Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Innovations in Zero-Trust Security for Large-Scale Cloud Infrastructures

Sandeep Kumar Reddy Basireddy

Independent Researcher, USA

ARTICLE INFO

Received: 12 July 2025

Revised: 24 Aug 2025

Accepted: 06 Sept 2025

ABSTRACT

This article reflects the current advances in the Zero-Trust security architectures of the business-scale cloud infrastructure. Rising above the old concept of using a perimeter to control security, the Zero-Trust concept is designed on the basis of never trust, always verify, which allows an organization to have strong security in the ever-distributed computing environment. The innovations mentioned consist of fine-grained policy controls adapting to real-time risk assessments on many dimensions, automated threat containment to significantly decrease response times, and context-aware authorization frameworks that consider access requests based on wide situational knowledge. Its implementation architecture is based on the microservices approach, which has specialized components that communicate using standardized APIs and can be deployed in a modular fashion and improved in an incremental manner. Future research directions involve quantum-resistant cryptography, behaviorally verifiable biometrics, privacy-preserving verification, autonomous security systems, and long-range device attestation in the IoT setting. All of these innovations enhance the defenses of enterprises against a sophisticated range of cyber attacks and enable safe digital transformation with effective data protection, which addresses the difficulties of complex hybrid environments, where the traditional boundaries have likely long since been disregarded.

Keywords: Zero-Trust Security, Cloud Infrastructure Protection, Context-Aware Authorization, Automated Threat Containment, Distributed Policy Enforcement

1. Introduction

As organizations move important workloads to cloud environments, legacy perimeter models of security have been found wanting in the face of maturing threats. Zero-Trust security model, on "never trust, always verify," has become a better model for defending contemporary distributed architectures [1]. This seismic change accommodates the blurring of well-defined network perimeters and more maturing threat actors.

Zero-Trust deployment is a result of profound shifts in enterprise IT infrastructure. Enterprises today handle hybrid environments consisting of on-premises data centers, various clouds, and edge computing platforms. Such architectural complexity introduces unparalleled challenges to security teams in terms of maintaining visibility and control across multiple environments with varied security models, governance frameworks, and compliance mandates [1]. Zero-Trust delivers a single security model safeguarding resources irrespective of locations.

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Contemporary Zero-Trust solutions go beyond network segmentation to include advanced identity authentication, ongoing monitoring, and context-based access control [2]. The framework presumes threats both from outside and within networks and demands ongoing verification of each access request against multiple criteria before even granting restricted permissions.

Good Zero-Trust architectures combine ongoing validation, least privilege enforcements, and overall monitoring. This is a radical shift from the earlier models that had implicitly trusted corporate network users. Instead, Zero-Trust applies strict authentication to all access requests while monitoring continuously for suspicious activities that could reflect compromised credentials [2].

With cloud environments becoming more distributed, organizations need to implement scalable security models that provide consistent protection. Top organizations are rolling out enterprise Zero-Trust frameworks that address the entire range of emerging threats, offering tremendous benefits in preventing breaches, detecting threats, and responding to incidents over legacy methods [1,2].

2. Zero-Trust Evolution in Enterprise Cloud Environments

The Zero-Trust paradigm has significantly changed from its theoretical inception. Originally, network segmentation, when codified by Forrester Research analyst John Kindervag in 2010, modern implementations now go far beyond this narrow scope [3]. Kindervag's original architecture dissipated the idea of trusted internal networks that needed authentication and authorization regardless of their origin.

Zero-Trust has evolved in the last ten years to meet cloud-native designs where the traditional network boundaries have been erased. The current applications include identity management, continuous security posture, and data-centric protection, which follow information assets irrespective of the location and route of transmission.

Enterprise-level cloud deployments must be sensitive to performance, scalability, and complexity of operation. NIST Special Publication 800-207 calls for balancing operational requirements against security requirements using phased implementation [4]. Balance is especially important in high-throughput usage where latency effects are pronounced.

Current architectural developments enable granular enforcement with non-prohibitive overhead. Sophisticated deployments utilize distributed points of policy enforcement with local decision caches coordinated to centralized policy services, minimizing authorization latency while ensuring security. Sophisticated risk-scoring functionality allows adaptive security actions to apply strict controls only where context factors identify possible threats.

