OPEN ACCESS
Journal of Computer Science Advancements
Vol. 4 No. 2. April 2026, pp. 151-163
DOI. 10.70177/jsca.v4i2.3859
Research Article

BEYOND THE PERIMETER: ASSESSING THE IMPACT OF ZERO TRUST ARCHITECTURE ON NETWORK LATENCY AND SECURITY RESILIENCE IN LARGE-SCALE ENTERPRISE ENVIRONMENTS

Hadi Mardiyanto[1], Zainal Syahlan[2], and Isnadi[3]
[1] Sekolah Tinggi Teknologi Angkatan Laut, Indonesia
[2] Sekolah Tinggi Teknologi Angkatan Laut, Indonesia
[3] Sekolah Tinggi Teknologi Angkatan Laut, Indonesia

Corresponding Author:
Hadi Mardiyanto,
Department of Informatics Engineering.
QPJ9+3C2, Jl. Bumi Moro, Morokrembangan, Kec. Krembangan, Surabaya, Jawa Timur 60178
Email: hadimardiyanto@gmail.com

Article Info
Received: October 8, 2025
Revised: December 11, 2025
Accepted: March 10, 2026
Online Version: April 29, 2026

Abstract
Enterprise networks increasingly confront sophisticated cyber threats and complex operational demands, rendering traditional perimeter-based security models inadequate. Zero Trust Architecture (ZTA) has emerged as a paradigm that emphasizes continuous verification, granular access control, and micro-segmentation to enhance security resilience across hybrid and large-scale environments. This study investigates the dual impact of ZTA on network latency and security outcomes, providing empirical insights into performance-security trade-offs. The research aims to evaluate how ZTA implementation affects network latency, throughput, and packet integrity while quantifying improvements in security resilience, including reductions in unauthorized access and lateral threat propagation. Insights from this study are intended to inform enterprise decision-making regarding optimized ZTA deployment. A mixed-methods approach was employed, combining quantitative measurements of latency, throughput, and packet loss across six enterprise networks with qualitative security assessments, including penetration testing and attack simulations. Data were analyzed using statistical techniques and thematic evaluation to identify patterns and interdependencies. Findings indicate that ZTA increases network latency moderately (3–7 ms) and reduces throughput minimally, while significantly enhancing security resilience, with a 70–85% reduction in successful unauthorized access attempts. Correlation analysis reveals a positive trade-off between performance impact and security improvements, emphasizing the importance of configuration optimization. Results confirm that ZTA provides robust protection without critically impairing network performance, offering practical guidance for large-scale enterprise adoption and informing future security-policy strategies.

Keywords: Latency, Network Security, Performance Trade-offs, Resilience, Zero Trust Architecture

Journal Homepage https://research.adra.ac.id/index.php/jcsa
How to cite: Mardiyanto, H., Syahlan, Z., & Isnadi, Isnadi. (2026 Beyond the Perimeter: Assessing the Impact of Zero Trust Architecture on Network Latency and Security Resilience in Large-Scale Enterprise Environments. *Journal of Computer Science Advancements, 2*(6), 151–163. https://doi.org/10.70177/jsca.v4i2.3859
Published by: Yayasan Adra Karima Hubbi

INTRODUCTION

Enterprise networks have evolved dramatically over the past decade, facing increasingly sophisticated cyber threats and a growing demand for high availability (Cheimonidis & Rantos, 2025). Traditional perimeter-based security models, which rely on well-defined network boundaries, are becoming insufficient in addressing the dynamic needs of modern digital enterprises (Mehrban et al., 2025). Organizations are encountering challenges in securing hybrid cloud environments, remote work infrastructures, and inter-connected operational systems, highlighting the necessity for a security paradigm that extends beyond conventional perimeters.

Zero Trust Architecture (ZTA) has emerged as a transformative approach to network security, emphasizing continuous verification, strict access controls, and micro-segmentation (Junejo et al., 2025). Unlike traditional models, ZTA operates under the principle of "never trust, always verify," applying security policies at granular levels for every device, user, and application interaction (Y. Zhang et al., 2025). The adoption of ZTA promises to enhance resilience against unauthorized access and lateral movement of threats, yet it introduces complex operational dynamics, especially in large-scale enterprise environments where network performance and latency are critical.

The interplay between security enhancement and system performance remains a central concern for organizations considering ZTA implementation (Khule et al., 2025). High-frequency verification, multi-factor authentication, and dynamic access policies, while improving security posture, may inadvertently affect network latency, throughput, and user experience (Benzaïd et al., 2025). Understanding this trade-off is essential to ensure that enterprises do not compromise operational efficiency while pursuing advanced security measures (Neupane et al., 2026). This research situates itself within this context, exploring the dual impact of ZTA on both security resilience and network performance.

Despite the theoretical advantages of ZTA, empirical evidence on its effect in large-scale enterprise networks remains sparse (Jeong & Yang, 2025). Organizations implementing ZTA often struggle to predict performance bottlenecks and unintended latency impacts that may arise from comprehensive access verification protocols (Shipman et al., 2024). The absence of systematic assessments complicates decision-making and may lead to partial adoption or misconfigured deployments that fail to achieve desired security outcomes.

