Journal of Management and Economics (ISSN: 2751-1707)

Received: 18 December 2025 | Accepted: 03 January 2026 | Published: 21 January 2026

RESEARCH ARTICLE

Reconceptualizing Zero-Trust Security for Clinical Workstations: Integrating AI-Driven Architectures, Legacy Medical Devices, and Operating System Modernization in Healthcare Environments

Prof. Altheon R. Kryss

Faculty of Computer Science, KU Leuven, Belgium

VOLUME: Vol.06 Issue01 2026

PAGE: 20-27

Abstract

The accelerating digitization of healthcare infrastructures has intensified the exposure of clinical environments to sophisticated cyber threats, particularly as hospitals increasingly depend on interconnected clinical workstations, legacy medical devices, and heterogeneous operating systems. Traditional perimeter-based cybersecurity models have proven inadequate in addressing the complex risk landscape of modern healthcare systems, where implicit trust, static access controls, and outdated endpoint protections create systemic vulnerabilities. Zero Trust Architecture (ZTA) has emerged as a transformative cybersecurity paradigm that challenges legacy assumptions by enforcing continuous verification, least-privilege access, and dynamic risk assessment. Within this evolving discourse, the adoption of modern operating systems, notably Windows 11, has been positioned as both a technical enabler and a governance challenge for implementing Zero Trust principles in hospital clinical workstations. This article develops a comprehensive, theory-driven, and empirically grounded examination of Zero Trust security in healthcare, with a particular focus on bridging AI-driven ZTA frameworks, legacy medical device constraints, and operating system modernization strategies.

KEYWORDS

Zero Trust Architecture, Healthcare Cybersecurity, Clinical Workstations, Legacy Medical Devices, AI-Driven Security, Operating System Modernization

INTRODUCTION

The digital transformation of healthcare systems represents one of the most consequential technological shifts in contemporary society, reshaping how clinical services are delivered, how patient data are managed, and how institutional accountability is enforced. Hospitals, clinics, and specialized care centers increasingly rely on complex digital ecosystems composed of electronic health record platforms, networked diagnostic equipment, telemedicine interfaces, and clinical workstations that serve as the operational backbone of patient care. While these advancements have enhanced efficiency and clinical precision, they have simultaneously expanded the attack surface for cyber adversaries, rendering healthcare one of the most targeted sectors for cybercrime globally (Southwick, 2023). This growing exposure has revealed the structural inadequacies of traditional cybersecurity models that were designed for more static, perimeter-defined organizational environments.

Historically, healthcare cybersecurity strategies have been rooted in perimeter-based defense models that assume a clear boundary between trusted internal networks and untrusted external actors. Such models prioritize firewalls, intrusion detection systems, and network segmentation as primary safeguards. However, the contemporary healthcare environment no longer conforms to these assumptions. Clinical workflows routinely traverse internal and external networks, clinicians access systems from multiple locations, and medical devices communicate autonomously across heterogeneous platforms. This erosion of the traditional network perimeter has rendered implicit trust models increasingly obsolete, prompting a paradigm shift toward Zero Trust Architecture (Kindervag, 2010).

Zero Trust Architecture fundamentally challenges the notion of inherent trust within organizational networks by asserting that no user, device, or application should be trusted by default, regardless of its location. Instead, access decisions are continuously evaluated based on contextual factors such as identity, device posture, behavior, and risk signals (Mattsson, 2022). While the conceptual foundations of Zero Trust are well-established in enterprise and defense contexts, their translation into healthcare environments introduces unique complexities. Healthcare systems must balance stringent security controls with the imperatives of patient safety, clinical efficiency, and regulatory compliance, creating a multifaceted tension that complicates Zero Trust adoption (Edo, 2023).

Within this broader transformation, the role of operating system modernization has received comparatively limited scholarly attention. Clinical workstations remain a critical but often overlooked component of healthcare cybersecurity, serving as the primary interface between clinicians and digital health systems. Many hospitals continue to rely on legacy operating systems due to compatibility constraints with medical devices, vendor support limitations, and risk-averse organizational cultures. Recent scholarship has begun to interrogate this issue, emphasizing that operating system upgrades are not merely technical decisions but strategic interventions that can enable or constrain Zero Trust implementation (Nayeem, 2026). The adoption of Windows 11, with its enhanced security features such as hardware-based isolation, secure boot, and integrated identity protections, has been proposed as a potential catalyst for advancing Zero Trust principles in clinical environments.

