FROM STATIC TO ADAPTIVE: STRENGTHENING ZERO TRUST WITH CONTINUOUS ENDPOINT VERIFICATION FOR ORGANIZATIONS

Jared Quah Foo Zhun (TP074056)
TP074056@mail.apu.edu.my

ABSTRACT

Traditional perimeter-based security models have become utterly ineffective against newer and more sophisticated cyber threats, leading to the adoption of Zero Trust Architectures (ZTA). ZTA aims to improve security by enforcing continuous authentication and verification. Existing implementations often emphasize network-level controls and multi-factor authentication applied uniformly across all activities. However, as a result, organizations face challenges like performance bottlenecks and increased deployment costs. Furthermore, the lack of dynamic posture checks and reliance on static checks can be resource intensive when conducted continuously, making it difficult for organizations to sustain at larger scale. Hence, this proposal introduces an improved ZTA model that integrates adaptive endpoint verification to address and eliminate these limitations by combining continuous monitoring with context-aware capabilities, the proposed system seeks to ensure strong security with reduced performance overhead. Thus, contributing towards a practical, cost-conscious Zero Trust implementation for organizations.

KEY TERMS

Zero Trust, Perimeter-based Security, NIST SP 800-207, Advanced Malware, Fileless Malware, Continuous Endpoint Posture Verification, Multi-factor Authentication, Context-Aware

1. INTRODUCTION

Cybersecurity has become a critical element in an increasingly connected digital environment, where traditional perimeter-based defenses are no longer sufficient against evolving threats. Malware has adapted to exploit trusted systems and bypass conventional detection, making endpoint security a central challenge. As a result, Zero Trust architecture (ZTA) has emerged as the next generation of malware defense by discarding implicit trust and requiring continuous verification of users, devices, and applications. (Rose et al., 2020).

Emerging malware such as fileless or zero-click malware have made a name for itself by utilizing in-built operating system applications to exploit vulnerabilities and executing in memory (Side Liu, Guojun Peng, et al., 2024), making it difficult to trace. Typically, malware is stored as an .exe file and is loaded into memory from the hard drive. This results in marks of the assault on the disk. Enabling signature-based antivirus systems to identify it (Kara, 2022). However, recently attackers have been innovating and bypassing AV engine scanning via fileless attacks. These attacks do not save traces onto the disk. They are instead executed in memory or through OS system utilities like PowerShell and Windows Management Instrumentation (WMI), allowing them to blend in with normal processes. In many instances, this behavior is not flagged by traditional system security measures (Sudhakar & Kumar, 2020).

In response to the current limitations of traditional perimeter-based security models, Zero Trust challenges the outdated notion of implicit trust within a perimeter by following the principle of “Never trust, always verify.” (Gambo & Almulhem, 2025)

Access is granted based on continuous authentication and authorization, regardless of whether a user or device is inside or outside the organization’s network. (NIST, 2020) While Zero Trust models are widely deployed, most implementations emphasize identity verification and segmentation, whereas endpoint posture, continuous verification, and health checks remain less mature (Sensors, 2024).

This research focuses on Zero Trust Endpoint Verification as a strategy for adaptive malware defense, examining how it showcases resilience and adaptability against sophisticated attacks.

2. PROBLEM STATEMENT

Traditional perimeter-based security models and signature-driven antivirus systems are no longer sufficient to defend against modern malware threats. (Gambo & Almulhem, 2025). Emerging strains such as fileless and zero-click malware exploit legitimate system utilities and execute directly in memory, leaving minimal or no artifacts on disk (Sudhakar & Kumar, 2020; El-Sayed et al., 2023).

With perimeter-based models phasing out, Zero Trust architectures are starting to set the standard for security, with companies marking Zero Trust as a modern security solution, however, their implementation has primarily focused on network segmentation and identity verification, which ultimately gives limited attention given to continuous endpoint posture verification especially since current implementations remain immature (Yeoh et al., 2023) and organizations are reluctant to fully adopt it. (Itodo & Ozer, 2024). This creates a blind spot in which compromised devices can remain authenticated, as long access has been granted. (Rose et al., 2020). The lack of robust and real-time verification of endpoint security increases the risk of undetected intrusions, lateral movement, and persistent threats within organizations. (Rose et al., 2020). Addressing this flaw is essential to ensure that Zero Trust principles are properly incorporated to provide a more effective malware defense at an endpoint level.

