Conference Proceedings International Conference on Sustainable Development Goals-Challenges, Issues & Practices by TMIMT- College of Management, Teerthanker Mahaveer University, Moradabad 25th & 26th April 2025. TMIMT International Journal (ISSN: 2348-988X)

# Never Trust, Always Verify: Analysis of Zero Trust Best Practices for Conditional Access

Shubham Rawat
MBA- 2nd Year
Teerthanker Mahaveer Institute of Management & Technology
Teerthanker Mahaveer University,
Moradabad (U.P.)

**Abstract**

The rise in advanced persistent threats (APTs) requires more robust security measures to protect an organization's sensitive data. This study examines the effectiveness of Microsoft Entra's Conditional Access policies in thwarting adversarial bypass attempts, particularly in light of vulnerabilities exposed by recent high-profile breaches, such as those involving the Lapsus $ hacking group. These incident shave highlighted the need for more resilient security frameworks, especially concerning traditional multifactor authentication (MFA) systems. Through comprehensive testing, this research evaluates the strengths and limitations of various Conditional Access policies in addressing MFA attacks. It identifies potential enhancements to improve their robustness within a Zero Trust framework. The findings provide practical insights into the current capabilities of Microsoft Entra Conditional Access and offer recommendations for organizations seeking to strengthen their identity and access management (IAM) strategies against evolving cyber threats.

**Keywords:** Multi-Factor Authentication (MFA), Least Privilege Access, Continuous Verification, Threat Detection, Secure Access Control

## Introduction

In today’s cyber security Landscape, defending against advanced persistent threats (APTs) is more crucial than ever. Conditional access is a critical element of zero trust architectures that help protect access to data by enforcing access policies based on the conditions of the request. Microsoft Entra Conditional Access is a cloud-native solution for Azure environments, providing enhanced security to strengthen an organization’s cloud security posture.

Recent analyses by MITRE have shed light on the threat of advanced persistent threats. Their articles, such as "Advanced Cyber Threats Impact Even the Most Prepared" (MITRE, 2023a),

"Technical Deep Dive: Understanding the Anatomy of a Cyber Intrusion" (MITRE, 2023b), and "Infiltrating Defenses: Abusing VMware in MITRE's Cyber Intrusion" (MITRE, 2023c), reveal the sophisticated methods used to breach well- defended environments protected with Multifactor Authentication (MFA).

MicrosoftexperiencedabreachthatexploitedMFAfatigueattacks.Inthisattack, the hacker group Lapsus$ used stolen credentials to bombard users with MFA push notifications, hoping the users would eventually approve one out of frustration or confusion. This social engineering attack is known as MFA bombing or push notification spam, which preys on people's tendency to seek relief from persistent notifications. Once the user approves the malicious request, the attacker gains access to the account (Bleeping Computer, 2023; Security Week, 2022).

Conditional access can play a significant role in preventing such attacks by ensuring that only verified users access critical resources under secure conditions, taking into account a variety of signals that may include user location, device, time, and behavior. Microsoft Entra Conditional Access policies enforce continuous authentication and integrate remote attestation, enhancing security measures. These policies can dynamically adjust access controls based on real-time risk assessments, ensuring that only trusted devices and users can access sensitive resources.

However, setting up and configuring these policies is not straightforward and is susceptible to misconfiguration or needs to be appropriately enforced (Colley,B,2022). They are not enabled by default, and cloud administrators must be well-versed in designing, testing, and deploying accurate and secure conditional access policies. Microsoft Azure and the Center for Internet Security (CIS) offer conditional access policy templates and guidance to help organizations improve the ircloud security posture. While these templates are valuable, there are areas to increase security and enable automation of these policy configurations to tackle the complex tactics, techniques, and procedures (TTPs) of APTs.

The research will evaluate the effectiveness of Microsoft Entra Conditional Access policies against various attack scenarios. The aim is to uncover any gaps in the template policies and suggest enhancements for a more robust Zero Trust security framework. This study

contributes to the broader discussion on IAM best practices and the continuous improvement needed to address cyber threats.

**Research Method**

The primary research question for this study is: What is the effectiveness of MicrosoftEntra's(formerlyAzureActiveDirectory)ConditionalAccessindetectingand preventing adversarial bypass attempts under various attack scenarios? The hypothesis assumes that Microsoft's Conditional Access effectiveness can be validated through a comprehensive approach involving simulated attack scenarios, policy variation testing, and iterative refinement.

**Data Collection and Analysis**

The responses from the simulated attack scenarios are recorded and cross- validated with conditional access logs in MicrosoftEntraID. This high-level procedure is as follows:

Collect logs from the Azureportal, focused on conditional access and sign-in logs.