At the same time, the rise of artificial intelligence in cybersecurity has introduced new possibilities for dynamic risk assessment, behavioral analytics, and adaptive access control. AI-driven Zero Trust frameworks leverage machine learning algorithms to detect anomalies, predict threats, and automate policy enforcement in real time (Chokkanathan et al., 2025). In healthcare contexts, these capabilities hold particular promise for addressing sophisticated threats such as ransomware, phishing, and insider misuse, which have been shown to disproportionately impact clinical systems (Mondal et al., 2025). However, the integration of AI-driven security mechanisms with legacy medical devices and heterogeneous operating systems raises critical questions about interoperability, explainability, and trustworthiness.

Despite a growing body of literature on Zero Trust Architecture, AI-driven cybersecurity, and healthcare information systems, significant gaps remain in understanding how these domains intersect at the level of clinical workstations and operating system infrastructure. Much of the existing research focuses either on high-level architectural models or on isolated technical components, offering limited insight into the socio-technical dynamics that shape real-world implementation. Moreover, there is a tendency to treat legacy systems as static constraints rather than as evolving elements within adaptive security ecosystems. This article addresses these gaps by developing an integrative analysis that situates operating system modernization, particularly Windows 11 adoption, within the broader trajectory of Zero Trust transformation in healthcare.

The central argument advanced in this study is that Zero Trust Architecture in healthcare cannot be fully realized without a nuanced understanding of how operating system capabilities, AI-driven security mechanisms, and legacy device ecosystems interact within clinical workflows. By synthesizing insights from cybersecurity theory, healthcare informatics, and organizational governance, the article seeks to reconceptualize Zero Trust as an adaptive socio-technical paradigm rather than a purely technical blueprint. In doing so, it builds on recent empirical evaluations of Windows 11 adoption in hospital clinical workstations (Nayeem, 2026) and extends their implications through extensive theoretical elaboration and critical discussion.

The remainder of the article is structured to progressively deepen this analysis. The methodology section outlines the qualitative, design-analytic approach employed to synthesize and interpret the relevant literature. The results section presents a descriptive and interpretive analysis of key findings, focusing on the interplay between Zero Trust principles, AI-driven security, and operating system modernization in healthcare settings. The discussion section offers an extensive theoretical interpretation, engaging with competing scholarly perspectives, identifying limitations, and proposing directions for future research. The conclusion synthesizes the core insights and reflects on their implications for both academic inquiry and practical cybersecurity governance in healthcare.

METHODOLOGY

The methodological foundation of this research is grounded in a qualitative, interpretive, and design-analytic approach that aligns with the complexity and interdisciplinarity of Zero Trust Architecture in healthcare contexts. Given the absence of a unified empirical dataset capable of capturing the full scope of operating system modernization, AI-driven security mechanisms, and legacy medical device integration, this study deliberately avoids positivist or experimental methodologies. Instead, it adopts a systematic and theoretically informed synthesis of existing scholarly and practitioner-oriented literature, treating these sources as empirical artifacts that reflect evolving knowledge, assumptions, and debates within the field (Gambo & Almulhem, 2025).

The first methodological pillar of the study is an integrative literature analysis that spans cybersecurity architecture theory, healthcare information systems research, and applied studies on Zero Trust implementation. This process involves the critical examination of peer-reviewed journal articles, technical reports, and conceptual frameworks that collectively illuminate the multifaceted nature of Zero Trust in clinical environments. Particular emphasis is placed on recent contributions that explore AI-driven Zero Trust models, healthcare-specific security challenges, and the role of operating system infrastructure in enabling advanced security controls (Adamson & Qureshi, 2025; Edo, 2023). The inclusion of contemporary evaluations of Windows 11 adoption in hospital clinical workstations provides a concrete empirical anchor for the analysis (Nayeem, 2026).

