International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(6s) 2026 pp. 342-351
https://doi.org/10.70917/ijcisim-2026-2915
Article

Zero-Trust Network Access on IBM z/OS: Applying BeyondCorp Principles to Mainframe Perimeter Architecture

Rohit Kumar Shaw[1], Artem Kulagin[2]*

[1] Infrastructure Engineer.
Email: rohitshaw.infosec@gmail.com
ORCID: 0009-0009-3751-0809
Email: artemk.research@gmail.com
ORCID: 0009-0004-0248-9142
Corresponding Author: Artem Kulagin

Abstract: Traditional perimeters for IBM z/OS depend on trusted zones, virtual private networks (VPNs), firewalls, and security assumptions that are static in nature. Hybrid cloud integration, z/OS Connect APIs, z/OSMF administration, and DevSecOps pipelines, however, have expanded the IBM z/OS attack surface. In this study, a conceptual Zero-Trust-Network-Access approach for IBM z/OS, including BeyondCorp and incorporating it into the mainframe perimeter architecture, is proposed. The design process adopted a mixed-method approach, dominated by qualitative methods such as document analysis, control mapping, gap analysis, architecture synthesis, and expert review. Evidence comprised practitioner, technical, academic, and standards documents, complemented by a purposive selection of key practitioner, technical, and standards documents and selected key mainframe security, IAM, and network security professionals. BeyondCorp principles could be applied to six z/OS security domains: identity verification, device posture, encrypted transport, session authorization, API mediation, and monitoring. RACF, SAF, MFA, AT-TLS, z/OSMF, z/OS Connect, SMF records, and SIEM integration provide strong foundations, while device posture scoring and adaptive access remain weak areas. The study provides a multi-layered modernization model that enables access to the mainframe while improving existing z/OS controls. The framework should be validated in future research through production-like tests that measure measurable latency, compliance, reliability, and risk-reduction parameters in enterprises.
Keywords: Zero-Trust Network Access, IBM z/OS Security, BeyondCorp Architecture, Mainframe Perimeter Security, RACF Access Control, and z/OS Connect API Security.

1. Introduction

Many banks, insurers, governments, healthcare payers, airlines, and card processors continue to run transaction systems on IBM Z, with reports of more than 70% of transactions by value running on the platform as a whole and CICS-based workloads responsible for around 30 billion transactions a day and an estimated $1 trillion in value per week. These statistics illustrate that z/OS security is not a legacy issue; it is an operational concern for systems of record that need to stay available and accurate and have audit trails well maintained. However, access to the mainframes has changed. APIs are now available in the modern z/OS estate exposed through z/OS Connect and accessible from a browser with z/OSMF, via an encrypted TCP/IP service using AT-TLS, and via an automated deployment path to DevSecOps pipelines. They are also responsible for traffic to cloud services, vendors, remote admins, and privileged engineers who do not live within the data center.

Traditional mainframe security and clear mainframe boundaries have been part of the security solution. RACF, SAF authorization, dataset profiles, SMF logging, certificates, and encryption are all integral components of strong accountability within z/OS. However, users who log into a protected network via a VPN, jump servers, or a corporate internal subnet are assumed to be more trustworthy [1]. Zero Trust Architecture, as defined in NIST SP 800-207, is an

approach that requires authentication and authorization of a subject or device before granting access to an enterprise resource, based on the identity of the requesting subject or device, context, and policy but not on network location.

Both Zero Trust and Google BeyondCorp have been extended in the security community to cloud and web security. However, there is no extensive discussion of how these two concepts fit into the IBM z/OS perimeter architecture in security professional or academic circles. The BeyondCorp solution shifts the focus from privileged corporate networks to verified users, managed devices, and application-specific authorization. Here is the problem: many mainframe environments have evolved their own controls and may still be managed under static perimeter assumptions. Key research questions focus on how to do more than implement BeyondCorp Zero Trust Network Access (ZTNA) for z/OS while still maintaining reliability, compliance, transaction throughput, and operational stability.

This research has four aims. It includes an introduction to the z/OS security architecture, the fundamentals of BeyondCorp, and the principles of ZTNA. The z/OS components for supporting zero trust, such as RACF, MFA, AT-TLS, z/OSMF, and z/OS Connect, are also described. It offers a conceptual plan to modernize the mainframe perimeter. The study covers the potential of the study, implementation challenges, governance issues, and operating risks.

It is a network access focus, including network administrative connections, connections through application programming interfaces (APIs), remote user access, privileged access and workflows, and access to several integration points to a hybrid cloud IBM z/OS. Excludes application modernization, hardware cryptographic engineering, and non-IBM mainframes to any degree other than limited comparison. This article has been broken into several chapters. Chapter 2 provides a literature review addressing Zero Trust, BeyondCorp, z/OS security, and mainframe perimeter architecture. Chapter 3 presents the method and techniques. Chapter 4 shows the architectural findings and discussion. The study suggests further research. The study concludes with a summary of the key contribution.

