Zero Trust for Remote Workforce: Enhancing Security in Evolving Environments

Desmond Pang2, b), Siew-Chin Chong1, 2, a), Lee-Ying Chong1, 2, c) and Kuok-Kwee Wee1, 2, d)

*1Centre for Advanced Analytics, CoE for Artificial Intelligence, Multimedia University, Jalan Ayer Keroh Lama, 75450 Melaka, Malaysia.*

*2Faculty of Information Science & Technology, Multimedia University, Jalan Ayer Keroh Lama, 75450 Melaka, Malaysia.*

*a) Corresponding author:* [*chong.siew.chin@mmu.edu.my*](mailto:chong.siew.chin@mmu.edu.my)

*b) 1211103038@student.mmu.edu.my*

*c) lychong@mmu.edu.my*

*d) wee.kuok.kwee@mmu.edu.my*

**Abstract.** The increase in the popularity of remote and hybrid working modes has posed severe security issues. Perimeter-based enterprise security models founded on implicit trust and pre-determined access controls fail to deal with present day cyber threats, such as insider attacks, lateral movements, and Advanced Persistent Threats (APTs). In order to alleviate those problems, Zero Trust Architecture (ZTA) has emerged as one of the most promising security frameworks that enforce continuous validation, least-privilege access, and micro-segmentation to protect distributed workforces. This research includes experimental investigation of ZTA within a simulated enterprise network to ascertain its performance in regard to security compared to the conventional perimeter-based security approaches. Three major security performance measures including probability of detection, false positive rate, and false negative rate are included in the analysis. The evaluation of these measures will enable this study to provide empirical data on how ZTA can enable the enhancement of cybersecurity depending on remote workforce configurations. The proposed model reinforces security with such features as persistent user and device authentication, restricting destructive lateral migrations across the network, and finally encryption of confidential information to prevent any breaches whatsoever. All these machinations amplify the detection of threats, reduce false positives and mitigate unprecedented attacks. The findings will be included in a systematic shift of the organizations to relocate out of the conventional security structures to a Zero Trust model having improved threat visibility and mitigation capabilities.

# Introduction

The remote and hybrid working modes are better in terms of flexibility but have created new security threats. Employees are using corporate systems at various points which means the systems are prone to a greater number of cyber threats. It is also added by the fact that cloud-based applications and remote working tools are widespread, which makes the traditional security model ineffective [1]. Munusamy and Khodadadi state that the transition to remote working after COVID-19 has accelerated cyber vulnerabilities, and conventional cybersecurity designs are no longer sufficient because they deploy fixed protection schemes [2].

Security models that are perimeter-based are susceptible to insider attacks, unauthenticated access, and sophisticated cyberattacks because they are founded on implicit trust and stationary access controls [3]. These models had been developed on the centralized office systems and have difficulty in adjusting to the dynamic and decentralized networks. Stiff security policies also restrict prompt actions against evolving threats, posing more risks of information breach. There are also operational concerns of organizations to maintain a scalable and context-aware security and achieve compliance.

Zero Trust Architecture (ZTA)overcomes these shortcomings through the implementation of continuous validation and least privilege access. Munusamy and Khodadadi emphasize that the attributes of cyber resilience, including readiness and resistance, are consistent with the adaptive security measures of ZTA [2]. In contrast to the traditional models, Zero Trust (ZT) requests mandatory authentication and authorization of each access request [4]. This study evaluates the performance of ZT in providing security to remote workforce environment through deployment of a simulated enterprise network and evaluation of detection probability, false positive rate and false negative rate.

This research aims at achieving three goals: to understand shortcomings of perimeter-based security, to apply and test a simulated ZT framework, and to design a guided migration plan. The findings provide organizations a procedural way of enhancing cybersecurity without losing operational adaptability.

# literature review

## Perimeter-Based Security Model

The perimeter based security model provides security to the enterprise networks through firewall, intrusion detection systems, intrusion prevention systems and virtual private networks [5]. It presumes that the main risk is external threats, and internal users can be trusted. This model was effective in the traditional office setup but does not work with the modern decentralized offices.

