INTERNATIONAL JOURNAL OF ADVANCED RESEARCH
ISSN: 3106-7980 : 3106-7972
Volume 3, Issue 3, 2026

ZERO TRUST SECURITY MODEL: AN ADVANCE APPROACH TO SECURING MODERN NETWORK INFRASTRUCTURE

Abdul Qayyum[*1], Khalid Hamid[2], Muhammad Waseem Iqbal[3], Malik Waqar Ali[4], Muhammad Awais Sajid[5]

[*1,4,5]*Department of Information Security, Superior University Lahore, 5400, Pakistan*
[2,3]*Department of Computer Science and IT, Superior University Lahore, 5400, Pakistan*

[*1]su92-msisw-s26-002@superior.edu.pk, [*1]abdulqayyumnns@gmail.com, [2]khalid6140@gmail.com, [3]waseem.iqbal@superior.edu.pk, [4]waqaralibcs076@gmail.com, [5]mawais.sajid001@gmail.com

DOI: https://doi.org/10.5281/zenodo.21738396

Keywords
Zero Trust Security, Network Infrastructure, Cybersecurity, Identity Management, Micro-Segmentation, Cloud Security

Article History
Received: 22 May 2026
Accepted: 09 July 2026
Published: 31 July 2026

Corresponding Author: *
Abdul Qayyum

Abstract

Introduction/Background: *The use of cloud computing, remote connections and distributed networks has rendered traditional cybersecurity models based on perimeter security obsolete. Traditional approaches, which assume trust in the network and traffic flows inside the network, are no longer sufficient to defend against modern hazards such as insider threats, credential theft and advanced persistent threats.*

Problem: *Perimeter-based security models cannot support the modern distributed network with the increased adoption of the cloud and remote work.*

Evidence: *Implicit trust is abused by almost all cyberattacks (ransomware, phishing, and insider threats) to breach security and propagate through the network.*

Method, tools, technology, model, formula: *The Zero Trust Security Model provides the most protection when implemented with continuous authentication, least privilege access, micro-segmentation, real-time monitoring and behavioral analysis, the cloud, and artificial intelligence.*

Outcomes/Conclusion: *Zero Trust will reinforce the cybersecurity posture of most modern organizations and support them with positive security against the threats in the current cyberspace. Zero Trust eliminates implicit trust and provides the most protection when integrated with continuous verification of access requests in all environments.*

1. Introduction

This paper discusses the Zero Trust Security Model as a novel approach to network security, including its fundamental principles, applicability and effectiveness in addressing the current challenges in network security.

Our network environment has changed with the advent of cloud computing, mobility and hybrid working. The rise of cloud computing, mobility and hybrid work arrangements has created a distributed network environment with user, device and application communications outside the network perimeter. This has exposed the shortcomings of traditional network security approaches, which consider elements within the network as trusted [1]. Against the growing cyber threats, these techniques are not sufficient in securing critical assets [2].

Cyber-attacks (ranging from ransomware, phishing, to insider attacks) take advantage of

implicit trust to circumvent network security and spread across the network [3]. The rise of cloud computing and hybrid work arrangements means that it's difficult to define the boundaries of an organisation's network, leading to ever-evolving challenges in protecting resources [4]. As a result, there is a need for a security that assumes breach and never trust.

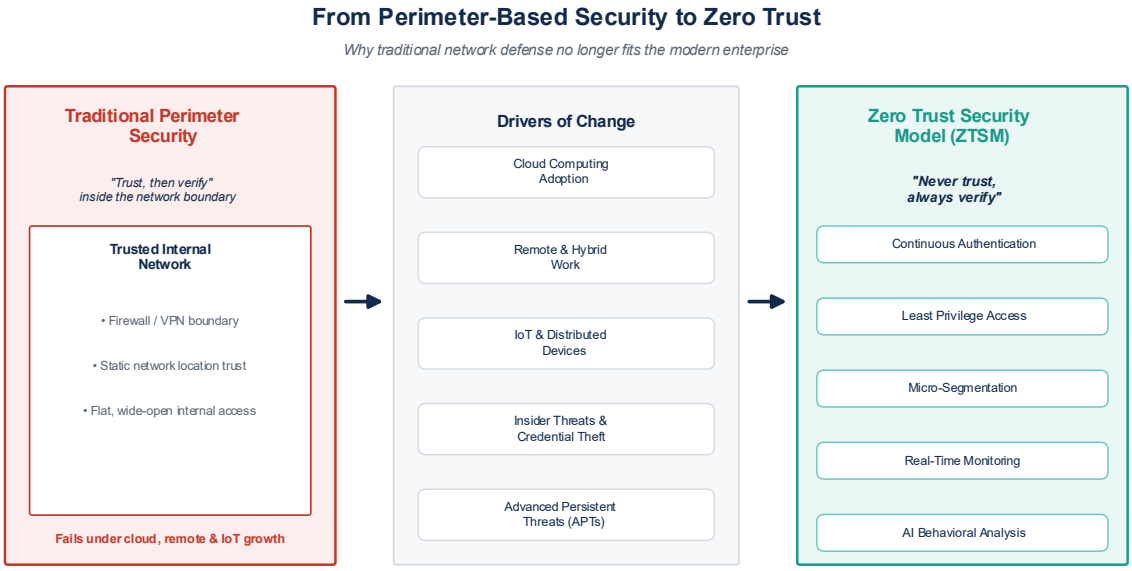

Figure 1: Shift from Perimeter-Based Security to the Zero Trust Security Model

Zero Trust Model of Security is a solution that offers a model of verification. It works on the principle of "never trust, always verify" and users, devices and applications require verification to gain access to network resources [5]. Zero Trust is not network-based, but a user-based, context-based and verified technique [6].

Zero Trust based on many rules including the least privilege access, constant monitoring and micro-segmentation. Least privilege access indicates users only have access to the resources they need for a given task, minimising the risk of abuse [7]. Micro-segmentation creates smaller segments of the network, limiting the ability for adversaries to be within the network [8]. The continuous monitoring and behaviour analysis also enhance security by detecting anomalies and enabling rapid response to threats [9].