2. Literature Review

2.1 Zero-Trust Network Access and the Decline of Perimeter-Based Trust

Zero-Trust Network Access is a paradigm change from location-based to resource-based verification. In the traditional perimeter model, a user, device, or service accessing a trusted subnet might be granted access to internal systems. It is not suitable for IBM z/OS environments that are now remotely administered, API supported, hybrid cloud, and third-party integrated [2]. Zero Trust does not eliminate firewalls, encryption, RACF controls, or monitoring; it eliminates the implicit trust in users, devices, applications, and network paths.

It is based on a principle called “Never trust, always verify," which means that all access requests are verified, then authorized, tracked, and subsequently monitored by ongoing risk signals. The concept of least privilege is key because a system programmer, API client, batch service, or database administrator should have only the rights necessary to perform a specific job. Studies on ISP routing vulnerabilities demonstrate that network paths can be represented as graphs with weak nodes and edges, where network vulnerability is the degree to which traffic traverses an approved path; thus, trust should not be assumed solely based on the path [3].

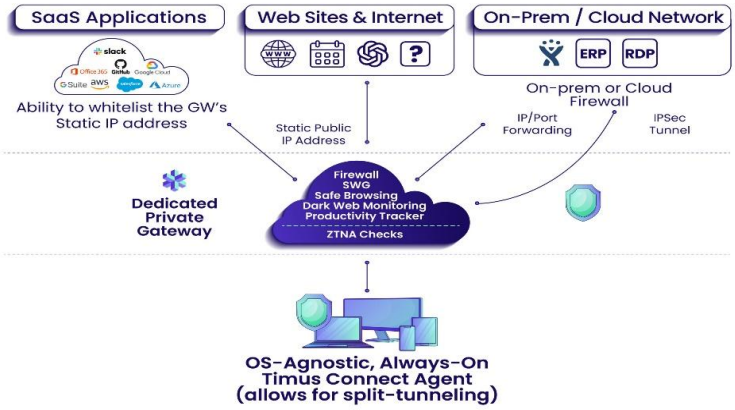

Figure 1: ZTNA gateway provides identity, context, and least-privilege checks for SaaS, internet, and hybrid resources.

Figure 1 shows a Zero-Trust Network Access (ZTNA) model in which users/devices use an always-on agent to connect to a dedicated private gateway before connecting to SaaS applications, websites, internet services, or on-premises/cloud networks. Today, resource-centric verification, least-privilege routing, encrypted access, and rejecting trust solely on network location or approved internal paths are reinforced by the gateway, which acts as a firewall, secure web gateway, monitoring, productivity tracking, and/or ZTNA device.

2.2 BeyondCorp as a Practical Zero-Trust Model

BeyondCorp is a practical approach to identity-aware access rather than VPN-based access. The primary security boundary is no longer the privileged corporate network, which is thus removed as a major component of security [4]. Rather, access is determined by the user's verified identity, the device's verified identity, the application's sensitivity, and the context policy. This is important for z/OS because the z/OS administrator can access z/OSMF via a browser, developers can invoke services by using z/OS Connect, and the operations team can access consoles remotely from managed endpoints outside the data center.

BeyondCorp style design allows the access broker to validate user credentials, assess device posture, analyze risk, and authorize applications at the application level, while only allowing encrypted sessions. For instance, SAML-based federation can be used to provide enterprise SaaS access by passing authenticated identity assertions between trusted domains, a pertinent example for mapping external identity providers to controlled access flows to the mainframe [5; 6]. This means there is less traditional VPN access and more granular access decisions on a per-application basis.

2.3 IBM z/OS Security Architecture and Mainframe Access Control

Existing IBM z/OS security tools can address many Zero Trust requirements. RACF is used to identify users, ensure that users provide the proper password or credentials, administer groups, authorize access to resources, protect against unauthorized access to datasets, record accesses, and report on them. The System Authorization Facility is a z/OS facility that can be used to request centralized authorization decisions before accessing a network service, terminal, job, started task, or dataset [7]. A user might have thousands of user IDs and service IDs under the control of an RACF profile, and privileged access to these services could be split by role, group ownership, and audit rules for a production bank or insurer. Datasets, including business records, payment files, claims data, and customer indexes, are rescued and preserved with the utmost importance. Logging to SMF and RACF will provide useful forensic, compliance, or anomaly-detection data. To maximize authentication, MFA can be implemented across both on-premises domains and external IDPs, and to reduce credentials revealed during remote access, certificates and encrypted channels can be used.

2.4 Applying BeyondCorp to Mainframe Perimeter Architecture

The use of BeyondCorp on IBM z/OS does not replace existing mainframe controls; rather, it changes the perimeter design. The first layer should ensure user and device identities before the connection reaches sensitive z/OS services. The second layer should incorporate a policy decision point that checks if the role, device health, location, session risk, time, and requested resource are met [8]. The third layer should provide access control via an identity-aware proxy, an API gateway, or a controlled z/OS Connect endpoint. IBM z/OS Connect can be used to support third-party authentication patterns in which the REST client is responsible for authenticating with the third party, obtaining a token, and then having the token authenticated and mapped to a user identity.