Perimeter defenses are incapable of stopping cyber threats like phishing, credential theft, and insider attacks, which can enable an attacker to move freely within a network [6]. The presence of static security policies also makes it hard to respond quickly to emergent threats. Due to the extension of enterprise infrastructure beyond fixed perimeters, perimeter-based security is ineffective anymore. In order to eliminate such challenges, organizations are moving to ZTA, which requires strong verification and granular access control.

## Zero Trust Architecture (ZTA)

ZTA eliminates implicit trust by requiring strict authentication and continuous monitoring for every access request. This approach mitigates risks associated with insider threats, lateral movement, and unauthorized access by enforcing granular security policies across the network [7]. According to Munusamy and Khodadadi, ZTA’s granular controls, such as micro-segmentation, enhance resistance by isolating network segments to prevent lateral movement [2].

ZT important security principles are multi-factor authentication, least privilege access, device trust, micro-segmentation, and data encryption [8]. With multi-factor authentication, identity checks are more secure, and the likelihood of stealing credentials is minimal. Least privilege access restricts users and devices to just the resources they require in their jobs, reducing the possible harm caused by intrusions. Device trust is how to make sure that endpoints accessing corporate resources are secure and compliant. Micro-segmentation is used to isolate workloads to reject horizontal movement, whereas encryption secures data both in transition and at rest.

By having ZT, there will be an improved threat detection mechanism within organizations, reduced false positives, and enhanced regulatory compliance. This security model is better suitied to the contemporary enterprises, which operate in remote and hybrid environments compared to the conventional perimeter-based security.

# Proposed methodology

This paper proposes a ZTA architecture to enhance security of remote workforce environment. The framework takes into consideration the fundamental concepts of security like identity verification, device trust, micro-segmentation, least privilege access, and encryption. These components work concurrently to strength access management, in addition to reducing cybersecurity risks.

The ZTA framework follows a systematic implementation approach that includes architectural design, workflow implementation, and flowchart diagram. The architectural design identifies security elements and functions. Integration and operation of security mechanisms are described by the workflow execution. Authentication, access control and continuous monitoring are visually demonstrated in the flowchart. Such a systematic procedure leads to the consistent enforcement of security policy at every entry point and helps to quickly identify the threats.

In contrast to the currently deployed ZTA solutions which are centred around a particular technology, this paradigm follows a modular, context-sensitive and adaptive security approach to suit remote workforces. It applies continuous verification, least privilege access and micro-segmentation to a scalable architecture. With the help of open-source instruments, it is both affordable and flexible without the need to replace the entire system [9]. Specific measures such as real time monitoring and granular control increase resilience to external and insider threats, offering a balanced solution towards security and operational efficiency.

## Design of the Zero Trust Architecture (ZTA)

The suggested ZTA deploys stringent access controls on all layers of the network to protect remote workforces. Several security tools are interconnected to undertake complementary roles:

* Keycloak performs identity and access management using authentication and multi-factor authentication [10].
* Wazuh unifies threat detection, log analysis, and incident response into an open-source SIEM that secures endpoints and infrastructure [11]. Tay et al. show that machine learning models improve threat detection accuracy, complementing Wazuh’s capabilities in securing remote environments [12].
* Micro-segmentation is simulated in GNS3 to limit the lateral movement and unauthorized accessibility [13].
* OpenSSL ensures secure communication through provision of SSL/TLS encryption, certificate management and cryptographic functions on various platforms [14].
* Snort can be used to offer threat detection services by inspecting the network traffic and alerting on intrusions [15]. Tay et al. demonstrate that machine learning, such as Random Forest with 99.35% accuracy, can enhance intrusion detection systems like Snort for identifying DDoS attacks [12].

All the components provide Zero Trust principles through identity verification, device security assessment, controlled movement, data encryption, and threat monitoring. The combination creates a coherent security system with minimal vulnerabilities and enhanced security of remote workforces.

