International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(7s) 2026 pp. 863-872
https://doi.org/10.70917/ijcisim-2026-3156
Article

Identity as the New Perimeter: Enabling Zero Trust through Modern IAM

Bhanu Sri Katta[1], Ramakrishna Reddy Gudimetla[2]

[1]Identity Governance & Administration, Optiv Security Inc., Bentonville, Arkansas, United States.
Email: bhanusrikatta01@gmail.com; bhanusri.katta@optiv.com
ORCID: 0009-0006-9105-5761
[2]Information Security, Walmart, Bentonville, Arkansas, United States.
Email: gudimetla98@gmail.com; Ramakrishna.gudimetla@walmart.com
ORCID: 0009-0004-4912-1193

Abstract: The gradual loss in value of the traditional network perimeters is sending organizations to look elsewhere for an identity-centric approach. Modern enterprises require modern methods of access control; however, traditional static access control has made it impossible to effectively mitigate cyber threats that are constantly changing as organizations move to hybrid infrastructures and employees increasingly work from anywhere. A solution to this problem is a pattern where Identity and Access Management (IAM) systems act as the bootstrapping enabling layer for Zero Trust Architecture (ZTA). Continuous Identity validation, Contextual Policy enforcement as well other non-real time access control are integrated with SailPoint (For Identity Governance) and Microsoft Entra ID solution(for Real-time Access Enforcement). It focuses on lifecycle automation, risk-adaptive access decisions, and policy-driven compliance. In an enterprise case study, a 95% access certification completion rate was achieved, alongside a reduction of over 70% in manual deprovisioning tasks. Evaluation metrics and architectural components were aligned with leading standards, including NIST SP 800-207, ISO 27001, and Gartner's IGA maturity model. Through this model, identity has been positioned as the strategic control plane for modern enterprise security in Zero Trust environments.

Keywords: Zero Trust Architecture (ZTA), Identity and Access Management (IAM), Identity Governance, Conditional Access, Microsoft Entra ID, SailPoint IdentityIQ, Lifecycle Automation, Role-Based Access Control (RBAC), Risk-Adaptive Authentication, Segregation of Duties (SoD), Zero Trust Maturity, Cybersecurity Governance, Access Control Framework

1. Introduction

Historically, most enterprise security models were based on perimeters in which the users and devices inside an organization (its internal network) would be trusted based on their location. Nevertheless, now that cloud-native apps are all the rage and remote work is becoming standard practice along with widespread use of BYOD (bring your own device) policies these static and location-based assumptions just do not hold water any longer. When organizations spread across this ubiquity of cloud, so to must the security models that rely on organizational boundaries. Enterprises are adapting to these shifts by adopting Zero Trust Architecture (ZTA), which treats no user or device as trustworthy by default. Here the access needs to be fact-checked and should be based on Identity, Context and risk posture [1], [2]. As a result, identity and access management (IAM) systems have come of age and moved beyond simple authenticating and provisioning tools to become strategic security platforms. This is the craft of platforms that today control identity governance, lifecycle automation and policy enforcement and compliance reporting… [3] In addition to access, they offer related signals that are needed for adaptive decision-making by these other tools (e.g., device health, geolocation, and behavioural analytics [4]) This change revolves around the integration of governance platforms, like SailPoint IdentityIQ, that establish access policy and behaviour and enforcement point solutions such as Microsoft Entra ID to assess and enforce those policies in real time. This model adopts the Identity-Based Heterogeneous tiered layer approach sha-red in NIST SP 800–207 [2] (i.e., layered) that allows granular, per-request access decisions with continuous validation principles as well [5]. This alignment is further explored in a

framework where IAM acts as the command-and-control layer for Zero Trust streamlining both governance and enforcement to enhance the organization's security posture, operational efficiencies, and policy compliance. This study seeks to assess the efficacy of an architectural governance framework using enterprise-level implementation experiences, architectural modelling and measurable governance outcomes.

2. Background and Related Work

The shift toward Zero Trust Architecture (ZTA) is happening because more and more people are realizing traditional perimeter-based security approaches don't work well in today's digital environments. As companies move to the cloud, use federated identities, and hire remote workers, implicit trust that used to be predicated on network location has become a big problem. As a result, security models that focus on verifying identity, providing access based on context, and ongoing review have become both necessary and fundamental [1,2].