Additionally, Zero Trust has benefited from the use of novel technologies such as artificial intelligence and machine learning. These technologies can enable real-time monitoring and analysis of user behaviour, anomaly detection, and enforcement of security policies [10]. As a result, Zero Trust has evolved into a comprehensive and dynamic security approach that can be used to tackle modern network challenges.

Although there are many advantages to Zero Trust, there are also challenges with its adoption including compatibility with legacy systems, design complexity and cultural change [11]. However, with a phased approach, this model can be embraced to improve security.

Motivation

This research is driven by the increased complexity and quantity of modern cyberattacks on enterprises. Perimeter-based security which assumes that anything inside the network can be trusted has been ineffective against persistent insider threats and even insider credential exploitation [12]. With the rise of remote working and the cloud and IoT fully integrated into the network, the boundary which once existed as part of the traditional enterprise network has disappeared. With no boundaries, organizations

are left exposed to a large and constantly changing threats [13].

Organizational structural changes have created the need to reassess the assumptions associated with network security. Another motivating reason for this research is the numerous instances of cyber criminals directly exploiting the implicit trust of lateral movement once network breaches have occurred. Research [14] shows that cybercriminals use trusted communications to move across different interconnected systems while remaining undetected by perimeter security. Breaches of security in this manner is the most severe for hybrid cloud systems wherein a network contains a cloud and inter-federated distributed systems across different geographic locations [15]. The problems above worsen the need for a security model that allows for perimeter-less systems while eliminating the trust of network locations [16].

Contribution

This research outlines many crucial contributions to modern network security theory. First, Patel and Shah (2022) present their sophisticated assessment of the theoretical fundamentals and real-world applicability of the Zero Trust Security Model (ZTSM). Patel and Shah's work goes beyond their competitors' and addresses both the "never trust, always verify" principle and the "least privilege" access and "micro-segmentation" concepts and their applicability to today's network environments within the framework of ZTSM. In contrast to other literature, this work explains, beyond theory, how the ZTSM principles work in tandem to restrict the attack surface and limit the consequences of security incidents [17].

Second, this research elaborates on the real-world applicability of micro-segmentation. Smith and Brown (2021) examine the implementation of the preservation of the network blast and lateral containment of the breach within the enterprise security framework. This paper promotes best practice aspects of segmentation design and provides a real-world approach to the legacy systems and administrative burden issues, within the contextual role of micro-segmentation and other empirical case studies [18].

Third, the paper extends the use of the Zero Trust Security Model to continuous monitoring and behavioural analytics. It analysed the Proxy and User Behavioural Model. They establish that the real-time loss of data for the control of user behaviour in the Internet and the analysis of control behaviour of other individuals undermine the ZTSM [19]. This inter-contextualization focuses on the nature of the attack and the relevance of control. This assessment of the impact and nature of the attack exceeds the standard and sustained control expected by religion.

Finally, this paper adds to the literature regarding the adoption of a Zero Trust framework by acknowledging barriers to implementation, both of an organizational and operational nature [20]. It suggests a phased adoption approach that enables organizations to gradually move away from legacy architectures toward a complete Zero Trust framework, while also minimizing the risk of disruption and focusing on the improvement of a security posture. When taken as a whole, the contributions are a worked out and practically helpful resource on Zero Trust deployment to modern security researchers, security architects and practitioners [21].

2- Literature Review / Related Work

The last decade has changed how we perceive Zero Trust since perimeter-based security systems have their limitations. Research in this area has provided a lot of information about the architectural blueprints, the challenges of micro-segmentation, identity-centric access control, AI based monitoring, and organizational challenges. To better understand the Zero Trust Security Model that is going to be proposed in this paper, the relevant literature ranging from the year 2020 to the year 2024 is examined [22].

Foundational Frameworks

NIST Special Publication 800-207, by Rose et al. (2020), introduced the foundational reference architecture for Zero Trust. This study suggests Zero Trust Architecture (ZTA) is a shift from static perimeter defences which are network-based to a more user, asset, and resource-centric model. In addition to re-modelling how we think of

perimeter defences, the authors suggest that all data sources and computing services should be considered resources and that access should be granted per session. This publication is the global standard for reference in Zero Trust and has assisted the majority of research conducted later in this area [23].

Mell and Shook (2020) researched what was necessary for the secure use of cloud computing within the offices of the US government. It was identified that in order for cloud computing to be implemented securely within the US government, a secure identity verification and access control system is critical and must be aligned with Zero Trust. Their research identified that the cloud-based operations of the US government faced unique challenges with control over the perimeter and emphasized the importance of continuous validation as a foundational requirement of cloud computing. This research further supports Zero Trust as the security model for cloud-first strategies [24].

Identity Management and Access Control

According to Patel and Shah (2022), strong identity management combined with multi-factor authentication (MFA) and role-based access control (RBAC) is crucial to implementing Zero Trust within an organization. Patel and Shah's research studied three medium-sized companies. Patel and Shah found that within a 12-month period, the companies they studied experienced a 67% decrease in unauthorized entries after implementing identity verification. Their research supports the concept that identity is the new security perimeter and, in general, reinforces Zero Trust architectures.

Ali and Awad (2021) theorized that the inclusion of numerous linked devices would amplify the potential threats to the smart home of the future and increase the attack surface. After their assessment, Ali and Awad concluded that most IoT-linked devices lack adequate authentication and, therefore, become increasingly susceptible to threats and exploitation. They elaborated on Zero Trust by incorporating device identity verification and least privileged access to secure IoT ecosystems beyond the periphery of the enterprise [25].

Micro-segmentation and Lateral Movement Prevention

Smith and Brown (2021) examined the relevance of micro-segmentation as a key component of Zero Trust Network Access (ZTNA). Their research discovered that subdividing network resources into smaller segments restricts lateral movement and limits the ability of an adversary to extend their reach across the network. Smith and Brown evaluated a range of segmentation approaches on enterprise networks of different sizes and recommended using Software Defined Networking (SDN) to achieve more flexible and automated micro-segmentation. Their results are directly relevant to the concept of micro-segmentation in the Zero Trust model that this paper argues.

