Effective Strategies for Implementing and Operating a Zero Trust Environment*

Seulgi Choi†, Jiyong Choi, Youngju Lee and Byungwook Ha
Korea Internet & Security Agency (KISA), Naju, Republic of Korea
{csg, cjynice, lyj5607, ha}@kisa.or.kr

Abstract

Zero Trust has emerged as a core paradigm amid the shift toward remote work, cloud services, and AI-driven automation. However, many organizations struggle with legacy integration, operational complexity, and cost. This paper presents concise strategies for introducing and operating Zero Trust across four perspectives—governance, technical, environmental, and compliance—and provides practical measures to ensure sustainable deployment while minimizing risks and side effects.

Keywords: Zero Trust, Security Governance, Security Architecture, Security System Operation

1 Introduction

John Kindervag first proposed Zero Trust in the 2010s under the principle of "never trust, always verify." Following COVID-19, the rapid adoption of cloud and hybrid work reshaped digital infrastructures, highlighting the need for identity-centric and adaptive security. The U.S. NIST SP~800-207 and NIST~1800-35 frameworks, along with Korea's KISA Guidelines [1~3], provide foundational models, yet practical implementation remains difficult due to integration and governance gaps. This study proposes a multidimensional strategy to guide effective Zero Trust adoption and sustainable operation..

2 Strategies for Implementation and Operation

2.1 Governance

Effective Zero Trust adoption begins with strong governance. Clear roles and responsibilities (R&R) must be established for identity, authorization, and access control. Security committees should oversee decision-making and coordination. Moreover, fostering a culture of least privilege and continuous verification ensures that Zero Trust principles become part of everyday operations [2~3].

* Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. P-26, December 16-18, 2025, Sapporo, Japan.
† Corresponding author: csg@kisa.or.kr

2.2 Technical

Technical stability is critical for maintaining trust enforcement. Policy Decision Points (PDPs) and Policy Enforcement Points (PEPs) must be redundant and monitored to prevent single points of failure. As automation grows, rollback and exception policies should be defined to handle policy conflicts or failures. Gradual transition from perimeter models to Zero Trust minimizes disruption [1, 4].

2.3 Environmental

Dynamic cloud environments require continuous visibility of assets. Tag-based policies, CSPM, and CNAPP tools help maintain consistent controls and compliance across hybrid and multi-cloud systems. Integrated asset management enhances Zero Trust maturity and supports automated policy decisions [3].

2.4 Compliance

Zero Trust architectures often rely on SASE and SOAR frameworks, which may conflict with national sovereignty policies. To align innovation with regulation, organizations should define data governance at the contract stage, apply encryption and tokenization to sensitive data, and adopt regionally certified sovereign cloud platforms [3].

3 Conclusion

Zero Trust is essential for protecting modern digital ecosystems. Successful deployment requires holistic management across governance, technology, environment, and compliance. Through phased implementation and continuous improvement, organizations can evolve from static, perimeter-based defense to adaptive and intelligent security architectures [1~3, 5].

4 Acknowledgment

This work was supported by the Ministry of Science and ICT (MSIT) and the Korea Internet & Security Agency (KISA) under the project “Demonstration and Expansion of Zero Trust-Based Next-Generation Security Architecture."

References

[1] NIST, SP 800-207: Zero Trust Architecture, 2020.
[2] KISA, Zero Trust Guideline 1.0, 2023.
[3] KISA, Zero Trust Guideline 2.0, 2024.
[4] Ward, R. et al., "BeyondCorp: A New Approach to Enterprise Security," 2014.
[5] Dhiman, P. et al., "A Review and Comparative Analysis of Relevant Zero Trust Architectures," Sensors, 24(4), 1328, 2024.