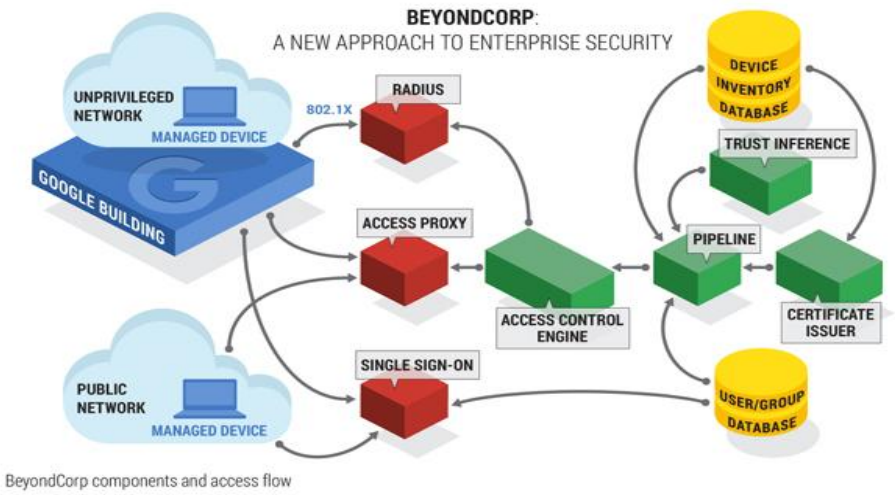

Figure 2: BeyondCorp access flow for mainframe perimeters that provides identity-aware, policy-driven, continuous verification for mainframe security.

Figure 2 is an access flow for managed devices in a BeyondCorp world, which access the network after authenticating via single sign-on, RADIUS, and access proxies. The access control engine allows sessions to be authorized using device inventory, certificates, trust inference, and user and group information, which supports z/OS perimeter redesign, token-based access, identity-aware gateways, continuous identity verification, and controlled integration with RACF, SMF, SIEM, and AT-TLS.

AT-TLS may then be used to provide secure transport for TCP/IP connections, without forcing each legacy application to implement its own TLS logic. RACF events, SMF, SIEM correlation, and behavioral analytics should all be used for continuous verification. The use of AI-powered operational systems in healthcare demonstrates how valuable automation can be when decisions are measurable, monitored, and integrated into workflows that are governed [9; 10]. Similarly, the deployment of ZTNA on z/OS should be accomplished through measurable controls: limiting standing privileges, limiting shared accounts, limiting session lengths, achieving ≥95% MFA coverage, and logging all privileged access.

3. Methods and Techniques

3.1 Data Collection Methods

This study used a mixed-method, qualitative-dominant approach to explore the implications of applying a BeyondCorp (BCP) approach to the implementation of a Zero-Trust Network Access (ZTNA) solution in the IBM z/OS perimeter architecture. The subject itself lends itself to no end-user surveys, so the data collection relied on documentary evidence and expert judgment. Four types of evidence were selected: Technical Standards and Frameworks, IBM Technical Documentation, Academic and Practitioner Literature, and Expert Input. The design fit for z/OS was appropriate, since various z/OS security tools (such as RACF, SAF, AT-TLS, z/OSMF, and z/OS Connect) related to Zero Trust also apply and must be interpreted at each layer of identity, device, policy, encryption, and monitoring.

The document sample consisted of a variety of research papers. It contained IBM technical documents on RACF administration, SAF authorization, AT-TLS configuration, z/OSMF REST services, and z/OS Connect authentication; standards or framework documents, such as NIST Zero Trust Architecture, BeyondCorp, and access-control models; peer-reviewed papers and conference papers on ZTNA and mainframe modernization; and practitioner reports, conference papers, or white papers on ZTNA and mainframe modernization. The study used purposive sampling because documents were needed that were directly related to Zero Trust, z/OS, identity federation, encrypted transport, API security, and perimeter redesign. At least one of the technical controls, architectural patterns, or implementation constraints was needed for each document, and they had to be relevant to z/OS access. This targeted sampling approach is supported by research on legacy financial modernization, as the transformation of the mainframe is not typically generic but rather based on domain-specific integration evidence [11].

Experts were sampled purposively, with 10 participants. The group included three mainframe security architects, two RACF administrators, two z/OS system programmers, two enterprise IAM engineers, and one network security architect. All participants had at least 5 years of experience in their field, with an expectation of 9-12 years. These 14 guiding questions were used to conduct semi-structured interviews for the data on existing access paths, existing privileged user controls, current MFA adoption, token mapping, current encryption boundaries, visibility in the SIEM, and operational risks. Organizational sensitivity was reduced by anonymizing the interviews.