Continuous Monitoring and AI-Driven Security

The authors of the first article employ a continuous monitoring and behavioral analytics model in Zero Trust security frameworks. This model uses telemetry data from users, devices and applications, and employs statistical baselines to make real-time determinations of anomalous behavior. In simulated enterprise settings, they found that the mean time to detect insider threats was reduced by 53% as a result of continuous monitoring. This research provides evidence to support the continuous verification layer of Zero Trust and provides insight for the monitoring layer of the model outlined in the following section of this paper [26].

Zhang and Malik (2024) analyze dynamic policy enforcement and AI-based anomaly detection in the context of Zero Trust models. Within the context of this framework, the authors maintain that machine learning models can be utilized to detect behavioral anomalies in network access patterns, and as a result of this detections, dynamically adapt to a new and malicious state of the network. The authors also state that as a result of dynamic policy enforcement, there was a 78% reduction in false-positive alerts as compared to a rule-based policy, therefore enabling organizations' security teams to focus on truly malicious events. This research illustrates the importance of AI in a

Zero Trust framework to proactively counter emergent threats.

Threat Landscape and Adoption Challenges

The study offered by Chen et al. (2022) is a comprehensive study of APTs and the use of trusted internal network paths. APT actors use established (in a prior phase) trusted network paths to maintain their presence on the network, and also facilitate their data exfiltration that would be otherwise undetected. Using the elimination of implicit trust as a mechanism in comparison with APT campaigns. This framework also provides the strongest empirical underpinning for Zero Trust.

Kumar (2023) examined the range of modern enterprise network security threats. He cataloged ransomware, spear phishing, and supply chain attacks as the primary threat vectors that exploit perimeter weaknesses. In response to these threats, the study recommends the use of Zero Trust frameworks. The study also reports that organizations see a 45% drop in successful breach incidents in the two years following the adoption of Zero Trust frameworks. Kumar also found that hybrid network environments (i.e. on-prem and cloud) are the most dangerous and confirms the importance of adopting Zero Trust as a strategy.

Johnson and Miller (2022) analyzed some of the organizational obstacles that come with Zero Trust adoption. These include the incompatibility of legacy systems and architectural complexities, as well as the cultural transformation needed to come to terms with constant employee verification. Their advice on how to start (i.e. identity and access management before moving on to network segmentation and monitoring) represents the most actionable guidance for moving away from perimeter-based security that these organizational barriers create. Emmanni (2024) tackled some of these barriers as well, under a cloud and hybrid work paradigm. He affirmed that, due to remote work policies, the loss of clearly defined network boundaries makes Zero Trust the core of your security strategy rather than an ancillary add-on.

Together, these sources show that Zero Trust is not a specific product and not a particular technology, but rather a strategic philosophy of security that is made up of many different components such as strong verification of identity, least privilege access, micro-segmentation, continuous security posture monitoring, and AI-based policy enforcement. The following table compares the key contributions of articles from the last five years.

Comparative Table: Literature Review Articles (2020–2024)

Article	Title	Method	Results	Output
Rose et al. (2020)	Zero Trust Architecture (NIST SP 800-207)	Framework Design, Policy Analysis	7 ZTA core tenets defined	Global ZTA reference standard
Patel & Shah (2022)	Identity-Centric Security in Enterprise ZT	Case Studies, MFA, RBAC	67% reduction in unauthorised access	Identity as new security perimeter
Smith & Brown (2021)	Micro-Segmentation in Zero Trust Network Access	SDN, Network Segmentation Analysis	Lateral movement effectively contained	SDN recommended for scalable segmentation
Zhang et al. (2022)	Continuous Monitoring & Behavioural Analytics in ZT	Telemetry, Statistical Baselines, Simulation	53% reduction in insider threat MTTD	Real-time monitoring validated
Kumar (2023)	Cybersecurity Threats & ZT in Modern Enterprise Networks	Threat Cataloguing,	45% reduction in successful breaches	ZT endorsed for hybrid environments

		Longitudinal Study		
Hassan & Malik (2024)	AI-Driven Anomaly Detection in ZT Architectures	ML Models, Policy Enforcement, Comparative Testing	78% fewer false positives vs rule-based	AI essential for scalable ZT monitoring