The second methodological pillar is architectural pattern analysis, which involves identifying recurring design patterns, control mechanisms, and governance structures across different Zero Trust implementations. This approach draws on established cybersecurity architecture methodologies that emphasize abstraction, comparison, and contextualization rather than direct measurement (Kim et al., 2024). By examining how identity verification, access control, device trust, and behavioral analytics are operationalized across diverse healthcare scenarios, the study constructs a conceptual map of Zero Trust practices that transcends individual technologies or vendors. This pattern-oriented perspective is particularly valuable for understanding how operating system features, such as those introduced in Windows 11, can support or constrain Zero Trust objectives.

A third methodological component involves conceptual modeling and interpretive synthesis. Rather than proposing a formal mathematical model or simulation, the study develops a narrative-based conceptual framework that integrates technical, organizational, and regulatory dimensions of Zero Trust adoption. This framework is informed by theories of socio-technical systems, organizational learning, and adaptive governance, which have been widely applied in information systems research but remain underutilized in cybersecurity scholarship (Filho, 2025). Through iterative comparison and synthesis, the study articulates how AI-driven security analytics, legacy device constraints, and operating system modernization co-evolve within healthcare institutions.

The methodological rigor of the study is further enhanced through reflexive engagement with limitations and counterarguments. Recognizing that literature-based research is inherently shaped by the availability, quality, and biases of existing sources, the study explicitly addresses potential gaps and inconsistencies in the reviewed material. For example, while AI-driven Zero Trust frameworks are often presented as universally beneficial, the analysis critically examines concerns related to algorithmic opacity, data quality, and clinical trust (Sophia, 2025). Similarly, while operating system upgrades are frequently framed as security improvements, the study interrogates the operational risks and transition costs associated with deploying Windows 11 in clinical environments characterized by legacy dependencies (Nayeem, 2026).

Ethical and regulatory considerations also inform the methodological approach. Healthcare cybersecurity is deeply intertwined with patient privacy, data protection regulations, and ethical obligations to ensure continuity of care. As such, the study incorporates regulatory perspectives from healthcare and cybersecurity governance literature, examining how standards such as NIST SP 800-207 shape Zero Trust implementation strategies (Tetrate, 2023). This regulatory lens ensures that the analysis remains grounded in the practical constraints and accountability structures that define real-world healthcare environments.

While the chosen methodology prioritizes depth, contextual richness, and theoretical integration, it also entails certain limitations. The absence of primary empirical data precludes statistical generalization or causal inference. Instead, the study aims to achieve analytical generalization by identifying patterns, tensions, and conceptual insights that can inform both future empirical research and practical decision-making. In this sense, the methodology aligns with interpretive research traditions that value explanatory power and theoretical contribution over predictive precision (Ogendi, 2025).

In summary, the methodological approach adopted in this study is deliberately aligned with the complexity of its subject matter. By integrating systematic literature analysis, architectural pattern examination, and conceptual synthesis, the research offers a robust and nuanced exploration of Zero Trust Architecture in healthcare. This approach provides a solid foundation for the subsequent results and discussion, enabling a comprehensive examination of how AI-driven security, operating system modernization, and legacy medical devices interact within clinical workstations.

RESULTS

The results of this study emerge from a comprehensive interpretive synthesis of the literature, revealing a set of interrelated themes that collectively illuminate the challenges and opportunities associated with implementing Zero Trust Architecture in healthcare clinical workstations. Rather than presenting discrete empirical measurements, the findings are articulated through descriptive and analytical narratives that reflect patterns, tensions, and convergences across scholarly and applied research. Each thematic result is grounded in existing studies and evaluated in relation to operating system modernization, AI-driven security mechanisms, and legacy medical device integration.