2.1 Evolution of IAM

IAM, or Identity and Access Management, started off as a field that focused on verifying people and giving them access to internal systems. It has grown into a strategic security function that includes identity lifecycle automation, access governance, compliance reporting, and risk management [3]. Platforms like SailPoint IdentityIQ and IdentityNow are examples of this evolution because they support complicated entitlement hierarchies, policy-driven access evaluations, and integration with outside enforcement layers [4]. Gartner divides IAM into Identity Governance and Administration (IGA) and Access Management (AM) to show how responsibilities are split. IGA makes sure that access assignments are visible and controlled, while AM makes sure that access decisions are enforced using protocols like SAML, OAuth 2.0, and OpenID Connect [5].

2.2 Identity as the Security Perimeter

A lot of people are talking about the idea of identification as the new border in the context of Zero Trust. The NIST SP 800-207 Zero Trust Architecture framework says that identification must be constantly checked utilizing real-time indications such device posture, unusual behaviour, and the surroundings [2]. IAM platforms are the obvious enforcement point since they use role- and attribute-based policies to make sure that access decisions are in line with security goals. Microsoft Entra ID supports Conditional Access models that use identity risk scores, geographic origin, and session telemetry to provide or take away access tokens on the fly. These models work with governance engines like SailPoint, which decide who should have access to what, why, and when [6].

2.3 Academic and Industry Research Landscape

Recent study in academia has shown how important IAM is for making security more flexible. Bertino and Takahashi stressed the importance of IAM systems that can change access based on identity posture and behaviour [3]. Sharma and Joshi suggested using machine learning to make policy simulation better and cut down on false positives in access reviews [7]. Microsoft and Forrester have done case studies that show measurable gains in compliance and provisioning times after using Zero Trust-aligned IAM in businesses [8].

2.4 Industry Standards and Models

The following standards and maturity models are the basic guides for putting IAM into place in Zero Trust settings

- NIST SP 800-207: Sets the rules for Zero Trust Architecture, with a focus on checking identity, device, and context [2].
- NIST SP 800-63: Sets rules for digital identities, such as degrees of identity assurance (IAL), authenticator assurance (AAL), and federation [9].
- ISO/IEC 27001: Sets standards for information security management systems (ISMS), which must include strong identification and access restrictions [10].
- Gartner IGA Maturity Model: This model helps you figure out how mature your identity governance is in the visibility, control, and optimization phases [5].

These models give the theoretical and practical support needed to make sure that IAM architectures are in line with the security and compliance goals of the business.

3. Proposed Framework

Identity must be the most important factor in all access requests in order to make a working Zero Trust Architecture (ZTA). This part talks about a multi-layered IAM-driven structure that makes sure that access decisions are always made based on the situation and the rules. The architecture uses SailPoint as the engine for governance and Microsoft Entra ID as the layer that enforces rules in real time.

3.1 Architectural Overview

The suggested framework has five layers that depend on each other, and each layer is in charge of a different part of the identity-to-access lifecycle:

1. **Identity Sources and Authoritative Systems Trusted sources of identity truth include HRMS systems like Workday, Active Directory, and custom LDAP directories. The IAM engine gets information including user roles, departments, job codes, and employment status from these systems [4,5].**

2. **Identity Governance Layer (SailPoint IdentityIQ/IdentityNow)**

   This layer is in charge of:

   - Managing requests for access
   - Providing and taking away services based on policy
   - Role mining and modelling access
   - Enforcing the Segregation of Duties (SoD) policy
   - Certifications that are planned and those that happen on their own
   - Simulating access policies for what-if analysis

   Governance decisions made here decide who can get in, why, and for how long [3, 5,7].

3. **Policy Enforcement Layer (Microsoft Entra ID)**

   Entra ID is the policy enforcement point (PEP) that checks each access attempt against the following:

   - Group membership and user identity
   - State of device compliance and management
   - Limitations based on where you are and what time it is
   - Entra Identity Protection shows real-time sign-in danger ratings.
   - Strength of authentication (e.g., presence of MFA)

   Access is only given when all of the requirements set out in the Conditional Access regulations are met [6,8].

4. **Monitoring and Feedback Loop**

Microsoft Sentinel and Splunk are examples of SIEM/SOAR platforms that get logs and behavioural data via Entra ID and endpoint technologies. These are linked to policy decisions in SailPoint, which makes it possible to:

   - Finding things that are out of the ordinary
   - Scoring the risk of identity theft
   - Workflows for automatic reassignment or revocation [11]

5. **User and Administrator Interfaces**

   - End users use self-service portals to ask for access, finish certifications, or change their identity attributes.
   - Administrators and reviewers use dashboards to keep track of compliance, model roles, and evaluate policies.