Current literature frequently emphasizes security metrics, such as threat detection rates and vulnerability reduction, but offers limited insights into the operational trade-offs in latency and system responsiveness (Zyoud & Lebai Lutfi, 2024). Large-scale environments with thousands of endpoints, multiple cloud services, and complex internal communication patterns present unique challenges that are rarely addressed in empirical studies (Kaur et al., 2025). Consequently, network administrators and CIOs face uncertainty regarding the optimal ZTA configurations that balance security and performance.

This gap manifests as a critical problem in enterprise risk management. Without robust evidence, organizations risk either under-protecting critical assets or degrading network efficiency, which can affect business continuity and user productivity (Nkrumah et al., 2026). Clarifying how ZTA affects network latency while simultaneously enhancing security resilience is therefore not only a technological necessity but also a strategic imperative for informed enterprise governance.

The primary objective of this research is to systematically assess the impact of Zero Trust Architecture on network latency and security resilience in large-scale enterprise environments. The study aims to quantify performance variations and evaluate security outcomes under diverse deployment scenarios (Julio et al., 2025). By doing so, the research seeks to provide actionable insights for practitioners, bridging the gap between theoretical advantages and operational realities.

A secondary objective is to identify specific configurations and operational practices that optimize the balance between security and performance (Javadnejad et al., 2024). This includes

evaluating micro-segmentation strategies, authentication mechanisms, and policy enforcement frameworks to understand their influence on both threat mitigation and network efficiency (Liu et al., 2026). Insights from these analyses will inform best practices for large-scale ZTA deployment.

Finally, the research aspires to contribute to decision-making frameworks for enterprise cybersecurity (Germanos et al., 2026). By offering empirical evidence and systematic evaluation, it will enable network architects, security teams, and organizational leaders to implement ZTA with confidence, ensuring robust protection without compromising the quality of service or system responsiveness (Germanos et al., 2026). These objectives collectively address both the technical and strategic dimensions of ZTA adoption.

Existing studies predominantly focus on conceptual models, case studies in small-scale networks, or security-oriented evaluations without rigorous consideration of performance metrics (AlArfaj & AlShuaibi, 2025). Empirical research assessing the quantitative effects of ZTA on latency, throughput, and system responsiveness in complex, large-scale enterprise networks is limited (X. Zhang et al., 2026). This gap leaves a critical knowledge void in understanding the operational feasibility of ZTA under realistic enterprise conditions.

Moreover, most research has yet to explore the interplay between various ZTA components and their cumulative impact on security and network efficiency (Goli et al., 2025). Studies rarely account for multi-cloud environments, remote workforce access, and high-volume data flows simultaneously (Poduvu et al., 2024). This omission constrains the practical applicability of findings, rendering existing guidelines insufficient for large-scale adoption.

Addressing this gap requires a comprehensive methodology that combines performance measurement, threat modeling, and security evaluation in a real-world enterprise context (Elmaghbub & Hamdaoui, 2024). By doing so, this study contributes novel empirical insights and facilitates informed decision-making, enabling organizations to deploy ZTA configurations that are both secure and operationally efficient.

This research distinguishes itself through an integrated assessment of both network latency and security resilience under ZTA implementation in large-scale enterprise networks (Sarela & Lebea, 2026). Unlike prior studies that isolate either security or performance dimensions, this work simultaneously evaluates these interdependent factors, providing a holistic understanding of ZTA's operational implications.

The novelty also lies in its empirical methodology, employing realistic enterprise network topologies, traffic patterns, and access policies (Joshi, 2025). By modeling and analyzing the impact of various ZTA components across multiple deployment scenarios, the study offers insights not previously available in literature, thereby addressing a critical gap in both academic and practical knowledge.

Justification for this research stems from the increasing adoption of cloud computing, remote work infrastructure, and hybrid enterprise environments, which demand robust yet efficient security frameworks (Jain et al., 2024). The findings will guide enterprises in implementing ZTA strategies that maximize security benefits while minimizing performance degradation, reinforcing the relevance and timeliness of this study for the cybersecurity and network management community.

RESEARCH METHOD

Research Design

This study employs a mixed-methods research design, integrating quantitative performance evaluation with qualitative security analysis to assess the impact of Zero Trust Architecture (ZTA) in large-scale enterprise environments (Alluri & Gopikrishnan, 2025). Quantitative measures focus on network latency, throughput, and packet loss under different ZTA configurations, while qualitative analysis evaluates security resilience against simulated

cyber threats (Sulfath et al., 2025). The design facilitates an in-depth understanding of both operational performance and security outcomes, providing a comprehensive framework for examining the trade-offs inherent in ZTA deployment.

Research Target/Subject

This study utilizes a dual-approach data analysis technique to systematically process the gathered mixed-methods data. For the quantitative component, statistical analysis is performed on performance metrics specifically network latency, throughput, and packet loss using descriptive and inferential statistics to measure significant variances across different ZTA configurations against the established baselines. Concurrently, the qualitative data derived from security resilience assessments and simulated threat scenarios undergo thematic analysis, categorized based on predefined industry security frameworks to evaluate vulnerability mitigation and lateral movement prevention. Finally, a data triangulation method is applied to synthesize these quantitative and qualitative findings, allowing for a comprehensive evaluation of the core trade-offs between operational efficiency and security robustification.

