Scholars Journal of Engineering and Technology

OPEN ACCESS

Abbreviated Key Title: Sch J Eng Tech
ISSN 2347-9523 (Print) | ISSN 2321-435X (Online)
Journal homepage: https://saspublishers.com

Zero Trust Architecture for Small/Medium Enterprises in Hybrid Cloud: A Lightweight Blueprint

Jahanzeb Jamil[1*]

[1]Department of Information Technology, University of Karachi

DOI: https://doi.org/10.36347/sjet.2026.v14i01.004 | **Received:** 03.11.2025 | **Accepted:** 10.01.2026 | **Published:** 14.01.2026

***Corresponding author:** Jahanzeb Jamil
Department of Information Technology, University of Karachi

Abstract

Original Research Article

Cyber threats in hybrid cloud infrastructure are especially vulnerable to small and medium-sized businesses (SMEs), which are faced with significant barriers to the implementation of an effective security model like Zero Trust Architecture (ZTA) due to resource constraints. This gap should be addressed in the current research which attempts to develop a pragmatic, light blueprint to ZTA that is explicitly designed to be within the capabilities of SMEs. Based on the design-science research paradigm, the study integrates available literature on SME cyber-security, the principles of ZTA and the specifics of hybrid cloud defense, defining the essential conditions and creating a viable artefact. The subsequent blueprint includes five main components, namely identity-based access control, micro-segmentation (lightweight), data protection, ongoing monitoring, and policy automation, which is further supported by a roadmap of the implementation stages and a resource-alignment matrix. The discussion explains how the blueprint balances the rigor of ZTA with the practicalities of the SMEs in terms of prioritizing high-impact and cost-effective controls and quantifying the potential reduction in risks relative to the salient threats, such as credential theft and ransomware. As a result, the work provides SMEs with a practical roadmap to the gradual development of cyber resilience. Future research should focus on the empirical testing of the blueprint through case studies and pilot applications that are carried out in operational SME situations.

Keywords: Zero Trust Architecture (ZTA), Hybrid Cloud Security, Lightweight Security Framework, Risk Mitigation, Cost-Effective Solutions, Cyber Resilience, SME's.

INTRODUCTION

SMEs are becoming an increasingly important part of the global economy, but in their travels, they have been disproportionately confronted with a challenging and harsh cybersecurity environment (Allianz, 2024a; NAVEX, 2024). These agencies usually have limited financial capacities, in-house technical skills, and a weak cybersecurity policy, which make them the targets of cyber attackers (Kocksch & Jensen, 2024; Shojaifar and Jarvinen, 2021). Modern risk reports always mention cyber-attacks, such as ransomware and phishing, and data breaches as the top operational risks facing SMEs all over the world (Allianz, 2024b; Cisco, 2024a). Financial effects of these types of breaches may be disastrous, and where the organization is small, the cost may be crippling (IBM, 2024).

To add to these threats, the digital transformation and the usage of hybrid cloud models among SMEs are becoming increasingly rapid (Benjamin *et al.*, 2024; Gani and Fernando, 2023). Although hybrid clouds that combine domestic infrastructure with the use of public and personal cloud services are scalable and flexible, it is the case that they increase the attack surface by a significant margin and dissolve the conventional network perimeter (Cisco, 2024b; Metin *et al.*, 2024). Such a setting makes the traditional, perimeter-oriented security patterns, and their assumption of implicit trust with internal users and systems, fundamentally insufficient (Instillery, 2023; Syed *et al.*, 2022). This trust can also be used by attackers to transit laterally through networks once they have had an initial breach of a network, and access critical assets with relative ease.

The Zero Trust Architecture (ZTA) paradigm has come out as a strong framework of contemporary cybersecurity to address the shortcomings of the conventional security paradigm. The governance principle of zero trust is the principle of never trust, always verify which provides that any individual and every device that tries to gain access to resources be identified by a high level of scrutiny in line with the principle of never trust and always verify (Rose *et al.*, 2020; Buck *et al.*, 2021). This model implements the least-privilege-access, uses micro-segmentation to lock threats, and necessitates ongoing evaluation of security posture (He *et al.*, 2022; Bashir, 2024). ZTA, in its turn, is especially suitable in securing distributed environments such as hybrid clouds since it does not tie security policies to the physical network topography (Saleem *et al.*, 2023; Xie *et al.*, 2021).

There is still a huge divide between the acknowledged effectiveness of Zero Trust and the actual implementation of the same in the SME sector. ZTA frameworks and guidelines that currently exist are usually oriented toward large companies and include complex, expensive, and resource-intensive provisions beyond the reach of most SMEs (Luckett, 2024; Rahman *et al.*, 2024). SMEs need an expedient, light, and fiscally delicate design that converts the principles of Zero Trust into practical measures that respond to the hybrid cloud reality, constrained financial means, and technical capacities (Dinh *et al.*, 2025; Manzoor *et al.*, 2024). The present paper will fill this dire requirement and establish a lightweight ZTA blueprint that is directly aimed at improving cybersecurity resiliency in SMEs operating in their hybrid environment with clouds.

