DDN1 Task 3: Technology-Supported Security Solution

Cybersecurity Graduate Capstone – D490

John Luong

Western Governors University

A. Policies Adopted from the Implementation of Zero Trust Architecture

The Zero Trust Architecture (ZTA) project at Jotoan Financial Services (JFS) led to the adoption of several critical cybersecurity policies. The main concept of the solution was the shift from a traditional perimeter-based model to a modern, identity-centric approach that's aligned with Zero Trust principles. The project introduced mandatory multi-factor authentication (MFA) for all users through Azure Active Directory (Azure, AD), the deployment of Privileged Identity Management (PIM) for role governance, and Conditional Access policies that evaluated access in real-time based on user risk, device compliance, and location (Microsoft, 2023). These measures aimed to reduce JFS's attack surface, limit credential abuse, and ensure that elevated access was granted only when necessary.

One central theme of the project was the principle of least privilege. Through the implementation of PIM, administrative access was granted on a just-in-time basis which minimized standing privileges and thereby reducing the potential for privilege escalation. Conditional Access rules were designed to adapt dynamically to risk contexts such as blocking or prompting MFA when logins originated from suspicious IP addresses or unregistered devices. This policy-based enforcement led the organization to overcome legacy limitations posed by Active Directory Federation Services (ADFS), which lacked cloud-native granularity and flexibility.

The project also introduced centralized monitoring policies. Microsoft Sentinel and Microsoft Defender for Identity were deployed to collect telemetry data, analyze threat signals, and generate security alerts. Policies were developed to govern log retention, incident response workflows, and reporting thresholds to all ensure traceability and audit readiness. These tools

brought consistency to enforce access control, identity verification, and governance across both JFS's cloud and on-premises environments (Microsoft, 2023; CISA, 2023).

A1. Improvement to Cybersecurity Decision-Making

The solution dramatically improved cybersecurity decision-making at JFS by leveraging automated, data-informed mechanisms to enforce policy and assess risk. Azure AD and Conditional Access allowed the security team to define and execute real-time access policies without manual intervention. This meant that access to sensitive resources was determined by contextual signals such as device posture, geolocation, and user behavior which enabled dynamic trust decisions aligned with Zero Trust tenets (NIST, 2020).

Microsoft Sentinel further enhanced decision-making by acting as a centralized logging and analytics engine. It correlated telemetry from Azure AD, Microsoft Defender for Identity, and endpoint agents to deliver insights on anomalous activity. By integrating MITRE ATT&CK threat simulations into the solution, JFS was able to test how well their controls responded to tactics like lateral movement and privilege escalation (MITRE, 2023). These simulations provided the security operations team with actionable intelligence and validated the effectiveness of implemented controls.

Historical audit logs and incident patterns informed the configuration of policies during the early implementation phase. For example, findings of over-permissioned legacy accounts and incomplete MFA coverage directly influenced the project's prioritization of identity hardening. As a result, JFS shifted from a reactive posture (threats were often discovered after exploitation) to a proactive stance based on early detection and automated responses (CISA, 2023).

B. Cybersecurity Assurance Criteria

The Zero Trust solution delivered by this project met multiple cybersecurity assurance benchmarks that reflect modernization, automation, and industry alignment.

First, the solution promotes automation in cybersecurity by leveraging Microsoft Sentinel and Conditional Access. Microsoft Sentinel uses machine learning and user behavior analytics to detect threats in real time and automatically correlate incidents across the hybrid infrastructure. Conditional Access policies automate decision-making regarding authentication requirements by triggering MFA or access denial without the need for manual oversight (Microsoft, 2023). This significantly reduced incident response times, enforced consistency, and minimized human error.

Second, the solution improves and modernizes security by replacing JFS's fragmented legacy environment with a unified Zero Trust Architecture. The migration from ADFS to Azure AD marked a shift from static identity federation to a cloud-native directory that supports dynamic policy enforcement and risk assessment. Microsoft Defender for Identity added modern threat detection capabilities such as lateral movement monitoring and account compromise alerts that were previously unavailable (Microsoft, 2023). The overall strategy that's aligned with CISA's Zero Trust Maturity Model is by integrating identity, device, network, application, and data control planes (CISA, 2023).