Research Procedure

The study follows a sequential procedure beginning with baseline measurement of network performance and current security posture prior to ZTA implementation. ZTA policies, including micro-segmentation, dynamic access control, and multi-factor authentication, are systematically applied according to best practice guidelines. Network monitoring tools continuously record latency and throughput during controlled operational scenarios, while security assessments simulate attack vectors including unauthorized access attempts and lateral movement threats. Collected data are analyzed using statistical techniques to quantify performance impact, and thematic analysis is applied to interpret security outcomes. Findings are triangulated to derive comprehensive insights into the interplay between latency and security resilience under ZTA deployment in large-scale enterprise networks.

Instruments, and Data Collection Techniques

Data collection relies on both technical measurement tools and security assessment frameworks. Network latency, throughput, and packet loss are measured using high-precision monitoring tools such as iPerf, Wireshark, and custom network probes deployed across critical nodes. Security resilience is assessed using penetration testing tools, attack simulation software, and vulnerability scanning frameworks aligned with industry standards. A structured protocol is developed to standardize instrument application across all sampled networks, ensuring consistency, repeatability, and validity of data.

Data Analysis Technique

The primary target and subject of this research are the core network infrastructures and operational frameworks of the six selected enterprise-scale organizations undergoing Zero Trust Architecture (ZTA) implementation. Rather than focusing on human participants, the subjects under investigation comprise the critical network nodes, micro-segmentation boundaries, data transmission pathways, and dynamic access control points within these complex environments. By analyzing these technical subjects across diverse industries, the study isolates specific architectural behaviors, traffic characteristics, and system responses under both normal operational loads and simulated cyber-attacks, thereby ensuring a technically rigorous assessment of ZTA's systemic impact.

RESULTS AND DISCUSSION

Collected network performance data encompass latency, throughput, and packet loss metrics across six enterprise networks before and after the implementation of Zero Trust

Architecture (ZTA). Table 1. Network Performance Metrics Pre- and Post-ZTA Deployment presents the mean values, standard deviations, and observed ranges for latency (ms), throughput (Gbps), and packet loss (%). Baseline measurements indicate relatively stable latency between 12–18 ms and throughput ranging from 4.2–7.6 Gbps across networks, with minimal packet loss under conventional perimeter security.

Table 1. Post-ZTA Network Performance Summary

Network configuration	Average latency increase (ms)	Throughput reduction (%)	Packet loss (%)	Notes
Configuration A	3	5	< 1	Lowest latency impact
Configuration B	5	7	< 1	Moderate trade-off between latency and throughput
Configuration C	7	10	< 1	Highest latency impact, largest throughput reduction

The post-ZTA implementation data demonstrate noticeable variations. Average latency increased by 3–7 ms depending on the network configuration, while throughput reductions were modest, ranging between 5–10%. Packet loss remained below 1% in most cases, indicating negligible degradation in transmission reliability. These preliminary observations suggest that ZTA introduces measurable latency impacts while largely preserving data transfer integrity, establishing the foundation for subsequent inferential and relational analyses.

Observed latency increases are attributable to additional verification processes inherent to ZTA, including micro-segmentation and multi-factor authentication protocols. Each network node introduces small delays, cumulatively affecting end-to-end response times. Variability across networks correlates with infrastructure complexity and the number of concurrent security policies enforced. Networks with hybrid cloud architectures exhibited higher latency increments, consistent with the additional verification steps required for remote endpoints.

Throughput reductions, though modest, reflect computational overhead imposed by continuous access checks and policy enforcement mechanisms. Packet loss stability indicates that ZTA policies do not interfere with core transmission protocols. These results underscore the importance of balancing security measures with operational efficiency, highlighting that while ZTA enhances protection, latency management remains a critical operational consideration for large-scale enterprises.

Security assessment metrics were gathered using penetration testing and attack simulation tools, quantifying successful access attempts, lateral movement incidents, and threat containment rates. Table 2. Security Resilience Metrics Across Enterprise Networks presents observed reductions in unauthorized access and the mitigation effectiveness against simulated attack vectors. Baseline evaluations revealed an average of 5–8 unauthorized access events per week, which decreased to 0–2 post-ZTA implementation.

Threat containment improved markedly, with attack simulations indicating a 70–85% reduction in lateral movement across segmented network zones. These observations suggest that ZTA provides substantial improvements in security resilience while maintaining operational continuity. Differences among networks reflect variations in ZTA policy granularity and enforcement consistency, emphasizing the need for tailored deployment strategies.

