American Journal of Innovation in Science and Engineering (AJISE)

ISSN: 2158-7205 (ONLINE)

VOLUME 5 ISSUE 1 (2026)

PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

American Journal of Innovation in Science and Engineering (AJISE)

Volume 5 Issue 1, Year 2026
ISSN: 2158-7205 (Online)
DOI: https://doi.org/10.54536/ajise.v5i1.5905
https://journals.e-palli.com/home/index.php/ajise

Zero Trust Architecture (ZTA) Design and Implementation, A Comprehensive Review

Zain Muhammad[1*]

Article Information

Received: August 07, 2024

Accepted: October 02, 2025

Published: February 2, 2026

Keywords

ABAC, BeyondCorp, Data-Centric Security, Identity and Access Management, Micro-Segmentation, PDP/PEP, RBAC, SASE, Zero Trust Architecture, ZTNA

ABSTRACT

Zero Trust Architecture (ZTA) has emerged as a transformative security model, evolving from perimeter-based defense systems to a more resilient, identity-centric approach in response to the growing complexity of modern cybersecurity threats. This review explores the design and implementation of ZTA, focusing on its core principles, including identity verification, least-privilege access, and continuous monitoring. With a particular emphasis on cloud-first, hybrid work environments, ZTA replaces implicit trust with real-time, context-aware access decisions, ensuring stronger security postures across distributed networks. The paper synthesizes key frameworks, such as NIST SP 800-207 and CISA's Zero Trust Maturity Model, to provide a comprehensive understanding of ZTA's components and their real-world applications. It also examines the challenges and risks associated with legacy systems, integration complexities, and tool interoperability, while offering strategies for overcoming these barriers. Through case studies from sectors like finance, healthcare, and government, the paper demonstrates the successful application of ZTA, highlighting measurable improvements in security and user experience. The review concludes by addressing future trends, such as the integration of AI/ML in policy decisions and the convergence of ZTA with SASE, ensuring Zero Trust remains adaptable to emerging cybersecurity needs.

INTRODUCTION

Enterprise security has shifted from defending fixed boundaries to protecting identities, devices, applications, and data that operate well beyond the traditional network perimeter. Zero Trust Architecture (ZTA) emerged to address this change, replacing implicit trust on "inside" networks with explicit, continuous verification tied to context and risk (Rose *et al.*, 2020). Similarly, public-sector momentum, most visibly the U.S. federal push following Executive Order 14028, accelerated adoption by turning principles into concrete milestones and controls (Young, 2022; NIST, 2021). Oversight bodies now track progress, reinforcing Zero Trust as both a technical approach and a governance imperative (U.S. Government Accountability Office [GAO], 2024). Therefore, ZTA is increasingly framed not only as a security model but also as an operational paradigm that enables organisations to remain resilient in a constantly evolving digital environment.

The evolution of cybersecurity threats further explains this shift. The modern threat landscape is defined by cloud-centric workloads, SaaS sprawl, remote and hybrid work, and sophisticated identity-driven attacks. These shifts erode the value of location as a trust signal and increase opportunities for lateral movement after an initial compromise (ENISA, 2021; Microsoft, 2021). In response, security guidance emphasizes secure-by-design practices and prioritises identity, device posture, and continuous monitoring as first-class controls rather than afterthoughts (CISA, 2023). Moreover, market data demonstrates how organisations increasingly standardise on phishing-resistant authentication and conditional access, establishing these as table-stakes capabilities for both the workforce and third-party access (Okta, 2023).

The limitations of perimeter-based security models have become even more apparent under these conditions. Traditional perimeter models assume that users and assets "inside" the network are trustworthy, which fails when users, apps, and data are dispersed across diverse environments. VPNs, for instance, extend implicit trust and often expose broad network ranges, thereby making lateral movement easier once credentials are stolen (NCSC, 2021; Rose *et al.*, 2020). Furthermore, federal readiness reviews have highlighted visibility gaps, legacy dependencies, and identity weaknesses that undermine perimeter defences and slow incident response. Collectively, these issues underscore the need for a Zero Trust redesign rather than incremental patching (Federal Trade Commission Office of Inspector General, 2023; Washington & Sharek, 2023).

In this context, a clear definition of Zero Trust Architecture (ZTA) becomes critical. ZTA is a holistic security strategy and reference architecture in which no request is trusted by default, whether it originates inside or outside the network. Every access decision is made dynamically based on identity, device health, application context, data sensitivity, and observed behaviour, and is enforced as close to the resource as possible (Rose *et al.*, 2020; CISA, 2023). In addition, implementation guidance now spans maturity models, control mappings, and hands-on builds that demonstrate how organisations can realise these principles at scale across identity, endpoints, networks, applications, and data (NIST, 2024a; NIST, 2024b).