3.2 Data Analysis

The study used thematic coding, control mapping, gap analysis, and architecture synthesis. Document coding began by dividing them into seven technical areas: identity assurance, device trust, encrypted transport, policy enforcement, logging, API mediation, and perimeter redesign. The evidence items entered under the themes were only those referred to by at least 7% of the 24 evidence items. This level was selected to eliminate anecdotal bias while preserving special-purpose mainframe results.

The mapping was also performed from BeyondCorp principles to the capabilities provided by IBM z/OS. User identity correlation was performed using RACF, MFA, certificates, SAF calls, and external IDPs. A mapping of the device context for endpoint management, certificate checks, and a proxy policy (among other items) was implemented so that encrypted access is routed to gateways that support both AT-TLS and TLS. Application-level authorization was reconciled with z/OSMF roles, z/OS Connect APIs, RACF resource classes, and least-privilege profiles. Machine learning's use in security governance has been studied mainly in the context of high-speed networks in the financial industry, where automated policy-based decision-making with low latency is key, with secondary considerations less well understood [12; 13].

A gap analysis was conducted to identify strong, partial, and weak capabilities. Overall, good controls such as authorization in RACF, auditability in SMF, protection of datasets, and transport encryption. Partial controls included identity federation, token mapping to users, and mediation via an API gateway. Others were areas that called for enhancement: Device posture scoring, adaptive risk scoring, continuous session assessment, and uniform governance scoring. Enhanced model of ZTNA-z/OS that was synthesized by the architecture synthesis: identity provider, device posture service, policy decision point, identity-aware proxy, z/OS enforcement layer, and telemetry layer.

3.3 Framework Validation Technique

The proposed framework has been discussed with experts. The experts were asked to agree/disagree on a 5-point scale for 5 criteria: technical feasibility, compatibility with existing z/OS controls, potential for improving security, usefulness for compliance and audits, and operational complexity. Any mean score of 4.0 or greater was rated as "strong acceptance," a score of 3.0–3.9 as "conditional acceptance," and a score of < 3.0 as "redesign need." Qualitative comments enhanced the setting for controls on privileged access, certificates, API handling, and logging granularity. Distributed-system leader selection research indicates that structured selection rules are essential to enable scalable coordination, which guided the framework's focus on clear policy-decision control and failover governance [14]. This allowed design recommendations to be auditable, implementable, and appropriate for regulated production environments having measurable risk controls.

4. Results and Discussion

4.1 Mapping BeyondCorp Principles to IBM z/OS Security Controls

The analysis indicated that the BeyondCorp principles can be mapped to the existing IBM z/OS capabilities, without changing the native security model. User identity verification is aligned with user ID in RACF, SAF authorization calls, MFA, certificates, and privileged access workflows [15]. The device-aware access solution is not well supported on z/OS and requires the use of enterprise IAM, endpoint posture platforms, managed device certificates, and an identity-aware proxy.

Table 1: Maps BeyondCorp to limits on z/OS controls for identity, encryption, least privilege, and monitoring.

BeyondCorp Principle	z/OS Implementation Area
User identity verification	RACF, SAF, MFA
Device-aware access	External IAM, endpoint posture tools, access proxy

Application-specific access	z/OSMF, z/OS Connect, API gateways
Encrypted communication	AT-TLS, TLS certificates
Least privilege	RACF profiles, groups, permissions
Continuous monitoring	SMF records, RACF logs, SIEM integration

Table 1 shows the BeyondCorp principles and how to map them to the IBM z/OS security implementation areas. It demonstrates through examples of RACF, SAF, MFA, external IAM, z/OSMF, z/OS Connect, AT-TLS, TLS certificate, RACF profile, SMF record, RACF logs, and SIEM integration how user verification, device-aware access, application-specific control, encrypted communication, least privilege, and continuous monitoring can be supported within a ZTNA architecture.

Application-specific access to z/OSMF, z/OS Connect, API gateways, and RACF resource classes. Encrypted communication is related to AT-TLS and TLS certificates, and least privilege is related to RACF groups, dataset profiles, command permissions, and started-task controls. Continuous monitoring translates into SMF records, RACF audit events, API logs, and ingestion into SIEMs. Thus, z/OS provides powerful enforcement and auditing, and BeyondCorp provides ongoing context-aware decisioning before traffic ever reaches the mainframe.

4.2 Proposed ZTNA Architecture for IBM z/OS Perimeter Modernization

The proposed architecture has 5 layers. The first one is the user and device identity layer, which involves MFA, device certificates, integration with identity providers, and privileged access management, providing user and endpoint verification. Multi-factor authentication for all logins to human administrative accounts is a reasonable goal for 95% or more, and for all automation accounts configured to use certificates for authentication, 100% [16]. The second is the policy decision layer, which evaluates the status of a user's role, group, device, source risk, time of day, transaction sensitivity, and app in question. In the insurance analytics realm, risk-scoring algorithms indicate that incorporating business data, predictive signals, and dashboard visualizations within a structured workflow under a governance framework can improve decision-making processes [17; 18]. It demonstrates how to adopt a risk-based access policy for payroll systems on z/OS, as well as for claims, card, and settlement systems.

