The American Journal of Management and Economics Innovations
ISSN 2693-0811 | Open Access

TYPE Original Research
PAGE NO. 56-70
DOI 10.37547/tajmei/Volume07Issue10-05

Check for updates

Zero Trust And Micro-Segmentation: Strengthening Network Security

Ibu A Wonor
Ph.D. student, City University, Cambodia

Dr Martha O Musa
University of Port Harcourt, Rivers State, Nigeria

Christopher M. Osazuwa
City University, Cambodia, African Campus

OPEN ACCESS
SUBMITED 15 August 2025
ACCEPTED 11 September 2025
PUBLISHED 13 October 2025
VOLUME Vol.07 Issue 10 2025

CITATION

Ibu A Wonor, Dr Martha O Musa, & Christopher M. Osazuwa. (2025). Zero Trust And Micro-Segmentation: Strengthening Network Security. The American Journal of Management and Economics Innovations, 7(10), 56–70. https://doi.org/10.37547/tajmei/Volume07Issue10-05

Abstract: Traditional perimeter-based security models, which assume trust within network boundaries, have become increasingly ineffective against evolving and sophisticated cyber threats. This study examines how Zero Trust Architecture (ZTA), based on the principle of "never trust, always verify," and micro-segmentation, which facilitates granular access control, can bolster network security. The research looks closely at the weaknesses of traditional security models, the ideas, and advantages of ZTA and micro-segmentation, the difficulties in using ZTA, the assessment of current Zero Trust frameworks, and the creation of a new combined framework. We conducted a systematic literature review to evaluate existing research, identify key themes, and pinpoint gaps in current knowledge. The findings indicate that significant challenges remain, while ZTA and micro-segmentation offer enhanced protection against insider threats and lateral movement. These include scalability issues in multi-cloud environments, difficulties integrating with legacy systems, interoperability problems, and a lack of standardised evaluation frameworks. The proposed framework aims to bridge existing gaps, fostering a more secure and adaptable approach to mitigating modern cybersecurity risks. The study concludes by emphasising the need for an integrated, scalable, and standards- compliant Zero Trust framework to

overcome these limitations and strengthen network security effectively.

Keywords: Zero Trust Architecture, Zero Trust framework, micro-segmentation, network security, threats.

Introduction: The growing complexity of cyber threats has revealed serious weaknesses in traditional security models that assume trust within specific network boundaries. As organisations shift toward hybrid IT infrastructures, cloud-native systems, and Internet of Things (IoT) ecosystems, the attack surface expands, rendering static defences inadequate. This evolving threat landscape necessitates the adoption of more adaptive security paradigms, with Zero Trust Architecture (ZTA) emerging as a compelling alternative. Built on the principle of "never trust, always verify," ZTA mandates continuous authentication, context-aware trust assessments, and strict enforcement of least-privilege access to limit exposure to both internal and external threats (Dhiman et al., 2024; Gambo & Almulhem, 2025).

An essential component of ZTA is micro-segmentation, which divides network environments into tightly controlled segments, thereby enabling granular access control and improving breach containment. This approach allows organisations to monitor user behaviour more precisely and enforce context-sensitive policies. The evolution of micro-segmentation technologies, particularly those leveraging identity-based access and automation, has enhanced deployment flexibility and scalability in dynamic environments (Vasconcelos, 2025).

However, implementing Zero Trust in real-world scenarios presents operational and technological hurdles. Organisations increasingly struggle with enforcing ZTA principles at scale, especially in multi-cloud and multi-tenant environments, where policy management and identity verification become fragmented (Gambo & Almulhem, 2025). The coexistence of modern cloud infrastructure with legacy systems further complicates integration, as older technologies are often structurally incompatible with Zero Trust requirements (Vasconcelos, 2025).

Though mostly unproven, creative technologies like quantum neural networks and AI-driven micro-segmentation promise to improve Zero Trust adoption. Their computational needs also create difficulties for adoption in limited settings such as Industrial IoT (Dhiman et al., 2024). Sector-specific implementations, especially in finance, healthcare, and IoT-heavy sectors, highlight Zero Trust adoption's potential and pragmatic difficulties. Among these are expensive deployment costs, complicated policy orchestration, and poor user experience (Parde, 2022).

Moreover, the absence of standardised performance metrics and alignment with global benchmarks hinders consistent evaluation of ZTA effectiveness. As Vasconcelos (2025) notes, current frameworks lack a unifying quality model, making it challenging to ensure compliance, optimise performance, and build trust in enterprise applications. Building on these insights, the present study seeks to develop an integrated, scalable, empirically validated Zero Trust–enabled micro-segmentation framework suitable for complex operational contexts.

Statement of The Problem

As cybersecurity threats change, traditional perimeter-based security strategies, which assume that inside networks are always safe, are becoming less and less effective. These models do not do a decent job of stopping advanced threats like lateral movement, ransomware, and data exfiltration, which often exploit trust relationships between people inside the company (Kumar, 2024; Roy, Zhang, & Iweala, 2024). Zero Trust Architecture (ZTA) has become more popular as a more secure approach based on continuous authentication, least-privilege access, and dynamic trust evaluation. Micro-segmentation makes ZTA frameworks even more secure by allowing for more precise policy enforcement and lowering the attack surface through workload segregation (Roy et al., 2024).

Even if the idea behind ZTA is strong, several technological and operational problems make it hard to implement. Scalability in distributed, multi-cloud, and multi-tenant setups is one of the most important problems. ZTA is theoretically scalable but hard to enforce when used on dynamic cloud-native infrastructures. Denzel and Ng'etich (2025) say that regulations for verifying identification and controlling access do not work the same way across all platforms. This makes enforcement less effective and adds to the