The core concept of "never trust, always verify" captures

[1] Newport's Institute of Communications and Economics: Karachi, Sindh, Pakistan
[*] Corresponding author's e-mail: zainmuhammad81@outlook.com

the operational mindset of ZTA. This principle means authentication and authorisation are continuous and context-aware rather than one-time events. NIST formalises this through a policy decision point (PDP) and policy enforcement point (PEP) pattern, along with a trust algorithm that evaluates real-time signals for each request (Rose *et al*., 2020). Similarly, agency and industry guidance align on enforcing least privilege per session, validating device posture, and brokering application-level access through ZTNA or equivalent proxies, all of which reduce network exposure and the blast radius of potential compromise (NSA, 2024b; Google Cloud, 2021; AWS, 2023; Microsoft, 2025).

Zero Trust also aligns with broader cybersecurity principles. Rather than replacing established frameworks, it operationalises them in measurable, automated ways. For example, controls in NIST SP 800-53 Rev.5 map naturally to ZTA pillars for identity, device, network, application, and data safeguards (NIST, 2020; CISA, 2023). Likewise, ISO/IEC 27001:2022 and 27002:2022 provide governance and control baselines that ZTA can automate and continuously evidence, thereby improving auditability and resilience (ISO, 2022; ISO/IEC, 2022). For high-threat environments, enhanced requirements for protecting sensitive information further reinforce the need for granular access, strong identity assurance, and robust telemetry (Ross, 2024).

With this foundation, the objectives of the this research is clear. First, it clarifies the evolution from perimeter models to Zero Trust, exposing the assumptions that no longer hold in cloud-first, hybrid workplaces (ENISA, 2021; CISA, 2023). Second, it synthesises leading frameworks such as NIST SP 800-207, CISA's Zero Trust Maturity Model, OMB M-22-09, and reference implementations like BeyondCorp, highlighting both common concepts and practical differences (Rose *et al*., 2020; CISA, 2023; Young, 2022; Google Cloud, 2021). Third, it maps architectural components and design choices to real-world implementation steps, including identity modernisation, micro-segmentation, ZTNA, and data-centric controls (NIST, 2024a; AWS, 2025; Microsoft, 2021). Finally, it distils organisational, technical, and financial challenges observed in public reviews and case studies, offering mitigation strategies and measurable outcomes (Federal Trade Commission Office of Inspector General, 2023; Washington & Sharek, 2023; SSH.COM, 2021; Sood *et al*., 2024).

The scope and structure of the paper are equally important. The discussion focuses on enterprise adoption across both private and public sectors, with examples from finance, healthcare, and government. Section 2 traces the historical path from perimeter defences to identity- and data-centric control planes, explaining the pressures created by cloud, SaaS, remote work, and APT tradecraft (ENISA, 2021; GAO, 2024). Section 3 outlines the core principles of strong identity, least privilege, micro-segmentation, device trust, data protection, and continuous monitoring, framed by recognised guidance (Rose *et al*., 2020; CISA, 2023; NSA, 2021). Section 4 compares design frameworks, emphasising NIST SP 800-207, CISA maturity guidance, and the engineering patterns popularised in BeyondCorp, supported by current NCCoE implementation work (NIST, 2024a; NIST, 2024b; Google Cloud, 2021). Section 5 details architectural components and their functions, tying IAM, ZTNA, SASE, API security, encryption, DLP, SIEM, and UEBA to the PDP/PEP pattern and policy-as-code practices (AWS, 2023; Microsoft, 2021; CISA, 2023). Section 6 proposes an implementation roadmap that begins with assessment and identity foundations, advances through micro-segmentation and application-level access, and institutionalises governance and continuous improvement (NIST, 2024a; CISA, 2024a). Section 7 addresses challenges in integrating legacy systems, consolidating tools, managing cultural change, and measuring progress, drawing on federal audits for concrete lessons (Federal Trade Commission Office of Inspector General, 2023; Washington & Sharek, 2023). Section 8 presents short case studies to connect design choices to outcomes, and Section 9 looks ahead to AI-assisted policy, SASE convergence, machine identity, PQC readiness, and Zero Trust beyond Earth-bound networks (Sood *et al*., 2024; CISA, 2024b; Adams, 2025; Ross, 2024).