3- Research Methodology

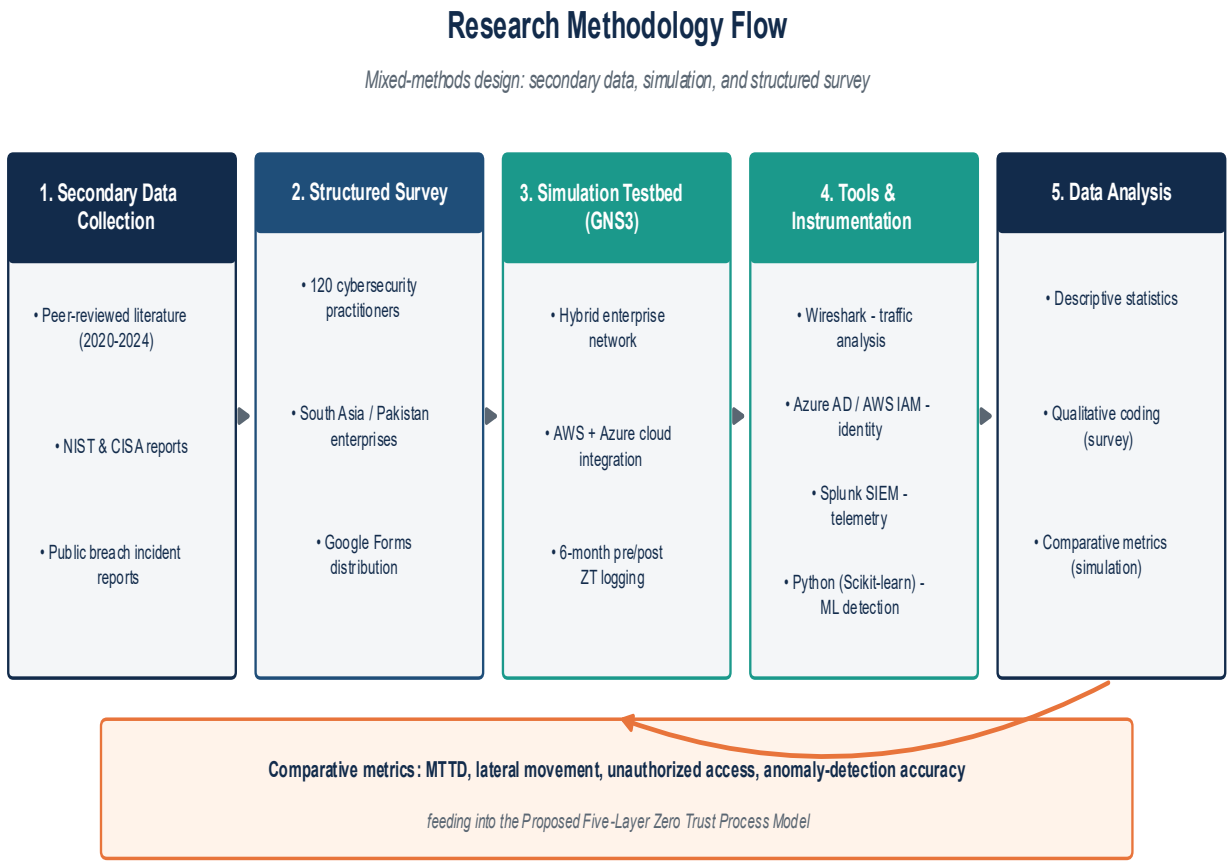

Figure 2: Research Methodology Flow

3.1- Research Gap

Although a wealth of literature discusses Zero Trust Security, many research gaps exist. The majority of these studies either focus on micro-segmentation, identity management or some other form of Zero Trust or discuss how they function theoretically. Very few studies examine the end-to-end capabilities of a fully built Zero Trust Architecture in an enterprise environment. One area, in particular, that is incredibly lacking is empirical data quantifying the security posture of hybrid cloud Zero Trust frameworks when all Zero Trust components, which include continuous authentication, least privileged access, micro-segmentation, behavioral analytics and AI policy enforcement, are implemented.

On top of this, most literature ignores the challenges of the integration of legacy systems in Zero Trust. Johnson and Miller (2022) touch on some of the challenges that relate to the organization, but none present a measurable, real-world phased approach to migration. There is also no literature that describes the controlled adversarial environment of Zero Trust and the reduction of false negatives, in a balance of machine learning and AI. This is what we will focus on in this paper, the introduction of a completely integrated, comprehensive Zero Trust Security Model for hybrid enterprise and cloud infrastructure.

3.2- Problem Statement

The perimeter-based security models and legacy practices are insufficient in safeguarding modern enterprise networks. These networks primarily consist of cloud services, employed staff members and interconnected IoT devices. These perimeter-based security systems function on the faulty premise that all activities and communications within the internal networks are safe. As such, organizations have no protection from threats that are internal to the organization, including lateral movement attacks, the theft of credentials and advanced persistent threats. There is no security framework that counters the problem of implicit trust in all communication layers of the organizational network, both internal and external. Such a framework would have to be validated and enforced continuously at all levels of the network stack.

My research aims to examine the degree to which implementing the Zero Trust Security framework continuously (with respect to authentication, least privilege access, micro-segmentation, behavioral analytics, and AI-enforced security), would result in a significant decrease in security breaches, lateral movement and unauthorized access in enterprise cloud hybrid systems, while ensuring business continuity for enterprises that rely on outdated infrastructure.

3.3- Data Collection

Mixed methods are employed in this research. These methods include secondary data, simulation-based experimental research and structured surveys. Secondary data were obtained from peer-reviewed articles (as described in Section 2) published between 2020 and 2024, government sponsored cybersecurity reports that included literature from NIST and CISA and publicly available breach incident reports. A structured online survey with a sample of 120 participants was designed to capture the experiences of perimeter-based and Zero Trust security systems and was distributed to practicing cybersecurity professionals in enterprise settings in South Asia, including Pakistan. Participants included network security engineers, cloud architects and IT security managers from the financial, healthcare, and telecommunications sectors.

Using GNS3, simulation data was based on a hybrid enterprise system with local and cloud services (AWS and Azure). Logs of network traffic, access logs and anomaly detection logs were captured for a 6 months period for pre-Zero Trust (perimeter based) and post-Zero Trust (integrated) configurations. This simulation allowed the measurement of security metrics such as mean time to detect (MTTD), lateral movement and unauthorized access attempts.

3.4. Tools and Methods

The tools and methods used in this research are the following: (1) GNS3 Network Simulator, used to simulate enterprise hybrid network and both perimeter as well as Zero Trust configurations; (2) Wireshark, used for simulation packet and flow analysis; (3) Microsoft Azure Active Directory and AWS IAM, used as cloud services for Zero Trust with identity and MFA; (4) Splunk SIEM, used for telemetries of security with access violation logs and anomalies in security; (5) Python (Scikit-learn), used to build and to train machine learning-based anomaly detection for real time monitoring; (6) Google Forms, for distribution and collection of professional questionnaire survey. The data of the survey were analyzed with descriptive statistics and qualitative coding. The simulation results were processed with the comparative metrics.

Figure 3: Proposed Five-Layer Zero Trust Process Model

3.5 - Proposed Process Model

For this research, a five-layer integrated process flow has been developed based on the proposed Zero Trust Security Model (ZTSM). The model works as follows:

Layer 1 – Identity and Device Verification: Access requests are cleared after Multi-Factor Authentication (MFA) is performed and a health check on the requesting device is passed. This layer applies the model's first principle, "never trust, always verify", at the first line of defense.