administrative cost. Another big problem is making ZTA work with older platforms. Backwards compatibility is often a goal of design. However, many older technologies do not have architectural flexibility to accommodate ZTA principles. This makes deployment less efficient and operations more complicated (Bondhala, 2025). Also, innovative technologies like AI-driven micro- segmentation and large language model (LLM)-based access control offer better security. However, they are usually unsuitable for applications with limited resources, like industrial IoT. These models provide extra work for computers and slow down the system more than embedded or low-power devices can manage (Selciya, Ayo, & Onwuegbuzie, 2024; Liu, Mendez, & Farouk, 2024). There have been suggestions for lightweight frameworks, but there is no practical advice on using these solutions in limited spaces. Zero Trust deployment is even more difficult because cloud systems might work together. Some frameworks talk about cloud-native security (Sheikh, Adeyemi, & Bello, 2021; Arora & Hastings, 2024), but there are no strong ways to enforce a single ZTA policy across different cloud infrastructures. These problems are made worse by differences in API design, identity federation systems, and enforcement protocols. Also, the operational complexity of real-time orchestration in federated contexts is typically not covered in the literature. Many of the proposed ZTA and micro-segmentation models lack sufficient practical applications, which is a big problem. Basta, Nwosu, and Eze (2021) and other studies give systematic ways to evaluate things. However, these are usually only examined in controlled or simulated settings. As a result, there are still issues about how well they work in the actual world and how useful they are. Studies in specific fields show that this gap is even bigger, pointing out problems with implementation costs, orchestration complexity, and user experience, especially in high-risk areas like finance, healthcare, and IoT-based systems (Hasan, 2024; Jimmy, 2022).

However, an equally essential issue is that no framework connects ZTA installations with quality and compliance standards recognized worldwide. Manzano, Lee, and Okafor (2024) have looked at key performance indicators, yet there is still a big gap between ZTA's capabilities and meeting the criteria set by organizations like ISO/IEC. This lack of alignment makes evaluating, benchmarking, and deploying ZTA in areas sensitive to regulations harder. Because of these persistent challenges, which include scalability, legacy integration, interoperability, resource efficiency, and standardization, there is an urgent need for a practical, flexible, and standards-compliant Zero Trust-based framework that can meet the needs of modern cybersecurity environments. The study aims to investigate how Zero Trust Architecture and micro-segmentation can strengthen network security.

Research Objectives

The specific objectives are to:

1. Analyze the limitations of traditional perimeter-based security models in addressing modern cybersecurity threats.

2. Investigate the principles and benefits of Zero Trust Architecture (ZTA) and micro- segmentation in enhancing network security.

3. Identify the key challenges and barriers hindering the effective implementation of ZTA, particularly in complex environments.

4. Evaluate existing Zero Trust and micro-segmentation frameworks, assessing their scalability, interoperability, and empirical validation.

5. Propose the development of an integrated, scalable, and standards-compliant Zero Trust-enabled micro-segmentation framework.

Research Questions

1. What are the fundamental limitations of traditional perimeter-based security models in defending against evolving cyber threats?

2. How do Zero Trust Architecture and micro-segmentation enhance network security and mitigate the risks of internal and external threats?

3. What are the primary challenges in implementing Zero Trust at scale, particularly in multi-cloud, multi-tenant, and legacy system environments?

4. How effective are the current Zero Trust and micro-segmentation frameworks in terms of scalability, interoperability, and real-world applicability?

5. What key components and capabilities should an integrated Zero Trust-enabled micro-segmentation framework include to ensure adaptability, efficiency, and standards compliance?

Conceptual Review

Traditional Perimeter-Based Security Models

The traditional perimeter-based security model emerged during the early networking stages, when organizational infrastructures were centralized and confined to physical office spaces. Often referred to as the "castle and moat" model, this security paradigm is predicated on the assumption that most security threats originate from external sources. As a result, the focus is on safeguarding the boundaries of a network to prevent unauthorised access. Key technologies such as firewalls, intrusion detection systems (IDS), and secure gateways were employed to define and enforce these boundaries, ensuring that internal systems remained isolated from potential external threats.

Stallings and Brown (2018) articulated that this model was effective for environments where physical perimeters were well-defined and network infrastructures were centralised. During this era, corporate networks adhered to a perimeter-centric approach, as internal users were considered inherently trustworthy and external connections were rare. This centralised structure mirrored the simplistic nature of threats at the time, brute-force attacks and malware aimed at exploiting vulnerable external entry points.

The perimeter-based security model underpins three fundamental principles: boundary defence, trust assumptions, and centralised access controls. Boundary defence involves physical barriers (network segmentation) and logical mechanisms (firewalls) to isolate internal systems from the external network. One of the core tenets of this approach is the implicit assumption of trust, an understanding that all entities within the established perimeter are regarded as benign. However, as Saltzer and Schroeder (1975) emphasised in their seminal work on secure systems design, this assumption of trust is fraught with vulnerabilities. If an attacker successfully breaches the outer defences, they are granted unmitigated access to the internal network.

Centralised access points are a crucial model component, as they concentrate monitoring and control at specific network gateways. These access points facilitate the filtration of incoming and outgoing traffic, enabling organisations to detect and respond to malicious activities. While this approach can effectively maintain visibility and control, it also introduces potential single points of failure. If an attacker compromises one of these critical access points, they can access the entire network, bypassing the perimeter's protective measures.

The traditional perimeter-based security model offers several notable advantages. Its simplicity makes it easier to manage and deploy, especially in smaller-scale environments. As Singh and Kaur (2020) point out, organisations can implement this model with low complexity, making it an appealing, cost-effective solution for small to medium-sized businesses. Secondly, the model is inherently suited for environments with well-defined boundaries, such as on-premises networks, where the limited number of external connections reduces the likelihood of exposure to sophisticated attack vectors.

Furthermore, centralised control mechanisms in the perimeter model provide organisations with comprehensive visibility into network traffic patterns, which is crucial for detecting anomalies and potential threats. The reliance on established security technologies, such as firewalls, ensures consistent protection against common, rudimentary threats. As Deeter and Friedman (2021) note, these technologies continue to offer reliable defences against basic intrusion attempts, contributing to the model's sustained effectiveness in environments with well-defined internal and external boundaries.

Despite its initial successes, the perimeter-based model has struggled to keep pace with the evolving demands of modern computing environments. As organisations increasingly embrace cloud computing, remote work, and the Internet of Things (IoT), the traditional concept of a fixed network perimeter has become less relevant. This shift, often referred to as "perimeter erosion" by Jones et al. (2023), highlights the inadequacy of static boundaries in protecting dynamic, distributed infrastructures, where data and resources are frequently located outside traditional network confines.

Furthermore, a major weakness in the approach has been its dependence on implicit confidence. Lateral movement inside networks, insider knowledge, and compromised credentials put companies in great danger. A Verizon (2022) poll found that 60% of security incidents included internal players, highlighting the perimeter-based approach's critical flaw in handling

threats from within trusted areas. These constraints have reconsidered conventional security strategies, pushing companies to use more flexible, adaptive models to handle the complexity of contemporary security issues.