The third layer is the access proxy/gateway layer. It should include an identity-aware proxy for administrative sessions, an API gateway for service traffic, z/OS Connect integration for REST-based integration, and z/OSMF access control for browser-based administration. When placed behind contextual policy controls, IBM z/OSMF REST services must be accessed with credentials or certificates, making them suitable for a zero-trust administrative model. The fourth layer is the z/OS enforcement layer, which checks permissions on datasets, general resources, commands, started tasks, and application profiles using RACF/SAF. The fifth layer is encryption and monitoring, where AT-TLS provides security for TCP/IP sessions, SMF maintains audit trail data, RACF log files track authorization events, and SIEM data can be correlated for continuous compliance reporting.

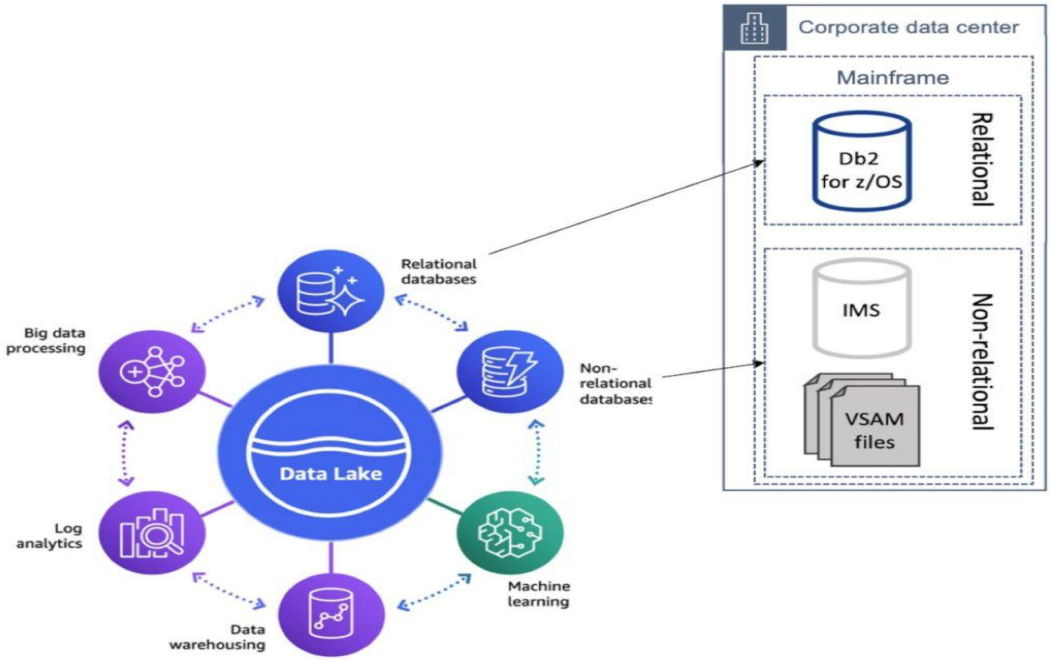

Figure 3: Simple data integration between enterprise analytics platforms and IBM Z/OS mainframe systems secured with ZTNA.

Figure 3 illustrates an architecture for modernizing z/OS that connects an enterprise data lake service to z/OS data resources, such as Db2 for z/OS, IMS, and VSAM files. It demonstrates, for regulated environments, how API-mediated analytics, machine learning, and hybrid-cloud access paths can be securely protected by showcasing how identity-aware gateways, policy decisions, RACF/SAF enforcement, encrypted AT-TLS transport, audit records, and SIEM monitoring can be used.

4.3 Expected Security Benefits

The primary advantage is that it reduces the need for a VPN. A VPN may establish a connection to a network, but it cannot verify that the user, device, session, and the requested resource are acceptable. ZTNA enhances access control for the paths users, devices, APIs, or service accounts take before accessing protected z/OS assets. Benefits include tighter administration of remote administrators, more robust security for z/OS Connect APIs, more comprehensive enforcement of least privilege, and more complete auditing. Some examples of practical features include automatic alerting for failed multi-factor authentication, odd locations of originating commands, access to a large number of datasets, 100% logging of privileged commands, and 0 standing access for emergency IDs. Another way AI-driven IAM research can facilitate adaptive access decisions is by continuously analyzing signals from identities, behaviors, and policies, rather than only at login time [19; 20].

4.4 Implementation Challenges and Discussion

Implementing is challenging. Many legacy apps use static IP ranges, common service IDs, long-lived sessions, and/or hard-coded authentication mechanisms. The mapping from external identity attributes to RACF identities can be complex, as there is no one-to-one relationship between enterprise roles, cloud groups, and RACF profiles. Proxy-mediated access can also result in latency, certificate management overhead, and the introduction of new failure points. Governance issues are serious when a privileged user is involved, and in the event of an incident, emergency access to the system may be required by a system programmer or a security administrator.