By combining standards, implementation playbooks, audits, and sector-specific case studies, this review aims to help architects and security leaders translate Zero Trust from an aspiration into a measurable operating model. In doing so, it seeks to demonstrate how Zero Trust can simultaneously improve resilience, compliance, and user experience (Rose *et al*., 2020; CISA, 2023; AWS, 2025).

LITERATURE REVIEW

Traditional approaches to enterprise security were rooted in perimeter-based models, where controls were concentrated at the network edge and internal traffic was implicitly trusted. This design reflected an earlier era dominated by on-premises applications, office-bound users, and predictable traffic flows. However, as organisations shifted to cloud adoption, mobile work, and distributed infrastructures, the assumption that "inside equals trusted" proved unsustainable. Attackers able to bypass perimeter defences could move laterally with little resistance, highlighting the fragility of firewall- and VLAN-centric models (NCSC, 2021; Rose *et al*., 2020). The widely cited castle-and-moat analogy illustrates the weakness of this paradigm: while the external boundary appeared fortified, interior defences were often sparse, enabling adversaries with stolen credentials to expand their reach before detection (Microsoft, 2021; FTC OIG, 2023; Washington & Sharek, 2023).

The limitations of perimeter security extended beyond conceptual flaws. Firewalls and VPNs, tuned for static north–south traffic, lacked visibility into east–west movement, API-to-API communications, and SaaS platforms that bypassed datacentres altogether. Even

when paired with extensive control catalogues, perimeter-focused architectures under-enforced critical factors such as device posture, identity assurance, and application context at the point of use (NIST, 2020; CISA, 2023). These weaknesses became increasingly dangerous in the post-2020 environment defined by SaaS proliferation, hybrid work, API-first design, and identity-driven attack vectors. As a result, security programmes began to elevate identity, device health, and data sensitivity as the central inputs for access control, replacing location-based trust signals with conditional and phishing-resistant mechanisms (ENISA, 2021; Okta, 2023).

Cloud adoption and hybrid environments accelerated the urgency of change. Applications and data now reside outside traditional perimeters, with traffic patterns shifting to many-to-many pathways across users, services, and automation. VPN backhauling added cost and latency without restoring meaningful security, while Zero Trust alternatives introduced app-level access brokers, identity-aware gateways, and decision points placed closer to resources (AWS, 2023; Google Cloud, 2021; NIST, 2024a). Remote and mobile work further erased the distinction between internal and external traffic. Devices connecting from unmanaged networks to SaaS applications bypassed firewalls entirely, forcing programmes to adopt continuous authentication, device posture attestation, and adaptive session-aware policies (Microsoft, 2025; CISA, 2024a). At the same time, insider threats and advanced persistent threats (APTs) exposed gaps in monitoring and privilege management, with account takeover, token theft, and MFA fatigue serving as common entry points. Mitigations in these contexts emphasised segmentation, just-in-time privilege assignment, and continuous validation aligned to data sensitivity and mission risk (ENISA, 2021; NSA, 2024b; Ross, 2024).

Regulatory and compliance pressures reinforced these technical drivers. In the United States, Executive Order 14028 mandated Zero Trust milestones across federal agencies, converting aspirational guidance into enforceable requirements (Young, 2022; NIST, 2021). Oversight bodies such as GAO tied compliance reviews to measurable outcomes, creating accountability and budget justification for adoption (GAO, 2024). Private-sector boards similarly demanded demonstrable risk reduction and audit-ready evidence of control effectiveness. Across industries, regulatory frameworks such as GDPR, HIPAA, and PCI-DSS placed renewed emphasis on access minimisation, encryption, auditability, and continuous monitoring, all of which map directly to Zero Trust principles (ISO/IEC, 2022; NIST, 2020).

Within this context, Zero Trust emerged as a reference architecture rather than a product, anchored in the principle of "never trust, always verify." Every request must be authenticated and authorised dynamically, drawing on identity, device, application, and data context, and continuously re-evaluated as conditions change (Rose *et al*., 2020; CISA, 2023). Key mechanisms include phishing-resistant multi-factor authentication, adaptive authentication informed by behavioural and environmental risk signals, and granular authorisation through a blend of role- and attribute-based controls (Microsoft, 2025; AWS, 2023). Micro-segmentation and software-defined perimeters limit lateral movement by brokering access at the application level, while device trust frameworks integrate posture data into access decisions (Google Cloud, 2021; NSA, 2024b). Data-centric enforcement builds on consistent labelling, encryption, and monitoring, ensuring that controls follow information regardless of location (ISO/IEC, 2022; Hernandez, 2024).