Modern attackers have increasingly adopted sophisticated techniques, such as ransomware and supply chain attacks, which bypass traditional perimeter defences. As Cybersecurity Ventures (2021) noted, conventional security tools, including firewalls and intrusion detection systems (IDS), often struggle to counter these evolving threats due to their dynamic and adaptive nature. Ransomware, for instance, typically infiltrates systems through phishing or vulnerabilities in third-party software, circumventing the protections offered by perimeter defences. Similarly, supply chain attacks exploit trusted relationships between organisations and their vendors, allowing attackers to infiltrate networks from within, bypassing the outer defences.

Considering these challenges, organizations have shifted towards more advanced security models such as Zero Trust Architecture (ZTA) and Secure Access Service Edge (SASE). These models recognise the limitations of perimeter-based security and offer more comprehensive, adaptable solutions for securing modern, distributed infrastructures.

Zero Trust Architecture (ZTA) operates on the principle of "never trust, always verify," treating all internal or external users as potential threats. According to Rose and Srinivasan (2020), ZTA emphasises continuous monitoring, identity-based access controls, and real-time analytics to ensure security is enforced at every access point. Instead of relying on static perimeter defences, ZTA insists on constantly verifying trustworthiness, regardless of the user's location or device. This model significantly enhances protection against insider threats, compromised credentials, and lateral movements within the network.

Similarly, Secure Access Service Edge (SASE) integrates networking and security functions into a unified, cloud-delivered solution. SASE provides context-aware protection, enabling secure access to resources regardless of a user's location or the network to which they are connected. By leveraging the cloud, SASE offers flexibility and scalability to meet the demands of modern, dynamic infrastructures. This integrated approach ensures that security is applied uniformly across all endpoints, providing consistent protection against emerging threats that transcend traditional physical network boundaries.

Both ZTA and SASE represent a paradigm shift in how organisations approach security, moving away from reliance on perimeter defences and embracing a more holistic, context- aware approach to safeguard against the sophisticated threats of today's digital landscape. These models are better suited to address the complexity and fluidity of modern technological environments, where data, applications, and users are no longer confined within a defined perimeter.

Principles of Zero Trust Architecture (ZTA)

Zero Trust Architecture (ZTA) is built upon several foundational principles designed to address the complexities of modern cybersecurity threats. One of the key principles is continuous authentication, which emphasises the need for ongoing verification of users and devices throughout their entire session. Unlike traditional models that rely on a single authentication event at the point of entry, ZTA continuously checks the legitimacy of users and devices. This is accomplished through various mechanisms such as multi-factor authentication (MFA), behaviourall analytics, and contextual signals like device health and geolocation. Machine learning and artificial intelligence (AI) further enhance continuous authentication by identifying subtle behavioral patterns that may indicate unauthorised access attempts, making it a dynamic and robust method for preventing breaches (Gambo & Almulhem, 2025; Dhiman et al., 2024).

Another ZTA principle is the least privilege access, which restricts users, devices, and applications to the minimum permissions necessary to perform their tasks. By limiting access rights, ZTA reduces the attack surface and minimises the potential damage from security breaches. This principle is enforced through granular access controls and dynamic policy enforcement, ensuring access permissions are continuously adapted based on real-time risk assessments. This approach is particularly practical in environments like cloud computing and the Internet of Things (IoT), where traditional perimeter security models are less effective. Research by Ghasemshirazi et al. (2023) and Dhiman et al. (2024) has shown that the least privilege access is crucial in safeguarding sensitive data in these

increasingly complex environments.

The principle of contextual trust evaluation replaces static trust models with dynamic, context-aware decision-making. In ZTA, access decisions are not based solely on a user's initial authentication but consider factors such as user behaviour, device status, and the sensitivity of the accessed resource. This adaptive model allows organisations to respond to evolving threats by assessing each access attempt in context. For instance, if a user typically accesses systems from a specific location but attempts to access sensitive resources from an untrusted device or unfamiliar location, the system may flag this behaviour as suspicious. This dynamic evaluation is further enhanced by integrating AI and machine learning, enabling more accurate and timely risk assessments, allowing for proactive responses to potential threats (Gambo & Almulhem, 2025; Ghasemshirazi et al., 2023).

Micro-segmentation Techniques

Micro-segmentation is a sophisticated cybersecurity strategy designed to enhance network security by dividing a network into smaller, isolated segments, each subject to specific security controls. This approach is highly effective in minimising the attack surface, containing breaches, and ensuring compliance with regulatory standards (Vasconcelos, 2025). By creating isolated segments within a network, organisations can better protect their critical assets from unauthorised access and reduce the potential impact of any security incidents (Srikanth, 2020).

Network segmentation is a foundational technique in cybersecurity that involves dividing a network into smaller sub-networks or segments. Each segment functions independently, with traffic flow controlled based on predefined policies (Bondhala, 2025). This division improves both security and performance by ensuring that sensitive data is isolated from less critical systems, limiting the chances of unauthorised access. Traditionally, network segmentation has been achieved through firewalls and access control lists (ACLs). However, with the advent of modern technologies such as software-defined networking (SDN), organisations can create more dynamic and flexible segmentation policies. This is especially valuable in hybrid and multi-cloud environments, where assets are dispersed across various platforms, requiring more adaptable and scalable segmentation solutions (Srikanth, 2020).

Granular policy enforcement applies highly specific security policies tailored to individual users, devices, or applications. Unlike broad, general policies, granular enforcement enables precise control over who can access resources and what actions they are permitted to perform. This is achieved through techniques such as role-based access control (RBAC) and attribute-based access control (ABAC), which evaluate a variety of factors, including user identity, device type, and location (Khan, 2014). The advantage of granular policy enforcement is that it helps minimise the risk of unauthorised access and potential data breaches while ensuring compliance with stringent data protection regulations. By tailoring security policies to the specific needs of each entity, organisations can more effectively safeguard sensitive resources.

Isolation of workloads is another critical component of micro-segmentation, particularly in cloud environments. This technique involves separating computing tasks into distinct, isolated environments to ensure that a compromise in one workload does not affect others. Workload isolation can be achieved through containerization, virtual machines, and network- level isolation (Mavridis & Karatza, 2018). This separation enhances security by limiting the "blast radius" of any potential breaches, preventing them from spreading across the entire network. Moreover, it can improve performance by dedicating specific resources to each workload, optimising resource allocation. In addition to bolstering security and performance, workload isolation simplifies compliance by clearly defining boundaries between different data sets and processing activities, which is crucial for meeting regulatory requirements.