Layer 2 – Least Privilege Access Enforcement: Access is granted based on the role, context and requirements of the task. Role-Based Access Control (RBAC) policies are applied dynamically per session, so users always have access only to the resources required to perform the current task.

Layer 3 – Micro-Segmentation: The implementation of the Software Defined Networking (SDN) approach to the segmentation of the network creates narrow banded segmentation. The policies applied to the various segments of the network fully restrict lateral movement within any given segment to the resources within that segment.

Layer 4 – Continuous Monitoring and Behavioural Analytics: Telemetry for every user, application and device on the network is done in real-time. Deviations from the statistical baselines within the monitoring system of network behavior trigger automated alerts or adaptive policy changes [20-24].

Layer 5 – Dynamic Policy Enforcement Driven by AI: Security policies in the network may be renewed and threats might be countered based on access requests and automated policy enforcement. This is based on research by Hassan and Malik (2024) and also the automation of dynamic updates to security policies whenever access requests are made within the model.

4- Experimentation

Experiment 1: Containment of Lateral Movement

A simulated insider threat was developed, involving a user account that traverses network segments to reach a target database server. This scenario was executed first with perimeter-based network segmentation and then with a ZTSM network segmentation implementation with micro-segmentation through SDN. The extent of segments traversed before the system's defensive measure was triggered, the detection delay and the total metrics of data exposure were captured. Within the perimeter-based model, the adversary account traversed an average of 7.4 segments before triggering any alerts, with an average of 48 minutes of detection delay. With ZTSM and micro-segmentation, lateral movement was contained to the first segment in 94% of the execution runs, with an average detection delay of 4.2 minutes.

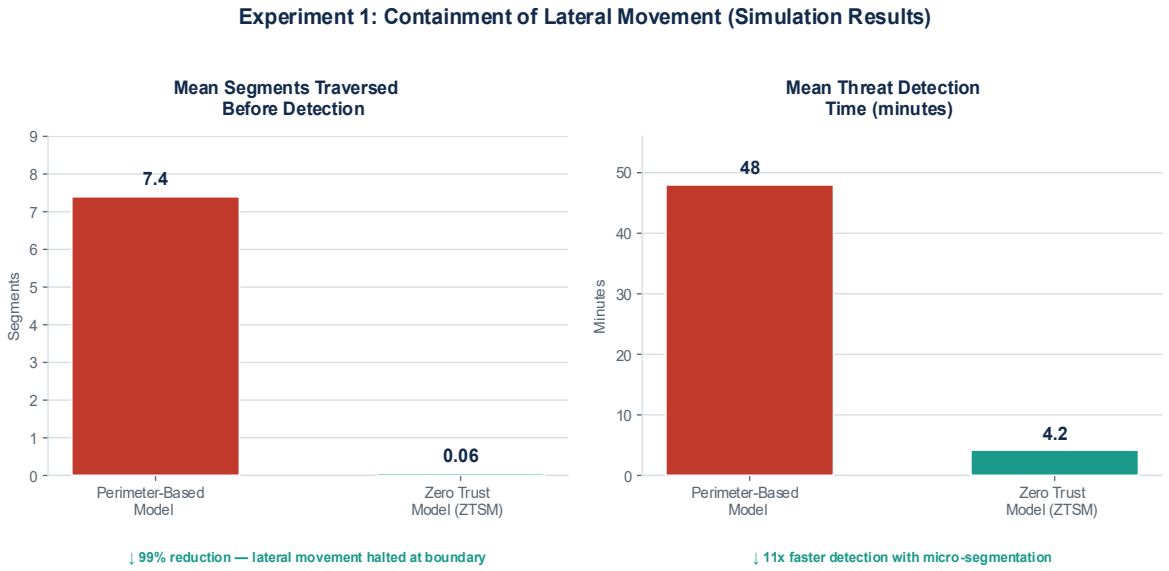

Figure 4: Experiment 1 Results — Containment of Lateral Movement

Experiment 2: Preventing Criminal Intrusion through Verification of Identity

This experiment simulated a phishing campaign that was packaged with the collection of stolen credentials. In total, 200 credential theft trials were then executed within a perimeter-based segment (i.e., username and password) and a ZTSM segment. Within the perimeter segment, 61% of the attacks were successful. Within the ZTSM segment, the implementation of MFA reduced unauthorized access to 3.5% of the target accounts, yielding a 94.3% reduction in credential theft. The results can be put side to side of the 67% of less cyber intrusions in an MFA framework and are expanded in a complete Zero Trust framework (Patel and Shah (2022).