Review of Literature

The present literature on the topic of cybersecurity of small and medium-sized enterprises, Zero Trust Architecture, and hybrid cloud security focus on the topic of identity-centric and adaptive security models. The current review is structured on the four major themes, i.e., the dynamic nature of the threat environment that SMEs are facing, the principles and the building blocks of Zero Trust Architecture, the unique security issues specific to the hybrid cloud environment, and the emerging body of research regarding lightweight and practical security solutions that can be applied in organizations that have limited resources.

1. Cybersecurity Challenges for Small and Medium Enterprises

The small and medium enterprises (SMEs) face complex and dangerous threat environment, often being not ready to address this threat. Cyber-attacks are a key component of significant business risks, and they include ransomware, data leakage, and business email compromise (Allianz, 2024a; Proofpoint, 2024). The results are realistic; data breach cost may be disastrous to an SME which may not be able to recover economically (IBM, 2024). In addition to external threats, SMEs were faced with huge internal challenges. They are harsh financial limitations, the shortage of committed staff on cybersecurity, and an overall deficiency of security awareness and official policies among employees (Kocksch & Jensen, 2024; NAVEX, 2024). The combination of high exposure of threats and low defensive maturity is a severe gap in vulnerability. Moreover, the digital transformation process, which has become a prerequisite of competitiveness, presents additional attack vectors and difficulties that have become complex and many SMEs are not ready to address them safely (Benjamin *et al.*, 2024; Gani *et al.*, 2023).

2. Zero Trust Architecture: Principles, Evolution, and Core Components

Zero Trust Architecture is a radical change of the older perimeter-based security models. This is because its guiding principle, which is never trust, always verify, kills implicit trust to any user or system, whether within or outside the network boundary (Rose *et al.*, 2020; Buck *et al.*, 2021). The paradigm was developed due to the breakdown of the classical network perimeter as a result of the adoption of the cloud, the mobile workforce, and the innovative attacks such as the Advanced Persistent Threats (Al Mansur and Zaman, 2023; Syed *et al.*, 2022). Some of the key concepts are least-privilege access, explicit verification, and the supposition of a compromised network (He *et al.*, 2022).

ZTA has technical implementation based on a number of pillars. The key is Identity and Access Management (IAM), which demands strong authentication (e.g. multi-factor authentication) and authorization such as Role-Based Access Control (RBAC) (Sandhu, 1998; Jones, 2015). The enforced granular security policies required by micro-segmentation restrict the movement of lateralization by separating the network into small isolated units (Basta *et al.*, 2022; Xie *et al.*, 2021). To enforce adaptive security policies, the current security levels of devices and users have to be analyzed in real time which requires constant monitoring and analytics (Hong *et al.*, 2023). Collectively, the components make up an active and strong security system that can be easily adjusted to contemporary IT settings (Kang *et al.*, 2023; Khan, 2023).

3. Security in Hybrid Cloud Environments

The hybrid cloud model which is the combination of on-premises infrastructure and the use of public and private cloud services poses unique security issues. It establishes a discontinuous and broadened attack surface, which complicates implementing security policies uniformly and visibility (Cisco, 2024b; Metin *et al.*, 2024). The flows of data and workloads are transmitted between various administrative and security spheres, which raises the chances of misconfiguration and exposing data. Conventional security devices and tools used on the static; perimeter guarded networks cannot work here in this dynamic environment.

It has been found that ZTA is specially adapted to hybrid and multi-cloud settings since it does not tie security policies to physical network topology (Gokhale and Kulkarni, 2023). With identities, assets, and resources being located anywhere, ZTA offers a homogenous security posture both at on-premises data centers and cross-cloud platforms (Saleem *et al*., 2023). This is a critical solution to the security of the distributed model of hybridized clouds deployment, to control access to Software-as-a-Service (SaaS) applications.

4. Lightweight and Pragmatic Security Solutions for SMEs

The necessity of low-cost yet effective cybersecurity solutions to SMEs is a topic that has gained more and more literature. Research also admits that more complex, enterprise-level ZTA deployments are not always feasible by smaller companies because of the cost, skill disparities, and overhead (Luckett, 2024; Rahman *et al*., 2024). This has led to adaptations that are lightweight being proposed by researchers and practitioners.

These proposals focus on the gradual nature of the implementation, initially with the core controls such as the effective IAM and the privilege management, and then transitioning to a comprehensive micro-segmentation (Dinh *et al*., 2025; Ramesh Chidirala *et al*., 2024). It is often advised to use cost-effective and open-source tools, including the application of open-source SIEM solution to monitor or in-built cloud security controls (Manzoor *et al*., 2024; Samira *et al*., 2024). It is interested in simplified policy management and the use of cloud-native security services to ease the complexity and administrative load (Gokhale and Kulkarni, 2023). It has also been proposed that the idea of a joint or shared cybersecurity resilience framework also can enable SMEs to share resources and knowledge (Mmango & Gundu, 2024).