Third, the project implements industry standard tools and infrastructure. Tools such as Azure AD, Microsoft Sentinel and Microsoft Defender for identity are recognized as enterprise-grade and compliant with frameworks such as NIST SP 800-207 and CISA Zero Trust Maturity Model (ZTMM) v2.0. Not to mention MITRE ATT&CK since it further anchored the solution in threat-informed defense practices (NIST, 2020; MITRE, 2023). These components provided

immediate protection and visibility which helped set the foundation for long term scalability and governance.

Altogether, the Zero Trust solution at JFS operationalized key assurance criteria that strengthened resilience, streamlined detection and response, and aligned security operations with recognized best practices.

C. Data Collection and Implementation Elements

Throughout the implementation of the ZTA at JFS, historical data and structured implementation metrics played a crucial role in shaping the solution's scope, guiding policy design, and ensuring alignment with both operational risks and modern cybersecurity practices. These data driven decisions allowed the project team to identify existing gaps, prioritize remediation efforts, and validate configurations during simulation phases.

The foundational data sources came from internal security assessments and Active Directory audits conducted prior to implementation. These audits exposed JFS's critical issues such as over-permissioned legacy accounts, the lack of role-based access controls, inconsistent MFA coverage, and excessive administrative privileges. As a result, the early sprints of the project focused on identity governance through Azure AD, Conditional Access, and PIM to eliminate unnecessary privileges and enforce access boundaries (Microsoft, 2023).

Audit logs from ADFS and internal system monitors revealed poor visibility into hybrid authentication traffic and limited policy enforcement across cloud and on-premises systems. These findings influenced the shift from ADFS to Azure AD, where Conditional Access and cloud-native telemetry enabled a more granular and risk-aware access control. Azure AD's

integrated sign-in logs and Conditional Access insights provided a more accurate view of user behavior which allowed JFS to identify anomalies and tailor policy enforcement with certainty.

Security teams also analyzed endpoint vulnerability scans and network threat intelligence reports to evaluate risks such as unpatched software, lateral movement paths, and credential reusage. These vulnerability reports were mapped to MITRE ATT&CK tactics to simulate realistic attack scenarios during the Microsoft Sentinel and Microsoft Defender for Identity configuration phases (MITRE, 2023). This approach allowed the team to validate detection rules and prioritize visibility enhancements based on previously unmonitored threat behavior.

In addition to internal data, compliance audit findings highlighted gaps in centralized policy enforcement, monitoring, and access documentation. These findings directly shaped the governance components of the roadmap, reinforcing the need for consistent, traceable security controls across all systems. Microsoft Sentinel's analytic dashboards and long-term log retention features were specifically configured to support this regulatory visibility and audit readiness.

Operational data from access reviews, ticketing systems, and end-user reports shown high levels of inefficiencies in account provisioning, password resets, and inconsistent enforcement of access policies. This influenced the redesign of identity lifecycle workflows and prompted the inclusion of onboarding automation and device compliance policies in the Conditional Access framework.

Additionally, several industry-leading frameworks and vendor recommendations supported JFS's approach to data collection and implementation. CrowdStrike advocated for identity-first protection and behavior-based threat detection which directly supports the choice of Microsoft Defender for Identity to user activity and detecting anomalous behaviors

(CrowdStrike, 2023). Palo Alto Networks emphasized device context and continuous validation as core Zero Trust practices which was used to shape JFS's Conditional Access rules that evaluated device health and sign-in risk signals before granting access (Palo Alto Networks, 2023). Google's BeyondCorp model showcased the success of replacing perimeter-based trust models with identity-aware, context-driven access control which was a core design influence on JFS's transition from ADFS to Azure AD (Google, 2020).

Altogether, the combination of internal assessments, compliance audits, and external Zero Trust models allowed JFS to pursue a data-informed, standards-driven implementation. These insights ensured the organization to mature its security posture while maintaining operational continuity across its hybrid cloud environment.