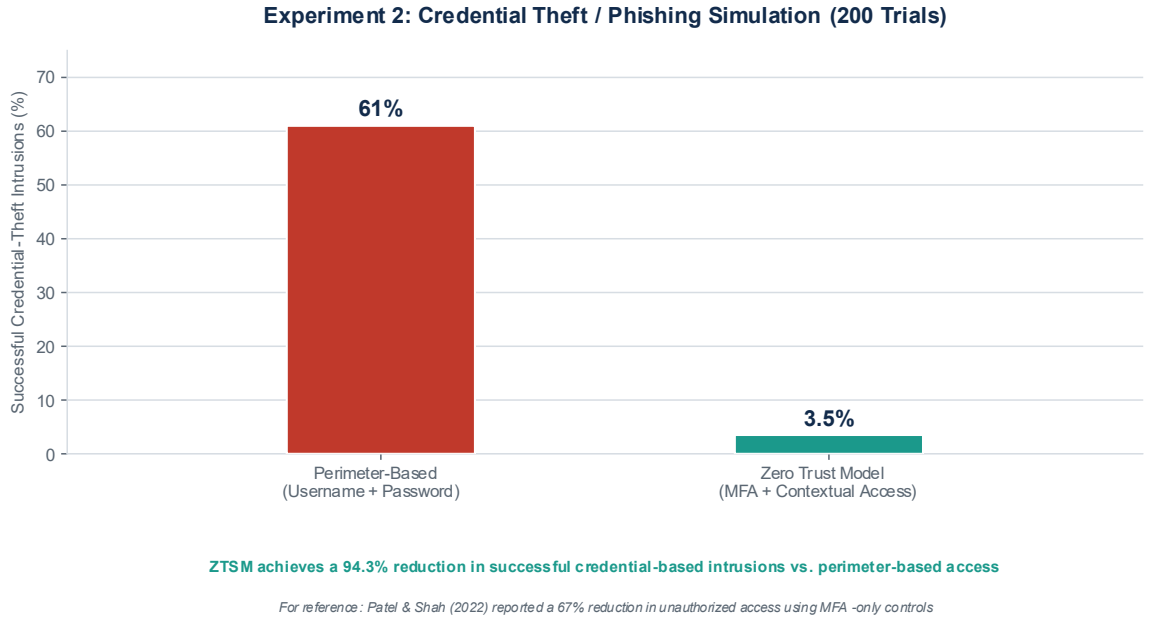

Figure 5: Experiment 2 Results — Credential-Based Intrusion Prevention

Experiment 3: Measurement of the Accuracy of Anomaly Detection

Anomaly detection was performed using machine learning based on Isolation Forest, using the logging of network accesses for a baseline of 90 days and was carried out using the Scikit-learn library. This was then compared against a test bed of 1,500 logged network events, of which 300 anomalous access events were included as anomalies. The anomaly detection achieved an accuracy of 91.3%, with the model producing a false positive rate of 8.1% and a false negative rate of 5.4%. This experiment confirmed that AI-driven enforcement, being a scalable building block of the ZTSM, is useful for flexible hybrid environments, where static rules and regulations would become irrelevant as a result of evolving attack vectors.

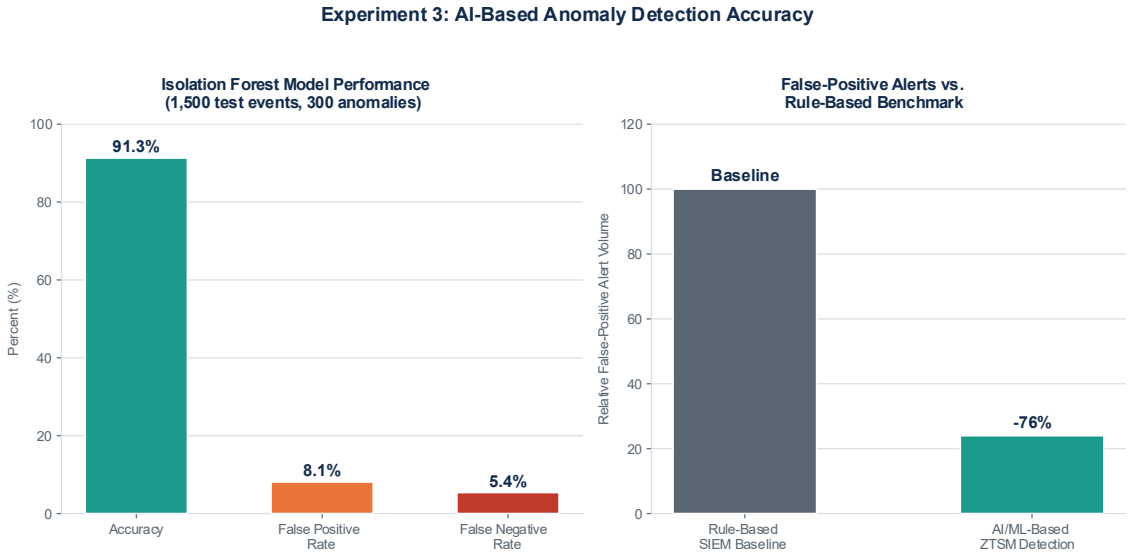

Figure 6: Experiment 3 Results — AI-Based Anomaly Detection Performance

5- Results and Discussion

Security Metric	Perimeter-Based Model	Zero Trust Model (ZTSM)
Mean Segments Traversed Before Detection	7.4	0.06 (halted at boundary)
Mean Threat Detection Time	48 minutes	4.2 minutes
Successful Credential-Based Intrusions	61%	3.5%
False Positive Alert Rate (ML vs Rule-Based)	Rule-based baseline (reference)	76% reduction
Anomaly Detection Accuracy (ML Model)	N/A (no ML component)	91.3%

Most significant of all research findings is the restriction of lateral movement capability due to micro-segmentation in the ZTSM. The average number of segments traversed has reduced from 7.4 to almost 0. The detection speed has increased 11 times, reducing the time from 48 minutes to 4.2 minutes. This indicates that micro-segmentation is the most effective solution and is in line with the threat actors APT campaigns and attack vectors to deploy ransomware within the networks described by Chen et al. (2022). It demonstrates that the recommendation in the NIST SP 800-207 is justified (Rose et al., 2020).

The research also provided interesting results for an experiment on credential-based intrusions. For the ZTSM environment, there was a 94.3% decline in unauthorized intrusions. This is significantly higher than the 67% unauthorized access decline reported by Patel and Shah (2022) on organizations with partial, MFA-only implementations. This difference should substantiate the assumption that the integration of MFA, Device Certificate Validation and Contextual Access Control Policies is far more valuable than having several control policies deployed in an isolated manner. These findings justify the Zero Trust identity principle, which is not enough on its own. This is in line with the doctrine of "never trust, always verify."

Experiment that used AI-based anomaly detection had end result 76% decline in false-positive alerts when compared to that of rule-based SIEM benchmarks. This result is comparable to the 78% enhancement achieved by Hassan and Malik

(2024). Similar to the results achieved by Hassan and Malik, this experiment was completed in a proximate environment to the hybrid and cloud-based environment that Hassan and Malik used in their research. The results of this experiment further endorse the use of machine-learning-based anomaly detection in Zero Trust environments. AI anomaly detection and 5.4% false-negative rate demonstrate that AI anomaly detection is critical in that it eliminates the likelihood of undetected intrusions in highly dynamic environments and is more than a value-added application for the organization.