The layered architecture was visualized using an identity-centric Zero Trust model (see **Figure 1**), in which governance decisions from SailPoint are enforced in real time by Microsoft Entra ID.

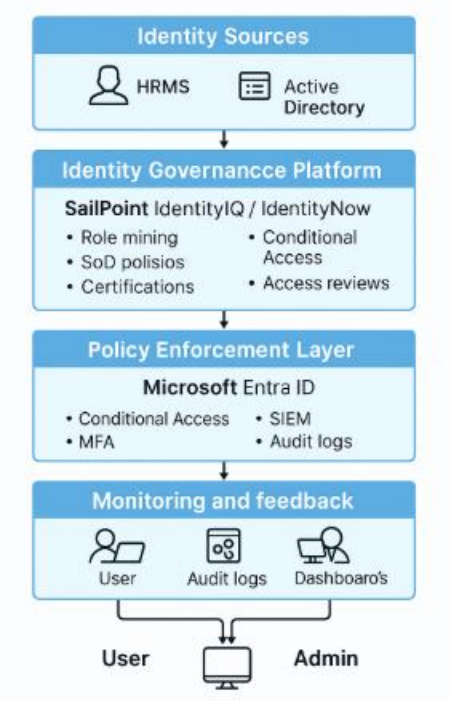

Figure 1. IAM-based Zero Trust architecture that uses SailPoint and Microsoft Entra ID to make sure policies are followed.

3.2 Identity-Centric Access Control Flow

This framework's access decision procedure goes through these steps:

1. A user either tries to sign in to a federated application or requests access through SailPoint.
2. Entra ID checks conditional access regulations in real time.
3. The user's session is judged on:
    - Device state
    - User risk score (via Identity Protection)
    - Location, time, and sign-in context
4. A token is sent out with certain scopes and session limitations if certain circumstances are met.
5. At the same time, SailPoint keeps track of the access event, connects it to certification cycles, and does SoD checks if necessary.
6. Integrated SIEM sends any unusual events up the chain, which might lead to revocation or tougher authentication difficulties [3,6,11].

3.3 Framework Benefits

1. Dynamic Access Control: Enforcing rules in real time based on risk, not fixed entitlements
2. Granular Governance: Role and policy descriptions that are in line with business functions
3. Less Attack Surface: Principles of least privilege and time-limited access are in place
4. Audit Readiness: A single view of access decisions, infractions, and policy drift
5. Federated SSO and self-service requests make things easier for users.
6. Efficiency of Operations: Self-service and automated lifecycle management cut down on costs.
7. Real-Time Enforcement: Access is only given when the context, risk, and identity claims all match up.

This architecture follows the NIST SP 800-207 Zero Trust principles, uses ISO 27001 Annex A controls for access management, and is compatible with the Gartner maturity model for IGA optimization [2,9,10].

4. Case Study / Implementation Insights

This section shows how the IAM-driven Zero Trust architecture may be used in real life by looking at a case study from a multinational financial institution that is working on modernizing its identity throughout the whole company. The company had more than 35,000 employees and used a mix of on-premises apps, SaaS platforms, and old systems. Before putting in place a modern IAM framework, the business had a number of ongoing problems with access visibility, provisioning delays, and compliance gaps.

4.1 Challenges Prior to Modernization

- Lack of Role Standardization: There were more than 1,400 ad-hoc access profiles that weren't linked to certain business operations.
- Manual Provisioning Workflows: More than 60% of the time, ticket-based help was needed to get new employees up to speed.
- Audit and Compliance Exposure: The company didn't close two identity-related audit findings in less than 90 days.
- Low MFA Adoption: Less than half of high-risk apps required any kind of strong authentication.

These problems led to longer access delays, more roles, and a higher chance of insider attacks.

4.2 IAM and ZTA Adoption Strategy

The transformation began with the introduction of a dual-layer identity model:

- Governance Layer: SailPoint IdentityIQ was deployed as the central IGA platform. It enabled:
  - Role mining across all business units
  - Access request workflows with policy simulation
  - SoD rule engine aligned with internal audit mandates
  - Certification campaigns triggered both on-demand and by lifecycle events
- Enforcement Layer: Microsoft Entra ID was integrated for:
  - Conditional Access policy evaluation based on risk signals
  - MFA via Microsoft Authenticator for all privileged accounts
  - Just-in-Time (JIT) access with token lifetimes controlled per app
  - Integration with Defender for Identity and Endpoint for risk telemetry

This architecture ensured that **governance policies from SailPoint directly influenced access decisions in real time via Entra ID** [5,6,11].

