EasyChair Preprint

№ 12200

Synergizing Security: Designing a Zero Trust Network Access Protocol in Patient Monitors

Ahmed Al Taheri Al Taheri, Abdulkarim Rashed,
Hamad Al Marzooqi and Hussam Al Hamadi

February 20, 2024

Synergizing Security: Designing a Zero Trust Network Access Protocol in Patient Monitors

Ahmad Al Taheri, Abdulkarim Rashed, Hamad Al Marzooqi, Hussam Al Hamadi

College of Engineering and IT

University of Dubai

Dubai, UAE

{S0000001240, S0000003899, S0000001355, Halhammadi}@ud.ac.ae

***Abstract*— This paper navigates the landscape of Zero Trust network security protocols, challenging conventional reliance on implicit trust within organizational networks. It specifically focuses on agent-based Zero Trust Network Access (ZTNA) solutions, redefining continuous monitoring, authentication, and compliance verification, particularly in healthcare devices like patient monitors. By delving into these agent-based solutions, this study scrutinizes their deployment across diverse domains. Through case studies and evaluations, it highlights the strengths, weaknesses, and amplified advantages of agent-based ZTNA adoption. These insights pave the way for future advancements, fortifying network security architectures to unparalleled resilience.**

Keywords—Zero Trust Security, Network Security Protocol, Cybersecurity Paradigm, Healthcare Devices, Trust Principles

I. Introduction

Network security has witnessed a dramatic evolution in response to increasingly sophisticated cyber threats, challenging traditional security models that rely on perimeter-based defenses and implicit trust [1]. The emergence of Zero Trust represents a fundamental shift, redefining network security by challenging inherent trust within networks and advocating for continuous verification of trustworthiness based on contextual factors. Now, with the integration of agent-based Zero Trust Network Access (ZTNA) solutions, the paradigm undergoes a further transformation.

Agent-based ZTNA solutions play a pivotal role in bolstering the Zero Trust framework by embedding continuous monitoring, authentication, and compliance verification capabilities within devices. This extends the concept beyond traditional models by facilitating real-time transmission of logs, enabling dynamic risk assessments and proactive security measures.

The primary objectives of this paper include exploring the core principles of Zero Trust, investigating the integration benefits of agent-based ZTNA solutions, analyzing their applications in healthcare devices, and conducting comparative evaluations. This comprehensive examination seeks to highlight not only the foundational concepts of Zero Trust but also the transformative impact of agent-based ZTNA in fortifying network security architectures.

Zero Trust, in its evolved state with agent-based solutions, transcends the limitations of conventional paradigms. These solutions mitigate lateral movement threats, enable real-time risk assessments through continuous log transmission, and foster secure connectivity across modern architectures like cloud-based and IoT networks [2].

II. Key Concepts and Principles of Zero Trust Security Model

The Zero Trust Security Model stands as a transformative approach, challenging conventional notions of implicit trust within organizational networks. This section delves into the foundational concepts, core principles, and recent enhancements, including the incorporation of agent-based Zero Trust Network Access (ZTNA) solutions.

A. Zero Trust Model Overview:

Zero Trust represents a fundamental departure from traditional security paradigms by challenging the long-held assumption of implicit trust within network perimeters. Recent advancements in the Zero Trust approach include the integration of ZTNA agents, which redefine trust establishment and enforcement. These agents are pivotal in ensuring a more dynamic, granular, and responsive security framework. Zero Trust architecture entails a holistic approach, mandating continuous authentication, authorization, and encryption across all network segments and devices, operating on the principle of 'never trust, always verify' [3].

B. Principles of ZT Protocol

Below are the principles of ZT protocol:

1) Networking in ZT Protocol

The introduction of ZTNA agents marks a significant stride in Zero Trust networking. These agents play a crucial role in ensuring secure and adaptive communication by continuously monitoring device behavior, enabling real-time risk assessment, and orchestrating adaptive responses [4]. They transcend the limitations of predefined protocols, promoting robust security through comprehensive log transmission.

2) Domain-specific Protocol

The incorporation of agent-based ZTNA solutions is particularly relevant in the context of hierarchical trust management, especially in scenarios involving Internet of Things (IoT) and Operational Technology (OT) networks [4]. These agents offer task capabilities across various operating systems and devices, establishing secure connections to the Central Network Access (CNA) server.