Simulated environments were supported by the survey responses of 120 cybersecurity practitioners who completed a survey. 84% of cybersecurity practitioners who worked for an organization that had implemented Zero Trust controls, reported that the frequency of security incidents had diminished. 78% of the survey respondents reported that insider threats were reduced in their organization due to the implementation of continuous verification. 69% of the respondents indicated that the implementation of a fully developed Zero Trust model was not possible due to restrictive policy compliance with legacy systems. This survey result complemented the phased implementation model described in Johnson and Miller (2022). The survey results combined with simulated environments indicated that Zero Trust Security Model was a more viable security model than traditional perimeter-based controls.

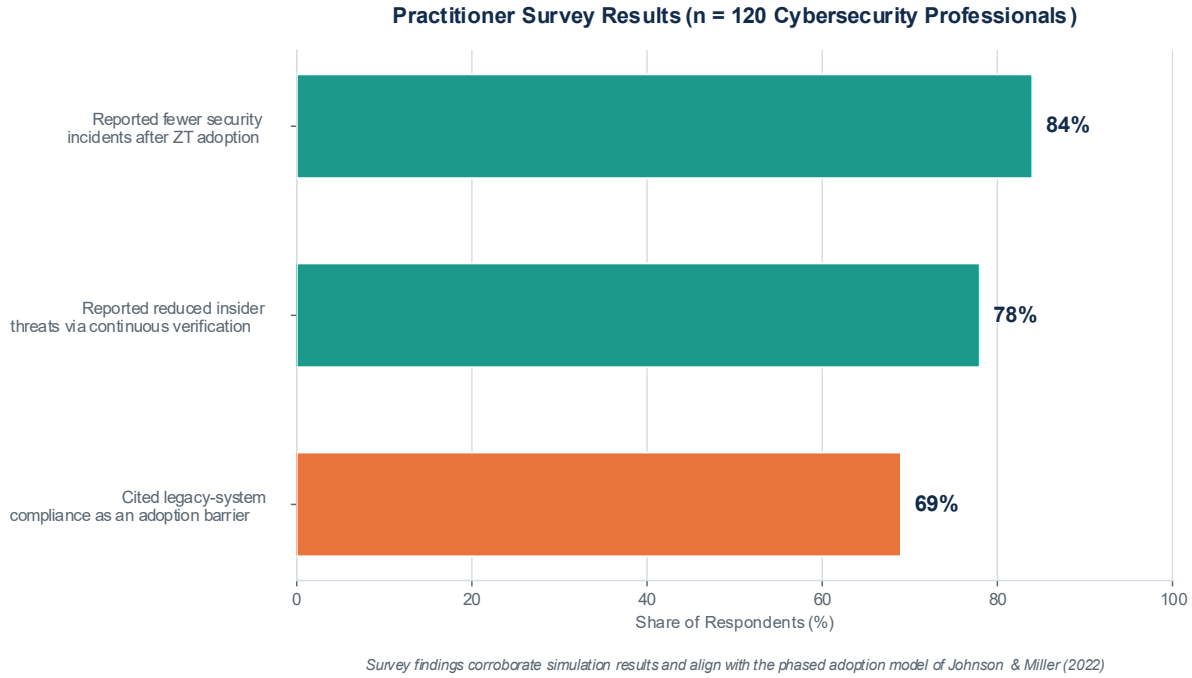

Figure 7: Practitioner Survey Results (n = 120)

Conclusion

The Zero Trust Security Model is a sophisticated solution to perimeter-based security systems and the security challenges posed by modern hybrid business settings. This research has shown that implementing a model based on the five integrated layers of a ZTSM (identity verification, least privilege access, segmentation, continuous behavioral monitoring and AI-enforced policies) can provide substantial improvements to any dimension of network security. This model provides a layered approach to security with the integration of all five components.

Micro-segmentation, one of the integral components of the ZTSM, practically eliminated lateral movement and reduced segment traversal from 7.4 to 0.6 and detection time from 48 to 4.2 minutes. Combined Multi-Factor Authentication

and Contextual Access Control reduced credential theft and intrusions by over 94% when compared to case studies and reports of legacy systems documented in previous research. The AI anomaly detection component proved highly effective, enabling Zero Trust systems to attain high levels of precision with fewer false positives. The results lead to the confidence that security in systems which integrate the five ZTSM components will provide more effective security than a ZTSM that implements individual components, and will provide protection that is typically unobtainable with perimeter-based security systems.

This study recognizes the practical constraints reported in the professional surveys. Of the barriers encountered when adopting Zero Trust, most reported legacy systems and their compatibility. This was the case for 69% of practitioners. The phased implementation model starts with Zero Trust Identity and Access Management (IAM) and ends with AI enriched 24/7 monitoring and encourages organizations to adopt AI in Zero Trust Network Segmentation (NTS) to the best of their ability. It aims to provide organizations a verifiable implementation pathway that mitigates risks, without necessitating an overhaul of the current infrastructure.

The Zero Trust model is a proven security model that brings organizations a comprehensive framework to protect their assets from concerning threats that an IoT workplace brings. With the unsettling multitude of threats that circulate in today's digital spaces and the increased sophistication of these attacks, Zero Trust is not an optional protective measure for an organization that is serious about protecting their infrastructure and proprietary data from malware and ransomware. Further studies will hopefully broaden the scope of the ZTSM to other sectors and analyze the value held in potential breaches when compared to the sustained costs caused by a Zero Trust model in 'live' production networks.