Multiple frameworks and models now articulate Zero Trust principles in practical terms. NIST SP 800-207 provides the canonical architectural blueprint, introducing the Policy Decision Point (PDP) and Policy Enforcement Point (PEP) pattern and formalising trust algorithms for dynamic access (Rose *et al*., 2020; NIST, 2024a). Forrester's Zero Trust eXtended (ZTX) model popularised a pillar-based view that influenced subsequent maturity models, such as CISA's Zero Trust Maturity Model, which provides agencies and enterprises with structured milestones (CISA, 2023). Industry implementations—Google's BeyondCorp, Microsoft's six-domain model, and AWS's brokered access patterns—translate these ideas into engineering practices at scale (Google Cloud, 2021; Microsoft, 2025; AWS, 2023). Complementary standards, including ISO/IEC 27001:2022 and NIST SP 800-53 Rev.5, align Zero Trust adoption with auditable controls and governance structures (ISO/IEC, 2022; NIST, 2020). Together, these frameworks form a converging body of knowledge that operationalises Zero Trust as both a technical paradigm and a governance imperative, preparing organisations to withstand evolving cyber threats while maintaining regulatory compliance.

Despite of this, several research gaps remain. First, while frameworks provide detailed architectural principles, less is known about how these translate into measurable operational outcomes across different sectors. Second, case studies highlight early adoption patterns, but there is limited comparative evidence on scalability and long-term resilience of Zero Trust implementations. Finally, the interplay between regulatory mandates, organisational culture, and technical adoption requires deeper analysis to determine how Zero Trust can move from compliance-driven adoption to sustainable, enterprise-wide transformation.

MATERIALS AND METHODS

The methodology adopted for this review follows a structured, multi-phase approach that integrates academic literature, policy documents, and industry case studies to capture the full scope of Zero Trust Architecture (ZTA). Given that Zero Trust has matured significantly in the past five years, the review concentrates on works published between 2020 and 2025, a period marked by accelerated

adoption following the U.S. Executive Order 14028 (2021) and the release of formal frameworks such as NIST SP 800-207 (2020) and CISA's Zero Trust Maturity Model (2021–2023 revisions). Earlier publications were selectively included where they introduced foundational metaphors or principles—for example, perimeter-based models described prior to 2018. This ensured both historical continuity and contemporary relevance.

In the first stage, source identification was conducted across multiple channels. Scholarly databases, including IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, and Taylor & Francis Online, were searched using combinations of keywords such as "Zero Trust Architecture," "ZTA implementation," "ZTNA," "micro-segmentation," "SASE," "identity-centric security," and "policy decision point/enforcement point (PDP/PEP)." Parallel to this, government and standards repositories (NIST, CISA, NSA, ENISA, GAO, ISO/IEC) were systematically reviewed for policy documents, technical guidance, and audit reports. To bridge theory with practice, industry whitepapers and reference implementations from Microsoft, AWS, Google Cloud, Cisco, Netskope, and Cloudflare were included. This triangulated search strategy ensured the review captured academic rigour, regulatory context, and applied industry insights.

The second stage involved source selection and evaluation. Documents were included if they satisfied at least one of four criteria: (i) explicit focus on ZTA principles, design, or deployment; (ii) presentation of frameworks, maturity models, or regulatory mandates; (iii) sector-specific application in finance, healthcare, or government; or (iv) measurable implementation outcomes such as reduced lateral movement, improved compliance, or enhanced user experience. Exclusion criteria removed works that merely referenced Zero Trust in passing, lacked sufficient technical or empirical grounding, or duplicated content without adding new insight. Each selected source was then assessed for credibility, originality, and recency, with priority given to peer-reviewed research, government-issued documents, and industry case studies backed by measurable data.

The final stage applied a thematic synthesis approach. Sources were categorised under recurring themes: (1) the historical evolution from perimeter models to identity- and data-centric architectures; (2) the definition and principles of ZTA, including "never trust, always verify"; (3) comparisons of frameworks such as NIST SP 800-207, CISA Zero Trust Maturity Model, BeyondCorp, and Forrester's ZTX; (4) architectural components including IAM, ZTNA, SASE, and data-centric security; (5) implementation roadmaps and phased rollouts; (6) challenges involving legacy integration, interoperability, organisational resistance, and skills gaps; and (7) sector-specific case studies with quantifiable outcomes. This thematic grouping enabled the review to move beyond descriptive summaries and instead provide a synthesised analysis of patterns, divergences, and lessons learned across domains.