Another limitation is skill gaps; the key to making it successful is getting staff that understands how to use and implement RACF, SAF, TLS, SIEM engineering, API gateway, and IAM federation [21]. It is therefore recommended to follow a phased migration approach, migrating the administration, API access, privileged workflows, and, finally, the application patterns. This gradual approach minimizes outages, facilitates rollback testing, and provides evidence of quality compliance for the enforcement of enterprise-wide, zero-trust controls within production z/OS estates.

5. Future Research Recommendation

5.1 Empirical Testing in Production-Like z/OS Environments

Future research challenges: conceptual testing needs to be transformed into empirical testing, including tests conducted in production environments/operating systems such as z/OS. There should be two logical partitions with users provisioned in RACF, traffic to and from z/OS Connect API, AT-TLS-protected TCP/IP services, hybrid-cloud identity federation with z/OS, and administrative access to z/OSMF. The environment should simulate a larger number of authentication events, such as 100k-500k per hour, privileged commands issued, failed MFA attempts, certificate rotations, or REST API calls.

Key metrics include authentication latency, decision time of the authentication policy, rate of failed sessions, rate of false rejections, API response overhead, and the mean time to revoke risky access [22]. The delay caused by ZTNA should be measured as the latency difference between baseline VPN access and identity-aware proxy access and confirmed to be acceptable, with ≤5% transaction overhead.

5.2 Development of Mainframe-Specific Zero Trust Maturity Models

Moving forward, research is needed, but not a Zero Trust maturity model imported from the cloud-only world; an IBM z/OS maturity model should be developed. The model for the dimensions to be measured comprises the following attributes: identity assurance, device validation, RACF governance, encrypted transport, API security, privileged access, and telemetry integration [23]. Each domain has a scoring of 0-5, where 0 means that the perimeter trust has not been documented, and 5 means there are continuous, auditable, policy-based access decisions. Some of the measurable indicators that should be defined in the model include coverage of 95% MFA, 100% logging of privileged command activations, a maximum of 24h to delete logged-out users, and logging RACF profiles every quarter for recertification. This maturity model would help banks, insurance firms, and other government corporations allocate more attention to investment without increasing their required workload.

5.3 Integration of AI-Driven Risk Scoring and Continuous Access Evaluation

Future research should focus on privileged account and service ID risk scoring, automated jobs, and AI-enabled API clients. Behavioral analytics can correlate logon access with any logon time discrepancies, command orders, access to data sets, source networks, and failed logon attempts. A model should be capable of both pre-session and real-time risk scoring, resulting in a step-up authentication, a security operations review, or session termination.

A recent review of the literature on BGP and MPLS suggests that proactive routing based on verification, segmentation, and the continual enforcement of policies should help reduce the need for trust [24]. The same rules will apply to z/OS access paths. For deterministic evidence to benefit mainframe environments, models must be explainable, auditable, and subject to proper rules and procedures for compliance incidents, liability, and accountability.

6. Conclusions

This study shows that in some businesses, specifically those that demand high levels of security for their transactions, integrity, fault tolerance, and auditability, z/OS continues to offer a viable platform for mission-critical enterprise computing applications. The merit-reviewed study shows that many banking, insurance, government, health care, airline, and payment processing applications remain mainframe-based, require high levels of compliance, and handle large volumes of transactions. As a result, legacy maintenance is more than just a legacy maintenance problem; it is a business imperative for organizations that will continue to deliver their core mainframe services via hybrid cloud, browser management, DevSecOps pipelines, open APIs, and remote management.

The research also indicates that traditional perimeter controls are still useful but no longer sufficient when users, devices, or services operate on an internal subnet, a virtual private network (VPN), or a jump server. There are already robust identity, authorization, encryption, and audit foundations in z/OS with RACF, SAF authorization, dataset profiles, SMF logging, certificates, MFA, and AT-TLS. When these controls are embedded in a zero-trust network access framework that validates identity, device posture, session purpose, the risk of the session, and the sensitivity of the resources being accessed, they become more effective. BeyondCorp also provides a practical approach to moving the mainframe perimeter from a network-based to an identity-aware, continually assessed, application-specific model.

The proposed architecture shows that ZTNA for IBM z/OS should be layered and not disruptive. The identity and device layer should be responsible for verifying users, certificates, endpoints, and privileged accounts. The policy

decision layer should consider role, device health, location, time, and requested resource. The proxy/gateway layer should sit between z/OSMF, z/OS Connect, administrative sessions, and API traffic. The z/OS enforcement layer needs to maintain RACF and SAF as authoritative control points, with the monitoring layer providing integration with AT-TLS, SMF, RACF logs, API telemetry, and SIEM correlation. This setup is useful for users, APIs, services, or automation before mainframe use.