One of the most salient findings concerns the centrality of clinical workstations as both security assets and vulnerability points within healthcare infrastructures. The literature consistently emphasizes that clinical workstations serve as the primary interface between healthcare professionals and digital systems, mediating access to electronic health records, diagnostic tools, and networked medical devices (Southwick, 2023). Despite their critical role, these workstations are frequently overlooked in strategic cybersecurity planning, with greater attention often directed toward network perimeter defenses or cloud-based systems. This imbalance has significant implications for Zero Trust implementation, as the effectiveness of continuous verification and least-privilege access depends heavily on endpoint integrity and operating system capabilities (Edo, 2023).

The adoption of modern operating systems, particularly Windows 11, emerges as a pivotal enabler of Zero Trust principles at the workstation level. Recent evaluations highlight that Windows 11 introduces a range of security enhancements, including hardware-based root of trust, virtualization-based security, and tighter integration with identity management frameworks (Nayeem, 2026). These features align closely with Zero Trust requirements for device attestation, secure boot processes, and continuous posture assessment. The literature suggests that such capabilities can significantly enhance an organization’s ability to enforce dynamic access controls and reduce reliance on static network boundaries (Filho, 2025).

However, the results also reveal persistent barriers to operating system modernization in healthcare settings. Legacy medical devices often depend on outdated operating systems or specific software environments that are incompatible with newer platforms. This dependency creates a structural tension between the desire to adopt modern security architectures and the operational imperative to maintain device functionality and regulatory certification (RocketMe Up Cybersecurity, 2024). Studies indicate that hospitals frequently delay or fragment operating system upgrades to avoid disrupting clinical workflows, inadvertently perpetuating security vulnerabilities that Zero Trust models are designed to mitigate (Nayeem, 2026).

Another key finding relates to the role of artificial intelligence in enhancing Zero Trust architectures. AI-driven security mechanisms are increasingly portrayed as essential for managing the scale and complexity of modern healthcare environments, where manual monitoring and rule-based controls are insufficient (Chokkanathan et al., 2025). Machine learning algorithms enable continuous behavioral analysis, anomaly detection, and adaptive risk scoring, supporting the Zero Trust principle of “never trust, always verify.” In clinical contexts, AI-driven analytics have demonstrated potential for early detection of ransomware attacks and phishing attempts, which are among the most prevalent threats to healthcare systems (Mondal et al., 2025; Tiwo et al., 2025).

Despite these advantages, the literature also highlights concerns regarding the integration of AI-driven security within healthcare Zero Trust frameworks. One recurring issue is the challenge of explainability, particularly in high-stakes clinical environments where security decisions can directly affect patient care. Clinicians and administrators may be reluctant to trust automated access controls or anomaly detection systems if their decision logic is opaque or poorly aligned with clinical realities (Sophia, 2025). This skepticism underscores the importance of aligning AI-driven Zero Trust mechanisms with organizational culture and professional norms, rather than treating them as purely technical solutions.

The results further indicate that Zero Trust adoption in healthcare is deeply influenced by governance and regulatory contexts. Healthcare organizations operate under stringent data protection and patient safety regulations, which shape both the scope and pace of cybersecurity innovation. Standards such as NIST SP 800-207 provide a conceptual framework for Zero Trust implementation but leave significant room for interpretation in healthcare-specific scenarios (Tetrate, 2023). This regulatory ambiguity can lead to inconsistent adoption practices, with some organizations implementing partial or superficial Zero Trust controls that fail to achieve the intended security outcomes (Abdelmagid & Diaz, 2025).

A related finding concerns the uneven maturity of identity and access management systems within healthcare institutions. Effective Zero Trust Architecture relies on robust identity verification, continuous authentication, and fine-grained authorization mechanisms. However, many healthcare organizations continue to rely on fragmented or outdated identity systems that are ill-suited to dynamic, context-aware access control (Uzougbo & Augustine, 2025). The literature suggests that operating system modernization can support improved identity integration, but only when accompanied by broader investments in IAM infrastructure and governance (Nayeem, 2026).

Finally, the results highlight the socio-technical nature of Zero Trust transformation in healthcare. Rather than a linear progression from legacy models to modern architectures, Zero Trust adoption is characterized by iterative experimentation, organizational learning, and negotiation among diverse stakeholders. Security teams, clinicians, IT administrators, and device vendors each bring distinct priorities and constraints, shaping how Zero Trust principles are interpreted and enacted in practice (Ogendi, 2025). This finding reinforces the argument that Zero Trust should be understood not as a fixed architecture but as an adaptive process that evolves in response to technological, organizational, and regulatory change.