Cloud-native security capabilities now offer API-based control planes enforcing Zero-Trust principles programmatically on distributed resources. Latest deployments use policy orchestration layers interpreting high-level security requirements into environment-specific controls for every cloud platform [4].

This resource-based paradigm is especially beneficial in serverless and containerized environments with ephemeral infrastructure components that operate across multiple clouds. With security based on the resources instead of network location, organizations have uniform defense as applications move between environments or dynamically scale.

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Time Period	Zero-Trust Focus	Key Characteristics	Implementation Approach
2010 (Initial Concept)	Network Segmentation	Elimination of trusted internal networks	Perimeter-focused controls
2015-2020	Identity & Access	Authentication for all traffic, regardless of origin	Role-based access controls
2020-Present	Comprehensive Security	Identity verification, continuous monitoring, adaptive controls	Resource-centric protection
Current State	Cloud-Native Integration	API-driven control planes, distributed policy enforcement	Microservices architecture
Near Future	Advanced Context Evaluation	Risk-scoring algorithms, behavioral analytics	AI-powered adaptive controls

Table 1: Zero-Trust Security Evolution: From Network Segmentation to Resource-Centric Protection [3, 4]

3. Fine-Grained Policy Controls

One of the most significant advancements in the implementation of Zero-Trust has been the emergence of highly granular policy control mechanisms. CISA's Zero Trust Maturity Model 2.0 dictates that organizations at peak maturity levels need to adopt fine-grained, dynamic policies that respond to risk in real-time in five different pillars of identity, device, network, application workload, and data [5]. This multi-faceted approach is a far cry from legacy role-based access control systems that depended mainly on static user attributes. The CISA model in particular calls for mature implementations to impose risk-based access decisions that revalidate trustworthiness at every point during a session, rather than at first authentication. User identity and authentication state are the basis of Zero-Trust policy controls, with leading-edge implementations going far beyond basic username and password verification. CISA's maturity model calls for leading-edge implementations to include phishing-resistant authentication mechanisms, automated account management workflows, and strong identity governance processes [5]. Device security posture assessment has also advanced, with the CISA framework suggesting ongoing monitoring of device compliance state, real-time vulnerability management, and remediation through automation. Resource sensitivity classification is dealt with in the data pillar, where the best implementations are to keep dynamic data categorization that keeps changing based on content sensitivity. Most contemporary policy engines can analyze these dimensions in real-time, authorizing decisions upon thorough risk assessments instead of static rules. This method enables organizations to enforce least-privilege access principles with unequaled accuracy while limiting the attack surface without restricting legitimate user operations. The computational cost of this real-time analysis has spurred architectural developments that offload processing onto several specialized pieces. CISA's maturity model promotes automated policy enforcement with least privilege access controls, microsegmentation, and real-time threat intelligence [5]. The model also details that best-practice implementations should be able to enforce policies consistently across hybrid environments with little need for human intervention. This practice is in tandem with the CDM program's focus on automation and continuous monitoring, which allows security teams to maintain end-to-end visibility across the complex environment while determining and resolving potential vulnerabilities before they can be used against them [6].

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Policy Component	Capability	Implementation Requirement	Maturity Indicator
Identity Controls	Authentication verification	Phishing-resistant mechanisms	Advanced
Device Assessment	Security posture evaluation	Real-time compliance monitoring	Continuous
Data Classification	Resource sensitivity tracking	Dynamic categorization	Adaptive
Access Decisions	Authorization enforcement	Risk-based evaluation	Real-time
Policy Automation	Rule enforcement	Cross-environment consistency	Minimal intervention
Monitoring	Vulnerability detection	Comprehensive visibility	Proactive

Table 2: Multi-Dimensional Components of Zero-Trust Policy Controls [5, 6]

4. Real-Time Threat Containment

Another key innovation in Zero-Trust deployments is combining sophisticated threat detection functions with automated containment processes. Such solutions regularly scan network traffic, API calls, and user activity for signs of possible security threats. The Cloud Security Technical Reference Architecture of the Federal Government emphasizes that good cloud security mandates "continuous monitoring capabilities that rapidly detect potential security incidents and enable automated or accelerated responses" [7]. This strategy is a paradigm shift from traditional periodic security reviews to ongoing security operations that are capable of detecting and responding to threats in real-time. The TRA itself emphasizes the need to build advanced security information and event management (SIEM) capabilities with the ability to aggregate and correlate security information from multiple sources within cloud environments.