## Workflow Execution

The ZTA framework follows a structured workflow to ensure seamless integration and effective security enforcement:

1. Initialization Phase – Predefined policies are applied to the security tools. Rules and policies for identity management, device trust, and network segmentation are configured to form a tight security base.
2. Integration Phase – Elements of security are integrated to work as a cohesive unit. Keycloak is used to manage authentication, Wazuh is used to provide device compliance and centralized monitoring, Snort is used to detect intrusions and GNS3 is used to impose network segmentation.
3. Simulation Phase – In GNS3, test scenarios are implemented to generate network traffic, user behavior and attacks vectors. These examinations evaluate how the system reacts to security risks and assist in showing where improvements are possible.
4. Optimization and Testing Phase – Security controls are tested through continuous improvement process. Weaknesses are identified, policies are adjusted and the framework is simplified to counter evolving threats.
5. Evaluation Phase – The performance of the ZTA framework is compared to the traditional security models to evaluate how much it helps to reduce the vulnerability and block the unauthorized access. During the process, Wazuh will capture and investigate security events, providing more visibility and facilitating quick incident response.

This workflow enables ZTA framework to provide strong security enforcement, monitoring, and responsive adaptive threats in remote workforce settings.

## Flowchart Representation

The ZTA workflow shown in Figure 1 enforces secure access and real-time monitoring. Upon authentication initiation by a user, Keycloak authenticates the identity based on policy, such as multi-factor authentication, and Wazuh records the event to the log for auditing. In the case of failed authentication, access is denied and the user can try again. Upon successful authentication, the access is granted and communications are encrypted using OpenSSL.

During the session, Snort will be used to monitor the network traffic and Wazuh will be used to monitor the user behavior to identify any anomalies. Ongoing trust assessment provides session termination and logging when an incident of policy violation is detected. Although GNS3 is operated in the design and testing processes to visualize the segmentation of networks, it does not operate in the real-time process. The operational framework emphasizes on implementation of security policies based on authentication, access control and monitoring. The ZTA framework supports a high level of cybersecurity in remote workers environments as it incorporates several security elements and enforced access controls, allowing high flexibility.

A diagram of a computer system

AI-generated content may be incorrect.

**FIGURE 1.** Workflow representation of the proposed Zero Trust Architecture (ZTA)

# Result and Discussion

## Performance Metrics

The proposed ZTA is analyzed through the effectiveness that is measured by three main security metrics: detection probability, false positive rate, and false negative rate. These measurements offer a numerical evaluation of the capacity of the system to distinguish threats, decrease false warnings and minimize attacks that are not detected [16].

Detection Probability as represented in Equation (1) is a measure of the capability of the system to accurately identify the malicious activities. The greater the probability of detection, the more formidable the threat detection and prevention.

(1)

False Positive Rate analyses the rate of legitimate actions which are incorrectly identified as threats. This may be determined through Equation (2). Reducing the false positive rate will minimize irrelevant alerts and enhance the efficiency of the security team.

(2)

False Negative Rate in Equation (3) assesses the likelihood of security threats going undetected. A lower false negative rate is a security benefit, as it will reduce the number of undetected cyberattacks.

(3)

A combination of these metrics will define the success of ZTA to increase threat detection, decrease false alarms, and provide a higher level of security.

## Benchmarking Against Traditional Security Models

In order to benchmark ZTA against the conventional perimeter-based security models, the three security metrics are used to compare them [16]. Table 1 shows the benchmarking comparison.

* Detection Probability: The traditional security models have a range of 85% to 96% whereas ZTA has a better range of 89% to 99% because of the feature of constant monitoring, real time analytics, and adaption of risk-based evaluation.
* False Positive Rate: Traditional security models have 18% to 20%, which results in too many false alarms. ZTA lowers this down to 1% to 2% with the help of context-aware security mechanisms and behavioural analytics, which improves operational efficiency.
* False Negative Rate: The false negative rate of traditional security models is up to 9.9%, whereas ZTA decreases it to 7.4% to10% due to the continuous access verification and micro-segmentation.