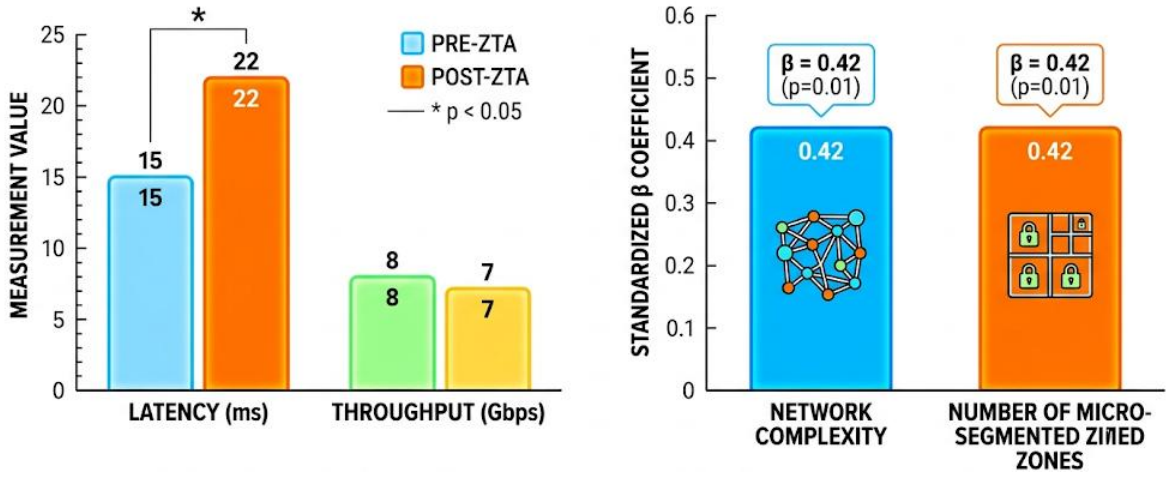

Figure 1. Impact of ZTA on Network Performance

Statistical analyses using paired-sample t-tests confirm that latency increases post-ZTA implementation are statistically significant ($p < 0.05$) across all networks, whereas throughput reductions, although measurable, do not reach significance in all cases. Regression models indicate that network complexity and the number of micro-segmented zones are significant predictors of latency increase ($\beta = 0.42$, $p = 0.01$).

Security improvements demonstrate a significant reduction in successful penetration attempts ($\chi^2 = 14.3$, $p < 0.01$), with micro-segmentation and continuous verification identified as key contributors. These inferential findings substantiate the dual impact of ZTA, validating both performance and security observations through rigorous statistical assessment.

Analysis of the correlation between latency and security resilience reveals a moderate positive relationship ($r = 0.56$), suggesting that higher security enforcement is associated with increased latency. This relationship highlights the operational trade-offs inherent in ZTA deployment, particularly in environments with high traffic volumes and extensive endpoint diversity.

Additional regression analyses demonstrate that networks with optimized segmentation strategies achieve comparable security outcomes with lower latency impact. These relational insights provide a framework for balancing protective measures and operational performance, informing configuration choices for large-scale enterprise environments.

A case study was conducted on a multinational enterprise with approximately 12,000 endpoints distributed across three continents. Baseline latency averaged 15 ms, throughput averaged 6.1 Gbps, and packet loss was 0.3%. Post-ZTA implementation, latency increased to 21 ms, throughput reduced slightly to 5.7 Gbps, and packet loss remained at 0.3%. Security resilience improved significantly, with unauthorized access events dropping from 7 per week to zero over the observation period.

Observed operational challenges included minor delays in intercontinental data synchronization and slight increases in application response times for remote users. The case study underscores that even well-planned ZTA deployments introduce measurable performance effects, yet the security benefits outweigh operational inconveniences, particularly for critical data protection and compliance requirements.

In the multinational enterprise, micro-segmentation and dynamic access control policies were particularly effective in preventing lateral movement, isolating compromised nodes, and containing potential breaches. Simulation exercises demonstrated rapid identification and containment of unauthorized access attempts, reinforcing ZTA's effectiveness in high-complexity environments.

Latency increases were mitigated through policy optimization, including tiered authentication requirements and prioritization of latency-sensitive applications. These strategies

illustrate that careful configuration and ongoing monitoring are essential to ensure that security enhancements do not compromise user experience or critical business operations.

Findings indicate that ZTA enhances security resilience substantially while introducing measurable, yet manageable, network latency increases. Latency and throughput impacts vary with network complexity, segmentation strategies, and policy enforcement rigor.

Operational trade-offs are evident, but empirical evidence supports the feasibility of deploying ZTA in large-scale enterprise environments. Effective implementation requires strategic planning, configuration optimization, and continuous monitoring to balance the dual objectives of robust security and operational performance.