The strength of this methodology lies in its combination of breadth and temporal precision. By focusing on 2020–2025 as the primary window of analysis, the review captures the period in which Zero Trust transitioned from a conceptual idea to an operational mandate supported by measurable government milestones and commercial deployments. At the same time, by including sector case studies and oversight audits, it balances theoretical constructs with practical realities. This approach ensures the conclusions of the review are both academically rigorous and practically applicable, offering a reliable foundation for researchers, policymakers, and practitioners engaged in Zero Trust adoption.

RESULTS AND DISCUSSIONS

The review of guidance documents, sector case studies, and implementation playbooks reveals a consistent set of results regarding Zero Trust adoption across industries and government agencies. While the literature underscores the limitations of perimeter models, the findings here demonstrate how organisations are translating Zero Trust principles into operational practice, what obstacles they face, and which patterns appear most effective in achieving measurable improvements.

One clear result is the centrality of identity modernisation. Programmes that prioritised single sign-on, phishing-resistant multi-factor authentication, and conditional access policies reported the most immediate reductions in risk. These initiatives not only constrained account takeover attempts but also enabled more consistent enforcement of least privilege. Evidence from audits showed that agencies with mature identity platforms were able to revoke compromised tokens faster, correlate requests with device posture more accurately, and satisfy oversight demands for logging completeness. This suggests that identity upgrades function as the first and most decisive step in any Zero Trust roadmap, providing measurable outcomes well before segmentation or advanced analytics are deployed.

A second set of findings concerns segmentation and access brokering. Organisations that replaced broad VPN tunnels with Zero Trust Network Access (ZTNA) or BeyondCorp-style access proxies reduced lateral movement and made exposure boundaries more explicit. Pilot projects in finance and healthcare demonstrated that brokering application-level access cut down on unnecessary network reach and simplified monitoring. Metrics collected from industry deployments, such as lower VPN backhaul, fewer password prompts, and more granular evidence trails, indicate that segmentation and ZTNA do not merely replicate perimeter controls but create a different operating model altogether. These results reinforce that application-centric connectivity, combined with just-in-time privilege, has a tangible impact on both security posture and user experience.

The findings also show that effective implementation requires phased rollouts rather than large-scale rewires.

Evidence from NCCoE prototypes and federal pilots confirms that delivering "vertical slices" across identity, device, access, and data for a limited set of applications yields early wins and surfaces policy gaps before scaling. This incremental strategy contrasts with ad hoc deployments of overlapping tools, which audits revealed as a recurring source of policy drift and weak accountability. Results therefore highlight the value of sequencing: identity modernisation first, followed by ZTNA pilots, then progressive application of micro-segmentation and data-centric controls.

Case studies across sectors illustrate further dimensions of success and challenge. In financial services, the use of privileged access management with Zero Trust enforcement passed stringent audit requirements while reducing network exposure around high-value systems. Healthcare deployments demonstrated that Zero Trust patterns could be adapted to legacy clinical applications without full rewrites, showing feasibility in constrained environments. Government agencies provided some of the most detailed evidence, as oversight reports documented both improvements and persistent weaknesses. Progress was recorded in adoption of phishing-resistant authentication, application-level brokering, and data tagging, while identity misconfigurations and incomplete logging remained bottlenecks. Across all sectors, the results converge on three recurring lessons: identity modernisation delivers the fastest gains, application-level access outperforms network expansion, and audit-ready evidence of policy decisions is as important as the enforcement itself.

The analysis of challenges yields equally significant results. Technical barriers remain concentrated in legacy dependencies and brittle identity stores, which resist per-request enforcement. Organisational barriers centre on change management, as users initially perceive conditional access prompts or new access brokers as sources of friction. Skills gaps in policy-as-code and telemetry design appear frequently in oversight letters, suggesting that human capability remains as crucial as technical tooling. Financial constraints also shape adoption paths; however, evidence indicates that consolidation through Secure Access Service Edge (SASE) can offset costs if policy and identity remain authoritative. Collectively, these results reveal that challenges are not uniform but vary by maturity, sector, and scale, requiring tailored mitigation strategies.

Looking forward, the review identifies emerging trends that shape the trajectory of Zero Trust adoption. Results point to the growing integration of AI and machine learning into trust algorithms, enhancing the ability to detect anomalies and adjust policies dynamically, though oversight reports stress the need for explainability and auditability of these models. Convergence with SASE illustrates another result: while unification of ZTNA, secure web gateways, and DLP at the edge lowers latency and operational load, policy drift becomes a risk if centralised decision logic is weakened. Finally, preparations for post-quantum cryptography have begun to appear in Zero Trust roadmaps, with agencies and providers inventorying dependencies and planning hybrid transitions to preserve resilience in the face of future cryptographic threats.