In case suspicious activities are spotted, the containment mechanisms are able to apply instant protective actions through automated response processes. The Cloud Security TRA identifies a number of key response capabilities that must be deployed in secure cloud environments, including automated incident response processes that are capable of initiating containment actions immediately without human intervention [7]. These containments include the capability to revoke or limit access tokens through the use of cloud identity and access management services to cancel suspicious sessions instantly. The TRA specifically suggests adopting just-in-time and just-enough-access models that reduce the damage of credential compromise by restricting privileges and access time. Isolation capacities are also highlighted, with the architecture suggesting that network segmentation controls should be able to quarantine possibly compromised resources.

This real-time response functionality is a far cry from the conventional security models, which tended to use post-incident analysis and human intervention. Through the automation of the containment process, organizations can effectively minimize the dwell time for probable attackers and reduce the effects of security incidents. The Cloud Security TRA itself highlights this benefit, suggesting that "automation of security processes can significantly reduce the time needed to detect and respond to threats" [7]. Gartner's review of XDR platforms also points to the role of automation in contemporary security operations, observing that such integrated solutions can "decrease the amount of time it takes for security teams to detect and respond to threats" by automating and consolidating security functions previously controlled by discrete tools [8].

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Containment Function	Capability	Implementation Mechanism	Security Benefit
Continuous Monitoring	Threat detection	SIEM correlation across sources	Early detection
Access Management	Token revocation	Cloud IAM services	Session termination
Privilege Control	Access limitation	Just-in-time/just-enough access	Credential compromise mitigation
Resource Protection	Isolation	Network segmentation	Compromise containment
Response Automation	Immediate action	Predefined workflows	Reduced dwell time
Security Integration	Cross-domain protection	XDR platform coordination	Comprehensive defense

Table 3: Zero-Trust Real-Time Threat Containment: Detection to Response [7, 8]

5. Context-Specific Authorization

Context-aware authorization is among the most advanced features of contemporary Zero-Trust architectures. These systems analyze requests for access based on a holistic knowledge of the situational context, taking into account factors that go beyond the conventional identity and role-based controls. Guidance from the National Security Agency regarding Zero Trust security implementation points out that organizations need to "leverage user behavior, endpoint health, service or workload, data sensitivity, and other telemetry as signals to define and enforce least-privilege access controls" [9]. This solution is an essential departure from historical authorization models that were based mainly on preassigned roles and permissions. NSA guidance specifically recommends ongoing validation that involves multiple factors for authorization and authentication decisions, rather than a one-time point-in-time verification. This adaptive method allows organizations to deploy adaptive security controls that react in an appropriate manner to evolving conditions while ensuring protection for critical assets.

Sophisticated context analysis engines utilize multiple analytical dimensions to create a broad knowledge base of each access request. Behavioral analytics functionality sets baselines of normal behavior for individual users and system elements and allows detection of low-level anomalies that may suggest account compromise or insider threats. The NSA guidance particularly suggests that organizations "consider the deployment of behavioral analytics to detect and defeat advanced persistent threats" since these capabilities offer "greater visibility into network and user-related activities" [9]. Environmental risk assessments analyze network properties such as the type of connection, location, and routing path to identify potentially malicious access behavior. Temporal analysis features identify suspicious access timing by contrasting current behavior with predefined patterns and raising alerts for untimely access attempts during non-standard working hours or non-standard days.

These contextual elements are analyzed using risk-scoring algorithms that dynamically adapt authorization levels according to the broad security posture and threat profile. The NSA document defines this functionality as part of an enterprise-wide security architecture in which "policy decision points (PDPs) provide authorization based on enterprise policy, system behavior, and multiple signals from the environment" [9]. Microsoft's Zero Trust guidance also points out the significance of risk-based conditional access policies that are able to "verify explicitly and use least privileged access" for

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

each access request [10]. Microsoft's strategy specifically suggests enacting "policies that evaluate the risk of the authentication request with signals from identity providers," allowing organizations to "demand stronger authentication methods for medium or high-risk sessions." This balanced strategy is especially critical in high-security situations where undue overrestraints can hinder operational efficiency.