As a result, with perimeter and signature-based security models, endpoint posture verification remains a weak point in malware defense, leaving gaps that sophisticated malware such as fileless or zero-click attacks can exploit. (William, Elijah, 2022). Without improved and adaptive endpoint verification mechanisms, organizations risk compromised security models and increased exposure and vulnerability to advanced threats. (Ahmadi, 2025)

3. RESEARCH AIM

To enhance endpoint security posture verification within Zero Trust architectures (ZTA) to strengthen organizational defenses against advanced malware attacks.

4. RESEARCH OBJECTIVES

- *To review current literature and existing implementations of Zero-Trust security models.*
- *To identify current limitations within both traditional perimeter-based and zero trust security posture implementations.*
- *To investigate and propose an enhanced endpoint posture verification system that combines Zero Trust principles with robust real-time security monitoring to reduce vulnerabilities exploited by malware including advanced ones without the cost of performance losses.*

5. RESEARCH QUESTIONS

1. *What challenges do organizations face when implementing Zero Trust security posture verification?*

2. *Which specific security posture attributes are most crucial for preventing malicious activity from infiltrating into an organization's network?*

3. *How can current implementations of Zero Trust endpoint security posture verification systems be improved to perform against newer and advanced malware threats?*

6. RESEARCH SIGNIFICANCE

This research is significant as it addresses the flaws and substandard performance of traditional perimeter-based security systems as well as underwhelming implementation of Zero Trust based security systems. This will contribute to the need to implement enhanced Zero Trust verification security posture and showcase its improvements over predecessors. As well as offering practical security solutions against evolving malware threats.

With remote work and BYOD (Bring Your Own Device) being increasingly adopted today, thereby increasing organizational risk. (Calias et al., 2024). This highlights the need for a more active and stronger security posture due to personal devices being potentially unsecured. (Calias et al., 2024). Hence, it is essential to explore enhanced Zero Trust endpoint posture verification as a core component of malware defense strategies.

In addition, academic literature consistently reports that many real-world Zero Trust implementations focus heavily on identity verification, segmentation, and least privilege access, but significantly under-utilize continuous device health verification and dynamic posture checks (Gambo & Almulhem, 2025; Oladimeji, 2024; Tabalipa, 2025). This underwhelming implementation of endpoint posture verification questions Zero Trust's effectiveness against advanced malware threats that operate without leaving left-over artifacts.

This research contributes to a clearer understanding of how Zero Trust can be better applied in endpoint protection and offers insights into the next step of organizational malware defense.

7. PROPOSED SYSTEM OVERVIEW

Zero Trust is widely seen as the next big step in cybersecurity, but research shows that putting it into practice is still messy and incomplete. However, many organizations do not fully understand or properly implement the model. (He et al., 2022). Even when it is adopted, companies run into problems like complexity, scalability, and performance issues. (Gambo and Almulhem, 2025). Whereas, in cloud environments, Zero Trust can slow systems down and require heavy investment to deploy. (Oladimeji, 2024) and (Cornelius Itodo, Murat Ozer, 2024) notes that existing research on Zero Trust implementation often has a narrow focus. For instance, some studies discuss only a few components of Zero Trust without providing guidance on how the other core components are a part of its implementation.

The new proposed system seeks to improve current implementations of both perimeter-based and underwhelming Zero Trust implementations by introducing continuous endpoint posture verification as an additional security layer for adaptability and flexibility when dealing with advanced malware threats. Which aims to improve current Zero Trust security implementations, by emphasizing more dynamic posture checks (Sudhakar & Kumar, 2020), this system will continuously evaluate the security posture of endpoints before and during access to critical resources. Ensuring a more rigorous, dynamic and adaptive security posture.

7.1 System Flow and Architecture

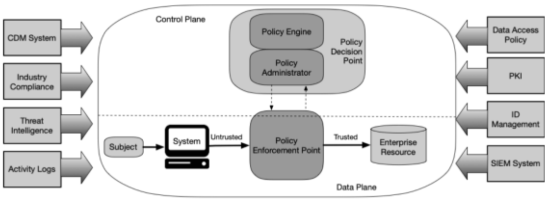

Figure 1 –NIST Zero Trust Security model (Rose et al., 2020)

A highly recognized Zero Trust model is the architecture defined in NIST SP 800-207 (Rose et al., 2020). The model in Figure 1 focuses on three main components, the Policy Engine (PE), which determines whether access should be granted or denied based on contextual input.

Then, the Policy Administrator (PA), executes these decisions by establishing or terminating communication sessions.