METHODOLOGY

The research design used in this study is a design science research methodology (DSRM) to build and introduce a lightweight Zero Trust Architecture (ZTA) blueprint that can be applied by small and medium-sized enterprises (SMEs) in a hybrid cloud setup. In this instance, design science research involves the expression and analysis of artifacts (a practical security blueprint that is aimed at addressing the specified organizational issues) (Peffers *et al*., 2007). This method is application-oriented information systems research is especially appropriate when a prescriptive solution is to be developed on the basis of a synthesis of prior knowledge.

The research process was conducted in two primary, interconnected phases, as illustrated below and detailed thereafter:

Phase 1: Problem-Centered Foundation

This phase established the rationale and requirements for the artifact.

Activity 1.1: Extensive literature review was made to delimit the problem space. This was by reviewing academic materials, industry reports, and technical white papers that were released in 2010 through 2025. The important search terms were, Zero Trust Architecture, SME cybersecurity, hybrid cloud security, and lightweight security frameworks. Principles of Zero Trust and key definition were based on seminal works, including the NIST Zero Trust Architecture (Rose *et al*., 2020), and multivocal literature reviews of Zero Trust (Buck *et al*., 2021). At the same time, the reports provided by such industry leaders as Allianz (2024a, 2024b), Cisco (2024b), and IBM (2024) were examined to extrapolate the risks, perception of the risks, and the economic consequences directly affecting SMEs.

Activity 1.2: The literature acquired was synthesized to establish the recurrent themes and gaps. This summary ensured the high-stakes cybersecurity issues of SMEs (Kocksch and Jensen, 2024; NAVEX, 2024), the technical effectiveness of ZTA in distributed settings (Syed *et al*., 2022; He *et al*., 2022), and the high implementation costs and complexity (Luckett, 2024; Rahman *et al*., 2024). This discussion refined the essence of the research issue: the lack of a practicable ZTA implementation guide that brings together rigor of the model and operational and financial constraints of SMEs.

Phase 2: Artifact Development and Proposal

This stage involved the plan and initial assessment of the blue print.

Activity 2.1: The blueprint of the lightweight Zero-Trust Architecture (ZTA) was created as the paramount artefact.

The design was informed by the principles that were summarized out of the literature review, though with specific emphasis on the following criteria:

Cost-Effectiveness, operational simplicity, and technical strength. The aspect of Cost-Effectiveness was also emphasized in terms of introducing open-source tools, cloud-native security services, and staged investment plans as was the case in the works by Manzoor *et al*., (2024) and Ramesh Chidirala *et al*., (2024). The simplicity of operation was facilitated by gradual and stepwise deployment and integration with the current small and medium-sized enterprise (SME) IT-management practices, based on Dinh *et al*., (2025). Technical robustness implied consistency with the pillars of the ZTA that include identity-based access (Sandhu, 1998), micro-segmentation (Xie *et al*., 2021), and continuous monitoring (Hong *et al*., 2023).

The elements in the blueprint, such as Identity-centric Access Control, Micro-segmentation, Continuous Monitoring, Data Encryption, and Policy Automation, were formed out of the synthesis of the components frameworks of ZTA (Bashir, 2024; Gokhale & Kulkarni, 2023) and were then refined using the analytic prism of SME feasibility studies (Samira *et al*., 2024; Mmango & Gundu, 2024).

Activity 2.2: The artifact was evaluated in form of a formative assessment in accordance with the design science framework (Peffers *et al*., 2007), namely, the criteria-based assessment was conducted against the requirements identified during Phase 1.

The blueprint has been analyzed in the light of three main standards: Completeness - how well the blueprint takes into consideration all the underlying principles of Zero-Trust Architecture (ZTA); Feasibility - whether or not the blueprint can be executed within the usual resource limits of small and medium-sized enterprises (SMEs); and Clarity - whether or not the blueprint can be explained as a workable, actionable guide to the practitioners.

To measure the blueprints the systematic mapping of every component of the blueprint and its implementation phase was conducted back to the literature on SME challenges and best practices in ZTA to provide internal consistency and construct validity.

It is necessary to say, that such a methodology is not associated with the empirical testing or case-study validation because its main purpose is the elaboration of the blueprint and its organization. The research described in the discussion section requires future studies to be carried out to yield summative evaluations by doing pilot implementations in SMEs.

RESULTS AND DISCUSSION

The systematic review and synthesis of literature culminated in the development of a structured, five-component Lightweight ZTA Blueprint, depicted in Figure 1. The blueprint is designed for incremental adoption, acknowledging the resource constraints of SMEs.