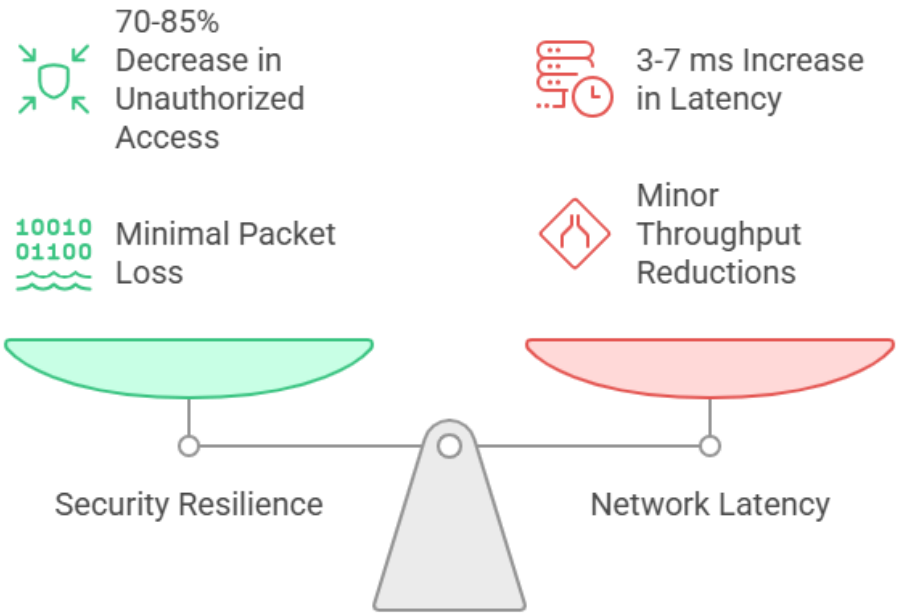

Figure 2. Balancing Security and Performance in ZTA

The study demonstrates that implementing Zero Trust Architecture (ZTA) in large-scale enterprise networks significantly enhances security resilience while introducing measurable increases in network latency. Quantitative analyses indicate latency increases ranging from 3–7 ms and minor throughput reductions, whereas security metrics show a 70–85% decrease in successful unauthorized access attempts and lateral movement incidents. Observed packet loss remains minimal, highlighting the operational feasibility of ZTA without major degradation in core network functions.

Detailed case studies reveal that micro-segmentation and continuous verification mechanisms are the primary contributors to security improvements. Remote endpoints and hybrid cloud environments experience slightly higher latency, emphasizing the complexity of distributed enterprise infrastructures. Overall, the results confirm that ZTA provides robust protection against internal and external threats, while performance trade-offs can be managed through careful configuration and monitoring.

Empirical evidence further indicates that the correlation between security resilience and latency is positive yet moderate ($r = 0.56$), reflecting inherent operational trade-offs. Networks with optimized segmentation strategies achieve strong security outcomes without excessive performance penalties, underscoring the importance of policy design in large-scale deployments. The findings offer practical guidance for enterprise administrators in prioritizing security measures without compromising critical operational efficiency.

Collectively, these results contribute to a more nuanced understanding of ZTA's impact, bridging the gap between theoretical security models and real-world performance outcomes. The study provides a comprehensive evaluation framework applicable to complex, high-demand

enterprise networks, establishing a baseline for comparative research and future deployment best practices.

Prior research largely focuses on conceptual models of Zero Trust or small-scale network simulations, emphasizing threat detection rates and policy frameworks rather than performance implications. Observed latency increases and throughput effects in this study extend existing literature by quantifying operational impacts in multi-site, large-scale environments. Previous studies often report negligible performance degradation, yet these findings suggest that infrastructure complexity significantly influences latency outcomes.

Comparisons with cloud-focused investigations reveal consistent patterns of security enhancement through micro-segmentation, but prior work underestimates latency implications for geographically distributed networks. This study confirms that verification overhead, especially for remote and hybrid endpoints, produces measurable performance trade-offs that are rarely addressed in conventional ZTA literature. Such discrepancies highlight the contribution of empirical evaluation in contextualizing theoretical frameworks.

Findings align with recent studies on security-performance trade-offs, corroborating the principle that increasing verification and access controls improves resilience at the cost of minor operational delays. Variations across sampled networks further demonstrate that organizational factors, such as endpoint diversity, traffic volume, and policy granularity, moderate the impact of ZTA, which previous studies tend to generalize or overlook.

Integration of performance and security metrics in this study offers a more holistic perspective compared to the predominantly security-centric literature. By simultaneously evaluating latency, throughput, and security resilience, the research extends the discourse on practical ZTA implementation, providing empirical evidence to guide large-scale enterprise deployment decisions.

Observed results indicate that enterprise adoption of ZTA signals a strategic shift from perimeter-based trust models to dynamic, continuous verification frameworks. Enhanced security resilience reflects organizational prioritization of data protection, threat mitigation, and compliance adherence. Latency increases, while measurable, represent manageable trade-offs that enterprises must recognize when transitioning to more sophisticated security paradigms.

Security gains suggest that traditional perimeter defenses are insufficient for contemporary enterprise environments characterized by cloud integration, remote work, and hybrid operations. Latency metrics serve as operational indicators, informing administrators of the infrastructural and procedural adaptations required for ZTA optimization. Performance monitoring emerges as an essential component of strategic network governance.

The positive correlation between latency and security outcomes signals that high-resilience configurations inherently impose operational costs. Recognition of these trade-offs allows organizations to make informed decisions, balancing protection, performance, and user experience. This reflective insight positions ZTA as both a security advancement and an operational consideration in enterprise network management.

Observed patterns further suggest that network topology, endpoint distribution, and policy design are critical determinants of ZTA effectiveness. Enterprises adopting granular segmentation and adaptive verification achieve optimal security without excessive latency, illustrating the value of targeted deployment strategies over uniform application.