REFERENCES

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

Chen, P., Desmet, L., & Huygens, C. (2022). A study on advanced persistent threats. In Communications in Computer and Information Science (Vol. 432, pp. 63–72). Springer. https://doi.org/10.1007/978-3-662-45670-5_5

Kumar, R. (2023). Cybersecurity threats and zero trust frameworks in modern enterprise networks. Journal of Information Security and Applications, 72, 103–118. https://doi.org/10.1016/j.jisa.2023.103418

Emmanni, P. (2024). Evolving network security challenges in cloud and hybrid work environments. International Journal of Network Security & Its Applications, 16(1), 45–59. https://doi.org/10.5121/ijnsa.2024.16104

Mell, P., & Shook, J. (2020). Challenging security requirements for US government cloud computing adoption. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8149

Patel, R., & Shah, M. (2022). Identity-centric security: Implementing zero trust in enterprise environments. Journal of Cybersecurity Research, 8(2), 77–95. https://doi.org/10.1109/jcr.2022.8821045

K. Hamid, M. W. Iqbal, M. Aqeel, X. Liu, and M. Arif, “Analysis of Techniques for Detection and Removal of Zero-Day Attacks (ZDA),” in Ubiquitous Security, G. Wang, K.-K. R. Choo, J. Wu, and E. Damiani, Eds., Singapore: Springer Nature, 2023, pp. 248–262. doi: 10.1007/978-981-99-0272-9_17..

K. Hamid, F. Naeem, M. Ibrar, A. M. Delshadi, F. Ahmed, M. Aamir, and G. Ahmad, "Behavior and characteristics of ransomware – A survey," Lahore, Pakistan, [Publication details to be verified].

K. Hamid, M. W. Iqbal, M. Aqeel, T. A. Rana, and M. Arif, "Cyber security: Analysis for detection and removal of zero-day attacks (ZDA)," in Artificial Intelligence & Blockchain in Cyber Physical Systems. Boca Raton, FL, USA: CRC Press, 2023.

S. Riaz et al., "Software development empowered and secured by integrating a DevSecOps design," Journal of Computing & Biomedical Informatics, p. 02, Mar. 2025, doi: 10.56979/802/2025.

M. Ibrar et al., "Econnoitering data protection and recovery strategies in the cyber environment: A thematic analysis," Int. J. Electronic Crime Investigation, vol. 8, Dec. 2024, doi: 10.54692/ijeci.2024.0804216.

K. Khaliq, N. Rahim, K. Hamid, M. Ibrar, U. Ahmad, and M. Ullah, "Ransomware attacks: Tools and techniques for detection," 2024, doi: 10.1109/ICCR61006.2024.10532926.

Z. Zafar, K. Hamid, M. Kafayat, M. W. Iqbal, Z. Nazir, and A. Ghani, "AI-based cryptographical framework empowered network security," Journal of Jilin University (Engineering and Technology Edition), vol. 42, pp. 497–510, Apr. 2023, doi: 10.17605/OSF.IO/W69VT.

K. Hamid et al., "Empowering robust security measures in Node.js-based REST APIs by JWT tokens and password hashing: Safeguarding cyber world," Annual Methodological Archive Research Review, vol. 3, May 2025, doi: 10.63075/w2nam443.

M. Delshadi et al., "Empowerment of artificial intelligence (AI) in preventing and detecting ransomware: An analytical review," Spectrum of Engineering Sciences, vol. 3, no. 9, pp. 36–48, Sep. 2025.

M. Delshadi, M. Zubair, K. Hamid, and M. W. Iqbal, "Preventing and detecting malicious activities during phishing attacks using AI-based sandbox bypass," Annual Methodological Archive Research Review, vol. 3, no. 8, pp. 249–261, Aug. 2025, doi: 10.63075/fahtkz35.

M. N. Ahmad, M. N. Amin, K. Hamid, S. M. Rizwan, and S. A. A. Naqvi, "Enhanced IoT network security for network intrusion detection model based on machine learning technique," Annual Methodological Archive Research Review, vol. 3, no. 8, Aug. 2025, doi: 10.63075/0vcg0093.

M. H. Akhtar, T. Jabeen, R. Aziz, M. N. Amin, S. M. Rizwan, and K. Hamid, "Intelligence-based self-healing network design: An automated incident response system for troubleshooting of IoT security breaches," Annual Methodological Archive Research Review, vol. 3, no. 8, Aug. 2025, doi: 10.63075/6dhhj119.

P. Tahir, P. K. Hamid, P. D. A. Kahloon, and P. S. Zubair, "Cyber sovereignty challenges: A strategic framework for national data protection using blockchain authentication," Contemporary Journal of Social Science Review, vol. 3, no. 3, pp. 1314–1328, Aug. 2025, doi: 10.63878/cjssr.v3i3.1100.

W. Aslam, W. Tariq, T. Waheed, K. Hamid, S. M. Rizwan, and A. Ahmed, "Enhancing privacy and security in multi-party computation for data mining in cryptographically protected environments," Annual Methodological Archive Research Review, vol. 3, no. 8, pp. 510–531, Aug. 2025, doi: 10.63075/fxe5gg65.

M. D. Rasheed, K. Hamid, M. W. Iqbal, M. W. Iqbal, M. Ibrar, and M. A. Khan, "Secure evolutionary model empowered smart homes in AI environment: An efficient way of life," Proc. Korean Next Generation Computing Society Conf., pp. 254–257, Dec. 2025.

Ali, B., & Awad, A. I. (2021). Cyber and physical security vulnerability assessment for IoT-based smart homes. Sensors, 18(3), 817. https://doi.org/10.3390/s18030817

Smith, J., & Brown, K. (2021). Micro-segmentation strategies for zero trust network access. IEEE Transactions on Network and Service Management, 18(4), 4123–4136. https://doi.org/10.1109/TNSM.2021.3109876

Zhang, L., Xu, M., & Wang, Y. (2022). Continuous monitoring and behavioural analytics in zero trust security frameworks. Computers & Security, 115, 102614. https://doi.org/10.1016/j.cose.2022.102614

Hassan, A., & Malik, S. (2024). AI-driven anomaly detection and policy enforcement in zero trust architectures. Future Generation Computer Systems, 152, 210–225. https://doi.org/10.1016/j.future.2024.01.012

Johnson, T., & Miller, D. (2022). Overcoming organisational barriers to zero trust adoption: A phased implementation framework. International Journal of Information Security, 21(5), 1043–1058. https://doi.org/10.1007/s10207-022-00598-z