International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 5, September-October 2023||

DOI:10.15662/IJRPETM.2023.0605025

AI-Driven Zero Trust Identity Security in Microsoft Azure: Adaptive Risk-Based Access Using Microsoft Entra ID

Shailaja Beeram

Azure Cloud Architect, USA

shbeeram1@gmail.com

ABSTRACT: The rapid adoption of cloud computing, remote work, Software-as-a-Service (SaaS), and hybrid enterprise environments has significantly expanded the identity attack surface. Traditional perimeter-based security models are increasingly inadequate because users and applications frequently access organizational resources from different devices, locations, and networks. Zero Trust security addresses this challenge by continuously evaluating identity, device, resource, and contextual signals rather than implicitly trusting access based on network location.

This paper proposes an **AI-driven adaptive identity security framework** for Microsoft Azure based on Microsoft Entra ID, Conditional Access, Identity Protection, Privileged Identity Management, and security telemetry. The framework uses risk signals and machine-learning-supported identity protection to dynamically evaluate authentication attempts and apply access decisions according to contextual risk. Rather than implementing uniform authentication requirements for every request, the proposed model applies adaptive controls such as multifactor authentication, access restriction, password remediation, or session blocking according to detected risk. The study examines architecture, automation strategies, and practical use cases including compromised-account detection, anomalous sign-in response, privileged-access protection, and automated identity-risk remediation. The proposed approach demonstrates how identity can function as a dynamic security perimeter for modern Azure environments while supporting Zero Trust principles.

KEYWORDS: Microsoft Azure, Microsoft Entra ID, Azure Active Directory, Zero Trust, artificial intelligence, machine learning, Conditional Access, Identity Protection, Privileged Identity Management, multifactor authentication, identity security, risk-based authentication, cloud security, security automation.

I. INTRODUCTION

Enterprise identity has become one of the most important security boundaries in cloud computing. Users no longer access applications exclusively from corporate networks or managed office devices. Remote employees, contractors, administrators, applications, and automated workloads may connect to enterprise resources from numerous locations and devices.

This shift reduces the effectiveness of conventional perimeter-oriented security.
Zero Trust addresses this problem through the principle of **"never trust, always verify."** Access decisions should be based on explicit verification of identity and contextual signals rather than assumptions derived from network location.

Microsoft's cloud identity platform, renamed Microsoft Entra ID from Azure Active Directory in 2023, provides identity, authentication, authorization, Conditional Access, and identity-risk capabilities for Azure and integrated applications.

Conditional Access enables organizations to evaluate signals such as user identity, location, device state, application, and risk before determining whether access should be granted, challenged, or blocked.

Microsoft Entra ID Protection complements these controls by identifying suspicious identity and sign-in behavior using risk detection and machine-learning-supported analysis.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 5, September-October 2023||

DOI:10.15662/IJRPETM.2023.0605025

This creates an opportunity to move enterprise authentication from a largely static model:
User → Password → Access
toward an adaptive model:
User → Contextual Signals → Risk Evaluation → Conditional Access Decision → Verification → Access
The central research question examined in this paper is:
How can machine-learning-supported identity-risk detection and adaptive Conditional Access policies improve Zero Trust security in Microsoft Azure without imposing unnecessary authentication friction on legitimate users?
This paper proposes an adaptive Zero Trust identity framework that integrates risk detection, Conditional Access, privileged-access governance, and automated remediation.

II. LITERATURE REVIEW

Traditional enterprise identity systems frequently relied on network boundaries and static authentication controls. However, cloud adoption and distributed workforces have challenged assumptions that users operating within organizational networks should automatically receive higher levels of trust.

Zero Trust architectures replace implicit trust with continuous verification. The National Institute of Standards and Technology (NIST) defines Zero Trust Architecture as an approach in which trust is not granted implicitly based on physical or network location and access decisions are continually evaluated.

Identity therefore becomes a central policy enforcement point.
Microsoft's Zero Trust architecture emphasizes explicit verification, least-privilege access, and the assumption that breaches may occur. Microsoft Entra ID provides the identity control plane through which these principles can be implemented for Azure and connected applications.

Conditional Access evaluates contextual signals and applies organizational access policies. For example, a normal sign-in from a known user and compliant device may be allowed, while a higher-risk authentication attempt may require multifactor authentication or be blocked.

Microsoft Entra ID Protection uses machine-learning and security intelligence to identify identity-related risks, including suspicious sign-in behavior and indicators associated with compromised credentials.

Privileged Identity Management (PIM) addresses another critical component of Zero Trust: persistent administrative privilege. PIM enables organizations to manage and monitor privileged roles and use time-bound or approval-based activation rather than maintaining unnecessary permanent administrator assignments.