D. Investigation and Mitigation of Incidents

The Zero Trust solution at JFS provided a unified, intelligent system for detecting, investigating, and responding to cybersecurity incidents across both on-premises and cloud infrastructure. Prior to implementation, the organization had poor visibility into authentication patterns, privilege use, and insider threats due to its reliance on fragmented logging and perimeter-based monitoring.

The deployment of Microsoft Sentinel centralized all security telemetry into a single analytics platform. Microsoft Sentinel's built-in detection rules were customized to identify credential-based attacks, brute force logins, and unusual behavioral patterns. Each alert generated within Microsoft Sentinel included actionable insights such as source IP, user account, device

compliance statuses, and geographic origin which helped analysts triage incidents quickly (Microsoft, 2023).

Microsoft Defender for Identity augmented this visibility by detecting identity-specific attack vendors such as lateral movement, Kerberos ticket abuse, and unusual privilege escalation. Simulated attacks were performed using tactics from the MITRE ATT&CK framework to validate detection rules and ensure coverage for the most common enterprise attack methods (MITRE, 2023).

Incident response workflows were created to define how alerts would be escalated, triaged, and remediated. Microsoft Sentinel's playbooks allowed for automated incident responses such as temporarily blocking users or requiring reauthentication under certain threat conditions. Logs and incident metadata were stored and categorized for long-term reviews which supported future audit requirements and retrospective analysis.

The solution also supported post-incident investigations through structured case tracking and full forensic logs. Microsoft Sentinel retained event data for historical trend analysis, allowing the SOC team to compare current incidents to known baselines or anomaly thresholds. These logs were especially important for understanding privilege misuse and replaying attack chains after lateral movement simulations.

In summary, JFS's incident detection and investigation capabilities evolved from reactive and fragmented to centralized, automated, and intelligence-driven. The system provided clear escalation paths, detailed threat insights, and forensic traceability that were not available prior to the Zero Trust implementation.

E. Cybersecurity Plans, Standards, or Procedures Developed

The ZTA implementation at JFS was supported by a structured cybersecurity plan that included standards, phased documentation, and long-term governance procedures. The foundation of the plan was a Zero Trust Implementation Roadmap that divided the solution into four phases: discovery and assessment, identity and access hardening, monitoring and threat detection, and governance and sustainment. These phases were executed over an eight-week simulation and followed Agile methodologies to integrate stakeholder feedback, maintain flexibility, and deliver iterative results.

The roadmap was guided by two key national cybersecurity frameworks: NIST SP 800-207 and CISA's ZTMM v2.0—both of which provided a baseline for measuring maturity across identity, device, application, network/environment, and data control planes (NIST, 2020; CISA, 2023). These frameworks also shaped project deliverables and risk prioritization strategies. During execution, key procedural artifacts were created which included standardized policy templates for MFA and Conditional Access, privileged access elevation procedures using PIM, and security monitoring configurations for Microsoft Sentinel and Microsoft Defender for Identity.

A significant governance deliverable was the ADFS Decommissioning Plan, which outlined the phased retirement of ADFS. While ADFS was retained during the project for compatibility with legacy systems, the plan defined milestones, fallback protocols, and application owner checklists brings for fully migrating towards Azure AD eventually This procedural document was included in the final governance package and is scheduled for execution as legacy dependencies are addressed.

All cybersecurity documentation was compiled in Microsoft Word and Visio formats to then be distributed across all relevant stakeholders, including technical teams (IT operators, security analysts), compliance personnel, and executive leadership (CISO, CIO). Cloud architects, application owners, and internal users were also engaged through stakeholder-specific guides and briefings. Documents were customized to reflect role-specific expectations such as technical implementation guides which were directed to security administrators, while executive summaries and governance strategies were provided to leadership and compliance officers for oversight and review.

E1. Alignment with Cybersecurity Initiatives or Regulatory Compliance

The implemented solution was fully aligned with modern cybersecurity initiatives and regulatory mandates. By enforcing "never trust, always verify" through Conditional Access and risk-based authentication, the project addressed foundational Zero Trust principles outlined in NIST SP 800-207 (NIST, 2020). Each ZTMM pillar was evaluated using CISA's maturity scoring rubric and with visible advancement in identity, device, and application workloads by project completion (CISA, 2023).