3) Principles of ZT Security Model

The Zero Trust model encompasses multiple foundational principles, including but not limited to:

- Trust in No One: The foundational principle asserts zero trust by default, meaning no user, device, or input is implicitly trusted. Continual trust verification occurs regardless of the entity's location or identity.
- Disappearing Parameters: In a cloud-centric environment with diverse insider threats, Zero Trust operates on the premise that traditional implicit trust zones have vanished. Parameters defining trust are dynamic and contextually assessed.
- Least Privilege Principle: Zero Trust adheres to the least privilege principle, restricting access to the minimum necessary for specific situations. Access is denied by default unless explicitly authorized.
- Dynamic Risk-based Policies: Contextual risk assessment is integral, enabling dynamic risk-based policies. Strict policy enforcement aligns with real-time risk evaluations.
- Authentication and Authorization Requirements: Strong authentication and authorization are mandatory for all resource access requests and network flows within the Zero Trust model.
- Log, Monitor, and Adapt Principle: Continuous traffic monitoring, status logging, input validation, and adaptive responses constitute this principle, ensuring constant vigilance and adaptability to evolving threats.
- Employee Defense in Depth: Zero Trust emphasizes securing devices and communications against adversaries by increasing the work factor for lateral movement, thereby reducing vulnerabilities.
- Full Life Cycle Approach: Integrated into the full life cycle of network design and operation, Zero Trust ensures continuous security considerations from inception to decommissioning.
- Confidentiality and Integrity by Default: Encrypting information communication, ensuring data at rest is encrypted, and maintaining data integrity are default practices within Zero Trust.
- Balancing Trade-offs: Zero Trust involves navigating trade-offs such as cost vs. benefits, security vs. usability, and proportionality of cost vs. mitigated risk, striking a balance in protocol adoption.
- Agent-Based ZTNA Solution: Addition of the agent-based ZTNA solution, providing real-time monitoring capabilities and log transmission to various security solutions and network monitoring platforms. This element enhances continuous compliance monitoring, fortifying the overall Zero Trust model with an additional layer of security.

III. Benefits of Zero Trust

Zero Trust architecture, bolstered by the integration of ZTNA agents, offers multifaceted advantages surpassing traditional security models. This section explores the enhanced benefits of Zero Trust principles enriched by agent-based network access solutions.

A. ZT Integration Benefits

The amalgamation of Zero Trust principles with ZTNA agents results in profound advantages for network security and operational efficiency [5]:

- Enhanced Security Posture: ZTNA agents contribute significantly to the continuous verification and stringent access controls within Zero Trust architecture. They bolster network security by enabling real-time monitoring of device behavior, reducing the attack surface, and mitigating lateral movement threats.
- Dynamic Risk Assessment: The incorporation of ZTNA agents facilitates real-time risk evaluations based on contextual factors. This adaptive approach allows organizations to dynamically adjust security policies and responses, proactively addressing evolving threat landscapes.
- Secure Connectivity in Modern Architectures: The adaptable nature of ZTNA agents aligns seamlessly with modern architectures, including cloud-based and hybrid environments. These agents ensure secure connectivity across diverse network segments, irrespective of location or device, without compromising security.
- Proactive Threat Detection: ZTNA agents embedded within the Zero Trust model enable proactive threat detection. They continuously monitor and transmit device behavior logs to various security solutions and network monitoring platforms, facilitating early identification of anomalous behavior and timely intervention to mitigate potential security breaches.
- Real-time Monitoring Capabilities: The agent-based ZTNA solution significantly enhances Zero Trust's capabilities by providing real-time monitoring of device behavior and transmitting logs to different security solutions. This continuous monitoring ensures compliance and fortifies the network against potential threats.

B. Good Practices in ZT Model Implementation

Successful implementation of the Zero Trust model augmented by ZTNA agents relies on adherence to several best practices:

Comprehensive Visibility: The incorporation of ZTNA agents provides comprehensive insight into network traffic and device activities, forming the basis for informed decision-making and precise access control.