Collectively, these results underscore the complexity of implementing Zero Trust Architecture in healthcare clinical workstations. They reveal that operating system modernization, AI-driven security, and legacy device management are not isolated challenges but interdependent dimensions of a broader socio-technical transformation. These insights provide a foundation for the subsequent discussion, which engages more deeply with theoretical implications, scholarly debates, and future research directions.

DISCUSSION

The findings of this study invite a deeper theoretical and critical examination of Zero Trust Architecture as it is conceptualized and operationalized within healthcare environments. At its core, the discussion advances the argument that Zero Trust should not be reduced to a set of technical controls or architectural diagrams, but rather understood as an adaptive governance paradigm that reshapes how trust, risk, and responsibility are negotiated in complex socio-technical systems. This reconceptualization is particularly salient in healthcare, where cybersecurity decisions intersect directly with patient safety, ethical obligations, and professional autonomy.

A central theme emerging from the discussion is the redefinition of trust itself. Traditional cybersecurity models implicitly equate trust with network location or organizational affiliation, assumptions that are increasingly untenable in distributed and interconnected healthcare ecosystems (Kindervag, 2010). Zero Trust disrupts this logic by treating trust as a dynamic and continuously assessed attribute, contingent on identity, context, and behavior (Mattsson, 2022). In clinical environments, this shift has profound implications. Clinicians who have historically enjoyed broad and persistent access to systems may perceive Zero Trust controls as intrusive or obstructive, particularly if they disrupt time-sensitive workflows. The literature suggests that successful Zero Trust adoption requires not only technical sophistication but also deliberate efforts to align security practices with clinical values and routines (Southwick, 2023).

Operating system modernization, exemplified by the adoption of Windows 11, emerges as a critical but contested enabler of this trust reconfiguration. From a technical perspective, modern operating systems provide foundational capabilities that are essential for Zero Trust, including secure boot, hardware-backed identity, and continuous device posture assessment (Nayeem, 2026). These features support a shift away from static credentials and toward context-aware access decisions. However, the discussion reveals that operating system upgrades are rarely perceived as neutral technical improvements within healthcare organizations. Instead, they are embedded in broader organizational dynamics, including budget constraints, vendor dependencies, and risk aversion shaped by regulatory scrutiny (RocketMe Up Cybersecurity, 2024).

The persistence of legacy medical devices complicates this landscape further. Many such devices are designed for long operational lifespans and are subject to stringent certification processes that discourage frequent software changes. While Zero Trust principles advocate for continuous verification and adaptability, legacy devices often resist such dynamism, creating architectural asymmetries within healthcare networks (Edo, 2023). The discussion highlights a key theoretical tension: Zero Trust assumes a level of technological fluidity that may be incompatible with the stability requirements of certain clinical systems. Addressing this tension requires a more nuanced understanding of risk that accounts for both cybersecurity threats and clinical harm.

Artificial intelligence introduces both promise and paradox into this equation. AI-driven Zero Trust frameworks offer the potential to reconcile security rigor with operational efficiency by automating risk assessment and adapting controls in real time (Chokkanathan et al., 2025). In theory, machine learning algorithms can distinguish between legitimate clinical activity and malicious behavior with greater precision than rule-based systems, reducing false positives and minimizing workflow disruption. However, the discussion underscores that AI is not a panacea. Concerns about algorithmic bias, data quality, and explainability are particularly acute in healthcare, where erroneous security decisions can delay care or undermine professional trust (Sophia, 2025).

Moreover, the integration of AI into Zero Trust architectures raises important governance questions. Who is accountable for automated access decisions? How are errors detected and corrected? And how can transparency be ensured without exposing sensitive security logic to adversaries? These questions highlight the need for governance frameworks that extend beyond technical design to encompass organizational oversight, ethical review, and continuous learning (Ogendi, 2025). The discussion suggests that AI-driven Zero Trust should be approached as a socio-technical system that requires ongoing calibration and stakeholder engagement, rather than as a self-regulating mechanism.