Compliance drivers such as HIPAA, PCI-DSS, and SOX directly supported the deployment of Azure AD, Microsoft Sentinel, and Microsoft Defender for Identity. These tools enforced traceable access control, ensured real-time monitoring, and provided audit logs for sensitive systems. Microsoft Sentinel's correlation rules and long-term log retention also ensured audit readiness and facilitated regulatory reporting.

E2. Applications, Tools, and Documentation Developed

The project deployed several enterprise-class Microsoft security tools to support ZTA goals:

- Azure Active Directory (Azure AD): Replaced ADFS as the primary identity platform for hybrid cloud access, enabling Conditional Access and MFA enforcement.
- Microsoft Sentinel: Centralized SIEM used to ingest logs, correlate incidents, and drive real-time alerting across JFS's hybrid environment.
- Microsoft Defender for Identity: Enhanced threat visibility across Active Directory, detecting insider threats and lateral movement attempts.
- Privileged Identity Management (PIM): Enforced just-in-time access elevation and removed standing admin rights.

Accompanying these tools were technical and procedural documents developed by the project team, including:

- Conditional Access and MFA enforcement guides
- PIM and access elevation workflows
- ADFS Decommissioning Plan with migration checklists
- Governance framework aligned with CISA and NIST standards
- Network architecture diagrams reflecting hybrid authentication paths

These materials were allocated based on stakeholder roles in conjecture with project managers, cloud architects, compliance officers, and technical staff each receiving tailored documentation and training support.

F. Post-Implementation Environment

Following implementation of the ZTA, JFS transitioned from its fragmented, perimeter-centric security model to a unified Zero Trust infrastructure that emphasizes identity, risk, and policy enforcement. Azure AD became the core authentication service while ADFS remained operational for select legacy applications with pending until their full migration to Azure AD. This dual authentication design was intentionally transitional and guided by a formally documented decommissioning plan, with steps in place to fully retire ADFS in the near term.

Microsoft Sentinel operated as a centralized logging and analytics engine, aggregating telemetry from Azure AD, Microsoft Defender for Identity, and endpoint agents. Microsoft Sentinel's dashboards provided the SOC team with visual alerts, incident timelines, and severity scoring which allowed for rapid triage and investigation. Meanwhile, Microsoft Defender for Identity delivered real-time behavioral analytics based on user privileges and authentication anomalies, offering protection against lateral movement and privilege escalation.

F1. Improvements in Security Posture and Efficiency

The Zero Trust implementation strengthened the organization's security posture. By enforcing MFA across the entire workforce, JFS was able to close a major gap in credential-based attack surface exposure. PIM replaced traditional standing administrative accounts with just-in-time access elevation which ensured privileges to be granted only when necessary and for a limited amount of time. This drastically reduced the risk of insider threats and privilege abuse.

Operational efficiency also improved as security decisions became more automated and situation-aware. Conditional Access policies evaluated device compliance, user risk, and location in real time that led to eliminating the need for manual access checks. Microsoft Sentinel's

automated alerting and incident correlation features reduced the SOC's mean time to detection and response, while centralized dashboards replaced fragmented monitoring tools. Help desk escalations for access issues declined as onboarding and provisioning workflows were aligned with policy templates and risk thresholds.

F2. New Data and Business Process Impact

Zero Trust Architecture implementation introduced multiple new data streams that reshaped how JFS monitored and governed identity and access. Azure AD generated detailed sign-in logs, Conditional Access evaluations, and policy enforcement results. Microsoft Sentinel aggregated this data and correlated it with behavioral analytics from Microsoft Defender for Identity to build real-time threat landscapes. These insights supported both operational decisions and strategic risk reviews.

Business processes were updated accordingly in which the security operations team began holding weekly threat review meetings using Microsoft Sentinel dashboards. Compliance officers used automated reports to conduct quarterly access recertifications. IT administrators gained visibility into failed login attempts, device compliance gaps, and access anomalies to allow for data-driven adjustments for Conditional Access rules. These procedural enhancements elevated both responsiveness and transparency across the organization.