Key Pillars of Modern System Design and Integration

Scalability

Scalability refers to a system's capacity to handle increasing demand effectively while maintaining performance standards. In cloud computing, scalability allows systems to dynamically allocate and deallocate resources based on usage fluctuations, ensuring both efficiency and reliability during periods of peak demand. As organizations grow, scaling systems without compromising performance become crucial. This characteristic enables businesses to accommodate growth while maintaining operational efficiency, preventing bottlenecks, and ensuring seamless user experiences. For instance, cloud infrastructure providers

like Amazon Web Services (AWS) and Microsoft Azure offer elasticity, allowing businesses to scale up resources during high-demand periods and down during low-demand periods, optimizing costs and performance (Estrach, 2023).

Interoperability

Interoperability is the ability of different systems, applications, or software to exchange and utilize information seamlessly. This capability is particularly important in industries such as healthcare, where interoperability allows disparate systems, such as electronic health records (EHRs), to share patient data securely and efficiently. Successful data exchange between various systems relies on syntactic and semantic compatibility. Syntactic compatibility ensures that data formats are standardised, while semantic compatibility ensures that data exchanged is interpreted correctly. For instance, in the healthcare sector, interoperability facilitates improved care coordination and decision-making by allowing healthcare providers to access comprehensive patient histories across multiple systems (HealthIT.gov, 2022).

Legacy System Integration

Legacy system integration connects older, outdated systems with modern technologies, allowing organisations to evolve without completely abandoning their existing infrastructure. Legacy systems are often integral to business operations but may be incompatible with newer technologies. Techniques such as Application Programming Interfaces (APIs) and Enterprise Service Buses (ESBs) are often used to bridge the gap between legacy systems and newer applications. For example, in the banking industry, integrating legacy systems with mobile payment platforms can enhance customer experience without compromising the core functionalities of the bank's infrastructure. Legacy system integration allows organisations to modernise incrementally, providing a path forward that maximises the utility of existing investments while incorporating new capabilities (Christiano, 2023).

Computational Efficiency

Computational efficiency refers to optimizing algorithms and systems to minimise the use of computational resources, such as time, memory, and processing power. Artificial intelligence (AI) advances, particularly in developing more efficient neural networks, have significantly reduced the computational costs associated with processing large datasets. Modern machine learning models, such as deep learning networks, have become more efficient, requiring less computational power to achieve higher accuracy than earlier models. This optimisation of algorithms allows organisations to process large volumes of data quickly and efficiently, improving performance and reducing the overall energy consumption of data processing systems (Meng, 2024).

Standards Compliance

Standards compliance ensures systems adhere to established regulatory, ethical, and operational guidelines. Adhering to relevant standards fosters responsible practices and ensures systems operate within acceptable legal and ethical boundaries. For instance, frameworks such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) set strict data protection, privacy, and security guidelines, particularly in sectors like healthcare and finance. Compliance with these standards is essential for protecting sensitive data, maintaining privacy, and building stakeholder trust. Moreover, standards compliance helps mitigate legal risks, improve organisational reputation, and ensure that organisations operate transparently and responsibly (SentinelOne, 2024).

Empirical Studies

Kumar (2024) presents a critical comparative analysis of Zero Trust Architecture (ZTA) and traditional security frameworks within hybrid IT environments. The study uses simulation- based testing to investigate metrics such as attack surface reduction, policy enforcement latency, and integrating Identity and Access Management (IAM) solutions. The results show ZTA's efficacy, employing a 39% drop in lateral threat movement during penetration testing, hence, it shows its ability to restrict unauthorized hybrid system access. The study, however, points out several issues, such as a 12–15% delay rise linked to ongoing authentication procedures, which underline the need forr strong IAM integration for dynamic policy enforcement and identity verification. Although Kumar's study helps to clarify ZTA's performance, it casts doubt on its relevance in large-scale deployments and multi-cloud settings.

Furthermore, Salmiya et al. (2024) emphasizes

improving Zero Trust enforcement in Industrial Internet of Things (IIoT) networks using AI-driven micro-segmentation methods. The study combines deep non-symmetric autoencoders with k-Nearest Neighbors (k-NN) hypergraphs to extract traffic features and simulate complicated data interactions. Flexible microsegmentation is obtained using adaptive clustering techniques such as DBSCAN, OPTICS, Incremental K-Means, ART, and CluStream. Empirical simulations show the system's ability to find abnormalities with 91.2% accuracy and lower lateral intrusion attempts by 67%. Although the study emphasises the changing power of including machine learning in security protocols, unresolved issues such as computing overhead, implementation feasibility, and scalability in resource-constrained settings call for more investigation.

By compiling data from 18 case studies on Zero Trust implementation across IoT systems, Roy et al. (2024) provide a meta-analytical viewpoint on important security metrics, including breach detection time, access violation frequency, and data exfiltration rates. Results demonstrate a 43% increase in breach detection time and a 60% drop in data exfiltration incidents compared to conventional models, confirming the efficacy of Zero Trust ideas and micro-segmentation. Practical issues remain, including legacy system incompatibility and slowness caused by multi-factor authentication procedures. The lack of thorough plans for overcoming these obstacles draws attention to an empirical gap that future studies must fill to allow smooth Zero Trust deployment in many IoT networks.

Meanwhile, Basta et al. (2021) tackles the lack of quantitative evaluation frameworks for micro-segmentation within Zero Trust systems. The study introduces a structured methodology for assessing exposure and robustness metrics post-deployment by combining network connectivity graphs and attack graphs. Experimental findings reveal substantial reductions in network exposure, ranging from 60% to 90%, alongside notable improvements

in security robustness across simulated enterprise networks. While the framework serves as a replicable tool for empirical validation, its applicability in real-time, dynamic network scenarios, particularly multi-tenant environments, remains an area requiring further development.

Additionally, Bondhala (2025) examines the integration of Zero Trust, Network Segmentation, and Micro-Segmentation as a comprehensive defence strategy across critical sectors, including healthcare, government, and industrial environments. Using cross-industry data from 50 documented security incidents, the study demonstrates improvements in breach costs (42% reduction), threat detection time (57% improvement), and containment efficiency (68% enhancement). Recommendations focus on leveraging artificial intelligence and automation to address legacy system compatibility and policy complexity challenges. While Bondhala's findings emphasise the efficacy of this integrated strategy, additional research is needed to develop scalable solutions for cross-sector implementation challenges.