Security solutions for the new and improved mainframe of the future will not be solutions that throw out previous security solutions. Instead, it should help them update to new capabilities such as zero-trust policy enforcement, adding more IDPs, device-aware access, least privilege, encrypted transport, and continuous verification. The deployment should be a carefully planned transition of APIs, privileges, workflows, and use cases to administrative use, followed by a live deployment to validate latency, compliance value, operational reliability, and measurable risk reductions. The staged adoption approach helps auditors, system programmers, and security architects observe the benefits that modernization initiatives can provide without impacting production change windows or rehearsed recovery events.

References;

1. Y. C. Tian and J. Gao, "Network security and privacy architecture," in Network Analysis and Architecture, Singapore: Springer Nature Singapore, 2023, pp. 361–402. https://link.springer.com/chapter/10.1007/978-981-99-5648-7_10
2. D. Quintero, T. Baumann, V. Cruz, N. Haldar, Y. Largou, P. Pandey, et al., IBM Power Systems High Availability and Disaster Recovery Updates: Planning for a Multicloud Environment. IBM Redbooks, 2022. https://books.google.com/books?hl=en&lr=&id=A95xEAAAQBAJ&oi=fnd&pg=PR7&dq=It+is+not+suitable+for+IBM+z/OS+environments+that+are+now+remote+administered,+API+supported,+hybrid+cloud,+and+third-party+integrated&ots=mlHG6GG2EB&sig=5aY3vpd5WZasn1Z7u5vp8XNMtWg
3. D. Prajapati, "Using graph theory to model routing vulnerabilities and defence mechanisms in ISP networks," in 2026 Second International Conference on Multi-Agent Systems for Collaborative Intelligence, pp. 1383–1390, IEEE, 2026.https://doi.org/10.1109/ICMSCI67830.2026.11469374
4. O. R. Arogundade, "Network security concepts, dangers, and defense best practices," Computer Engineering and Intelligent Systems, vol. 14, no. 2, 2023. https://www.academia.edu/download/100604849/Network_Security_Concepts_Dangers_and_Defend_Best_Practical_PB.pdf
5. K. Dhanashekar, "Identity threads in the cloud tapestry: A comprehensive study of federated identity management and its role in ensuring cloud security," in Cloud Security, Chapman and Hall/CRC, 2024, pp. 124–142. http://103.203.175.90:81/fdScript/RootOfEBooks/E%20Book%20collection%20-%202025%20-%20I/RARE%20BOOKS/CRC_Cloud_Security_Concepts_Applications_and_Practices.pdf#page=137
6. P. Gannavarapu, "Deploying Azure AD federation with SAML for secure enterprise SaaS integration," Computer Fraud & Security, 2025.https://computerfraudsecurity.com/index.php/journal/article/view/782
7. S. Shingornikar and R. R. Bhandari, Proactive Early Threat Detection and Securing Oracle Database with IBM QRadar, IBM Security Guardium Database Protection, and IBM Copy Services Manager by Using IBM FlashSystem Safeguarded Copy. IBM Redbooks, 2023. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=NS-zEAAAQBAJ&oi=fnd&pg=PR1&dq=The+System+Authorization+Facility+allows+z/OS+components+to+request+centralized+authorization+decisions+before+accessing+a+dataset,+command,+terminal,+job,+started+task,+or+network+service&ots=yapqirWm4F&sig=hQVw9zfloJus6HV0WIebDANJDlQ
8. U. U. James, O. M. Ijiga, and L. A. Enyejo, "Zero Trust Network Access Enforcement for Securing Multi-Slice Architectures in 5G Private Enterprise Deployments," International Journal of Scientific Research and Modern Technology, vol. 10, no. 8, 2025. [Online]. Available: https://www.researchgate.net/profile/Ugoaghalam-Uche-James/publication/394640284_Zero_Trust_Network_Access_Enforcement_for_Securing_Multi-Slice_Architectures_in_5G_Private_Enterprise_Deployments/links/692ef9f91a621a227cf74eb0/Zero-Trust-Network-Access-Enforcement-for-Securing-Multi-Slice-Architectures-in-5G-Private-Enterprise-Deployments.pdf
9. F. Chadwick, "Optimizing Healthcare Systems: An AI-Powered Approach to Public Health Challenges," 2025. [Online]. Available: https://www.researchgate.net/profile/Fenella-Chadwick/publication/392622985_Optimizing_Healthcare_Systems_An_AI-Powered_Approach_to_Public_Health_Challenges/links/684ae7164c64e82b927f936e/Optimizing-Healthcare-Systems-An-AI-Powered-Approach-to-Public-Health-Challenges.pdf
10. S. Rangu, "Analyzing the impact of AI-powered call center automation on operational efficiency in healthcare," JISEM Journal, 2025.https://www.jisem-journal.com/index.php/journal/article/view/8901
11. P. R. Vennamaneni, "Modernizing monoliths: Transitioning legacy financial systems to microservices," JISEM Journal, 2025.https://www.jisem-journal.com/index.php/journal/article/view/8896
12. P. Sethuraman and R. K. Chennareddy, "AI-Based Fraud Detection and Prevention at the Radio Access Network: Architectures and Mechanisms for Financial Wireless Service," International Journal of Artificial Intelligence, Data Science, and Machine Learning, vol. 4, no. 4, pp. 132–141, 2023. [Online]. Available: http://ijaidsml.org/index.php/ijaidsml/article/download/442/406