Continuous Authentication: ZTNA agents enable continuous user verification mechanisms, ensuring access privileges are consistently evaluated based on current context and device behavior.

Micro-Segmentation: The utilization of ZTNA agents facilitates effective network compartmentalization, minimizing lateral movement and granting access based on specific needs, thereby enhancing security.

Encryption of Data: ZTNA agents enforce encryption protocols for data in transit and at rest, ensuring confidentiality and integrity, particularly when transmitting logs to various security solutions.

C. ZT in Software Engineering

Zero Trust principles find practical application and significance in the realm of software engineering:

- Secure Software Development: Emphasis on incorporating security measures into every stage of the software development life cycle, including robust authentication mechanisms and encryption practices.
- Automated Security Analysis: Leveraging automation tools for security analysis aids in identifying vulnerabilities, performing code analysis, and enhancing the overall security posture of software systems.
- API Security and Compliance: Highlighting the significance of securing APIs, which serve as critical components in modern application development, aligning API security with compliance standards bolsters overall system security.

IV. Applying Zero Trust Principles to Healthcare Devices: Patient Monitors

A. Security Risks in Medical Device Connectivity

The integration of ZTNA agents into healthcare devices, notably patient monitors, addresses significant security risks arising from increased connectivity [5]. Patient monitors, among other medical devices, are susceptible to vulnerabilities jeopardizing critical health data integrity, confidentiality, and availability.

B. Zero Trust Framework Application to Patient Monitoring Devices

Incorporating ZTNA agents into patient monitoring devices represents a pivotal approach to mitigating security risks. These agents fundamentally redefine trust paradigms, necessitating a holistic transition from default trust stances to continuously validating and verifying each device's identity, behavior, and access permissions within the healthcare ecosystem.

C. Pillars of ZT Model Application to Patient Monitors

The utilization of ZTNA agents in patient monitors embodies various fundamental pillars:

- Identity: ZTNA agents enforce robust authentication mechanisms, extending beyond simple passwords to interactive, context-aware validations for user and device access. They continuously monitor and transmit device authentication logs for compliance assessment.
- Device: Comprehensive hardware asset management facilitated by ZTNA agents ensures visibility, understanding of risk exposure, regular patching, and robust security controls, protecting against vulnerabilities. These agents transmit logs detailing device health and status to ensure security compliance.
- Network: ZTNA agents advocate for secure device communication and segmentation within healthcare networks. They leverage the 802.1X protocol for port-based access control, ensuring strict authorization before device integration. The ZTNA agents continuously monitor network domains, facilitating authorization processes for patient monitoring devices.
- Application Workload: Focus on securing application execution both on-premise and in the cloud. ZTNA agents continuously monitor device behavior, enforce stringent access controls, and leverage micro-segmentation to detect and prevent anomalies in application workload.
- Data: ZTNA agents contribute to protecting electronically protected health information (ePHI) through access control enforcement, data mapping, and per-session authorization protocols, ensuring patient data security. These agents facilitate the transmission of secure data logs to maintain compliance and integrity.

This holistic application of the ZT model fortifies healthcare organizations' security posture, safeguarding critical patient data and mitigating potential vulnerabilities within the healthcare ecosystem.

V. Developing a Detailed Protocol and Defending the Protocol Design Using Paper and Pencil Analysis

The protocol design for patient monitors involves a multifaceted approach to authentication and access control measures, enriched by the incorporation of ZTNA agents for robust security:

Access Control Measures

a. Least Privilege Principle: Restricting access rights to the minimum necessary based on user roles, locations, and time, enabling granular access controls.

b. Role-Based Access Control (RBAC): Implementing RBAC to manage access permissions based on predefined roles and dynamically adjusting role assignments as organizational needs change.

c. Micro-segmentation: Dividing the network into smaller segments to limit lateral movement and control device communication based on specific needs.