F3. Summative Evaluation Plan, Test Results, and Remediation

A summative evaluation was conducted during the final implementation sprint to validate the effectiveness of the Zero Trust solution. The security team executed predefined test cases based on known-identity-based attack tactics which include lateral movement, privilege escalation, and anomalous authentication flows by using techniques mapped to the MITRE ATT&CK framework (MITRE,2023). These scenarios were simulated within controlled environments to assess whether the deployed controls responded as intended.

Key performance indicators (KPIs) confirmed the solution's success. MFA was enforced across 100% of user accounts. Conditional Access rules applied correctly in about 95% of test scenarios that reflected accurate policy logic. Microsoft Sentinel correlated security events in under five minutes on average, thus meeting organizational benchmarks for real-time threat visibility. Additionally, maturity assessments that were conducted using the CISA Zero Trust Maturity Model showed improvement from a "Traditional" to "Intermediate" level across at least three of the five control pillars (CISA, 2023).

One issue that was identified during testing was an overly restrictive Conditional Access policy that temporarily blocks authentication for a legacy application that relies on ADFS. This policy was revised to include a controlled exception, and the issue was logged in the governance matrix as part of the ADFS decommissioning strategy. Thus, the resolution ensured continuity while preserving the broader transition to Azure AD.

G. Post Implementation Maintenance Plan

To ensure the long-term sustainability, effectiveness, and governance of the Zero Trust Architecture (ZTA) implementation at Jotoan Financial Services (JFS), a formal post implementation maintenance was developed. This plan addresses policy lifecycle management, system monitoring, compliance alignment, stakeholder training, and change governance which were all essential to preserve security effectiveness in an evolving hybrid cloud environment.

A cornerstone of the maintenance strategy is the scheduled quarterly policy review cycle. This includes the assessment of Conditional Access rules, Privilege Identity Management (PIM) elevation configurations, and Microsoft detection analytics. These reviews are conducted jointly by representatives from the Security Operations Center (SOC), IT operations, and compliance teams to ensure enforcement consistency, to reduce misconfiguration risks, and to adapt policies to organizational changes or the evolving threat intelligence

Additionally, the phased decommissioning of Active Directory Federation Services (ADFS) remains a critical element of the maintenance roadmap. While ADFS is still operational to support specific legacy applications, regular compatibility evaluations and migration progress reviews are scheduled monthly. As systems become modernized or replaced, they are transitioned to Azure AD to eventually retire the legacy federation. This transition is governed by the documented ADFS Decommissioning plan, which includes fallback procedures, cutover milestones, and stakeholder approval processes.

Another major pillar of post implementation maintenance is role-based training and change management. Recognizing that the success of Zero Trust is as much about adoption as it

is about architecture, so the project included the rollout of tailored onboarding and refresher training for various roles:

- End-users received interactive tutorials and knowledge base resources explaining MFA prompts, secure login procedures, and self-service tools for password recovery.
- IT staff and system administrators were trained on Conditional Access rule management, PIM elevation workflows, and Microsoft Sentinel operations.
- Executive stakeholders and application owners received security briefings and governance documentation showing how policies aligned with audit and compliance standards.

To manage organizational change and ensure long-term support, the project team established a change communication framework. This included pre-deployment awareness campaigns, training session schedules, and ongoing support through the IT service desk. Feedback was collected after implementation via surveys and meetings in which the findings were integrated into the quarterly review cycles. This approach helped address early-stage resistance to MFA enforcement and conditional restrictions, especially with high-frequency system users.

Policy documentation and training materials are maintained in a version-controlled repository that's accessible to designated stakeholders. Documentation includes security configurations, access request procedures, system diagrams, and compliance reports. All updates to these materials undergo an internal review and are logged to support audit readiness and change transparency.

Responsibility for maintenance oversight is distributed across governance roles: security architect manages technical control assessments, compliance officer reviews policy alignment, and IT operations lead coordinates user support workflows. These roles collaborate through a governance committee that meets monthly to review new risks, policy change requests, and unresolved incidents.

Altogether, the maintenance plan ensures that JFS's ZTA solution remains adaptive, transparent, and aligned with organizational needs. By embedding role-specific training, scheduled policy evaluation, and structured governance into daily operations, JFS is well positioned to maintain its improved security posture over time.