Existing security research has established the importance of adaptive authentication and behavioral analysis. However, enterprise identity protection requires more than anomaly detection alone. Risk information must ultimately influence enforceable access decisions and remediation processes.

This paper therefore examines identity risk as part of a broader automated control loop connecting detection, decision, enforcement, remediation, and monitoring.

III. METHODOLOGY

This research uses a **scenario-based architectural analysis** to evaluate adaptive identity protection within Microsoft Azure.
The proposed framework is evaluated across four security dimensions:

- **Identity Risk Detection:** Identification of suspicious authentication behavior.
- **Adaptive Access Enforcement:** Modification of authentication requirements according to risk.
- **Privileged Access Governance:** Reduction of standing administrative privilege.
- **Automated Remediation:** Response to identities classified as potentially compromised.

The evaluation considers representative authentication scenarios including:
1. normal employee authentication;
2. authentication from an unusual location;

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 5, September-October 2023||

DOI:10.15662/IJRPETM.2023.0605025

3. suspicious or high-risk sign-in;
4. privileged administrator authentication;
5. authentication from unmanaged or noncompliant devices.

The effectiveness of the framework can be assessed using:

- suspicious sign-in detection rate;
- false-positive rate;
- blocked high-risk authentication attempts;
- successful MFA challenges;
- privileged-role exposure duration;
- remediation completion rate;
- authentication friction for legitimate users.

The objective is not simply to maximize blocked authentication attempts. Instead, the framework attempts to improve security while maintaining usable access for legitimate users.

IV. ARCHITECTURE AND AUTOMATION FRAMEWORK

The proposed architecture uses identity as the primary Zero Trust decision point.
The operational flow is:

User / Administrator
↓
Microsoft Entra ID Authentication
↓
Identity + Device + Location + Application Signals
↓
Identity Protection Risk Evaluation
↓
Conditional Access Policy Engine
↓
Adaptive Security Decision
↓
Allow / Require MFA / Require Remediation / Block
↓
Application or Azure Resource

The architecture combines several Azure identity-security components.

4.1 Risk-Based Identity Evaluation

Microsoft Entra ID Protection can detect identity-related risks associated with users and authentication events.
Instead of treating every authentication request equally, the framework evaluates contextual information to determine whether additional verification is required.
Conceptually:
Low Risk → Normal Access
Medium Risk → Additional Verification
High Risk → Block or Identity Remediation
This enables security controls to adapt to authentication context.

4.2 Conditional Access Enforcement

Conditional Access serves as the policy enforcement layer.
Policies can consider signals such as:

- user or group;
- application being accessed;
- location;
- device state;
- authentication context;
- sign-in or user risk where supported.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 5, September-October 2023||

DOI:10.15662/IJRPETM.2023.0605025

The resulting decision may allow access, require additional controls such as MFA, or block the request.
The advantage of this approach is that stronger authentication can be concentrated around higher-risk activity rather than indiscriminately applied to every access event.

4.3 Privileged Identity Protection

Administrator accounts represent particularly high-value attack targets.
Microsoft Entra Privileged Identity Management can reduce standing privilege by allowing eligible administrators to activate privileged roles only when required.
A Zero Trust administrative workflow can therefore follow:
Administrator → Request Role → Verification/MFA → Approval → Temporary Activation → Work Performed → Role Expiration
This limits the time during which privileged credentials can be exploited.

4.4 Automated Identity Remediation

Risk detections can be connected to automated response processes.
Depending on organizational policy and risk severity, remediation may include:

- requiring multifactor authentication;
- requiring secure password change;
- blocking access;
- revoking active sessions;
- notifying security teams;
- initiating investigation workflows.

Azure Logic Apps and Microsoft Sentinel automation can supplement identity controls by orchestrating notifications and security-response processes.
The result is a closed identity-security workflow:
Detect → Evaluate → Enforce → Remediate → Monitor

V. USE CASE SCENARIOS

5.1 Compromised Account Detection

An employee's credentials are potentially compromised.
A suspicious authentication attempt occurs under conditions inconsistent with expected behavior.
Identity-risk signals increase the authentication risk level.
Rather than granting normal access, Conditional Access can require stronger verification or prevent access according to organizational policy.
This reduces reliance on passwords as the sole security boundary.

5.2 Adaptive MFA

Traditional MFA strategies may require additional authentication at every sign-in, potentially increasing user friction.
A risk-based approach applies stronger controls when contextual indicators justify them.
For example:
Normal Context + Low Risk → Standard Authentication
Unexpected Context + Elevated Risk → MFA
High-Risk Authentication → Block/Remediate
The objective is to balance security with user experience.