To validate the protocol design, a paper and pencil analysis can simulate potential attack scenarios:

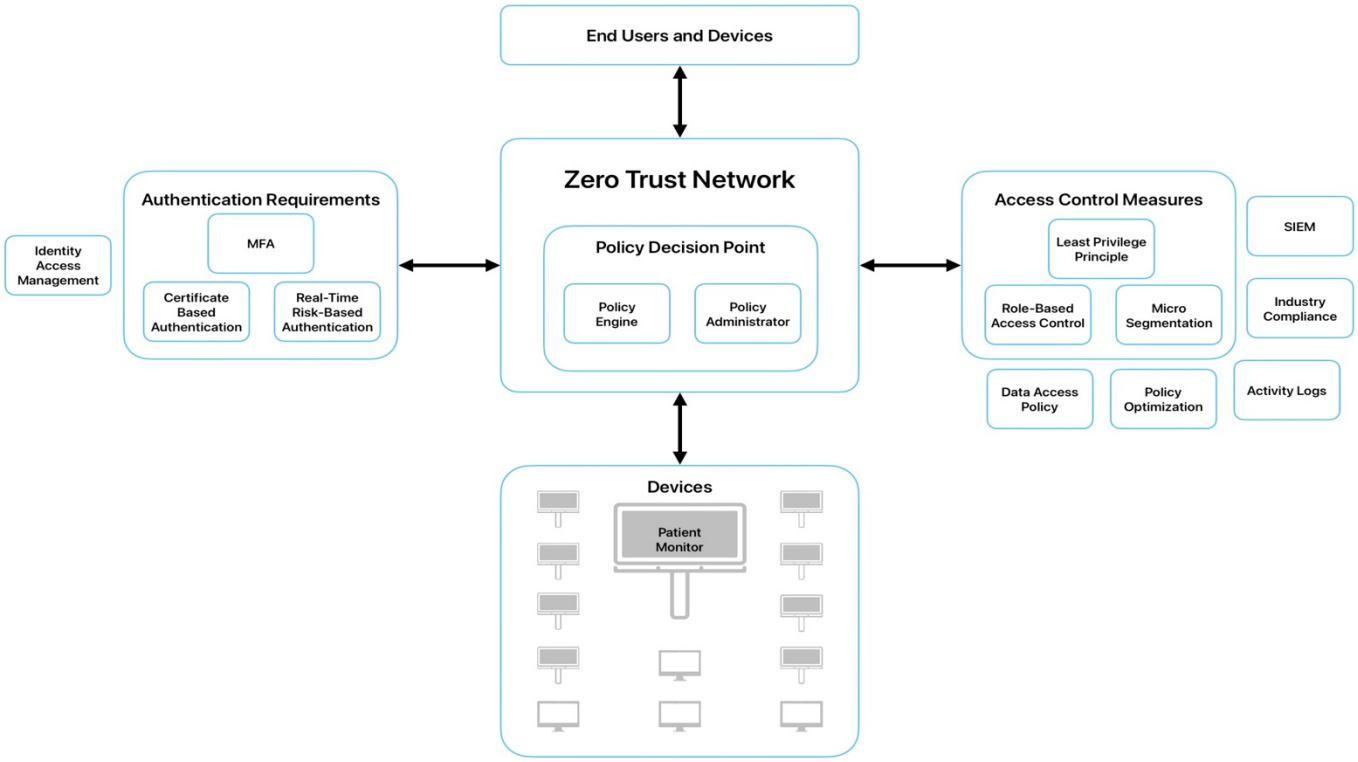

Figure I: Proposed ZTNA Architecture.

A. Authentication Requirements

a. Multifactor Authentication (MFA): ZTNA agents implement MFA utilizing at least two authentication factors—passwords, biometrics, or tokens—to continuously verify user identities and device integrity. These agents monitor and transmit multifactor authentication logs for compliance assessment.

b. Certificate-Based Authentication: Leveraging digital certificates, ZTNA agents regularly validate and renew certificates for trustworthiness assurance, transmitting authentication logs to ensure continuous device trust verification.

c. Real-time Risk-based Authentication: Dynamic authentication based on risk assessments derived from user behavior, network context, and device attributes triggers re-authentication through ZTNA agents for suspicious activities or context changes. These agents continuously monitor and transmit risk-based authentication logs for compliance checks.