Another critical dimension explored in the discussion is the role of regulatory and standards-based frameworks in shaping Zero Trust adoption. While standards such as NIST SP 800-207 provide valuable guidance, they are inherently abstract and require contextual interpretation (Tetrate, 2023). In healthcare, this interpretive flexibility can be both an asset and a liability. On one hand, it allows organizations to tailor Zero Trust implementations to their specific clinical and regulatory contexts. On the other hand, it can result in uneven adoption and superficial compliance, where Zero Trust is invoked rhetorically without substantive architectural change (Abdelmagid & Diaz, 2025).

The discussion also engages with counterarguments that question the feasibility and desirability of Zero Trust in healthcare. Critics argue that the complexity and cost of Zero Trust architectures may outweigh their benefits, particularly for resource-constrained institutions. Others contend that excessive security controls risk undermining clinician autonomy and contributing to burnout. While these concerns are not unfounded, the literature reviewed in this study suggests that they often stem from narrow or poorly implemented interpretations of Zero Trust (Filho, 2025). When Zero Trust is approached as an adaptive and participatory process, rather than a rigid control regime, it can enhance both security and usability.

Importantly, the discussion reframes operating system modernization as a strategic lever for organizational learning. The transition to platforms such as Windows 11 forces healthcare organizations to confront legacy dependencies, reassess risk assumptions, and invest in new skills and governance structures (Nayeem, 2026). In this sense, operating system upgrades can serve as catalysts for broader Zero Trust transformation, provided they are accompanied by deliberate change management and stakeholder engagement. This perspective aligns with organizational learning theories that emphasize the role of technological change in reshaping institutional practices and norms.

The limitations of the current study also warrant reflection. As a literature-based analysis, the findings are necessarily constrained by the scope and quality of existing research. There is a relative scarcity of longitudinal studies that track Zero Trust implementation outcomes over time in healthcare settings. Similarly, empirical evidence on the real-world impact of Windows 11 adoption on clinical security and workflow remains limited. These gaps highlight the need for future research that combines qualitative insights with empirical evaluation, including case studies, ethnographic observation, and mixed-methods analysis.

Future research directions emerging from this discussion are multifaceted. Scholars could explore comparative analyses of Zero Trust adoption across different healthcare systems and regulatory regimes, shedding light on how institutional contexts shape security outcomes. There is also a need for deeper investigation into clinician perceptions of Zero Trust controls and their impact on professional practice. Finally, interdisciplinary research that integrates cybersecurity, healthcare ethics, and organizational studies could offer richer insights into the socio-technical dynamics of trust and risk in clinical environments.

In sum, the discussion advances a holistic and critical understanding of Zero Trust Architecture in healthcare. By situating operating system modernization, AI-driven security, and legacy device management within a broader socio-technical and governance framework, it challenges reductive narratives and underscores the need for adaptive, context-sensitive approaches. This theoretical depth not only enriches academic discourse but also offers valuable guidance for practitioners navigating the complex realities of healthcare cybersecurity.

CONCLUSION

This article has undertaken an extensive and theoretically grounded exploration of Zero Trust Architecture as it applies to healthcare clinical workstations, with particular emphasis on the interplay between AI-driven security mechanisms, legacy medical devices, and operating system modernization. Through a comprehensive synthesis of contemporary scholarship, the study has demonstrated that Zero Trust adoption in healthcare is not merely a technical upgrade but a profound socio-technical transformation that reshapes how trust, risk, and responsibility are managed within clinical environments.

A central conclusion of the study is that operating system infrastructure, exemplified by the adoption of Windows 11, plays a foundational role in enabling Zero Trust principles at the endpoint level. Modern operating systems provide critical security capabilities that support continuous verification, device integrity, and identity-centric access control, aligning closely with the core tenets of Zero Trust (Nayeem, 2026). However, these technical advantages cannot be realized in isolation. Legacy medical devices, regulatory constraints, and organizational cultures exert powerful influences that shape the feasibility and effectiveness of operating system modernization initiatives.