Authorization Component	Functionality	Implementation Approach	Security Value
Behavioral Analytics	Normal activity baseline	User and system behavior profiling	Anomaly detection
Environmental Assessment	Network characteristics evaluation	Connection type and routing analysis	Suspicious access identification
Temporal Analysis	Access timing monitoring	Pattern comparison against baselines	Off-hours detection
Risk Scoring	Authorization threshold adjustment	Dynamic algorithm-based evaluation	Adaptive security posture
Policy Decision Points	Authorization determination	Enterprise policy and signal integration	Contextual access control
Conditional Access	Authentication strength variation	Risk-based verification requirements	Proportional security measures

Table 4: Multi-Dimensional Context Evaluation in Zero-Trust Authorization [9, 10]

6. Implementation Architecture

The architectural realization of such Zero-Trust innovations is breaking down into a microservices-based pattern, where each specialized component addresses various dimensions of the security model. Modern security architectures should adopt a "composable enterprise" pattern in which security capabilities are realized as independent, loosely coupled services that can be assembled and reassembled to address changing needs, states the Cloud Security Alliance's Enterprise Architecture Reference Guide v2 [11]. This architecture style complies with general industry trends toward modular application architecture, where organizations can develop, deploy, and update individual security components in isolation. The CSA recommendation particularly advises that security architectures must abide by the same design paradigms as new applications, with well-defined service boundaries, standardized interfaces, and self-scaling capabilities. This methodology allows organizations to deploy Zero-Trust controls that will easily change with shifting business needs while continuing to provide end-to-end security coverage in diverse environments.

Identity providers for authenticating users and systems with contemporary protocols such as OAuth 2.0, OpenID Connect, and SAML are the central elements of this design. Policy management services establish and deliver security policies, keeping the authoritative definition of the policy while enabling intricate governance processes. Context evaluation engines evaluate risk factors in real-time, analyzing telemetry data from a variety of sources to determine holistic risk scores. Enforcement points enforce access decisions at boundaries of resources, installing controls suitable to their particular technology environment. Monitoring systems identify anomalies and threats by continuously analyzing security-relevant events as well as behavioral patterns. Orchestration services

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

manage security responses among these varied components to provide uniform security operations across the environment. NIST Special Publication 800-204 titled "Security Strategies for Microservices-based Application Systems" stresses that security services must be designed with the same architectural concepts as the applications being secured, enabling them to "scale, evolve, and adapt" along with the secured workloads [12].

The components interact with each other using standardized APIs, enabling organizations to integrate solutions from multiple vendors with a unifying security architecture. This interoperability is crucial in enterprise settings where heterogeneous stacks of technologies are prevalent and security systems have to function well across disparate platforms. NIST SP 800-204 refers specifically to the significance of API security within microservices architecture, observing that "APIs represent both the primary attack surface and the primary control surface" for contemporary applications [12]. The recommendations call for the enforcement of strong API security controls such as good authentication, detailed authorization, validation of input, and overall monitoring. The CSA Enterprise Architecture Reference Guide also places a lot of emphasis on the role of API governance in security architecture and suggests that organizations have uniform standards for API design, security, and management for all parts [11]. This normalized communication plane is also robust with full audit capabilities, where every interaction between components is logged for compliance and security analysis.

This modular design accommodates incremental adoption and allows new security technology to be added as it comes along. The organization can start with core components such as identity management and simple policy enforcement and then add more advanced features incrementally, such as behavioral analysis and auto-response mechanisms. NIST SP 800-204 has referred to this incremental strategy as "evolutionary architecture," where systems are developed to support change with loosely coupled components and clearly defined interfaces [12]. The advice itself points out that the security architectures shall be developed for ongoing evolution instead of fixed deployment, allowing organizations to evolve in sync with changing needs and emerging dangers. The CSA Enterprise Architecture Reference Guide likewise espouses an "adaptable security architecture" capable of adding new capabilities without necessitating wholesale redesign [11]. This evolution capability is particularly useful in rapidly changing threat environments where new methods of attack may require new defensive capabilities. By designing security architectures with extensibility in mind, organizations can develop effective security architectures that will be useful over time as technologies and threats continue to evolve.