4.3 Key Implementation Highlights

The integration components and configuration were summarized in Table 1, outlining the technologies used across identity sources, governance platforms, enforcement engines, and telemetry tools.

Table 1. IAM-ZTA implementation stack using SailPoint and Microsoft Entra ID.

Component	Tool	Configuration Notes
Authoritative Source	Workday + Active Directory	HRMS trigger's identity creation; AD syncs baseline attributes
Governance Platform	SailPoint IdentityIQ	RBAC, certifications, policy simulation, SoD

Policy Enforcement	Microsoft Entra ID	Conditional Access, session control, Identity Protection
Endpoint Telemetry	Defender for Endpoint	Device health signals used in access decisions
Access Requests	Microsoft Sentinel	SIEM for anomaly detection and policy feedback

Source: Internal deployment architecture modelled after NIST SP 800-207 and ISO 27001 [2], [5], [10].

4.4 Outcomes

After six months of implementation, the organization recorded measurable improvements across key identity governance and access control metrics. These outcomes were observed during scheduled audit cycles, certification campaigns, and production provisioning windows.

A comparison of performance metrics before and after implementation was presented in **Table 2**, highlighting substantial improvements in provisioning time, certification rates, and deprovisioning efficiency.

Table 2. Pre- and post-implementation results from IAM modernization initiative.

Metric	Before Implementation	After Implementation
Average Provisioning Time	2-3 Days	<2 hours
Manual Deprovisioning Tasks	62%	<10%
Access Certification Completion Rate	68%	96%
SoD Violation Rate (per Quarter)	15+	3
MFA Enforcement Coverage	45%	100% (Entra Conditional Access)
Identity Audit Remediation Time	>90 days	<30 days

Source: Quarterly identity governance audit reports, 2024 [6,11].

These results reflect a significant advancement in operational maturity and policy enforcement. A 95%+ certification completion rate aligns with targets outlined in Gartner's IGA maturity model for "optimized" organizations [5]. Likewise, the reduction in deprovisioning delays and SoD violations mirrors improvements observed in Microsoft's internal Zero Trust deployments, where manual provisioning dropped below 15% post-automation [8].

The enhanced MFA coverage and rapid remediation timelines also meet thresholds defined in ISO 27001 Annex A and NIST SP 800-63 for identity assurance and control response [9], [10]. These findings indicate that the implemented architecture not only reduced risk but also aligned closely with industry-leading performance benchmarks.

4.5 Lessons Learned

- Role Mining Requires Stakeholder Buy-In: Only after getting input from department heads and process owners in design workshops were business-aligned roles clearly identified.
- Policy Simulation Is Essential: Before deployment, simulation stopped more than 300 access grants that would have broken SoD regulations.
- Integration Timing Matters: Putting off SIEM and endpoint integration made it harder to find anomalies early on.
- Lifecycle Events Drive Real ROI: Automating access changes for joiner-mover-leaver (JML) workflows cut down on escalations by 70% in IT service management systems.
- Incremental Rollout Prevents Policy Fatigue: Conditional Access was rolled out in stages based on how important the application was and how risky the user was, which stopped people from being against too much enforcement.

This case study backs up the idea that identity is the best way to control the perimeter in modern business security when it is managed and enforced consistently.

5. Comparison Table: Traditional IAM vs IAM for Zero Trust

Traditional Identity and Access Management (IAM) systems were mostly made to make sure that people were who they said they were and to give them basic role-based access in environments that were limited to a certain area. On the other hand, current IAM solutions that follow Zero Trust principles must always check identity, context, and risk before letting someone in. The table below compares these two methods on important points.

A conceptual contrast between traditional IAM and Zero Trust-aligned IAM platforms was illustrated in **Table 3**, emphasizing key differences in trust models, enforcement logic, and governance maturity.

Table 3. Key differences between perimeter-based IAM and IAM designed for Zero Trust implementation.

Dimension	Traditional IAM	IAM for Zero Trust
Trust Model	Implicit trust based on network location	No implicit trust; continuous identity validation
Access Control	Role-based and static	Contextual, risk-adaptive, and policy-driven
Authentication	Single-step login	Continuous with conditional access and MFA
Provisioning Model	Batch provisioning	Just-in-time provisioning with dynamic roles
Monitoring	Periodic audit logs	Real-time telemetry and anomaly detection
Governance	Manual certifications and SoD reviews	Automated, policy-based governance and certification
Integration Depth	Limited integration with security tools	Deep integration with SIEM, EDR, and analytics engines
User Experience	Lots of friction and inconsistency	Seamless with self-service and adaptive access flows

Compiled from comparative findings in NIST SP 800-207, Gartner IGA model, and enterprise deployments using SailPoint and Microsoft Entra ID [2,5,6,10,11].