H. Original Artifact: Zero Trust Network Architecture Diagram

As part of the project deliverables, a network architecture diagram (Figure 1) was created to visualize the transformation from JFS's legacy perimeter-based model to a modern Zero Trust Architecture. The diagram captures the key elements of the hybrid-cloud environment which showcases how Microsoft's security stack of Azure Active Directory (Azure AD), Microsoft Sentinel, and Microsoft Defender for Identity interact with enterprise identity, endpoints, and cloud workloads.

The diagram illustrates how JFS adopted a centralized identity plane, replacing ADFS with Azure AD as the primary authentication service for both cloud and on-premises resources. Conditional Access enforcement points are mapped between the user and resource layers, demonstrating how access decisions are based on real-time context (device compliance, risk scoring, location, etc.) rather than network perimeter or static credentials. Integration points with

Microsoft Defender for Identity are shown monitoring domain controller and privileged access flows that highlight how identity telemetry informs threat detection and policy response.

The network architecture also reflects transitional elements such as the coexistence of ADFS and Azure AD to support legacy authentication workflows. This coexistence was essential during the implementation phase and is documented as part of the ADFS Decommissioning Plan to ensure legacy applications are migrated without operational disruption.

In addition to securing JFS's access paths, the diagram emphasizes telemetry flow to Microsoft Sentinel, which acts as the central SIEM. Microsoft Sentinel aggregates signals from endpoints, cloud applications, and identity providers to then enable threat detection, incident response, and compliance reporting.

This artifact served as both a design reference and communication tool for stakeholder presentations, audit walkthroughs, and change management briefings. It helped clarify how policy enforcement is decoupled from the traditional network boundary and recentered around identity, behavior, and device risk. The visual model also enabled application owners and network engineers to understand where integrations or dependencies existed, supporting alignment across teams.

Overall, the network architecture diagram is a critical output of the project that encapsulates the technical transformation to Zero Trust and provides ongoing value for planning, troubleshooting, and governance oversight.