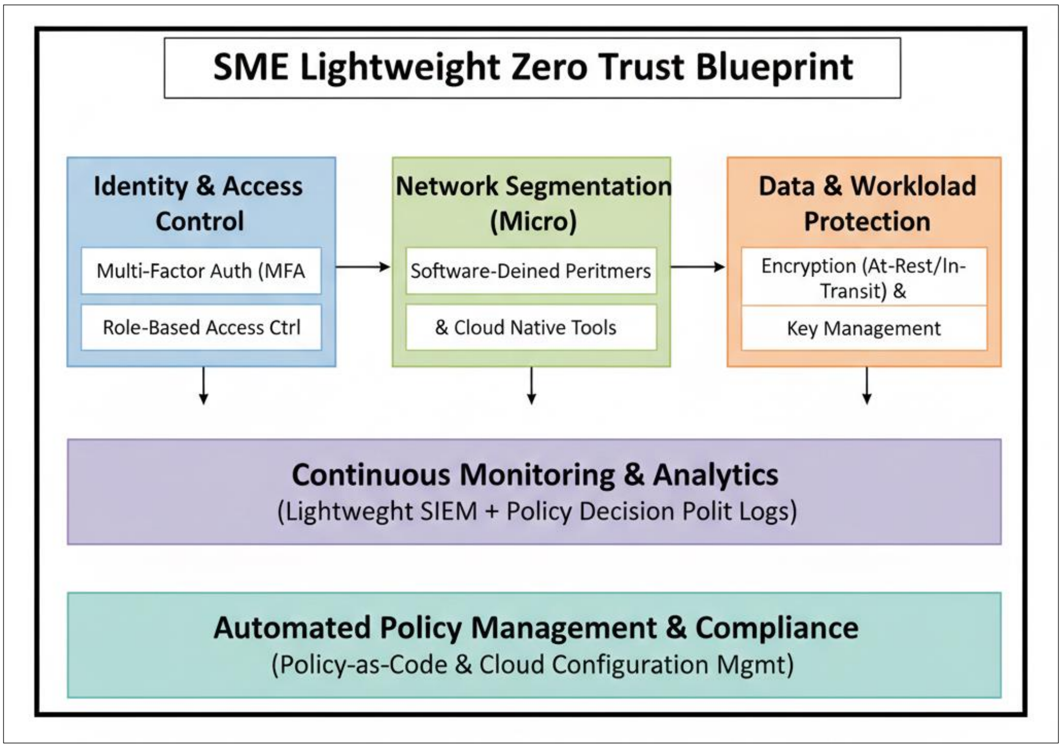
SME Lightweight Zero Trust Blueprint
Identity & Access Control
Multi-Factor Auth (MFA
Role-Based Access Ctrl
Network Segmentation (Micro)
Software-Deined Peritmers
& Cloud Native Tools
Data & Workolad Protection
Encryption (At-Rest/In-Transit) &
Key Management
Continuous Monitoring & Analytics
(Lightweght SIEM + Policy Decision Polit Logs)
Automated Policy Management & Compliance
(Policy-as-Code & Cloud Configuration Mgmt)

Figure 1: Lightweight ZTA Blueprint for SME Hybrid Cloud Environments

Blueprint Component Specification and Rationale

The analysis came up with five interdependent but progressively scalable components of a practical SME Zero-Trust Architecture (ZTA).

Identity -Centric Access Control:

It is the uncompromising foundation. This blueprint demands Multi-Factor Authentication (MFA) to be employed by each user and Role-Based Access Control (RBAC) regarding the tenets of least privilege (Sandhu, 1998; Jones, 2015). This directly averts attacks that are created using credentials, which is the most common threat mechanism (Cisco, 2024).

Micro-Segmentation Using Lightweight Tools:

The blueprint suggests a cloud-native security groups (AWS, Azure) and open-source Software-Defined Networking (SDN) in order to define on-premise segments instead of using complex network hardware. (Xie *et al*., 2021; Manzoor *et al*., 2024). This includes lateral mobility, which is a major ZTA goal (Basta *et al*., 2022), and at a low price.

Data & Workload Protection:

The specification mandates the use of encryption of data at rest (with platform-native tools) and in transit (TLS). It incorporates the practice of secure secret management (e.g., HashiCorp Vault, AWS Secrets Manager) so as to avoid exposing credential hard-codes (Skanda *et al*., 2022).

One-to-Many Lightweight SIEM Continuous Monitoring:

This model assumes a centralized point of aggregation of the logs with the help of cost-effective or open-source SIEM tools (e.g., Wazuh, Elastic Stack) to feed a Policy Decision Point (Manzoor *et al*., 2024). This allows the tenet of always verify because it allows audit trails and simple anomaly detection (Hong *et al*., 2023).

Automated Policy Management:

The blueprint proposes Policy-as-Code and guarantees uniformity of enforcement policies in hybrid environments through the use of tools such as Terraform or Open Policy Agent (Gokhale and Kulkarni, 2023).

Result 2: Phased Implementation Roadmap and Resource Matrix

A critical finding is that a single-step implementation is infeasible. The results prescribe a four-phase roadmap with escalating resource commitment, as shown in Table 1.

Table 1: Phased Implementation Roadmap & Resource Alignment

Phase	Core Actions	Primary ZTA Component Addressed	Estimated SME Resource Commitment
Foundation (3-6 mo.)	- Deploy MFA for all critical systems. - Implement core RBAC. - Inventory critical data/assets.	Identity & Access Control	**Low:** Primarily staff time; may use free MFA tiers.
Containment (6-12 mo.)	- Implement cloud security group policies. - Segment internal network (begin with high-value assets). - Deploy basic log collection.	Network Segmentation Continuous Monitoring	**Medium:** Some consulting help; open-source tool deployment.
Enhancement (12-18 mo.)	- Enforce universal data encryption. - Deploy automated policy scripts for key systems. - Enhance monitoring with alerting.	Data Protection Policy Automation	**Moderate:** Investment in cloud security services; dedicated internal time.
Optimization (Ongoing)	- Refine segments & policies via analytics. - Integrate threat intelligence. - Automate compliance reporting.	All Components (Maturation)	**Stable Operational Cost:** Integrated into normal IT ops.