The analysis further underscores the transformative potential of AI-driven Zero Trust frameworks, particularly in addressing the scale and complexity of contemporary healthcare cyber threats. Machine learning–based behavioral analytics and adaptive risk assessment offer promising avenues for enhancing security resilience while minimizing disruption to clinical workflows. Yet, the study cautions against uncritical adoption of AI, highlighting the importance of transparency, governance, and alignment with clinical values to ensure trust and accountability.

Ultimately, the article argues that Zero Trust in healthcare should be conceptualized as an adaptive governance paradigm rather than a static architectural model. Sustainable and effective Zero Trust implementation requires ongoing organizational learning, stakeholder engagement, and contextual sensitivity. By bridging theoretical insight with practical relevance, this study contributes to a deeper understanding of how healthcare organizations can navigate the complex challenges of cybersecurity in an increasingly digital and interconnected world.

REFERENCES

1. RocketMe Up Cybersecurity. (2024). Implementing Zero Trust Security Models in Clinical Environments — A Comprehensive Approach.
2. Kim, Y., et al. (2024). Exploring Effective Zero Trust Architecture for Defense Cybersecurity: A Study. KSII Transactions on Internet and Information Systems.
3. Nayeem, M. (2026). Bridging zero-trust security and legacy medical devices: An evaluation of Windows 11

adoption in hospital clinical workstations. Frontiers in Emerging Artificial Intelligence and Machine Learning, 3(1), 1–8. https://doi.org/10.64917/feaiml/Volume03Issue01-01

4. Gambo, M. L., & Almulhem, A. (2025). Zero Trust Architecture: A Systematic Literature Review.

5. Sophia, E. (2025). AI-Driven Behavioral Biometrics For Continuous Authentication in Zero Trust.

6. Southwick, R. (2023). The Paradigm Shift: Healthcare Embraces a Zero Trust Approach to Cybersecurity.

7. Edo, O. C. (2023). A zero trust architecture for health information systems. Health and Technology.

8. Mondal, B., Dukkipati, S. S. N. C., Rahman, M. T., & Taimun, M. T. Y. (2025). Using Machine Learning for Early Detection of Ransomware Threat Attacks in Enterprise Networks. Saudi Journal of Engineering and Technology.

9. Abdelmagid, A. M., & Diaz, R. (2025). Zero Trust Architecture as a Risk Countermeasure in Small–Medium Enterprises and Advanced Technology Systems.

10. Filho, W. L. R. (2025). The Role of Zero Trust Architecture in Modern Cybersecurity: Integration with IAM and Emerging Technologies.

11. Uzougbo, O. I., & Augustine, A. O. (2025). A Review of Authentication and Authorization Mechanisms in Zero Trust Architecture.

12. Chokkanathan, K., et al. (2025). AI-Driven Zero Trust Architecture: Enhancing Cyber-Security Resilience. IEEE.

13. Adamson, K. M., & Qureshi, A. (2025). Zero Trust 2.0: Advances, Challenges, and Future Directions in ZTA.

14. Ogendi, E. G. (2025). Leveraging Advanced Cybersecurity Analytics to Reinforce Zero-Trust Architectures within Adaptive Security Frameworks.

15. Tiwo, O. J., et al. (2025). Improving Patient Data Privacy and Authentication Protocols against AI-Powered Phishing Attacks in Telemedicine. Asian Journal of Research in Computer Science.

16. Mattsson, U. (2022). Zero Trust Architecture. Controlling Privacy and the Use of Data Assets.

17. Tetrate. (2023). Zero Trust and NIST SP 800-207: What CISOs Need to Know.

18. Qudus, L. (2025). Advancing Cybersecurity: Strategies for Mitigating Threats in Evolving Digital and IoT Ecosystems.

19. Kindervag, J. (2010). Build security into your network's DNA: The zero trust network architecture. Forrester Research Inc.

20. Okunlola, O. A. (2025). Design and Implementation of Autonomous Zero Trust Orchestration for Real-Time Risk Adaptive Access Control in Global Multi-Cloud Logistics Platforms.