Finally, The Policy Enforcement Point (PEP), which sits between users and resources to enforce security controls. These components are supported by various data sources, such as Continuous Diagnostics and Mitigation (CDM) systems, threat intelligence feeds, compliance systems and identity management infrastructure. All of these provide the contextual awareness necessary to make informed trust decisions. Together, these elements ensure that all requests are evaluated continually before access is granted.

While this model provides a robust foundation, it also has its own set of limitations. Its reliance on central decision making can cause network latency, whereas constant posture checks can strain resources and MFA is often applied uniformly regardless of risk. To address these challenges, the proposed system builds on the NIST architecture but enhances it for efficiency and scalability.

Specifically, it introduces event-driven telemetry, policy decision caching, and risk-based MFA, allowing organizations to strengthen defenses while minimizing the performance and cost drawbacks that often hinder Zero Trust adoption. (Rose et al., 2020)

This tackles a significant vulnerability in current security frameworks, where device compromises following initial authentication frequently goes undetected. (Adahman et al., 2022)

7.2 Proposed System Diagram

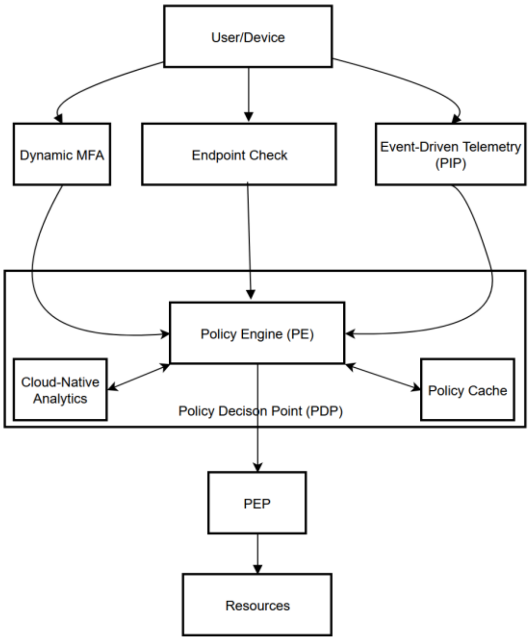

Figure 2 – Proposed Enhanced Zero Trust model.

The proposed system intends to improve the downsides of current zero trust implementations such as under-utilized continuous verification and negative performance impacts.

Hence, the addition of risk-adaptive trust engine in the Policy Decision Point (PDP). Instead of applying the same level of verification for every request, the system dynamically adjusts the depth of checks based on various factors such as device history, location and behavior. Basically, it uses the context-aware rules to help decide how much verification is needed. (N. F. Syed et al, 2022). For example, a user accessing the network from a familiar corporate laptop in the office might undergo lighter checks, while access attempts from an unknown or unusual device will trigger full security posture verification. This selective approach reduces resource use and latency while maintaining security for high-risk scenarios. (Kandula et al., 2024)

To further reduce performance hits, Policy Information Point (PIP) is optimized through lightweight, event-driven telemetry collection rather than continuous polling of endpoint health. Traditional posture checks such as antivirus status and firewall configuration can be resource intensive when done constantly. (Heino et al., 2022). Whereas in the proposed model, endpoint agents report only when changes occur, in situations where security software is disabled or a patch is missing. This lowers bandwidth use and endpoint strain all whilst ensuring that posture data is accurate and kept up to date.

Also, the system implements a tiered verification process for authentication and access control. Rather than implementing multi-factor authentication (MFA) and revalidation equally for all actions (Reddy, Kassetty, Alang & Pandey, 2024), verification is dynamically tailored to match the sensitivity of the resource being accessed. Low risk activities, such as accessing non-sensitive information, can utilize single sign-on (SSO), whereas high risk activities like retrieving financial information or altering system settings will require enhanced multi-factor authentication or behavioral confirmation. This strategy proposes enhancements in efficiency for end users while maintaining the security of important assets. In addition to this, it also intends to lower the chances of system compromises from advanced malware since it is able to make smarter and more dynamic decisions

Another performance improvement is the introduction of centralized policy caching with edge enforcement. In traditional Zero Trust models, every access request must be routed to the central Policy Administration Point (PAP) and Policy Decision Point (PDP) for evaluation which introduces latency and bottlenecks. By deploying local policy caches at edge nodes or cloud gateways. These caches can temporarily store policy decisions locally for recurring requests. When stored locally, it allows for easier and quicker access to policy decisions instead of having to always go through PAP and PDP evaluation, thereby reducing network overhead and response times while still ensuring compliance with central policies. (Eiza et al., 2025)