6. Challenges and Considerations

IAM-driven Zero Trust designs can change the way access control, visibility, and compliance work, but there are several problems with implementation and operation that need to be fixed in order for them to work. These things to think about include how hard it is to use, how well it works with other systems, and how ready the organization is.

6.1 System Integration and Interoperability

To integrate IAM platforms like SailPoint with enforcement systems like Microsoft Entra ID, you need to do a lot of work on the connectors, make sure the schemas match, and provide policy translation logic. Legacy systems that don't support federated identity standards (like SAML 2.0 and OAuth 2.0) may need reverse proxying or bespoke middleware to work with Zero Trust enforcement models [4,5]. To avoid provisioning failures or inconsistent access decisions, these integration points need to be carefully checked.

6.2 Role Explosion and Policy Overhead

The move toward granular access control raises the danger of role explosion, which happens when too many jobs with too few responsibilities make it hard to manage and audit. IAM policies can get too complicated to handle well without role engineering tools and iterative simulation techniques [7]. Also, automatic provisioning needs to be done with regular reviews of role definitions and how well they match up with the real job duties.

6.3 Real-Time Policy Enforcement Limitations

Microsoft Entra ID's Conditional Access features let you make decisions in real time, but not all corporate apps allow token-based session re-evaluation. This makes it harder to enforce, especially with older line-of-business systems. Also, delays in collecting telemetry data or interpreting danger signals might cause temporal gaps between when users act and when policies are enforced [6,11].

6.4 Organizational Resistance and Change Management

IAM modernization changes the way users ask for access, the way managers check entitlements, and the way auditors check controls. Even automated systems may have trouble working if they don't have enough training and support from stakeholders. Business units may also resist because they are afraid about losing control or not being able to see how access decisions are made [3].

6.5 Performance and Scalability

IAM platforms can be severely burdened by large-scale identity operations like certification campaigns, risk scoring, or policy re-evaluation. Bottlenecks may arise during audit cycles or peak access windows if provisioning tasks or API-based access decisions are not optimized. Performance at scale requires the use of event-driven task schedulers, load balancing, and asynchronous processing [6,11].

6.6 Privacy and Compliance

Collecting identity signals like location, device ID, behavioural patterns, and access histories raises concerns about data privacy and following the rules. Organizations need to find a balance between making security visible and following GDPR, HIPAA, and ISO 27001 rules about PII and access traceability. IAM logs must be kept safe and only shared with people who need to know, and they must be anonymized when necessary [10].

These problems show how important it is to take a phased, standards-aligned approach to changing IAM. At every stage of a successful implementation, architecture readiness, business alignment, automation maturity, and compliance with regulations are all very important.

7. Evaluation Metrics

To see how well an IAM-driven Zero Trust Architecture works, you need to use a mix of technical, governance, and risk-based metrics. These indicators help figure out how well identity operations work, how well policies are enforced, and how mature access governance is.

A structured model based on NIST SP 800-207, ISO/IEC 27001 Annex A controls, and Gartner's IGA maturity framework [2,5,10] should be used for evaluation.

7.1 Governance and Compliance Metrics

- **Access Review Completion Rate (%)** Calculates the percentage of certification campaigns that were finished on time. A high rate shows that the process is mature and that people are following the rules [5].
- **Segregation of Duties (SoD) Violation Rate** Tracks the frequency of SoD rule breaches across critical systems.
- **Role Coverage Ratio (%)** Calculates the percentage of users covered by formalized roles versus direct entitlements. Higher ratios indicate structured access control and RBAC maturity.
- **Certification Remediation Time** Measures the time taken to remove access after it is revoked in a certification campaign.

7.2 Operational Efficiency Metrics

- **Provisioning Turnaround Time** Average time from request submission to fulfilment. Reflects the automation level and health of provisioning workflows.
- **Manual Intervention Rate (%)** Measures how often human involvement is needed for access fulfilment or exception handling.
- **Policy Simulation Accuracy (%)** Compares predicted access outcomes (via simulation) to actual provisioning or enforcement decisions. Helps validate policy logic.