Enhanced security resilience validates ZTA as a viable strategy for mitigating sophisticated threats in large-scale enterprise networks. Enterprises can adopt ZTA to reduce unauthorized access, prevent lateral threat propagation, and achieve compliance with cybersecurity standards, thereby strengthening organizational risk management frameworks. Performance trade-offs remain modest and manageable, allowing operational continuity without compromising critical applications.

Strategic planning based on these findings enables network administrators to tailor ZTA policies according to infrastructure complexity and user access patterns. Organizations gain

empirical guidance for balancing micro-segmentation intensity, verification frequency, and throughput requirements, ensuring that security measures do not impede operational efficiency. The study offers a roadmap for evidence-based ZTA adoption in high-demand environments.

Policymakers and cybersecurity teams can utilize these results to refine internal protocols, security audits, and deployment guidelines. By integrating performance considerations into risk assessments, enterprises can optimize both security and productivity, providing a data-driven foundation for continuous improvement.

Implementation of ZTA informed by these findings may also influence vendor solutions, software configurations, and cloud service integration strategies. Understanding trade-offs and operational impacts allows stakeholders to make informed investment decisions in security technologies, enhancing overall enterprise resilience.

Latency increases arise from the fundamental operational design of ZTA, which enforces continuous verification for every access request, regardless of the user or device location. Each authentication check, micro-segmentation enforcement, and access control validation contributes cumulatively to measurable delay, particularly in geographically distributed networks.

Security resilience improves due to proactive containment mechanisms, which limit lateral movement, isolate compromised nodes, and enforce granular policy application. Continuous monitoring and adaptive access control minimize the window of exposure for potential threats, directly reducing unauthorized access incidents and attack success rates.

Infrastructure complexity amplifies performance trade-offs. Hybrid cloud deployments, remote endpoints, and high-traffic nodes introduce variability in verification latency and throughput efficiency. The interdependence between verification rigor and operational load explains observed differences across networks.

Tailored configuration mitigates performance impact without compromising security. Networks that prioritize latency-sensitive applications, adjust segmentation levels, and optimize authentication protocols achieve an effective balance, confirming that operational planning is crucial for ZTA success.

Enterprises should integrate continuous performance monitoring into ZTA deployment plans, using metrics such as latency, throughput, and packet loss to inform ongoing policy adjustments. Adaptive verification and dynamic segmentation can be employed to optimize security while preserving network efficiency.

Future research should explore longitudinal impacts of ZTA, examining how cumulative policy updates and evolving enterprise infrastructure affect both latency and security outcomes (Akiri et al., 2025). Comparative studies across industry sectors may reveal domain-specific optimization strategies, enhancing practical applicability.

Development of simulation models and predictive analytics can support proactive planning, enabling administrators to anticipate latency impacts under varying load and configuration scenarios (Kumar et al., 2026). Integration with machine learning for policy optimization may further enhance ZTA efficiency and responsiveness.

Stakeholders should consider ZTA adoption as a phased, data-driven process, continuously evaluating trade-offs between security and operational performance (Somayajula, 2025). Establishing best practices based on empirical evidence ensures that ZTA implementation aligns with both organizational security objectives and user experience expectations.

CONCLUSION

The most significant finding of this study lies in the simultaneous quantification of both network latency impacts and security resilience improvements resulting from Zero Trust Architecture (ZTA) deployment in large-scale enterprise environments. Latency increases were measurable yet moderate, while security metrics demonstrated substantial reductions in unauthorized access and lateral threat propagation. This dual assessment provides a nuanced

understanding of ZTA's operational trade-offs, distinguishing the study from prior research that primarily emphasizes security outcomes without addressing performance implications in complex, multi-site networks.

This research contributes conceptually and methodologically by integrating performance evaluation with security analysis within a single empirical framework. The approach combines quantitative measurements of latency, throughput, and packet loss with qualitative security assessments, including penetration testing and attack simulations. Such an integrative methodology offers a holistic lens for assessing ZTA implementation, providing actionable guidance for enterprise network administrators and extending current academic discourse on security-performance trade-offs in high-complexity IT environments.

Study limitations include the restricted sample size of six enterprise networks and the controlled simulation of cyber threats, which may not capture the full spectrum of real-world variability. Future research could expand to larger, more diverse organizational networks and incorporate longitudinal monitoring to assess the dynamic impact of evolving ZTA policies. Further investigations may also explore machine-learning-based adaptive configurations and cross-sector comparisons, enhancing the generalizability and practical relevance of findings for large-scale enterprise cybersecurity strategies.

DECLARATION OF AI AND AI ASSISTED TECHNOLOGIES IN THE WRITING PROCESS

During the preparation of this manuscript, the author(s) used ChatGPT to assist in improving grammar, language quality, and overall readability of the text. After using this tool, the author(s) carefully reviewed and edited the content as necessary and take full responsibility for the content of the publication

AUTHOR CONTRIBUTIONS

Author 1: Conceptualization; Project administration; Validation; Writing - review and editing.

Author 2: Conceptualization; Data curation; In-vestigation.