And finally, to balance scalability and cost, the proposed design seeks to incorporate cloud-native analytics for resource-intensive processing such as behavioral monitoring and anomaly detection. Complex computation tasks are offloaded to cloud platforms, while lightweight checks continue to run on-premises. This hybrid model will allow organizations to leverage advanced threat detection capabilities without overwhelming their local infrastructure. While traditional on-premises systems can handle basic posture verification tasks such as antivirus status checks or firewall validation, they often fall short when facing the computational demands of advanced analytics like anomaly detection or user behavior modeling. (Vargaftik et al., 2021). Running these workloads locally can strain enterprise servers, increase latency in decision making, and ultimately slow down the user experience. (Oladimeji, 2024). Cloud-native analytics addresses this issue by offering scalable computing power that increases or decreases dynamically depending on demand. This eliminates the need for requiring organizations to invest in costly hardware upgrades. In fact, hybrid models have been suggested as a way to minimize this cost, combining local enforcement with cloud-offloaded decision-making and caching mechanisms to reduce repeated computations (Eiza et al., 2025). Adding this hybrid approach seeks to further improve the efficiency and responsiveness of heavy computational tasks.

In Figure 2, the decision-making process is divided. Lightweight checks such as confirming whether a device has the latest security patches or whether a user’s credentials are valid are performed on-premises for speed and minimal resource consumption. In contrast, more demanding tasks like anomaly detection or large-scale behavior analysis are handled in the cloud. For example, logs and activity data from many devices can be sent to cloud-based security platforms (such as SIEMs or security data lakes), where more powerful detection models can process them more effectively.

This hybrid approach brings two big benefits. First, it prevents local infrastructure from being overloaded, which keeps the system responsive.

Secondly, it allows organizations to take advantage of the latest detection methods without needing to build them from scratch. Because cloud providers update their analytics tools frequently, organizations get access to cutting-edge threat detection automatically. (China & Goodwin, 2025). However, this approach also introduces new privacy considerations. Offloading data to the cloud raises questions about data privacy and regulatory compliance, especially in industries such as finance and healthcare where very sensitive data is often stored. Additionally, dependency on cloud connectivity could create potential bottlenecks if network availability is disrupted. To mitigate these risks, the design envisions caching essential decisions locally and encrypting sensitive data before it leaves the enterprise perimeter. This ensures that security verification continues seamlessly even in the event of cloud disruptions, while still gaining the scalability advantages of cloud-native analytics.

Together, these enhancements, risk-adaptive verification, event-driven telemetry, tiered Multi-factor Authentication (MFA), policy caching, and hybrid cloud processing can ultimately strengthen the security posture of the proposed system while mitigating certain challenges organizations may face such as performance loss, endpoint strain, and increased network latency.

8. CONCLUSION

This research addresses the limitations of traditional perimeter-based security models and highlights the urgent need for adaptive Zero Trust endpoint posture verification to fight against advanced malware. While existing implementations of Zero Trust provide improvements in identity verification and network segmentation, they often fall short in ensuring a continuous, efficient, and context-aware endpoint monitoring due to many organizations running into cost, performance and scalability issues. Thus, the proposed system introduces practical enhancements such as event-driven telemetry, risk-based multi-factor authentication, and policy caching. This combination seeks to collectively strengthen security while minimizing performance and cost overhead, thereby proposing a balanced model that improves organizational security and also cost-effectiveness.

9. REFERENCES

Gambo, M. L., & Almulhem, A. (2025, February 7). *Zero Trust Architecture: A Systematic Literature Review*. arXiv.org. https://arxiv.org/abs/2503.11659

Quan Shen, Yanming Shen, Endpoint security reinforcement via integrated zero-trust systems: A collaborative approach, Computers & Security, Volume 136, 2024, 103537, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2023.10353. (https://www.sciencedirect.com/science/article/pii/S0167404823004479)

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture*. https://doi.org/10.6028/nist.sp.800-207

William, Elijah. (2022). FROM PERIMETER DEFENSE TO ZERO TRUST: EVOLVING CYBERSECURITY

FOR A CHANGING WORLD. https://www.researchgate.net/publication/387170060_FROM_PERIMETER_DEFENSE_TO_ZERO_TRUST_EVOLVING_CYBERSECURITY_FOR_A_CHANGING_WORLD

Calias, S. E., Caoli, B., Padilla, R., Tum-En, J., Bacilio, K. C., Lyn, I., & Guaki, G. S. (2024, December 31). *The Impact of BYOD (Bring Your Own Device) on Network Security: A Literature review*. https://sajst.org/online/index.php/sajst/article/view/303?