Taken together, these results show that Zero Trust has moved from aspirational principle to measurable operating model. Identity, application-level access, and evidence collection form the core outcomes observed across industries, while phased rollouts and governance alignment underpin successful programmes. Persistent challenges remain, particularly in legacy integration, interoperability, and skills development, but the direction of travel is clear: organisations that embed Zero Trust as both a technical and governance framework demonstrate greater resilience, improved audit readiness, and enhanced user experience compared with those relying on perimeter-based designs.

CONCLUSION

Zero Trust reframes enterprise security away from static perimeter-based models toward continuous, context-aware verification rooted in identity, device posture, application context, and data sensitivity. The stable architectural pattern of policy decision points (PDPs) for decisions and policy enforcement points (PEPs) for implementation has proven resilient across technologies, while maturity models and playbooks have turned principles into operational practice (Rose *et al.*, 2020; CISA, 2023; NIST, 2024a). Evidence shows that organisations leading with strong identity assurance, segmented access, and evidence-ready telemetry achieve measurable reductions in lateral movement and accelerate incident response (Microsoft, 2025). In this way, Zero Trust is evolving from a conceptual paradigm into a measurable operating model that strengthens both resilience and user experience.

Limitations

Despite the breadth of literature, several limitations must be acknowledged. First, most available evidence is concentrated in government, finance, and healthcare sectors, leaving other industries underrepresented. Second, much of the published work remains prescriptive, offering frameworks and best practices but fewer longitudinal studies or quantitative evaluations of Zero Trust performance over time. Third, the dependence on case studies and audit reports means findings are shaped by contextual constraints, and results may not be universally generalisable. Finally, rapid technological shifts — particularly in AI-driven threats and post-quantum cryptography — mean that conclusions drawn today may require revalidation as architectures evolve.

Future Research Directions

Future research should build on these limitations by generating more comparative and empirical data across diverse organisational contexts. Rigorous longitudinal

studies are needed to examine whether Zero Trust controls deliver sustained improvements in resilience, audit readiness, and cost efficiency. Cross-sectoral comparisons could provide insight into scalability and adaptability in environments with different regulatory, cultural, or resource constraints. Moreover, further work is needed to investigate how Zero Trust interacts with emerging technologies such as AI-driven anomaly detection, quantum-resistant cryptography, and global regulatory harmonisation. Addressing these questions will move Zero Trust from compliance-driven adoption to a truly evidence-based security paradigm.

Practical Implications

The findings of this review carry important implications for practice. Enterprises should prioritise identity modernisation, phishing-resistant multi-factor authentication, and application-level access as the foundation of Zero Trust, as these produce the fastest and most visible reductions in risk. Governance must be treated as an equal partner to technology, with logging quality, segmentation depth, and evidence collection seen as decisive enablers rather than afterthoughts. Policymakers and regulators can reinforce adoption by framing Zero Trust milestones in measurable, auditable terms that align security investments with compliance outcomes. Finally, by embedding Zero Trust as a cross-functional operating model — where architecture, operations, and governance reinforce one another — organisations can improve both resilience and user experience, fulfilling the "never trust, always verify" principle at enterprise scale (Rose *et al.*, 2020; Homeland Security, 2025).

REFERENCES

Adams, M. (2025, May 15). *How the Microsoft Secure Future Initiative brings Zero Trust to life [Blog post]. Microsoft Security Blog.* https://www.microsoft.com/en-us/security/blog/2025/05/15/how-the-microsoft-secure-future-initiative-brings-zero-trust-to-life/

Amazon Web Services. (2023). *Embracing Zero Trust: A strategy for secure and agile business transformation* [White paper]. AWS Prescriptive Guidance. https://docs.aws.amazon.com/prescriptive-guidance/latest/strategy-zero-trust-architecture/introduction.html

Amazon Web Services. (2025). *Zero Trust on AWS*. https://aws.amazon.com/security/zero-trust/

Bokan, B. (2024). *Zero Trust for federal enterprise* [Conference presentation]. *Federal Cybersecurity and Privacy Professionals Forum.* https://csrc.nist.gov/csrc/media/Presentations/2024/cisa-and-zero-trust-for-federal-enterprise/images-media/CISA_and_Zero_Trust_for_Fed-Bokan_1115am.pdf

CISA. (2023). Secure-by-design. *Cybersecurity and Infrastructure Security Agency.* https://www.cisa.gov/resources-tools/resources/secure-by-design