Analyze the logs to determine the effectiveness of each policy in preventing unauthorized access and policy violations.

Compare results against the baseline to identify improvements or gaps in the conditional access policies (Splunk, 2022).

**Additional Considerations**

The study will be performed using iterative rounds of testing, where the refinement of conditional access policies will be based on initial findings and observed gaps in coverage. The test procedures, scripts, and infrastructure-as-code configurations will be made available to the security community to enable repeatability and further study. In addition to the test procedures, scripts, and IaC, comprehensive documentation of all configurations, test scenarios, and results will be maintained to ensure transparency (National Institute of Standards and Technology, 2020).

**Findings and Discussion**

This section presents a detailed analysis of the efficacy of various MicrosoftEntra Conditional Access policies when subjected to adversarial attack simulations. The testing was conducted

using a controlled environment where different conditional access policies were configured, manipulated, and evaluated for their ability to enforce security measures and prevent unauthorized access.

The findings show the strengths and vulnerabilities of these policies, specifically in scenarios where sophisticated tactics, techniques, and procedures (TTP) were employed to circumvent security controls. This section assesses the current state of Microsoft's Conditional Access solutions and provides insights into potential improvements that could enhance their resilience against emerging threats within a Zero Trust framework.

**Conclusion**

This study reaffirms the importance of robust Conditional Access policies in fortifying cloud environments against the ever-evolving landscape of cyber threats. The evaluation of Microsoft Entra Conditional Access policies has revealed their critical role in enforcing security controls but also exposed areas where these policies may be vulnerable to circumvention, mainly when adversaries employ sophisticated techniques like social engineering or exploit specific gaps in policy configurations.

To mitigate these risks, organizations must adopt a proactive approach, which includes regularly reviewing and updating their Conditional Access policies, implementing phishing-resistant MFA, and maintaining vigilant monitoring of sign-in logs for unusual activities. Organizations can achieve a more comprehensive and resilient security posture by supplementing the foundational policies recommended by Microsoft and CIS with additional, tailored controls. Moreover, future research should extend to advanced integrations and comparative analyses across different cloud platforms to ensure that security strategies remain effective and adaptable in response to emerging threats.

**References**


- Amazon Web Services(AWS).(n.d.).Access policies and permissions in IAM. AWS Identity and Access Management User Guide. https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html
- BleepingComputer. (2023). Microsoft enforces number matching to fight MFA fatigue

attacks. Retrieved from https://www.bleepingcomputer.com/news/microsoft/microsoft-enforces-number-

- matching-to-fight-mfa-fatigue-attacks
- CenterforInternetSecurity.(2022).CISMicrosoftAzureFoundationsBenchmark v1.3.0. Retrieved from https://www.cisecurity.org/benchmark/azure
- Colley, B. (2022, September 15). Five most common conditional access misconfigurations.Practical365.https://practical365.com/five-most-common-
- conditional-access-misconfigurations/
- Cybersecurity&InfrastructureSecurityAgency(CISA).(2022,October).Implementing Phishing-Resistant MFA [Fact sheet]. https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-
- phishing-resistant-mfa-508c.pdf
- Department of Defense. (2022, July). Zero Trust Reference Architecture (Version 2.0). https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep
- 22.pdf
- HashiCorp.(2021).Terraform: Up& Running(3rd ed.).O'Reilly Media.
- Microsoft. (2023a). Conditional Access in Microsoft Entra. Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/conditional-access

- Microsoft.(2023b).WhatisMicrosoftEntraPrivilegedIdentityManagement?Retrieved from https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-
- management/pim-configure
- Microsoft. (2024a). Plan a Conditional Access deployment. Retrieved from https://learn.microsoft.com/en-us/entra/identity/conditional-access/plan-
- conditional-access#prerequisites
- Microsoft(2024b).Requirecompliantdevice,MicrosoftEntrahybridjoineddevice,or multifactor authentication for all users. Retrieved from https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-
- conditional-access-policy-compliant-device
- MITRE. (2023a, March 30). Advanced cyber threats impact even the most prepared. Medium.https://medium.com/mitre-engenuity/advanced-cyber-threats-impact-
- even-the-most-prepared-56444e980dc8
- MITRE.(2023b,April1).Technicaldeepdive:Understandingtheanatomyofacyber intrusion. Medium. https://medium.com/mitre-engenuity/technical-deep-dive-
- understanding-the-anatomy-of-a-cyber-intrusion-080bddc679f3
- MITRE. (2023c, April 5). Infiltrating defenses: Abusing VMware in MITRE's cyber intrusion.Medium.https://medium.com/mitre-engenuity/infiltrating-defenses-
- abusing-vmware-in-mitres-cyber-intrusion-4ea647b83f5b