Sudhakar, N., & Kumar, S. (2020). An emerging threat Fileless malware: a survey and research challenges. *Cybersecurity*, *3*(1). https://doi.org/10.1186/s42400-019-0043-x

Side Liu, Guojun Peng, Haitao Zeng, Jianming Fu, A survey on the evolution of fileless attacks and detection techniques, Computers & Security, Volume 137, 2024, 103653, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2023.103653

Cornelius Itodo, Murat Ozer, Multivocal literature review on zero-trust security implementation, Computers & Security, Volume 141, 2024, 103827, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2024.103827

Kara, I. (2022). Fileless malware threats: Recent advances, analysis approach through memory forensics and research challenges. *Expert Systems With Applications*, *214*, 119133. https://doi.org/10.1016/j.eswa.2022.119133

Oladimeji, G. (2024). A critical analysis of foundations, challenges and directions for zero trust security in cloud environments. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2411.06139

Heino, J., Hakkala, A., & Virtanen, S. (2022). Study of methods for endpoint aware inspection in a next generation firewall. *Cybersecurity*, *5*(1). https://doi.org/10.1186/s42400-022-00127-8

Ghasemshirazi, S., Shirvani, G., & Alipour, M. A. (2023, September 7). *Zero Trust: applications, challenges, and opportunities*. arXiv.org. https://arxiv.org/abs/2309.03582

Tabalipa, A. (2025, August 20). *Bridging the mobile trust gap: A zero trust framework for Consumer-Facing applications*. arXiv.org. https://arxiv.org/abs/2508.16662

Sudhakar, Kumar, S. An emerging threat Fileless malware: a survey and research challenges. *Cybersecur* **3**, 1 (2020). https://doi.org/10.1186/s42400-019-0043-x

Stamford, & Conn. (2024, April 22). *Gartner Survey Reveals 63% of Organizations Worldwide Have Implemented a Zero-Trust Strategy*. gartner.com. https://www.gartner.com/en/newsroom/press-releases/2024-04-22-gartner-survey-reveals-63-percent-of-organizations-worldwide-have-implemented-a-zero-trust-strategy

Lee, S., Huh, J.-H., & Woo, H. (2025). Security system design and verification for zero trust architecture. Electronics, 14(643). https://doi.org/10.3390/electronics14040643

Adahman, Z., Malik, A. W., & Anwar, Z. (2022). An analysis of zero-trust architecture and its cost-effectiveness for organizational security. *Computers & Security*, *122*, 102911. https://doi.org/10.1016/j.cose.2022.102911
N. F. Syed et al. (2022, May 12). *Zero Trust Architecture (ZTA): Comprehensive Survey*. ieeexplore.ieee.org. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9773102

lnaim, A.K. Adaptive
Zero Trust Policy Management Framework in 5G Networks. Mathematics 2025, 13, 1501. https://doi.org/10.3390/math13091501

Kandula, S. R., Kassetty, N., Alang, K. S., & Pandey, P. (2024). Context-Aware Multi-Factor Authentication in Zero Trust Architecture: Enhancing Security Through Adaptive Authentication. https://doi.org/10.21428/e90189c8.f525ef4

Eiza, M. H., Akwirry, B., Raschella, A., Mackay, M., & Maheshwari, M. K. (2025). A hybrid zero trust deployment model for securing O-RAN architecture in 6G networks. *Future Internet*, *17*(8), 372. https://doi.org/10.3390/fi17080372

The State of Zero Trust report 2025 | Tailscale. (n.d.). https://tailscale.com/resources/report/zero-trust-report-2025

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

Ahmadi, S. (2025, January 10). *Autonomous Identity-Based threat segmentation in zero trust architectures*. arXiv.org. https://arxiv.org/abs/2501.06281v1

Vargaftik, S., Keslassy, I., Orda, A., & Ben-Itzhak, Y. (2021). RADE: resource-efficient supervised anomaly detection using decision tree-based ensemble methods. *Machine Learning*, *110*(10), 2835–2866. https://doi.org/10.1007/s10994-021-06047-x

China, C. R., & Goodwin, M. (2025, September 2). IaaS PaaS SaaS. *IBM*. https://www.ibm.com/think/topics/iaas-paas-saas