13. A. C. Jha, P. Gannavarapu, and S. Durgam, “Machine Learning-Driven Security System for Next-Generation Ultra-Low-Latency Financial Network Governance,” 2025. https://ieeexplore.ieee.org/abstract/document/11374574
14. Z. Sayyed, “Application level scalable leader selection algorithm for distributed systems,” International Journal of Computational and Experimental Science and Engineering, vol. 11, no. 3, pp. 6676–6681, 2025. https://doi.org/10.22399/ijcesen.3856
15. V. K. Amarnath, “Improved Authentication And Authorization For Data Security: Integrating MFA And SSO,” Journal of International Crisis & Risk Communication Research, vol. 8, 2025. [Online]. Available: https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=25760017&AN=190052833&h=%2F7EwR2wjelECeOXVCw%2F0jngTjNt8%2B%2BiMGLb7%2B%2FYP678Y77qt2Bn85S8%2Buub%2FTbLGs%2FmXP9bq9IHAGQsF2pHyaw%3D%3D&crl=c
16. A. H. Y. Mohammed, R. A. Dziyauddin, and L. A. Latiff, “Current multi-factor of authentication: Approaches, requirements, attacks and challenges,” International Journal of Advanced Computer Science and Applications, vol. 14, no. 1, 2023. [Online]. Available: https://www.researchgate.net/profile/Ali-Mohammed-172/publication/367987835_Current_Multi-factor_of_Authentication_Approaches_Requirements_Attacks_and_Challenges/links/673857b968de5e5a307829c7/Current-Multi-factor-of-Authentication-Approaches-Requirements-Attacks-and-Challenges.pdf
17. S. Das, “Enhancing Agent Interactions and Decision-Making in Insurance with Intelligent Technologies,” Journal of Computational Analysis & Applications, vol. 33, no. 8, 2024. [Online]. Available: https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=15211398&AN=183965492&h=4XcVC%2FX264K%2FiqU20wVMevUcCukqChjy4KljXSPx7mVFf8YyUbsGu5B%2B8fvBIEV2lGxU5%2FxiuCJG6psTn9EJQA%3D%3D&crl=c
18. K. S. Chadha, “Predictive risk modeling in P&C insurance using Guidewire DataHub and Power BI Embedded Analytics,” IJNS, 2025.https://www.academicpublishers.org/journals/index.php/ijns/article/view/5754
19. R. Reddivari, B. B. Chavan, and B. Pandey, “AI-Integrated Identity and Access Management: Advancing Cybersecurity through Intelligent Access Control and Continuous Authentication,” in Proc. 2025 IEEE Madhya Pradesh Section Conference (MPCON), Aug. 2025, pp. 505–511. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/11256518/
20. R. Hariharan, “AI-driven identity and access management in enterprise systems,” IJIOT, 2025.https://www.academicpublishers.org/journals/index.php/ijiot/article/view/4300
21. A. S. George, T. Baskar, and P. B. Srikaanth, “Bridging the Security Skills Gap: A Comprehensive Framework for Developing Application Security Competencies in Modern Software Engineering,” Partners Universal Innovative Research Publication, vol. 3, no. 3, pp. 96–123, 2025. [Online]. Available: https://puirp.com/index.php/research/article/download/118/102
22. T. S. Krishna, T. Pyatlo, and S. U. Kumar, “A Comprehensive Framework for Advanced API Security and Real-Time Monitoring,” in Proc. 2025 Innovations in Power and Advanced Computing Technologies (i-PACT), Sep. 2025, pp. 1–8. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/11307868/
23. L. Saidy, A. A. Abayomi, A. C. Uzoka, and B. I. Adekunle, “The API integrity and access control framework (AIACF): A zero-trust security model for US-connected consumer platforms,” International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 10, no. 2, pp. 897–904, 2024. [Online]. Available: https://www.researchgate.net/profile/Bolaji-Adekunle/publication/391923127_The_API_Integrity_and_Access_Control_Framework_AIACF_A_Zero-Trust_Security_Model_for_US-Connected_Consumer_Platforms/links/682ddd7ddf0e3f544f56212f/The-API-Integrity-and-Access-Control-Framework-AIACF-A-Zero-Trust-Security-Model-for-US-Connected-Consumer-Platforms.pdf
24. D. Prajapati, “Proactive security architectures for ISP backbone routing: A zero-trust model for BGP and MPLS,” International Journal of Data Science and Machine Learning, vol. 5, no. 2, pp. 145-153, 2025. https://doi.org/10.55640/ijdsml-05-02-13