is guessed.
Credential Access	Credentials from Password Stores (T1555)	PIM restricts use of stolen credentials without re-authentication.
Initial Access	Phishing (T1566)	Short elevation windows and MFA reduce impact of phished credentials.
Persistence	Create Account (T1136)	PIM enforces elevation and auditing for new account creation.
Privilege Escalation	Exploitation for Privilege Escalation (T1068)	Time-limited elevation reduces window for exploitation.

Azure PIM enforces key mitigations aligned with MITRE ATT&CK by requiring elevation for sensitive actions, limiting persistence, and enforcing time-bound, verified access. These controls reduce risk from both internal and external threats.