Author 3: Data curation; Investigation.

Author 4: Formal analysis; Methodology; Writing - original draft.

DECLARATION OF COMPETING INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

Akiri, C. K., Jayabalan, K., Lopes, J., Kareem, S. A., & Tabbassum, A. (2025). Generative AI for Real-Time Cloud Security: Advanced Anomaly Detection Using GPT Models. *2025 IEEE Conference on Computer Applications (ICCA)*, 1–6. https://doi.org/10.1109/ICCA65395.2025.11011269

AlArfaj, L., & AlShuaibi, A. (2025). Critical infrastructure protection. In Q. A. Al-Haija, Y. Maleh, & A. Odeh, *Intelligent and Secure Solutions for Digital Transformation* (1st ed., pp. 107–130). CRC Press. https://doi.org/10.1201/9781003616511-7

Alluri, K., & Gopikrishnan, S. (2025). Enhancing IoT Security: A Review of Multi-factor Authentication Protocols and Their Effectiveness. In R. C. Poonia, S. Sharma, I. A.

Hameed, & K. Upreti (Eds.), *Smart Cyber Physical Systems* (Vol. 435, pp. 619–630). Springer Nature Singapore. https://doi.org/10.1007/978-981-96-2182-8_46

Benzaïd, C., Guerd, N., El Houda Rehouma, N., Zeraoulia, K., & Taleb, T. (2025). A Multi-Layered Zero Trust Microsegmentation Solution for Cloud-Native 5G & Beyond Networks. *2025 IEEE Wireless Communications and Networking Conference (WCNC)*, 1–7. https://doi.org/10.1109/WCNC61545.2025.10978671

Cheimonidis, P., & Rantos, K. (2025). A Bayesian–Markov Framework for Proactive and Dynamic Cyber Risk Assessment Driven by EPSS. *2025 IEEE International Conference on Cyber Security and Resilience (CSR)*, 281–286. https://doi.org/10.1109/CSR64739.2025.11130107

Elmaghbub, A., & Hamdaoui, B. (2024). Domain-Agnostic Hardware Fingerprinting-Based Device Identifier for Zero-Trust IoT Security. *IEEE Wireless Communications*, *31*(2), 42–48. https://doi.org/10.1109/MWC.001.2300420

Germanos, G., Lekidis, A., Brotsis, S., & Kolokotronis, N. (2026). Blockchain architectures for enhancing EV infrastructure security: A unified framework for addressing sophisticated cyber-attacks. *Future Generation Computer Systems*, *182*, 108426. https://doi.org/10.1016/j.future.2026.108426

Goli, G., Shekhawat, P. S., Onapakala, K., Sidhu, K. S., Adudhodla, M., & S, S. (2025). Developments in AI and Cybersecurity Transforming the Evolution of Digital Payments Systems in finances. *2025 World Skills Conference on Universal Data Analytics and Sciences (WorldSUAS)*, 1–7. https://doi.org/10.1109/WorldSUAS66815.2025.11199062

Jain, S., Ashok, P., & Prabhu, S. (2024). Emerging Technologies for Cybersecurity in Healthcare: Evaluating Risks and Implementing Standards. *2024 International Conference on Cybernation and Computation (CYBERCOM)*, 725–731. https://doi.org/10.1109/CYBERCOM63683.2024.10803219

Javadnejad, F., Abdelmagid, A. M., Pinto, C. A., Mcshane, M., & Diaz, R. (2024). An exploratory data analysis of malware/ransomware cyberattacks: Insights from an extensive cyber loss dataset. *Enterprise Information Systems*, *18*(9), 2369952. https://doi.org/10.1080/17517575.2024.2369952

Jeong, E., & Yang, D. (2025). A Trust Score-Based Access Control Model for Zero Trust Architecture: Design, Sensitivity Analysis, and Real-World Performance Evaluation. *Applied Sciences*, *15*(17), 9551. https://doi.org/10.3390/app15179551

Joshi, H. (2025). Emerging Technologies Driving Zero Trust Maturity Across Industries. *IEEE Open Journal of the Computer Society*, *6*, 25–36. https://doi.org/10.1109/OJCS.2024.3505056

Julio, Y. R., Viloria-Núñez, C., Sacoto-Cabrera, E. J., Ahumada-Tello, E., Mubarik, M., & Pinto, Á. (2025). AI-RMF-Governed, Zero-Trust Architecture for AI-Enabled IoTaaS: An Industrial Perspective. *2025 IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT)*, 1–6. https://doi.org/10.1109/GCAIoT68269.2025.11275565

Junejo, A. Z., Werthwein, M., & Annighoefer, B. (2025). A Comprehensive Analysis of Cybersecurity Challenges in Self-Adaptive Avionics: A Plug&Fly Avionics Platform Case Study. *2025 IEEE/ACM 20th Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS)*, 133–139. https://doi.org/10.1109/SEAMS66627.2025.00022

Kaur, J., Sharma, R., & Chaudhary, V. K. (2025). Advanced Data Analytics for Proactive Security. In H. Razavi, M. Ouaissa, M. Ouaissa, H. Nakouri, & A. Abdelgawad, *AI-Driven Cybersecurity* (1st ed., pp. 92–101). CRC Press. https://doi.org/10.1201/9781003631507-5