**TABLE 1.** Benchmarking comparison between perimeter-based security and ZTA

|  |  |  |  |
| --- | --- | --- | --- |
| **Performance Metric** | **Traditional Security**  **Model** | **Zero Trust Architecture**  **(ZTA)** | **Benchmark Significance** |
| Detection Probability | 85% to 96% | 89% to 99% | ZTA enhances threat detection which minimizes the chances of an undetected attack. |
| False Positive Rate | 18% to 20% | 1% to 2% | ZTA minimizes false positives, enhancing operational efficiency. |
| False Negative Rate | Up to 9.9% | 7.4% to 10% | ZTA lowers false negatives, providing better proactive threat mitigation. |

These findings underline the outstanding performance of ZTA in terms of all three metrics, proving its suitability to address the cybersecurity risks and adverse effects associated with the traditional security models.

# Conclusion

Remote and hybrid working models have brought enormous security challenges, and the previous perimeter-based security models are no longer effective. This study developed a ZTA framework as an enforcement of continuous authentication, least privilege access, micro-segmentation, and real-time security monitoring to enhance the security resilience without compromising operational flexibility. The evaluation outcomes indicated that ZTA can maximize the likelihood of identifying threats and reducing false alarms and missed attacks. Through benchmarking, it was reaffirmed that ZTA is always more effective than perimeter-based security models in the detection of both known and evolving threats. With continuous verification, adaptive access control, and proactive monitoring, ZTA significantly reduces security vulnerabilities and improves network resilience. Munusamy and Khodadadi affirm that adaptive security strategies, such as those employed in ZTA, strengthen organizational resilience against evolving cyber threats [2]. These findings emphasize the need for organizations to transition from static perimeter-based security to a more adaptive, intelligence-driven approach.

Although it has several benefits, ZTA must be implemented carefully, encompassing integrating security tools, enforcement of policies, and constant monitoring. Possible improvements that can be investigated in the future include threat detection based on artificial intelligence and automatic response mechanism [17]. By providing 99.35% accurate DDoS attack detection results, Tay et al. define that machine learning has a potential to enhance the threat detection capacities of ZTA [12]. Also, it would be beneficial to test ZTA in the conditions of real enterprise settings to gain more insights into its scalability and real-life adoption. This paper consists of a systematic review of ZTA as a cybersecurity model in remote worker settings. The results support the suitability of ZTA to overcome the contemporarily security risks besides providing safe and effective access control. In a more decentralized digital environment, organizations that aim to improve their security position are advised to consider ZTA as a means of protecting critical assets.

# Acknowledgement

This work is supported under the grant provided by the Malaysia’s Fundamental Research Grant Scheme

(FRGS/1/2023/ICT02/MMU/03/2, 2023).

# References

1. Kadechka, J. “The Impact of Remote Work on Security and Compliance.” 2024.
2. Munusamy, T., and T. Khodadi. “Building Cyber Resilience: Key Factors for Enhancing Organizational Cyber Security.” *Journal of Informatics and Web Engineering*, **2**(2), 59–71 (2023).
3. Houghton, S. “Zero Trust vs Traditional Perimeter Security: What’s the Difference?” 2024.
4. Tackley, K. “What is Zero Trust Architecture, and is it a must in your security?” 2024.
5. Mo, C. “The Perimeter Problem: Why Traditional Network Security Fails.” *Pomerium*, 2023.
6. Bernosky, D. “What You Can Do About Lateral Movement.” *BastionZero*, 2023.
7. Katz, E. “9 Benefits of Zero Trust Architecture.” *Spectral*, 2024.
8. Kochanik, M. “The Five Pillars of Zero Trust Security.” *NetFoundry*, 2024.
9. Krysik, A. “Benefits of Open-Source Software for Developers, Managers and Business.” *Stratoflow*, 2023.
10. Bayoglu, M. B. “What Is Keycloak? What Is Behind Of The Keycloak? How Does Keycloak Work?” *Medium*, 2024.
11. “Introduction to Wazuh.” *GeeksforGeeks*, 2022.
12. Tay, W.-W., S.-C. Chong, and L.-Y. Chong. “DDoS Attack Detection with Machine Learning.” *Journal of Informatics and Web Engineering*, **3**(3), 190–207 (2024).
13. Again, M. C. S. G. “Exploring the Power of GNS3: Simulating Networks for Ultimate Learning.” *Medium*, 2023.
14. C. T. C. S. I. P. Ltd. “OpenSSL.” *Medium*, 2023.