B. Access Control Measures

a. Least Privilege Principle: ZTNA agents enforce access rights restriction to the minimum necessary based on user roles, locations, and time, ensuring granular access controls. Logs of access control activities are transmitted to ensure compliance.

b. Role-Based Access Control (RBAC): Implementing RBAC, ZTNA agents manage access permissions based on predefined roles, dynamically adjusting role assignments. Logs are transmitted to ensure real-time access control compliance.

c. Micro-segmentation: ZTNA agents facilitate network compartmentalization, limiting lateral movement and controlling device communication based on specific needs. Logs detailing segmentation activities are transmitted to ensure compliance and security.

C. Simulation of Attack Scenarios

a. Threat Modeling: ZTNA agents assist in identifying and analyzing potential attack vectors specific to patient monitors, including data interception or device tampering. These agents continuously monitor and transmit threat modeling logs for analysis.

b. Role-Playing Scenarios: Simulating user access attempts and potential breach scenarios evaluates authentication robustness and access control effectiveness facilitated by ZTNA agents. Logs of simulated scenarios are transmitted for validation.

D. Protocol Evaluation against Scenarios

a. Authentication Evaluation: Rigorous assessment of multifactor authentication, certificate-based authentication, and risk-based authentication against simulated attacks ensures effectiveness in preventing unauthorized access. ZTNA agents transmit authentication logs for compliance checks.

b. Access Control Assessment: Simulating breach attempts evaluates least privilege principle, RBAC, and micro-segmentation effectiveness in preventing unauthorized access. ZTNA agents transmit access control logs for compliance validation.

E. Comprehensive Comparison

a. Zero Trust vs. Traditional Models: Contrasting ZTNA-driven continuous verification and strict access controls with traditional security models emphasizes the robustness of the protocol design. Logs of comparative analysis are transmitted to validate the protocol's efficacy.
b. Simulation Insights: Detailed documentation of simulated attack responses, authentication successes, and access control effectiveness through ZTNA agents validates the protocol's resilience and compliance.

VI. Case Studies and Practical Applications

A. ZT Implementation in Healthcare Devices - Patient Monitors

Implementing Zero Trust (ZT) in healthcare devices, particularly patient monitors, presents a transformative approach to bolstering security measures within medical settings. Case studies reveal successful integration of ZT principles into healthcare devices, showcasing efficacy in fortifying the security infrastructure [7].

Patient monitors, crucial for real-time patient health tracking, have revamped their security protocols by adopting ZTNA agents. These agents facilitate multifaceted authentication, strict access controls, and continuous monitoring, enhancing resilience against potential threats. By incorporating ZTNA's identity verification and robust network segmentation, patient monitors establish a formidable defense mechanism against unauthorized access attempts.

The ZT implementation in patient monitors significantly reduces the risk of data breaches, safeguarding sensitive health information. These case studies serve as a testament to the adaptability and effectiveness of ZT in addressing unique security challenges within healthcare devices.

B. Lessons Learned from Practical Deployments

Practical deployments of Zero Trust within healthcare devices have yielded invaluable insights and lessons, underscoring its significance and challenges [8]:

- Holistic Security Approach: Implementing ZT requires a comprehensive and integrated security strategy encompassing hardware, software, network, and user access controls.
- Continuous Adaptation: ZT's effectiveness relies on its adaptability to evolving threats and technological advancements. Deployments highlight the importance of continuous monitoring, frequent updates, and adaptive security measures.
- User Education and Adoption: Educating healthcare professionals about the ZT model and its implications is crucial for successful deployment. Ongoing training and awareness programs ensure effective utilization of ZT principles.
- Interoperability Challenges: Integrating ZT into existing healthcare systems and devices often encounters interoperability challenges. Deployments emphasize the complexities of integrating ZT with legacy systems and the need for interoperable solutions.
- Regulatory Compliance: Meeting regulatory standards, such as HIPAA, while implementing ZT in healthcare devices remains critical. Lessons learned stress aligning ZT practices with regulatory requirements without compromising security.

These practical deployments and the lessons derived from them serve as a roadmap for future implementations, guiding healthcare organizations toward robust and adaptive security frameworks while navigating device interoperability and regulatory adherence.