CISA. (2024a, March 12). *CISA publishes SCuBA hybrid identity solutions guidance*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/alerts/2024/03/12/cisa-publishes-scuba-hybrid-identity-solutions-guidance

CISA. (2024b). *Space systems security and resilience landscape: Zero Trust in the space environment.* Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/sites/default/files/2024-06/Space%20Systems%20Security%20and%20Resilience%20Landscape%20-%20Zero%20Trust%20in%20the%20Space%20Environment%20%28508%29.pdf

Cisco. (2024). *Zero Trust network access (ZTNA) demystified* [White paper]. Cisco Systems. https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2024/pdf/BRKSEC-2079.pdf

Cloudflare. (2022). *Top 10 productivity improvements: The business impact of Zero Trust* [White paper]. Cloudflare. https://www.cloudflare.com/static/5116783b5c6dabad22889d5f014f0da5/Zero_Trust_Business_Impact_-_Top_10_Productivity_Improvements__rev__2022_Q4_.pdf

Cloud Security Alliance. (2023). *Advancing Zero Trust maturity throughout the device pillar.* CSA. https://cloudsecurityalliance.org/resources/advancing-zero-trust-maturity-throughout-the-device-pillar

CyberEdge (for Palo Alto). (2021). *A step toward Zero Trust for the cloud* [White paper]. CyberEdge Group. https://cyberedgegroup.com/wp-content/uploads/2021/02/PaloAltogBookZeroTrust.pdf

Cybersecurity and Infrastructure Security Agency. (2021). *Trusted Internet connections (TIC) 3.0: Security capabilities catalog.* CISA. https://www.cisa.gov/sites/default/files/publications/CISA%20TIC%203.0%20Security%20Capabilities%20Catalog%20v2.0_0.pdf

Dakić, V., Morić, Z., Kapulica, A., & Regvart, D. (2025). Analysis of Azure Zero Trust architecture implementation for mid-size organizations. *Journal of Cybersecurity and Privacy, 5*(1), 2. https://doi.org/10.3390/jcp5010002

Doherty, D. H., & McKenney, B. (2021). *Zero Trust architectures: Are we there yet?* MITRE. https://www.mitre.org/news-insights/publication/zero-trust-architectures-are-we-there-yet

ENISA. (2021). *ENISA threat landscape 2021.* European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Ericom Software. (2023). *What's the Zero Trust-SASE connection?* Ericom. https://www.ericom.com/whats-the-zero-trust-sase-connection/

Federal Trade Commission, Office of Inspector General. (2023). *Audit of the FTC progress on the implementation of Zero Trust architecture* (redacted). FTC. https://oig.ftc.gov/reports/audit/audit-ftc-progress-implementation-zero-trust-architecture-redacted

Google Cloud. (2021). *Secure access to SaaS applications with BeyondCorp Enterprise* [White paper]. Google Cloud. https://services.google.com/fh/files/misc/secure_access_to_saas_apps_with_bce.pdf

Grasset, J.-Y., Jumelet, A., Ndouga, F., Roques, M., Aubert, G., Simon, B., Bordier, G., Giblain, I.,

Gardette, M., Lacour, E., Guégan, J.-M., Flichy, M., Curel, R., & O'Hara, L. (2021). *How to initiate your Zero Trust transformation project?* Capgemini.

Hernandez, S. (2024). *Federal Zero Trust data security guide*. CISO Council & CDO Council. https://www.cio.gov/federal-zero-trust-data-security-guide/

Homeland Security. (2025). *Zero Trust architecture implementation: Fiscal year 2024 report to Congress*. U.S. Department of Homeland Security. https://www.dhs.gov/sites/default/files/2025-04/2025_0129_cisa_zero_trust_architecture_implementation.pdf

ISMS Online. (2020). *ISO 27002: The code of practice for information security controls. ISMS Online*. https://www.isms.online/iso-27002/

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 information security management systems*. ISO. https://www.iso.org/standard/27001

Mavroudis, V. (2024). *Zero Trust network access* (ZTNA). arXiv preprint. https://arxiv.org/abs/2410.20611

Microsoft. (2021). *Evolving Zero Trust: How real-world deployments and attacks are shaping the future of Zero Trust strategies*. Microsoft. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Evolving-Zero-Trust-Microsoft-Position-Paper.pdf

Microsoft. (2024). *Zero Trust security*. Microsoft. https://www.microsoft.com/en-us/security/business/zero-trust