Although, Sheikh et al. (2021) investigate a cloud-native micro-segmentation framework tailored for Zero Trust implementations in dynamic cloud environments. By examining port and protocol metadata, the framework enables real-time policy enforcement based on workload behaviors. Empirical results show enhanced containment and reduced unauthorised inter-service communications, validating the framework's adaptability to cloud-native workloads. However, Sheikh et al. note that cross-cloud interoperability and federated identity systems remain unexplored, presenting a critical gap in achieving scalable Zero Trust principles across diverse cloud platforms.

Denzel and Ng’etich (2025) synthesise findings on Zero Trust Network Architecture (ZTNA) components, including the least privilege access, contextual authentication, and identity- based segmentation. The survey highlights integrating emerging technologies like blockchain, artificial intelligence, and Secure Access Service Edge (SASE) into Zero Trust systems to enhance security. While the study provides valuable insights into the effectiveness of ZTNA components, limitations related to scalability in multi-tenant environments and dynamic policy orchestration persist, necessitating further empirical research to address these challenges.

However, Arora and Hastings (2024) explore Zero Trust and micro-segmentation in multi- cloud environments, leveraging open-source tools for secure connectivity across

Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) domains. Findings highlight improved

segmentation flexibility and vendor neutrality, addressing operational silos and insecure inter-service communication. While the study offers tested solutions to real-world challenges, hybrid strategies combining proprietary and open-source tools may further enhance deployment agility and security outcomes in multi-cloud ecosystems.

Liu et al. (2024) introduce the Large Language Model Enhanced Graph Diffusion (LEGD) algorithm, which uses hierarchical graph-based trust modelling for optimized micro- segmentation in Next-Generation Networks (NGNs). The algorithm achieves over 90% efficiency in segmentation and reduces service outages by more than 50%, highlighting the potential of AI-driven optimization for Zero-Trust architectures. However, reliance on advanced computational resources and lack of validation across diverse operational scenarios suggest areas for further improvement and exploration.

Dhiman et al. (2024) provides a comprehensive survey of Zero Trust principles, focusing on their application in contemporary network security. Their review identifies key components, including authentication, access control, encryption, and automation, all of which are integral to enforcing secure access and mitigating internal and external threats. Micro-segmentation emerges as a pivotal mechanism in their analysis, enabling networks to be subdivided into smaller, tightly controlled zones that facilitate stricter access controls and granular monitoring of user behaviourr and traffic patterns. Additionally, the authors introduce a taxonomy of Zero Trust features, offering a structured framework for categorising strategies and tools within this model. This holistic examination supports theoretical understanding and practical deployment of Zero Trust principles, particularly within critical infrastructures.

Ahn and Shin (2024) propose the integration of Zero Trust with the MITRE ATTACK matrix, which achieves a constructive collaboration between proactive threat modelling and reactive defence mechanisms, thereby advancing the field. Their work underlines how micro-segmentation isolates hostile actions, restricting lateral movement inside internal systems. Aligning Zero Trust frameworks with ATTACK strategy helps companies to improve visibility and control over network entities and gain an advantage from real-time threat indicators and detection techniques. This study emphasizes the need to integrate various approaches to improve organisational cyber resilience and offer practical measures for efficient execution.

Conversely, Singh (2024) introduces the "Zenith Armourr" framework, which operationalises Zero Trust principles across multi-device environments. The framework integrates micro- segmentation with dynamic access control, encryption, and incident response mechanisms. It incorporates adaptive risk assessments and real-time monitoring to adjust privileges and policies based on user behaviour and contextual factors. Singh highlights the critical role of micro-segmentation in limiting lateral threat movements, which is often overlooked as a vulnerability in traditional perimeter-based models. By embedding these principles deeply into network architecture, Zenith Armourr offers a scalable and practical approach to safeguarding digital assets in increasingly dynamic environments.

Ahmadi (2024) explores the applicability of Zero Trust within cloud environments, addressing challenges such as insider threats, lateral movement, and identity mismanagement. Through systematic reviews and case studies, the research identifies micro-segmentation as a key tool for isolating workloads and enforcing least-privilege access. Additionally, Ahmadi demonstrates how integrating machine learning and artificial intelligence can enhance automation and predictive threat analysis within Zero Trust frameworks. While Zero Trust is still maturing in cloud ecosystems, the study reveals clear improvements in incident response and access governance, highlighting its potential to transform cloud security practices.

Bishukarma (2023) investigates the scalability of Zero Trust frameworks in multi-cloud Software-as-a-Service (SaaS) ecosystems. The study emphasises the importance of integrating micro-segmentation with real-time threat detection and Identity and Access Management (IAM) systems to enable fine-grained controls across distributed systems. By decoupling trust decisions from location or static credentials, Bishukarma demonstrates how Zero Trust can enhance security and compliance in hybrid cloud architectures while maintaining operational agility. The findings underline the importance of continuous authentication and dynamic policy enforcement in achieving scalable and effective security solutions.

Hasan (2024) delivers a sector-based analysis of Zero Trust adoption, focusing on finance, technology, and healthcare industries. The study identifies IAM and micro-segmentation as foundational components for mitigating insider threats and lateral movement. Empirical case studies reveal that Zero Trust improves threat containment and reduces unauthorised access. However, Hasan acknowledges the practical challenges associated with implementation, including complexity, costs, and policy orchestration difficulties. Emerging technologies, such as AI, machine learning, and blockchain, are proposed as future enablers to address these hurdles and enhance Zero Trust adoption across industries.

Moreover, Ahmed et al. (2025) push the boundaries of Zero Trust by proposing a Quantum Neural Network-Enhanced Zero Trust Framework (QNN-ZTF) tailored for 7G networks. This innovative architecture integrates Quantum Neural Networks (QNNs) with ZTA principles such as dynamic anomaly detection, continuous policy adaptation, and quantum micro-segmentation. The framework significantly enhances scalability and detection accuracy while reducing false positives and response times by leveraging quantum properties like entanglement and superposition. This research demonstrates a futuristic application of Zero Trust in ultra-low latency environments, addressing the cybersecurity demands of next- generation networks.