VII. Comparative Analysis and Evaluation

A. Comparison with Traditional Security Models

Agent-based ZTNA solutions represent a significant departure from traditional security models, necessitating a comprehensive comparative analysis to elucidate their differences:

- Perimeter-Based Security vs. ZTNA's Assumption of Compromise: Traditional models rely on perimeter-based security, trusting internal networks while fortifying external defenses. In contrast, ZTNA operates on the principle of "never trust, always verify," facilitated by agents continuously monitoring and transmitting logs, assuming no inherent trust [9].
- Implicit Trust vs. Continuous Authentication: Legacy models operate on implicit trust once access is granted. ZTNA emphasizes continuous authentication and verification, facilitated by agents ensuring ongoing trust verification beyond initial access [9].
- Access Control Mechanisms: Traditional models typically use network segmentation and access control lists (ACLs) for limited access within the network. ZTNA agents implement micro-segmentation and granular access controls based on contextual parameters [9].
- Response to Breaches: Traditional models focus on breach detection and mitigation after occurrence. ZTNA prioritizes prevention by implementing dynamic risk-based policies, enabled by agent-based real-time monitoring and response [9].
- Scalability and Flexibility: ZTNA offers more scalable and flexible security, facilitated by agent-based adaptability across diverse environments, including cloud services and various devices [9].

B. Strengths and Weaknesses of ZTNA Implementation

1) Strengths

- Enhanced Security Posture: ZTNA, supported by agents, strengthens security by eliminating implicit trust, enforcing strict access controls, and reducing the attack surface [10].

- Adaptive and Contextual Security: Agent-based ZTNA provides contextual security, considering user behavior and network conditions for dynamic policy enforcement [10].
- Reduced Risk of Data Breaches: ZTNA agents continuously monitor and transmit logs, significantly mitigating the risk of data breaches by preventing unauthorized access [10].
- Compatibility with Modern Infrastructure: ZTNA, facilitated by agents, aligns seamlessly with modern IT infrastructure, ensuring security without compromising functionality [10].

C. Weaknesses

- Complex Implementation: Implementing ZTNA with agents across an organization requires meticulous planning and architecture redesign [10].
- Interoperability Challenges: Integrating ZTNA agents into legacy systems might present interoperability challenges that need addressing [10].
- User Experience Impact: Stricter access controls and continuous authentication facilitated by agents might impact user experience, requiring user education [10].
- Logs transmitted by ZTNA agents serve as evidence validating the strengths and challenges of ZTNA implementation. [10]

VIII. Future Directions and Innovations

A. Emerging Trends in Agent-Based ZTNA Security

Extended Application to IoT and OT: Agent-based ZTNA solutions are expanding beyond conventional IT networks, integrating with the Internet of Things (IoT) and Operational Technology (OT) [11], enhancing security across diverse environments. Logs transmitted by these agents aid in ensuring security in IoT and OT realms.

- AI-Driven Agent-Based ZTNA: The integration of Artificial Intelligence (AI) within ZTNA agents allows dynamic adaptation to threats, utilizing predictive analytics for proactive security measures based on transmitted logs [11].
- User-Centric Agent-Based ZTNA: ZTNA agents are evolving towards a more user-centric approach, leveraging transmitted logs to understand user behavior and preferences for better security alignment.
- Continuous Authentication Enhancement: Agent-based ZTNA solutions are enhancing continuous authentication, utilizing logs for real-time user validation without compromising user experience.
- ZTNA as a Service (ZTNAaaS): ZTNA solutions delivered as a service are anticipated, leveraging transmitted logs for scalable and adaptable security frameworks.

B. Potential Enhancements in Agent-Based ZTNA

Refinement of Access Controls: Future enhancements focus on refining access controls facilitated by ZTNA agents, utilizing transmitted logs for more dynamic and granular access policies.

- Integration with DevSecOps: Seamless integration of ZTNA agents into DevSecOps practices ensures security is inherently embedded in the development lifecycle, aided by transmitted logs for compliance verification.
- Interoperability Standards: Efforts towards establishing interoperability standards are ongoing, facilitating smoother integration of ZTNA agents across varied platforms, as depicted by transmitted logs.
- Enhanced User Experience: Future enhancements aim to balance stringent security measures facilitated by agents with a seamless user experience by refining authentication mechanisms based on transmitted logs [12].
- Automated Threat Response: Advancements in automation enable ZTNA agents to automate threat response actions, swiftly detecting and mitigating potential security threats based on transmitted logs.