7. Future Directions

Zero-Trust architecture is evolving with companies having to handle complex threats and complex IT environments. The future innovations are bound to be determined by some of the emerging trends in this area. IBM Research's examination of NIST's post-quantum cryptography standardization effort emphasizes the pressing need for quantum-resistant algorithms as quantum computing developments threaten to undermine existing cryptographic underpinnings [13]. The study highlights that, as yet, large-scale quantum computers are still in development, the "harvest now, decrypt later" attack vector—where enemies gather today's encrypted data to decode when quantum computing is ready—poses a real risk to sensitive data worth having in the long term. IBM observes that NIST has chosen early quantum-resistant algorithms such as CRYSTALS-Kyber for general encryption and CRYSTALS-Dilithium for digital signatures, with other algorithms being considered for standardization. Organizations implementing Zero-Trust architectures must begin planning this quantum-resistant migration and evaluating where to implement post-quantum algorithms initially and how to manage both hybrid implementations during transition. This planning is necessary for ensuring long-term security as quantum computing is further developed.

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Next-generation behavioral biometrics for ongoing continuous authentication are another major area of Zero-Trust evolution. Next-generation authentication systems, as studied by HyperVerge through research on biometric technologies, are shifting away from the conventional fingerprint and facial recognition to more advanced methods capable of constantly verifying identity during the course of a session [14]. The study points out innovative techniques such as gait analysis, voice pattern analysis, keystroke dynamics, and even cardiac rhythm analysis that have the ability to passively authenticate users without explicit verification activities. These ongoing authentication solutions are most useful in Zero-Trust designs, where the "never trust, always verify" philosophy necessitates continuous validation instead of point-in-time authentication. HyperVerge asserts that multi-modal biometric solutions with multiple factors are much more accurate than single-factor-based methods, with error rates less than 0.1% under controlled environments. With these modern biometric capabilities integrated, Zero-Trust systems can provide continuous identity verification with reduced user friction.

Privacy-enhancing verification methods that reduce exposure of sensitive data are becoming more relevant as organizations weigh security demands against privacy regulations. HyperVerge's study identifies the increased uptake of "privacy-by-design" strategies in biometric systems, wherein methods such as tokenization, local device processing, and encrypted biometric templates secure sensitive personal information [14]. Such methods enable organizations to conduct rigorous identity verification without establishing centralized stores of biometric data that become attack targets. IBM Research also emphasizes the value of privacy-preserving cryptography in post-quantum security, indicating that technologies such as homomorphic encryption and secure multi-party computation can support verification without revealing underlying data [13]. These functions are especially valuable to organizations within areas with strong data protection policies, allowing for compliance without sacrificing strong security controls.

Autonomous security solutions that learn to adapt under evolving conditions without the intervention of humans are perhaps the most revolutionary path in the advancement of Zero-Trust. HyperVerge's whitepaper outlines how artificial intelligence is revolutionizing security functions, where sophisticated systems are able to recognize anomalies, update security policies, and direct response with little human intervention [14]. The AI systems are able to examine large volumes of telemetry data to spot mild signals of compromise that may go unnoticed by humans. By processing at machine speed, autonomous security solutions are able to detect and isolate potential threats before any real damage is done. IBM Research also points to the contribution of AI in security procedures, specifically for identifying advanced attacks that take advantage of quantum weakness in classical cryptosystems [13]. With increasingly complex and high-speed attack methods, such autonomous functions will need to be an integral part of effective Zero-Trust deployments.

Comprehensive device attestation solutions for IoT and edge computing environments are becoming increasingly necessary with the increasing trend of computing going outside of traditional data centers and cloud spaces. HyperVerge's work points to the difficulty of securing heterogeneous IoT devices with different computational powers and the necessity of light authentication mechanisms for resource-limited settings [14]. The study specifically touches upon the increasing importance of edge computing to process biometrics, in which sensitive processing is done locally for better privacy and less latency. IBM also mentions the same difficulties in the adoption of post-quantum cryptography for limited environments, stressing the importance of optimized implementations that can be applied on devices with less processing power and memory [13]. These are especially relevant since Zero-Trust concepts are being extended to include the intelligent edge, where only uncompromised and approved devices can be used to access sensitive assets.