Manzano et al. (2024) adopt a novel perspective by mapping Zero Trust systems' quality attributes (QAs) against the ISO/IEC 25010 quality model. Using their methodical review, they find 17 QAs—including security, performance, resilience, and scalability—and observe that just eight are now covered in the ISO standard. This disparity emphasises the inadequacies of current software quality standards in handling the architectural complexity that Zero Trust systems provide. Their study provides insightful analysis for consistent implementation in actual settings by matching ZTA security objectives with more general system performance requirements.

Prydybaylo (2024) focuses on the core logical architecture of Zero Trust, including components such as the Policy Decision Point (PDP), Policy Enforcement Point (PEP), and Policy Administrator. The study emphasises identity verification, least privilege principles, no implicit trust, and data encryption at rest and in transit. Special attention is given to micro-segmentation as a logical and network-based strategy for isolating workloads and controlling traffic granularity. By examining ZTA-aligned workflows tailored for containerised environments, the paper provides practical insights into implementing Zero Trust in dynamic cloud and DevOps scenarios.

However, Jimmy (2022) strategically evaluates Zero Trust adoption in modern enterprises. Key components, such as micro-segmentation, IAM, Multi-Factor Authentication (MFA), and continuous monitoring, are essential for minimizing insider threats and lateral movement. A notable contribution of this study is its cost-benefit analysis, which quantitatively compares Zero Trust with traditional security architectures over five years. Metrics such as access attempt success rate and threat dwell time are proposed as indicators of ZTA effectiveness. The study notes barriers such as user experience degradation, legacy system limitations, and integration overhead despite its advantages.

Rocha and Sousa (2021) examine Zero Trust's effectiveness in preventing Advanced Persistent Threats (APTs) in IoT ecosystems. By integrating Next-Generation Firewalls (NGFWs) with micro-segmentation, the proposed model enhances control over east-west traffic and isolates vulnerable endpoints. The study demonstrates how Zero Trust can limit lateral movement by persistent adversaries, reducing the potential impact of espionage and breaches in IoT-heavy infrastructures. Their work highlights the importance of ZTA in securing highly vulnerable IoT environments.

Methodology

This study utilises a systematic literature review to explore how Zero Trust Architecture (ZTA) and micro-segmentation can strengthen network security. This approach involves identifying and selecting relevant studies, followed by a comparative analysis of their findings, to discern key themes, identify research gaps, and synthesise current knowledge in the field.

Results and Discussion

The results indicate that traditional perimeter-based security models, often called the "castle and moat" approach, are no longer sufficient to address the complex and evolving nature of cyber threats. This approach inherently assumes that entities within the

network are trustworthy. However, studies highlight significant vulnerabilities in this assumption, particularly as cloud computing, remote work, and mobile device usage dissolve traditional network perimeters. Jones et al. (2023) describe this phenomenon as "perimeter erosion", emphasising how the rigid boundaries of traditional security models fail to account for the fluidity of modern network environments. Moreover, Verizon (2022) claims that a significant percentage of violations include insider participants, undermining internal confidence. Cybersecurity Ventures (2021) emphasizes the failure of perimeter-based technologies to combat sophisticated threats such as supply chain attacks or ransomware. These results imply that conventional security models are outdated and require more dynamic systems like Zero Trust.

The study establishes ZTA, anchored in its "never trust, always verify" principle, and micro- segmentation as superior paradigms for cybersecurity. ZTA eliminates implicit trust, requiring continuous verification of every user and device within the network. Dhiman et al. (2024) and Gambo & Almulhem (2025) advocate for ZTA, describing its adaptability to diverse threat scenarios, including hybrid and cloud-based infrastructures. Concurrently, micro-segmentation enhances security by dividing the network into isolated segments, thereby minimising the potential impact of a breach. Vasconcelos (2025) demonstrates how micro-segmentation limits lateral movement within compromised networks, further strengthening organisational defences. These findings build directly on the inadequacies of perimeter-based security models and illustrate how these advanced paradigms address modern cybersecurity challenges.

A key advantage of ZTA lies in its ability to mitigate vulnerabilities arising from insider threats and compromised credentials, which often bypass traditional defences. Continuous monitoring, real-time authentication, and rigorous verification processes form the backbone of ZTA, ensuring that no internal or external entity operates without scrutiny. Rose and Srinivasan (2020) emphasise that these mechanisms counteract the implicit trust assumptions exploited by malicious insiders or attackers using stolen credentials. Kumar (2024) provides compelling empirical data illustrating how ZTA adoption significantly reduces lateral threat movement in hybrid environments. This finding reinforces the argument for ZTA's efficacy in proactively addressing some of the most persistent challenges in cybersecurity.

Micro-segmentation emerges as a critical mechanism within Zero Trust, focusing on minimizing the attack surface by isolating network segments. Vasconcelos (2025) and Srikanth (2020) describe how this approach limits the spread of security incidents, containing breaches to individual segments. This segmentation reduces the complexity of detecting and responding to attacks. In cloud environments, where threats can propagate rapidly, micro- segmentation provides an essential containment layer. Sheikh et al. (2021) further validates its utility through case studies in cloud-native architectures, emphasising its role in safeguarding sensitive data and critical applications.

Despite its advantages, the scalability of Zero Trust in complex environments poses a significant challenge. As cloud adoption accelerates, organisations increasingly operate across multi-cloud and multi-tenant architectures, complicating the consistent enforcement of ZTA principles. Gambo & Almulhem (2025) identify gaps in scalability, noting that large, distributed systems often struggle with the uniform application of Zero Trust. Similarly, Denzel and Ng'etich (2025) highlight technical and operational limitations in multi-tenant environments, where resource sharing can introduce security blind spots. These challenges underline the importance of developing scalable solutions that balance Zero Trust's benefits with practical deployment needs.

Legacy infrastructure poses a substantial obstacle to Zero Trust implementation. Many older systems lack the architectural flexibility and technological compatibility required for ZTA. Roy et al. (2024) and Bondhala (2025) document the difficulties organisations face in retrofitting Zero Trust principles into legacy frameworks, which were designed with less dynamic threat landscapes in mind. Vasconcelos (2025) adds that legacy systems often hinder development by demanding major reconfiguration or replacement to fit ZTA criteria. This result emphasises the requirement of plans to close the gap between older systems and innovative security ideas.