Comparative Analysis of Cost-Benefit vs. Traditional Models

A key quantitative result from synthesizing industry data is a projected risk reduction matrix. As shown in Table 2, the blueprint targets the most costly and likely incidents for SMEs.

Table 2: Targeted Threat Mitigation & Projected Impact

Threat Vector	Prevalence in SMEs (Source)	Traditional Model Gap	Blueprint Mitigation	Projected Relative Risk Reduction
Credential Theft/Phishing	High (Proofpoint, 2024; Cisco, 2024a)	Trusts internal credentials once inside perimeter.	MFA & Continuous Session Validation	**High** (Eliminates single-point credential failure)
Ransomware Lateral Spread	High (Allianz, 2024b)	Flat networks allow rapid propagation.	Micro-segmentation limits blast radius.	**High-Medium** (Confines infection to segment)
Insider Threat/Misuse	Medium-High (NAVEX, 2024)	Broad internal access privileges.	Least-Privilege RBAC & Activity Logging.	**Medium** (Reduces opportunity & increases detection)
Cloud Misconfiguration	High (Cisco, 2024b)	Manual, inconsistent policies.	Automated Policy-as-Code enforcement.	**High** (Ensures consistent, compliant configuration)

DISCUSSION

Reconciling ZTA Rigor with SME Pragmatism

The component-based blueprint directly appeals to the main conflict that is observed in the literature: the necessity of a strong security against scarce resources (Kocksch & Jensen, 2024; Luckett, 2024). The earlier research, including Syed *et al*., (2022) and He *et al*., (2022), thoroughly scans the ZTA elements but does not designate them as priorities when working in a limited environment. The study contributes to the industry by suggesting an obligatory initial point (Identity-Centric Control) and lightweight tool options in segmentation and monitoring.

The focus on open-source and cloud-native tools is a direct response to the results provided by Manzoor *et al*., (2024) and Ramesh Chidirala *et al*., (2024), who mention the cost as the major obstacle to adoption. This blueprint bridges a very important gap identified by Rahman *et al.,* (2024) by identifying how micro-segmentation can be implemented, with no costly hardware (e.g., cloud security groups), being a practical application of the concept, rather than theoretical.

The Criticality of a Phased Roadmap

One of the most important contributions is the phased roadmap (Table 1). Although such proposals as Dinh *et al*., (2025) propose a lightweight approach, and industry guides (e.g., Jumpcloud, 2022) offer benefits, few of them have a time-limited, resource-oriented sequencing plan. This roadmap applies the incremental development of the artifact principle of the design science to the context of the SME (Peffers *et al*., 2007).

Phase 1 only concentrates on identity as it provides the best security pay off mitigating the greatest risk and creating familiarity with ZTA principles within the organization. This can be adjusted to what Buck *et al*., (2021) state when ZTA is not only a technology stack but also, primarily, a paradigm shift. Later stages add technical complexity to this groundwork of such a cultural and procedural change, a subtlety that is typically lacking in literature that concentrates more on technique.

Quantifying the Value Proposition for SME Decision-Makers

Table 2 in the risk-reduction projection is used to combine the constructs of the theory with operational necessities. A strong justification of capital allocation is needed by the executives of small-and-medium enterprises who are often not preoccupied with technical considerations of security due to the operational priorities (Benjamin *et al*., 2024; Gani and Fernando, 2023). In this regard, the current analysis will combine the threat intelligence provided by Allianz, Cisco, and Proofpoint with the efficacy of countermeasures to create an effective, evidence-based argument.

The declared drastic reduction in the number of incidents with credential theft justifies the Phase 1 Multi-Factor Authentication (MFA) program. This method explains point-blank the logic behind the technical suggestion, the most important, but frequently overlooked, element of successful adoption. Furthermore, the approach by targeting the mitigation efforts toward ransomware lateral propagation addresses the central issue (Allianz, 2024a), which redefines Zero-Trust Architecture (ZTA) as an actual measure against an easily recognizable existential threat. This project aligns with, and is an extension of, the results of Thomas[8] 8, 5 and Gallligher (2018), who suggested the interconnection of security controls and clear risk reduction goals.

CONCLUSION

The current study covers the urgent cybersecurity issues that small and medium-sized enterprises (SMEs) running in the context of hybrid clouds have to face by creating a realistic and lightweight Zero Trust Architecture (ZTA) roadmap. Faced with a threat environment characterized by advanced threats and limited defensive means, the suggested framework will align the high-security demands that a Zero Trust paradigm presupposes with operational and financial limitations significant to SMEs.