These future directions and potential enhancements underscore the continuous evolution of Zero Trust Security, emphasizing its adaptability, scalability, and responsiveness to emerging security challenges and technological advancements.

IX. Conclusion

In the landscape of modern cybersecurity, the integration of agent-based Zero Trust Network Access (ZTNA) solutions has emerged as a pivotal paradigm shift, redefining network security models and access control paradigms. This study has extensively explored the multifaceted dimensions of ZTNA, delineating its core principles, applications in diverse domains, and its significance for future secure network architectures.

Agent-based ZTNA solutions have revolutionized traditional security models by embedding continuous monitoring, authentication, and compliance verification capabilities within devices, ensuring a proactive approach to cybersecurity. The consistent transmission of logs by these agents forms the backbone of the proactive security measures enabled by ZTNA.

The application of agent-based ZTNA principles to various sectors, including healthcare and software engineering, elucidates its practicality and significance in fortifying critical systems and addressing specific industry intricacies. Agent-based ZTNA solutions stand as a testament to the adaptability and effectiveness in safeguarding network access.

Moreover, the comparative analysis showcases the substantial advantages of agent-based ZTNA over traditional security models, leveraging transmitted logs to validate enhanced security postures, adaptive security measures, and reduced vulnerabilities.

As agent-based ZTNA continues to evolve, future directions and innovations, guided by logs transmitted by these agents,

underscore its adaptability, scalability, and responsiveness to emerging security challenges and technological advancements.

In essence, agent-based ZTNA solutions represent not merely a security model but a philosophy continually verified through transmitted logs, charting a path towards a resilient, adaptive, and secure digital future.

X. References

[1] T. M. M. T. M. M. Z. &. Z. M. W. Muhammad, "Integrative Cybersecurity: Merging Zero Trust, Layered Defense, and Global Standards for a Resilient Digital Future," *INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY,* vol. 6, no. 4, pp. 99-135, 2022.

[2] M. J. Khan, "Zero trust architecture: Redefining network security paradigms in the digital age," *World Journal of Advanced Research and Reviews,* vol. 19, no. 3, pp. 105-116, 2023.

[3] C. O. C. S. A. V. F. &. E. T. Buck, "Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust," *Computers & Security,* vol. 110, p. 102436, 2021.

[4] D. &. N. S. Horne, "Introducing zero trust by design: Principles and practice beyond the zero trust hype," *Advances in Security, Networks, and Internet of Things,* pp. 512-525, 2021.

[5] C. &. P. J. Cunningham, "The eight business and security benefits of zero trust," 2017.

[6] D. &. V. T. Tyler, "Trust no one? a framework for assisting healthcare organisations in transitioning to a zero-trust network architecture," *Applied Sciences,* vol. 11, no. 16, p. 7499, 2021.

[7] B. Q. S. Z. J. L. D. S. X. L. M. .. &. Z. Y. Chen, "A security awareness and protection system for 5G smart healthcare based on zero-trust architecture," *IEEE Internet of Things Journal,* vol. 8, no. 13, pp. 10248-10263, 2020.

[8] HealthTech, "Zero Trust Lessons Healthcare Organizations Can Learn from the Federal Government," 18 Jan 2023. [Online]. Available: https://healthtechmagazine.net/article/2023/01/zero-trust-lessons-healthcare-organizations-can-learn-federal-government.

[9] theinstillery, "Zero Trust vs Traditional Security Models: How Do They Compare?," 24 May 2023. [Online]. Available: https://theinstillery.com/stories/zero-trust-vs-traditional-security-models/.

[10] T. E. &. A. A. A. M. Nyamasvisva, "A COMPREHENSIVE SWOT ANALYSIS FOR ZERO TRUST NETWORK SECURITY MODEL," *International Journal of Infrastructure Research and Management,* vol. 10, no. 1, 2022.

[11] Y. H. D. C. L. N. Y. &. M. X. He, "A survey on zero trust architecture: Challenges and future trends," *Wireless Communications and Mobile Computing,* 2022.

[12] S. S. G. &. A. M. A. Ghasemshirazi, "Zero Trust: Applications, Challenges, and Opportunities," arXiv preprint, arXiv:2309.03582, 2023.