Emerging technologies like AI-driven micro-segmentation and language model-based access control mechanisms offer promising advancements in Zero Trust. These tools provide dynamic and context-aware

decision-making capabilities, enhancing overall security. Selciya et al. (2024) and Liu et al. (2024) highlight their potential, citing improved breach containment and adaptive access control examples. However, they also caution against the computational demands these approaches introduce, which can strain resources in environments with limited hardware or bandwidth. Balancing innovation with efficiency will be crucial for the sustainable implementation of these technologies.

The shift to multi-cloud strategies exacerbates interoperability issues in Zero Trust adoption. Sheikh et al. (2021) and Arora & Hastings (2024) identify discrepancies in cloud provider APIs, standards, and security frameworks as significant barriers. These inconsistencies hinder the seamless implementation of Zero Trust policies across diverse platforms, reducing efficiency and increasing operational complexity. Addressing these interoperability challenges will be critical to maintaining robust security as cloud ecosystems grow more interconnected.

A notable limitation in current Zero Trust research is the reliance on simulated environments for validation. While simulations offer valuable insights, they do not capture the nuances of real-world applications. Basta et al. (2021) emphasise the need for empirical studies to bridge this gap, advocating for field tests that account for practical constraints like budget, personnel, and infrastructure. Hasan (2024) and Jimmy (2022) echo these concerns, urging researchers to prioritise real-world scenarios to validate theoretical frameworks.

The absence of standardised evaluation frameworks for Zero Trust solutions creates challenges in assessing their effectiveness. Manzano et al. (2024) argue that aligning ZTA capabilities with established compliance benchmarks, such as ISO/IEC standards, is essential for widespread adoption. A unified framework would enhance interoperability and provide a consistent basis for measuring performance, quality, and return on investment, ensuring that organisations can make informed decisions about their security strategies.

Recommendations

Organisations should move from perimeter-based models to Zero-Trust Architecture (ZTA) in steps, starting with network audits and stakeholder training. High-risk assets should receive the most attention, and identity and access management (IAM) and continuous authentication mechanisms should facilitate gradual deployment.

Micro-segmentation should be used to separate important resources and make it harder for attackers to move about. Security regulations should be specific to each group, backed up by AI-driven automation, and checked routinely through penetration testing.

To protect against internal threats, businesses should use behavioural monitoring technologies, impose multi-factor authentication (MFA), and follow the concept of least privilege. Setting up clear rules for responding to incidents can make the organisation even more resilient.

Companies that use more than one cloud or a mix of clouds should use cloud-native Zero Trust solutions, make sure that rules are the same on all platforms, and work with vendors to make APIs more compatible and enforcement easier across platforms.

International standards like ISO/IEC should align with Zero Trust and micro-segmentation frameworks. Anything that works in the real world, follows the rules, and can adapt to new dangers needs to be tested in a variety of fields.

Conclusion

This study looked closely at the problems with traditional perimeter-based security models and showed how Zero Trust Architecture (ZTA) and micro-segmentation might help protect against modern cybersecurity threats. It talked about the practical benefits of ZTA, like making it harder for attackers to get in and easier to contain breaches, as well as the main problems with scalability, legacy integration, and cloud interoperability. The research adds to the ongoing discussion about modern security frameworks by combining theoretical ideas with new empirical evidence. It also suggests a ZTA-based model that is customisable and aligned with standards for complex, multi-cloud systems. Future research should look into how to use AI-enhanced Zero Trust systems in places where resources are limited, develop universal compliance standards, and test these frameworks in high-risk areas to make sure they perform in the real world and are more resilient.

References

1. Ahmadi , S. (2024). Zero Trust Architecture in Cloud Networks: Application, Challenges and Future

Opportunities.Journal of Engineering Research and Reports, 26(2), 215–228. https://doi.org/10.9734/jerr/2024/v26i21083

2. Ahmed, S., Shihab, I., & Khokhar, A. (2025). Quantum-driven Zero Trust Framework with Dynamic Anomaly Detection in 7G Technology: A Neural Network Approach. https://doi.org/10.48550/arXiv.2502.07779

3. Ahn, G. Jang, J. Choi S. and Shin, D. "Researchon Improving Cyber Resilience by Integrating the Zero Trust Security Model With the MITRE ATT&CK Matrix," in IEEE Access, vol. 12, pp. 89291-89309, 2024, doi: 10.1109/ACCESS.2024.3417182.

4. Arora A. Hastings A. (2024). Microsegmented Cloud Network Architecture Using Open- Source Tools for a Zero Trust Foundation. International Conference on Security of Information and Networks.

5. Basta, N., Ikram, M., Kaafar, M. A., & Walker, A. (2021). Towards a Zero-Trust Micro- segmentation Network Security Strategy: An Evaluation Framework. Retrieved from arXiv.org.

6. Bishukarma, R. (2023). Scalable Zero-Trust Architectures for Enhancing Security in Multi- Cloud SaaS Platforms. International Journal of Advanced Research in Science, Communication and Technology.

7. Bondhala, S. (2025). Modern Defence Paradigms: Zero Trust Architecture, Network Segmentation, and Micro-Segmentation. International Journal of Scientific Research in Computer Science Engineering and Information Technology, 11(2), 2230-2239. https://doi.org/10.32628/CSEIT25112714

8. Bouchrika, I. (2025, March 12). What is empirical research? Definition, types & samples for 2025. Research.com.

9. Christiano, P. (2023, November 4). Legacy system integration in 2025: Top 4 methods, pros & cons. ExpertBeacon.

10. CrowdStrike. (2025). What is threat detection and response (TDR)??

11. Cybersecurity Ventures. (2021). 2021 Ransomware Landscape. Available at https://cybersecurityventures.com.

12. Deeter, M., & Friedman, G. (2021). Network Security Models in Transition. Cybersecurity Review.

13. Denzel, K., & Ng'etich, S. (2025). A survey of security in zero trust network architectures. GSC Advanced Research and Reviews, 22(2), 0036. https://doi.org/10.30574/gscarr.2025.22.2.0036

14. Dhiman, P., Saini, N., Gulzar, Y., Turaev, S., Kaur, A., Nisa, K. U., & Hamid, Y. (2023). A Review and Comparative Analysis of Relevant Approaches of the ZeroZero Trust Network Model. Sensors, 24(4), 1328. https://doi.org/10.3390/s24041328

15. Estrach, P. (2023, August 18). Scalability in cloud computing: A deep dive. MEGA. Fortinet. (2025). What is an attack surface? Definition and how to reduce it.