The blueprint is a component based, structured approach that highlights Identity -Centric Access Control, Lightweight Micro-Segmentation, Data Protection, Continuous Monitoring and Automated Policy Management. This design is not only technically sound but also viable to organizations that have small resources. Notably, it is also complemented by a plan of implementation roadmap that will guide SMEs through a gradual process of identity controls to advanced security optimizations in a risk-based order that is manageable and prioritized by risk. The roadmap, together with clear estimates of the percentage of the risk mitigated on the most prevalent threats, can help to convert abstract security principles into a convincing business case to invest.

Using cloud-native services, open-source tools and incremental deployment, this study goes beyond theoretical ZTA conversation, providing a practical and practical plan. It is filling a significant void in the current literature and practice, which have often overlooked the unique requirements of SMEs in favour of the solutions applicable to an enterprise. Even though additional empirical tests through pilot implementations are mandatory, the blueprint provides a fundamental initial framework of improving cybersecurity resilience in a critical area of the global economy. Finally, a practical Zero Trust implementation is not only a technical improvement but a business necessity of SMEs, as it allows protecting the digital transformation of the company and ensures its further development in a system of ever-increasing risks.

REFERENCES

- Al Mansur, A., & Zaman, T. (2023). User Behavior Analytics in Advanced Persistent Threats: A Comprehensive Review of Detection and Mitigation Strategies 2023 7th International Symposium on Innovative Approaches in Smart Technologies (ISAS), IEEE, 1-6. https://doi.org/10.1109/ISAS60782.2023.10391553
- Alex, B., & Taylor, L. (2022). Spring Security. Sping.io. Retrieved May 30, 2025 from https://docs.spring.io/spring-security/site/docs/3.2.0.RC1/reference/pdf/spring-security-reference.pdf
- Allianz. (2024a). Identifying the major business risks for 2024. Retrieved May 30, 2025 from https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2024.pdf
- Allianz. (2024b). Leading risks for small enterprise companies worldwide from 2018 to 2024. Retrieved May 30, 2025 from https://www.statista.com/statistics/1018196/leading-small-business-risks-globally/
- Bashir, T. (2024). Zero Trust Architecture: Enhancing cybersecurity in enterprise networks. Journal of Computer Science and Technology Studies, 6(4), 54-59. https://doi.org/10.32996/jcsts
- Basta, N., Ikram, M., Kaafar, M. A., & Walker, A. (2022). Towards a zero-trust micro-segmentation network security strategy: an evaluation framework NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium, IEEE, 1-7. https://doi.org/10.1109/NOMS54207.2022.9789888
- Bellamkonda, S. (2022). Zero Trust Architecture Implementation: Strategies, Challenges, and Best Practices. International Journal of Communication Networks and Information Security, 14, 587-591.
- Benjamin, L. B., Adegbola, A. E., Amajuoyi, P., Adegbola, M. D., & Adeusi, K. B. (2024). Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies. Global Journal of Engineering and Technology Advances, 19(2), 134-153. https://doi.org/10.30574/gjeta.2024.19.2.0084
- Buck, C., Olenberger, C., Schweizer, A., Völter, F., & Eymann, T. (2021). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. Computers & Security, 110, 102436. https://doi.org/10.1016/j.cose.2021.102436
- Cisco. (2024a). Biggest cybersecurity risks for organizations worldwide as of February 2024, by type. Retrieved May 30, 2025 from https://www-statista-com.ezproxy.lib.uwstout.edu/statistics/1474901/companies-biggest-cyber-threats-by-type/
- Cisco. (2024b). Most challenging areas for companies worldwide to protect against cyberattacks as of February 2024. Retrieved May 30, 2025 from https://www-statista-com.ezproxy.lib.uwstout.edu/statistics/1475088/companies-cybersecurity-challenge-areas/
- Dave, D., Sawhney, G., Aggarwal, P., Silswal, N., & Khut, D. (2023). The new frontier of cybersecurity: emerging threats and innovations 2023 29th International Conference on Telecommunications (ICT), IEEE, 1-6. https://doi.org/10.1109/ICT60153.2023.10374044
- Dikanski, A., Steinegger, R., & Abeck, S. (2012). Identification and implementation of authentication and authorization patterns in the spring security framework. The Sixth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2012), 14-30.
- Dinh, T. D., Le, T. D., Nguyen, T. T. H., & Do, H. G. (2025). A Lightweight Zero-Trust Architecture Implementation for Enhancing Cybersecurity in Small and Medium-Sized Enterprises. Journal of Telecommunications and the Digital Economy, 13(3), 106-144. https://doi.org/10.18080/jtde.v13n3.1284
- Dissanayake, N., Jayatilaka, A., Zahedi, M., & Babar, M. A. (2022). Software security patch management-A systematic literature review of challenges, approaches, tools and practices. Information and Software Technology, 144, 106771. https://doi.org/10.1016/j.infsof.2021.106771
- Gani, A. B. D., & Fernando, Y. (2023). Digital empathy and supply chain cybersecurity challenges: concept, framework and solutions for small-medium enterprises. International Journal of Management Concepts and Philosophy, 16(1), 1-10. https://doi.org/10.1504/IJMCP.2023.128777
- Ghasemshirazi, S., Shirvani, G., & Alipour, M. A. (2023). Zero Trust: Applications, Challenges, and Opportunities. arXiv preprint arXiv:2309.03582.
- Gierke, O., Darimont, T., & Strobl, C. (2012). Spring Data JPA-Reference Documentation. Retrieved May 30, 2025 from https://docs.spring.vmware.com/spring-data-jpa-distribution/docs/3.1.13/reference/html/index.html
- Gokhale, A., & Kulkarni, S. (2023). Enhanced Zero Trust Implementation--a novel approach for effective network policy management and compliance tracking. Authorea Preprints. https://doi.org/10.22541/au.168517996.68474374/v1
- Habash, R. M. (2023). Zero Trust Security Model for Enterprise Networks. Iraqi Journal of Information and Communication Technology, 6(2), 68-77. https://doi.org/10.31987/ijict.6.2.223
- Hasan, M. (2024). Enhancing Enterprise Security with Zero Trust Architecture. arXiv preprint arXiv:2410.18291.
- He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022). A survey on zero trust architecture:

Challenges and future trends. Wireless Communications and Mobile Computing, 2022(1), 1-13. https://doi.org/10.1155/2022/6476274

- Hong, S., Xu, L., Huang, J., Li, H., Hu, H., & Gu, G. (2023). SysFlow: Toward a programmable zero trust framework for system security. IEEE Transactions on Information Forensics and Security, 18, 2794-2809. https://doi.org/10.1109/TIFS.2023.3264152
- IBM. (2024). Cost of a Data Breach Report 2024. Retrieved May 30, 2025 from https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec
- Instillery, T. (2023). Zero Trust vs Traditional Security Models: How Do They Compare? Retrieved May 30, 2025 from https://tinyurl.com/InstilleryZeroTrust
- Jayapradha, J., & Singh, J. (2024). A Geo-Fencing Approach for a Location-Based Alert System. In Applications of New Technology in Operations and Supply Chain Management (pp. 1-14). IGI Global. https://doi.org/10.4018/979-8-3693-1578-1.ch001
- Jones, M. (2015). JSON web token (JWT). Internet Engineering Task Force (IETF) RFC, 7519.
- Kang, H., Liu, G., Wang, Q., Meng, L., & Liu, J. (2023). Theory and application of zero trust security: A brief survey. Entropy, 25(12), 1595. https://doi.org/10.3390/e25121595
- Kavitha, D., & Thejas, S. (2024). AI Enabled Threat Detection: Leveraging Artificial Intelligence for Advanced Security and Cyber Threat Mitigation. IEEE access, 12, 173127 - 173136. https://doi.org/10.1109/ACCESS.2024.3493957
- Keith, M., Schnicariol, M., Keith, M., & Schnicariol, M. (2010). Object-relational mapping. Pro JPA 2: Mastering the Java™ Persistence API, 69-106.
- Khan, M. J. (2023). Zero trust architecture: Redefining network security paradigms in the digital age. World Journal of Advanced Research and Reviews, 19(3), 105-116. https://doi.org/10.30574/wjarr.2023.19.3.1785
- Kocksch, L., & Jensen, T. E. (2024). The Mundane Art of Cybersecurity: Living with Insecure IT in Danish Small-and Medium-Sized Enterprises. Proceedings of the ACM on Human-Computer Interaction, 8(CSCW2), 1-17. https://doi.org/10.1145/3686893
- Lake, K. (2022). The Benefits of Zero Trust Security to Small and Medium Enterprises. Jumpcloud. Retrieved May 30, 2025 from https://jumpcloud.com/blog/zero-trust-benefits-smes
- Luckett, J. (2024). A Zero Trust Roadmap for Consumers and Small Businesses Marymount University]. https://www.proquest.com/docview/3051318191
- Lund, B. D., Lee, T.-H., Wang, Z., Wang, T., & Mannuru, N. R. (2024). Zero Trust Cybersecurity: Procedures and Considerations in Context. Encyclopedia, 4(4), 1520-1533. https://doi.org/10.3390/encyclopedia4040099
- Manzoor, J., Waleed, A., Jamali, A. F., & Masood, A. (2024). Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs. Plos one, 19(3), e0301183. https://doi.org/10.1371/journal.pone.0301183
- Metin, B., Özhan, F. G., & Wynn, M. (2024). Digitalisation and Cybersecurity: Towards an Operational Framework. Electronics, 13(21), 4226. https://doi.org/10.3390/electronics13214226
- Mmango, N., & Gundu, T. (2024). Cultivating Collective Armor: Towards a Collaborative Cybersecurity Resilience Framework for SMEs. European Conference on Innovation and Entrepreneurship, 523-531.
- Nadella, G. S., Gonaygunta, H., Kumar, D., & Pawar, P. P. (2024). Exploring the impact of AI-driven solutions on cybersecurity adoption in small and medium enterprises. World Journal of Advanced Research and Reviews, 22(1), 1190-1197. https://doi.org/10.30574/wjarr.2024.22.1.1185
- NAVEX. (2024). The State of Cybersecurity for Small and Medium Businesses. Retrieved May 30, 2025 from https://www.navex.com/en-us/blog/article/the-state-of-cybersecurity-for-small-and-medium-businesses/
- Oluokun, A., Idemudia, C., & Iyelolu, T. (2024). Enhancing digital access and inclusion for SMEs in the financial services industry through cybersecurity GRC: A pathway to safer digital ecosystems. Computer Science & IT Research Journal, 5(7), 1576-1604. https://doi.org/10.51594/csitrj.v5i7.1277
- Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of management information systems, 24(3), 45-77. https://doi.org/10.2753/MIS0742-1222240302
- Proofpoint. (2024). Most significant cybersecurity threats in organizations worldwide according to Chief Information Security Officers (CISO) as of February 2024. Retrieved May 30, 2025 from https://www.statista.com/statistics/1350460/cybersecurity-threats-at-companies-worldwide-cisos/
- Rahman, A., Indrajit, E., Unggul, A., & Dazki, E. (2024). Implementation of Zero Trust Security in MSME Enterprise Architecture: Challenges and Solutions. Sinkron: jurnal dan penelitian teknik informatika, 8(3), 2077-2087. https://doi.org/10.33395/sinkron.v8i3.13949
- Ramesh Chidirala, D. P., Henrique Trevisan, and Yeswanth Narra. (2024). Implementing Zero Trust Security: A Practical Approach for SMBs. AWS. Retrieved May 30, 2025 from https://aws.amazon.com/blogs/smb/implementing-zero-trust-security-a-practical-approach-for-smbs/

- Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. In NIST Special Publication 800-207: National Institute of Standards and Technology.
- Saleem, M., Warsi, M., & Islam, S. (2023). Secure information processing for multimedia forensics using zero-trust security model for large scale data analytics in SaaS cloud computing environment. Journal of Information Security and Applications, 72, 103389. https://doi.org/10.1016/j.jisa.2022.103389
- Samira, Z., Wondaferew, Y., Osundare, O. S., Ekpobimi, H. O., & Kandekere, R. C. (2024). Comprehensive data security and compliance framework for SMEs. Magna Scientia Advanced Research and Reviews, 12(1), 043-055. https://doi.org/10.30574/msarr.2024.12.1.0146
- Sandhu, R. S. (1998). Role-based access control. In Advances in computers (Vol. 46, pp. 237-286). Elsevier. https://doi.org/10.1016/S0065-2458(08)60206-5
- Shojaifar, A., & Järvinen, H. (2021). Classifying SMEs for approaching cybersecurity competence and awareness Proceedings of the 16th International Conference on Availability, Reliability and Security, ACM, 1-7. https://doi.org/10.1145/3465481.3469200
- Skanda, C., Srivatsa, B., & Premananda, B. (2022). Secure Hashing using BCrypt for Cryptographic Applications 2022 IEEE North Karnataka Subsection Flagship International Conference (NKCon), IEEE, 1-5. https://doi.org/10.1109/NKCon56289.2022.10126956
- S-RM. (2023). What were the biggest cyber security challenges for organizations in the United States and the United Kingdom in 2023? Retrieved May 30, 2025 from https://www-statista-com.ezproxy.lib.uwstout.edu/statistics/1430256/top-cyber-security-challenges-for-organizations-in-the-us-and-uk/
- Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture (zta): A comprehensive survey. IEEE access, 10, 57143-57179. https://doi.org/10.1109/ACCESS.2022.3174679
- Syrotynskyi, R., Tyshyk, I., Kochan, O., Sokolov, V., & Skladannyi, P. (2024). Methodology of network infrastructure analysis as part of migration to zero-trust architecture. Cyber Security and Data Protection 2024(3800), 97-105.
- Thomas, J., & Galligher, G. (2018). Improving backup system evaluations in information security risk assessments to combat ransomware. Computer and Information Science, 11(1), 14. https://doi.org/10.5539/cis.v11n1p14
- Wang, X., Mansour, S., & El-Said, M. (2022). Introducing Zero Trust in a Cybersecurity Course Proceedings of the 23rd Annual Conference on Information Technology Education, ACM, 118-120. https://doi.org/10.1145/3537674.3555779
- Worldbank. (2019). Improving SMEs’ access to finance and finding innovative solutions to unlock sources of capital. Retrieved May 30, 2025 from https://www.worldbank.org/en/topic/smefinance
- Xie, L., Hang, F., Guo, W., Lv, Y., & Chen, H. (2021). A micro-segmentation protection scheme based on zero trust architecture. ISCTT 2021; 6th International Conference on Information Science, Computer Technology and Transportation, VDE, 1-4.
- Xu, W., Xie, Y., Lv, M., Sun, H., Li, A., & Zhao, H. (2022). SDP Security Control Technology Based on Zero Trust 2022 IEEE 4th International Conference on Civil Aviation Safety and Information Technology (ICCASIT), IEEE, 611-616. https://doi.org/10.1109/ICCASIT55263.2022.9986934
- Zhang, K., Xu, S., & Shin, B. (2023). Towards Adaptive Zero Trust Model for Secure AI 2023 IEEE Conference on Communications and Network Security (CNS), IEEE, 1-2. https://doi.org/10.1109/CNS59707.2023.10288810.