5.3 Privileged Administrator Protection

An administrator requires temporary access to a highly privileged Azure role.
Instead of maintaining permanent role membership, PIM can provide eligible, time-limited activation with additional verification and, where configured, approval.
This reduces the attack surface associated with standing administrative privilege.

5.4 Lost or Unmanaged Device Access

A valid user attempts to access sensitive enterprise information from a device that does not satisfy organizational requirements.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 5, September-October 2023||

DOI:10.15662/IJRPETM.2023.0605025

Conditional Access can incorporate device-related conditions and require an approved security posture before access is permitted.

This demonstrates an important Zero Trust principle:
Valid identity does not automatically imply trusted access.

5.5 Automated High-Risk Identity Response
When an identity is classified as high risk, an automated workflow can initiate containment and investigation.
A representative process is:
Risk Detection → Access Restriction → Session Control → User Remediation → Security Notification → Investigation
This reduces the delay between identity-risk detection and protective action.

VI. DISCUSSION

AI and machine-learning-supported identity protection enables Zero Trust security to evolve from static authentication toward adaptive access control.
The principal advantage is contextual decision-making.
A conventional access model asks:
Are the credentials valid?
An adaptive Zero Trust model asks:
Are the credentials valid, is the authentication context trustworthy, what resource is being requested, and what additional verification is appropriate for the observed risk?
This distinction is important because valid credentials can be compromised.
The proposed framework also demonstrates that AI does not replace identity policy. Machine learning provides risk signals, while security administrators define the policies determining how the organization responds to those signals.
This separation is essential for governance and accountability.
Several challenges remain. False-positive risk detections can interrupt legitimate access. Organizations must therefore calibrate policies according to workload sensitivity and business requirements.
Identity security also depends on appropriate licensing, configuration, device-management integration, and operational maturity. Poorly designed Conditional Access policies may either provide insufficient protection or create excessive authentication friction.
Another challenge is privileged identity. Even sophisticated risk detection cannot compensate for excessive permanent administrator assignments. Identity analytics should therefore be combined with least privilege and just-in-time administrative access.
The resulting security model can be summarized as:
AI detects risk → Policy interprets risk → Conditional Access enforces controls → Automation responds → Humans govern exceptions
This combination provides a practical approach to AI-assisted Zero Trust security.

VII. CONCLUSION

The transition to cloud computing and distributed work has transformed identity into a primary enterprise security boundary. Static authentication mechanisms alone cannot adequately address compromised credentials, changing device conditions, suspicious sign-ins, and privileged-access risks.

This paper proposed an AI-driven adaptive Zero Trust identity framework for Microsoft Azure using Microsoft Entra ID, Identity Protection, Conditional Access, Privileged Identity Management, and automated security-response processes.

The framework integrates machine-learning-supported risk detection with policy-based access enforcement, allowing authentication controls to adapt according to user, device, application, location, and identity-risk context.

Practical scenarios demonstrate how the architecture can support compromised-account protection, adaptive MFA, privileged-access governance, device-aware access, and automated high-risk identity remediation.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 5, September-October 2023||

DOI:10.15662/IJRPETM.2023.0605025

The research highlights an important principle for cloud identity security:
Authentication should establish identity, while continuous risk evaluation should determine trust.
As cloud environments continue to become more distributed, adaptive identity protection provides a foundation for implementing Zero Trust architectures in which access is dynamically evaluated rather than permanently assumed.
Future research should investigate behavioral identity analytics, privacy-preserving risk modeling, cross-cloud identity-risk correlation, adaptive authentication models, and the use of explainable AI to improve transparency in automated identity-security decisions.

REFERENCES

[1] Microsoft, "Zero Trust Guidance Center," *Microsoft Learn*, 2023.
[2] Microsoft, "Azure Active Directory is Becoming Microsoft Entra ID," Microsoft, 2023.
[3] Microsoft, "What is Identity Protection?," *Microsoft Entra Documentation*, 2023.
[4] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," NIST Special Publication 800-207, National Institute of Standards and Technology, Aug. 2020.
[5] Microsoft, "What is Conditional Access?," *Microsoft Entra Documentation*, 2023.
[6] Microsoft, "What is Microsoft Entra Privileged Identity Management?," *Microsoft Learn*, 2023.
[7] Microsoft, "Azure AD Multi-Factor Authentication," *Microsoft Learn*, 2023.
[8] Microsoft, "Microsoft Sentinel Automation," *Microsoft Learn*, 2023.
[9] Microsoft, "Microsoft Entra Security Operations Guide," *Microsoft Learn*, 2023.
[10] National Cyber Security Centre, "Zero Trust Architecture Design Principles," NCSC, 2021.