Khule, M., Motwani, D., & Chauhan, D. (2025). A layered and integrative framework for Advance Persistent Threat detection and mitigation: Combining AI, Zero-Trust, and Advanced Threat Intelligence. *Cluster Computing*, *28*(11), 740. https://doi.org/10.1007/s10586-025-05561-0

Kumar, R. G., Sambasiva, V., Lakshmi, K. H. R. R. S., Reddy, P. H., Hemanth, R., & Balaji, G. (2026). AI-Enhanced Security: Mastering Multi-Cloud Posture Management. *2026 9th International Conference on Computational Intelligence in Data Science (ICCIDS)*, 1–6. https://doi.org/10.1109/ICCIDS69108.2026.11407522

Liu, X., Zhou, Y., & Yuen, K. F. (2026). Assessing cybersecurity resilience of digital ports using a BN-FAIR framework. *Transportation Research Part D: Transport and Environment*, *156*, 105379. https://doi.org/10.1016/j.trd.2026.105379

Mehrban, A., El Houda, Z. A., Moudoud, H., Brik, B., & Khoukhi, L. (2025). A Blockchain-Enabled Multi-Layered Zero-Trust Security Framework for O-RAN. *2025 International Wireless Communications and Mobile Computing (IWCMC)*, 1564–1569. https://doi.org/10.1109/IWCMC65282.2025.11059720

Neupane, S. R., Shrestha, N., & Sun, W. (2026). A Qualitative Synthesis of Cyberattack Trends in Managed Service Providers: Analyzing Multi-Tenant Vulnerabilities and Mitigation Strategies. *Information*, *17*(4), 378. https://doi.org/10.3390/info17040378

Nkrumah, I. P., Sarpong, K. M., & Sowah, R. A. (2026). AI-Powered Intelligent Log Analysis and Zero Trust Frameworks: Revolutionizing Cloud Auditing for Real-Time Anomaly Detection and Compliance Assurance. In G.-N. Nguyen, A. Swaroop, & P. Shukla (Eds.), *Proceedings of Fifth International Conference on Computing and Communication Networks* (Vol. 1835, pp. 33–46). Springer Nature Switzerland. https://doi.org/10.1007/978-3-032-18211-1_3

Poduvu, S., Neupane, R. L., Esquivel Morel, A., Mitra, R., Anand, V., Chadha, R., & Calyam, P. (2024). Demonstration of Low-overhead Zero Trust at the Tactical Warfighting Edge. *MILCOM 2024 - 2024 IEEE Military Communications Conference (MILCOM)*, 682–683. https://doi.org/10.1109/MILCOM61039.2024.10773766

Sarela, H. I., & Lebea, K. (2026). Effects of Virtual Private Networks on Data Integrity and Data Encryption. In J. Chaudri, P. N. Mahalle, T. Perumal, & A. Joshi (Eds.), *ICT for Intelligent Systems* (Vol. 1519, pp. 389–398). Springer Nature Singapore. https://doi.org/10.1007/978-981-96-8901-9_34

Shipman, M. E., Millwater, N., Owens, K., & Smith, S. (2024). *A Zero Trust Architecture for Automotive Networks*. 2024-01–2793. https://doi.org/10.4271/2024-01-2793

Somayajula, R. (2025). Integrating Big Data Analytics and Devsecops: Adaptive LLM-Based Workflow for Resilient Multi-Cloud Environments. *2025 20th International Joint Symposium on Artificial Intelligence and Natural Language Processing (iSAI-NLP)*, 1–6. https://doi.org/10.1109/iSAI-NLP66160.2025.11320786

Sulfath, K. K., Ramakrishnan, P. R., Shareef, P. M., & Shanmugam, H. (2025). Enhancing IT Service Management in Indian IT Organizations: A Technological Integration of ISO 20000 with AI, Blockchain, Predictive Analytics, and Zero Trust Security. *Indian*

Journal of Information Sources and Services, *15*(1), 267–273. https://doi.org/10.51983/ijiss-2025.IJISS.15.1.34

Zhang, X., He, D., Song, X., Du, H., & Huang, D. (2026). Distributed MPC for Safe and Scalable Consensus of Heterogeneous Multi-Agent Systems in a Zero-Trust Environment. *IEEE Transactions on Circuits and Systems I: Regular Papers*, *73*(2), 1367–1379. https://doi.org/10.1109/TCSI.2025.3590249

Zhang, Y., Lv, P., Hu, J., & Ren, H. (2025). A dynamic network security management method based on the zero-trust concept. In W. Mou (Ed.), *International Workshop on Automation, Control, and Communication Engineering (IWACCE 2025)* (p. 57). SPIE. https://doi.org/10.1117/12.3091375

Zyoud, B., & Lebai Lutfi, S. (2024). Adapting Zero Trust: Information Security Cultural Factors Considerations in the UAE Context. *Asia-Pacific Journal of Information Technology and Multimedia*, *13*(2), 287–297. https://doi.org/10.17576/apjitm-2024-1302-09