Such developments will also enhance the security position of business environments in the clouds as they cope with emerging threats because of privacy regulations, remote workforce, and larger digital ecology. Through such next-generation features integrated into their security infrastructure, the

organizations will be in a position to still enjoy high protection even as threats and technologies continue to evolve.

Conclusion

Zero-Trust innovations in cloud-wide security systems have fundamentally altered how organizations safeguard their sensitive resources and offer opportunities to undergo digital transformation projects. The paradigm shift in the understanding of security as the perimeter to end-to-end context-aware verification is not only a technical change but a philosophical redefinition of the enterprise security strategy. By enabling real-time containment of threats at dramatically low attacker dwell time, state-of-the-art context-sensitive authorization that can balance both security and operational requirements, and fine-grained policy controls that are in essence continuous risk evaluation, these architectures offer strong defenses against advanced attacks without subjecting operations to prohibitive operational overhead. The approach to the implementation of microservices allows organizations to integrate the principles of Zero-Trust in stages, and it is also flexible to include new technologies and respond to new threats. With the computing landscape continuing to grow beyond the traditional scope to include multi-cloud, edge, and IoT, the further development of the Zero-Trust solutions will prove instrumental in ensuring some level of uniformity in the security of the increasingly distributed digital environments. By adopting such innovations, organizations are placed in a secure position to support an ever-growing number of digital services without introducing weak data protection controls into an increasingly difficult threat environment.

References

[1] Thales, "Cloud Security in 2024: Addressing the Shifting Landscape," Cloud Security Alliance, 2024. [Online]. Available: https://cloudsecurityalliance.org/blog/2024/06/27/cloud-security-in-2024-addressing-the-shifting-landscape

[2] Palo Alto Networks, "What is Zero Trust Architecture (ZTA)?". [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture

[3] John Kindervag et al., "No More Chewy Centers: Introducing The Zero Trust Model Of Information Security," Forrester Research, 2016. [Online]. Available: https://www.forrester.com/report/no-more-chewy-centers-introducing-the-zero-trust-model-of-information-security/RES56682

[4] Scott Rose et al., "Zero Trust Architecture," NIST Special Publication 800-207, 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[5] Cybersecurity and Infrastructure Security Agency, "Zero Trust Maturity Model," 2023. [Online]. Available: https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

[6] Centers for Medicare & Medicaid Services, "Continuous Diagnostics and Mitigation (CDM)," CMS Security, 2023. [Online]. Available: https://security.cms.gov/learn/continuous-diagnostics-and-mitigation-cdm

[7] Cybersecurity and Infrastructure Security Agency, United States Digital Service, and Federal Risk and Authorization Management Program, "Cloud Security Technical Reference Architecture," 2022. [Online]. Available: https://www.cisa.gov/sites/default/files/2023-05/Cloud%20Security%20Technical%20Reference%20Architecture%20v2.pdf

[8] Barry Fisher, "Gartner's report on innovation insight for XDR," Cisco Security Blog, 2020. [Online]. Available: https://blogs.cisco.com/security/gartners-report-on-innovation-insight-for-xdr

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[9] National Security Agency, "Embracing a Zero Trust Security Model,". [Online]. Available: https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.pdf

[10] Microsoft, "Zero Trust deployment plan with Microsoft 365," Microsoft Learn, 2025. [Online]. Available: https://learn.microsoft.com/en-us/security/zero-trust/microsoft-365-zero-trust

[11] Cloud Security Alliance, "CSA Enterprise Architecture Reference Guide," 2021. [Online]. Available: https://cloudsecurityalliance.org/artifacts/enterprise-architecture-reference-guide-v2

[12] Ramaswamy Chandramouli, "Security Strategies for Microservices-based Application Systems Share to Facebook Share to X Share to LinkedIn," NIST SP 800-204, 2019. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/204/final

[13] IBM Research, "NIST's post-quantum cryptography standards are here,". [Online]. Available: https://research.ibm.com/blog/nist-pqc-standards

[14] Nupura Ughade, "Future Of Biometrics: Trends, Innovations, And Challenges Ahead," HyperVerge, 2025. [Online]. Available: https://hyperverge.co/blog/future-of-biometrics/