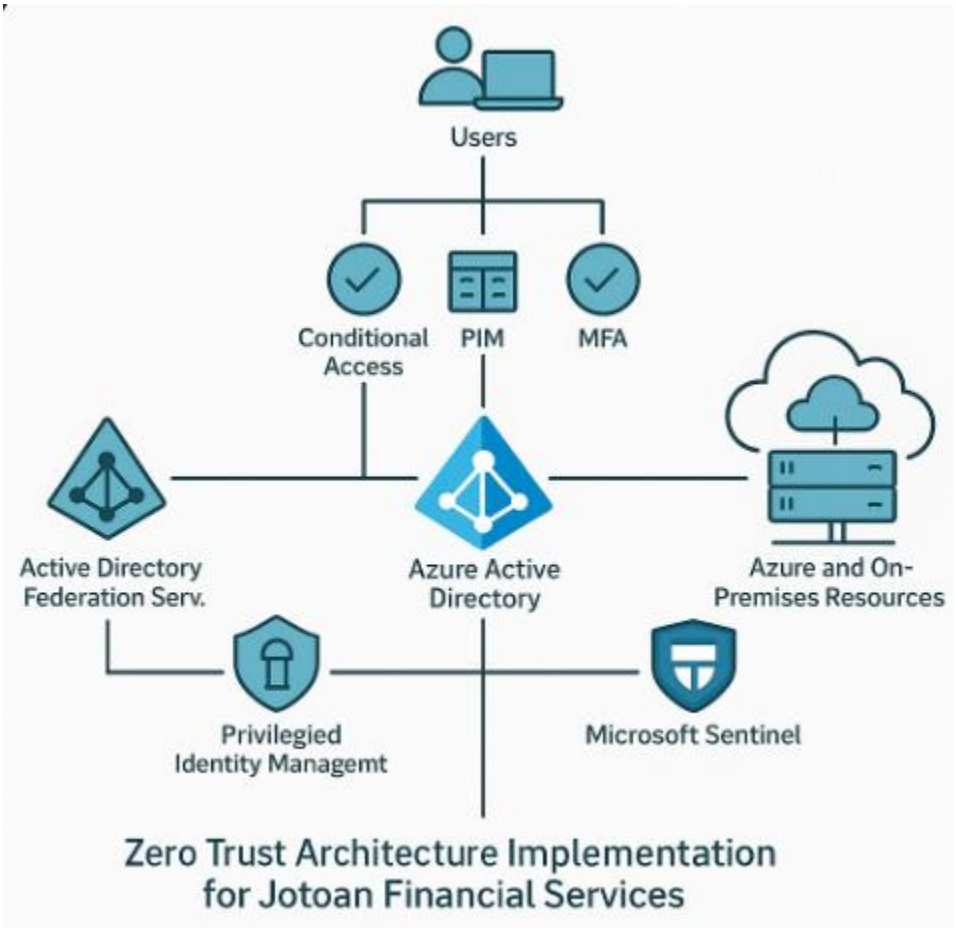

Figure 1: Zero Trust Network Architecture at Jotoan Financial Services (JFS), illustrating identity-centric access control, hybrid coexistence with ADFS, and telemetry flow into Microsoft Sentinel for threat detection and compliance monitoring.

Appendix: Zero Trust Maturity Model Comparison

The following table summarizes the improvement in Jotoan Financial Services' (JFS) cybersecurity maturity as a result of the Zero Trust Architecture (ZTA) implementation. The assessment is based on the CISA Zero Trust Maturity Model (ZTMM) Version 2.0, which outlines five core security pillars: Identity, Device, Network/Environment, Application Workload, and Data. Maturity is measured on a scale of "Traditional, Intermediate, and Advanced" that reflects the evolution capabilities across key domains (CISA, 2023).

Each pillar was evaluated before implementation (based on audit findings and access reviews) and after deployment of Azure Active Directory (Azure AD), Conditional Access, Microsoft Sentinel, and Microsoft Defender for Identity. This comparative table demonstrates the project's direct impact on access control, threat visibility, and governance.

ZTMM Pillar	Maturity (Before Implementation	Maturity (After Implementation	Key Improvements
Identity	Traditional	Intermediate	Azure AD, MFA enforcement, Conditional Access, Privilege Identity Management
Device	Traditional	Intermediate	Device compliance policies through Conditional Access
Network/Environment	Traditional	Traditional	Still partially reliant on perimeter-based controls and ADFS
Application workload	Traditional	Intermediate	Role-based access to SaaS workloads, identity-aware access policies
Data	Traditional	Traditional	Audit logs implemented; full data classification/encryption planned

While significant progress was made in three of the five pillars, the Network/Environment and Data pillars remain in the "Traditional" category due to ongoing

dependency on ADFS for select legacy systems and the absence of full-scale data loss prevention or encryption solutions. These areas are included in the long-term governance roadmap.

The maturity improvements reflect the effectiveness of JFS's phased implementation strategy. By focusing first on identity and access control, the organization established a secure foundation while planning for future expansion of Zero Trust principles into infrastructure and data governance.

I. References

CISA. (2023). Zero Trust Maturity Model Version 2.0. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/sites/default/files/2023-04/CISA-ZTMM_V2_FINAL.pdf

CrowdStrike. (2023). Zero Trust: Adopting a Threat-Centric Approach. https://www.crowdstrike.com/resources/white-papers/zero-trust/

Google. (2020). BeyondCorp: A New Approach to Enterprise Security. Google Cloud. https://cloud.google.com/beyondcorp

Microsoft. (2023). Microsoft Zero Trust Guidance and Best Practices. Microsoft Learn. https://learn.microsoft.com/en-us/security/zero-trust/

Microsoft. (2023). Microsoft Defender for Identity Documentation. Microsoft Learn. https://learn.microsoft.com/en-us/defender-for-identity/

Microsoft. (2023). Microsoft Sentinel Documentation. Microsoft Learn. https://learn.microsoft.com/en-us/azure/sentinel/

MITRE. (2023). MITRE ATT&CK Framework. https://attack.mitre.org/

NIST. (2020). Zero Trust Architecture (SP 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Palo Alto Networks. (2023). The Enterprise Roadmap to Zero Trust. https://www.paloaltonetworks.com/resources/whitepapers/enterprise-roadmap-to-zero-trust