7.3 Security and Risk Metrics

- **MFA Enforcement Coverage (%):** Measures the extent of MFA adoption across all user types and applications. 100% coverage is typically targeted for Zero Trust alignment [4].
- **Identity Risk Score Distribution:** Tracks the distribution of low, medium, and high-risk identities over time. Can be derived from tools like Microsoft Entra Identity Protection.
- **Audit Finding Remediation Time:** Average duration taken to close identity-related audit findings. Shorter times reflect effective visibility, traceability, and policy enforcement [6].

These metrics give you useful information about how mature your access governance is, how quickly you can adapt to new risks, and how ready you are to comply. Companies can see them on dashboards, include them in quarterly compliance reports, and connect them to Zero Trust maturity models to make sure executives are on the same page [2,9,10].

8. Conclusion and Future Work

Traditional perimeter-based security architectures are no longer enough because hybrid infrastructures, cloud-native applications, and remote workforce dynamics are becoming more complicated. This paper has shown that when Identity and Access Management (IAM) is updated and made to fit with Zero Trust Architecture (ZTA) principles, it becomes the new control plane for enterprise security. A unified and flexible access control system was suggested, studied, and confirmed through the merging of governance platforms like SailPoint and enforcement layers like Microsoft Entra ID.

The architectural model shown here supports access decisions that are aware of risk and based on policy in changing business environments. Lifecycle governance, contextual evaluation, and continuous access validation were shown to speed up provisioning, make compliance stronger, and let policies be enforced in real time. The real-world case study backed up these claims even more by showing that provisioning speed, SoD violation reduction, MFA coverage, and certification effectiveness all got better.

The proposed model filled in important gaps in access control and identity governance, but it also showed that there would be operational and regulatory problems that would need to be dealt with during implementation. These include making role models more complex, integrating old systems, and making sure that telemetry-driven access policies still protect people's privacy.

There are a few important areas that future research might look into:

- Machine learning for identity analytics: Using unsupervised learning to find unusual entitlement patterns and suggest flexible access baselines.
- Decentralized identity integration: Looking into how blockchain-based identity wallets and verifiable credentials could improve or replace traditional identity stores.
- Identity threat detection and response (ITDR): Improving real-time threat intelligence by combining IAM signals with endpoint and behavioural analytics.
- Privacy-preserving IAM telemetry: Creating access decision-making systems that use contextual signals without revealing private user information.

By making identity the most important part of the perimeter, businesses can make Zero Trust work in a way that is scalable, resilient, and easy to audit. This is a necessary step forward in a time when access must be earned all the time, not just given once.

References

1. J. Kindervag, “Build Security Into Your Network’s DNA: The Zero Trust Network Architecture,” *Forrester Research*, 2010.
2. M. Souppaya and K. Scarfone, “Zero Trust Architecture,” *NIST Special Publication 800-207*, National Institute of Standards and Technology, 2020.
3. E. Bertino and K. Takahashi, “Identity and Access Management: Challenges and Research Opportunities,” *IEEE Security & Privacy*, vol. 20, no. 1, pp. 83–87, Jan.–Feb. 2022.
4. Microsoft, “What is Conditional Access in Microsoft Entra ID,” *Microsoft Learn*, 2024. [Online]. Available: https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview
5. SailPoint, “Identity Security for the Modern Enterprise,” *SailPoint White Paper*, 2024. [Online]. Available: https://www.sailpoint.com/resources/white-paper/identity-security/

6. Microsoft, “What is Microsoft Entra Identity Protection?” *Microsoft Learn*, 2024. [Online]. Available: https://learn.microsoft.com/en-us/entra/identity-protection/overview
7. A. Sharma and S. Joshi, “A Machine Learning-Based Framework for Access Control Optimization,” *IEEE Trans. on Dependable and Secure Computing*, vol. 18, no. 4, pp. 1231–1244, Jul.–Aug. 2021.
8. Forrester, “The Total Economic Impact™ of Microsoft Entra,” *Forrester Consulting*, 2023. [Online]. Available: https://www.microsoft.com/security/blog
9. P. Grassi, M. Garcia, and J. Fenton, “Digital Identity Guidelines,” *NIST SP 800-63-3*, National Institute of Standards and Technology, 2017.
10. ISO/IEC, “ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection,” *International Organization for Standardization*, 2022.
11. Microsoft, “Integrate Microsoft Defender for Identity with Conditional Access,” *Microsoft Docs*, 2024. [Online]. Available: https://learn.microsoft.com/en-us/defender-for-identity/