16. Gambo, M. L., & Almulhem, A. (2025). Zero Trust Architecture: A Systematic Literature Review. Retrieved from arXiv.org.

17. Ghasemshirazi, S., Shirvani, G., & Alipour, M. A. (2023). Zero Trust: Applications, Challenges, and Opportunities. Retrieved from arXiv.org.

18. Harvard Business Review. (2020). Building organisational resilience.

19. Hasan, M. (2024). Enhancing Enterprise Security with Zero Trust Architecture. Retrieved from arXiv:2410.18291

20. HealthIT.gov. (2022, August 5, 2022. Interoperability.

21. Jimmy, F. N. U. (2024). Zero Trust Security: Reimagining Cyber Defence for Modern Organisations. International Journal of Scientific Research and Management (IJSRM), 10(4), 887-905. https://doi.org/10.18535/ijsrm/v10i4.ec11

22. Jones, T., Anderson, R., & Black, L. (2023). Erosion of the Network Perimeter: Challenges in Modern Security. Journal of Cyber Defence.

23. Khan, J. (2024). Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) (pp. 113-126). https://doi.org/10.4018/979-8-3693-1431-9.ch005

24. Kumar, R. (2024). An Extensive Analysis of Zero Trust Architecture. International Journal of Innovative Science and Research Technology, 9(5), 1056. 1 https://doi.org/10.38124/ijisrt/IJISRT24MAY1225

25. Li, D., Yang, Z., Yu, S., Duan, M., & Yang, S. (2024). A Micro-Segmentation Method Based on VLAN-VxLAN Mapping Technology. Future Internet, 16(9), 320. https://doi.org/10.3390/fi16090320

26. Liu, Y., Liu, G., Du, H., Niyato, D., Kang, J., Xiong, Z., Kim, D. I., & Shen, X. (2024). Hierarchical Micro-Segmentations for Zero-Trust Services via Large Language Model (LLM)-enhanced Graph Diffusion. https://doi.org/10.48550/arXiv.2406.13964

27. Manzano, C., Márquez, G., & Astudillo, H. (2024). Quality Attributes for Zero Trust Architecture-Based Systems. 2024 43rd International Conference of the Chilean Computer Science Society (SCCC), 1–11. https://doi.org/10.1109/SCCC63879.2024.10767657

28. Mavridis, I., & Karatza, H. (2018). Combining containers and virtual machines to enhance isolation and extend functionality in cloud computing. Future Generation Computer Systems, 94, 10.1016/j.future.2018.12.035

29. McKinsey. (2025). Building organisational resilience.

30. Meng, X. (2024, March 15). Optimisation of algorithmic efficiency in AI: Addressing computational complexity and scalability challenges. Applied and Computational Engineering, 45, 305-311.

31. Mujib, M., & Sari, R. (2020). Performance Evaluation of Data Centre Network with Network Micro-segmentation (pp. 27-32). https://doi.org/10.1109/ICITEE49829.2020.9271749

32. Networks360. (2025). Enhancing network security: A comprehensive guide.

33. Okta. (2024). What is an attack surface? (And how to reduce it).

34. Parde, N. (2022, May 17). Zero-trust architecture may hold the answer to cybersecurity insider threats. MIT News | Massachusetts Institute of Technology. https://news.mit.edu/2022/zero-trust-architecture-may-hold-answer-cybersecurity-insider-threats-0517

35. Prydybaylo, O. (2024). Zero trust architecture, logical components, and implementation approaches. Connectivity, 169. https://doi.org/10.31673/2412-9070.2024.

36. ds, J., & Smith, A. (2024). Effectiveness of Continuous Verification and Micro-Segmentation in Enhancing Cybersecurity through Zero Trust Architecture.

37. Rocha, B., Melo, L., & de Sousa Junior, R. (2021). Preventing APT attacks on LAN networks with connected IoT devices using a zero-trust-based security model (pp. 1-6). https://doi.org/10.1109/WCNPS53648.2021.9626270

38. Rose, S., & Srinivasan, R. (2020). Zero Trust Architecture and Its Applications. IEEE Journal of Secure Computing.

39. Roy, A., Dhar, A., & Sarker Tinny, S. (2024). Strengthening IoT Cybersecurity with Zero Trust Architecture: A Comprehensive Review. Journal of Computer Science and Information Technology, 1, 25. https://doi.org/10.61424/jcsit

40. Saltzer, J. H., & Schroeder, M. D. (1975). The Protection of Information in Computer Systems. Proceedings of the IEEE.

41. Selciya, G.., Zerubbabel, I.Kannan, K. & Ezhilarasie,, R. (2024). Enhancing IIoT Security using KNN-based Hypergraph Clustering through Zero Trust Micro-Segmentation for Dynamic Network Protection (pp.1-6). https://doi.org/10.1109/CINS63881.2024.10864440

42. SentinelOne. (2024). What is threat detection and response (TDR)??

43. SentinelOne. (2024, October 29). What is data compliance? Standards and regulations.

44. Sheikh, N., Pawar, M., & Lawrence, V. (2021). Zero trust using Network Micro Segmentation (pp. 1-6). https://doi.org/10.1109/INFOCOMWKSHPS51825.2021.9484645

45. Singh, J. (2024). Zenith Armour: Advancing Security with Zero Trust Measures. International Journal of Scientific Research in Engineering and Management, 8(04), 1-5. https://doi.org/10.55041/IJSREM31326

46. Singh, P., & Kaur, H. (2020). A Comparative Study of Perimeter-Based Security Models. International

Journal of Network Security.

47. Srikanth, B. (2020). Network Segmentation and Microsegmentation: Reducing Attack Surfaces in Modern Enterprise Security. International Journal of Innovative Research in Computer and Communication Engineering, 8(6), 2499-2507.

48. Stallings, W., & Brown, L. (2018). Network Security Essentials. Pearson Education.

49. Vasconcelos, A. (2025, February 25). Microsegmentation: How Microsegmentation Works: Benefits, Challenges, and Built-in Zero Trust. ero Networks. https://zeronetworks.com/blog/how-microsegmentation-works-benefits-challenges-zero-trust

50. Verizon. (2022). Data Breach Investigations Report. Verizon Cybersecurity Research. Zenarmor. (2025). What are the ways to improve network security?