Microsoft. (2025). *Microsoft Secure Future Initiative: Bringing Zero Trust to life*. Microsoft. https://www.microsoft.com/en-us/security/blog/2025/05/15/how-the-microsoft-secure-future-initiative-brings-zero-trust-to-life/

National Cyber Security Centre. (2021). *Zero Trust architecture design principles*. NCSC (UK). https://www.ncsc.gov.uk/collection/zero-trust-architecture

Netskope. (2024). *5 key considerations for selecting a Zero Trust network access solution*. Netskope. https://www.netskope.com/resources/ebooks/5-key-considerations-for-selecting-a-zero-trust-network-access-solution

NIST. (2020). *Security and privacy controls for information systems and organizations* (NIST SP 800-53 Rev. 5). National Institute of Standards and Technology. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

NIST. (2021). *Executive Order 14028: Improving the nation's cybersecurity*. National Institute of Standards and Technology. https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity

NIST. (2023). *Implementing a Zero Trust architecture* (Vol. E, Risk and compliance management) (NIST SP 1800-35 Draft). National Institute of Standards and Technology. https://csrc.nist.gov/pubs/sp/1800/35/2prd-(1)

NIST. (2024a). *Implementing a Zero Trust architecture (NIST SP 1800-35 Initial Public Draft)*. National Institute of Standards and Technology. https://csrc.nist.gov/pubs/sp/1800/35/ipd

NIST. (2024b). *Implementing a Zero Trust architecture. National Cybersecurity Center of Excellence*. https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture

NSA. (2021). *NSA issues guidance on Zero Trust security model*. National Security Agency. https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2515176/nsa-issues-guidance-on-zero-trust-security-model/

NSA. (2024a). *NSA releases guidance on Zero Trust maturity throughout the application and workload pillar*. National Security Agency. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3784301/nsa-releases-guidance-on-zero-trust-maturity-throughout-the-application-and-wor/

NSA. (2024b). *NSA releases maturity guidance for the Zero Trust network and environment pillar*. National Security Agency. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3695223/nsa-releases-maturity-guidance-for-the-zero-trust-network-and-environment-pillar/

Office of the U.S. Government Accountability. (2024). *Cybersecurity: Implementation of executive order requirements is essential to address key actions. U.S*. GAO. https://www.gao.gov/products/gao-24-106343

Okta. (2023). *State of Zero Trust* [Report]. Okta. https://www.okta.com/reports/state-of-zero-trust/

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust architecture* (NIST SP 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-207

Ross, R. (2024). *Enhanced security requirements for protecting controlled unclassified information* (NIST SP 800-172 Rev. 3). National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-172r3.ipd

Sabetto, R. (2022). *MITRE cloud strategy*. MITRE. https://www.mitre.org/news-insights/publication/mitre-cloud-strategy

Sood, N., Parlapalli, R., Sharma, P., & Kashyap, R. (2024). Application of Zero Trust model in preventing medical errors. *Frontiers in Health Services, 4*. https://doi.org/10.3389/frhs.2024.1453804

SSH Communications Security. (2021). *A finance and stock trading company passing audits with Zero Trust PAM* [Case study]. SSH. https://www.ssh.com/hubfs/2021%20Case%20studies/ssh_case_study_a_finance_stock_trading_company_passing_audits_with_zero_trust_PAM.pdf

ManageEngine. (2022). *How to mitigate insider threats by integrating UEBA with Zero Trust*. ManageEngine. https://www.manageengine.com/log-management/ebooks/integrating-ueba-with-zero-trust-to-secure-business.html

U.S. Department of Homeland Security. (2023). *CISA Zero Trust maturity model v2*. Cloud Security Alliance. https://cloudsecurityalliance.org/resources/cisa-zero-trust-maturity-model-v2

Washington, D., & Sharek, R. (2023). *Readiness review on Zero Trust implementation* [Redacted report]. U.S. Securities and Exchange Commission. https://www.sec.gov/files/fnl-mgmt-ltr-readiness-rvw-secs-prog-twd-implmntng-zero-trust-cyber-prncpls.pdf

Yeoh, W., Liu, M., Shore, M., & Jiang, F. (2023). Zero Trust cybersecurity: Critical success factors and a maturity assessment framework. *Computers & Security, 133,* 103412. https://doi.org/10.1016/j.cose.2023.103412

Young, S. (2022). *Memorandum for the heads of executive departments and agencies* (M-22-09). The White House. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

ZT PfMO. (2022). *Department of Defense Zero Trust strategy and reference architecture v2.0* [Pre-decisional draft]. U.S. Department of Defense. https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf