

Zero Trust Security for Multi-Cloud Infrastructures

Prepared by

ALI MMADI, PhD student-Midocean University





Research Issues (1)

Task 9

**Zero Trust Architecture for Multi-Cloud Environments: A Framework
Compliant with ISO/IEC 27001:2022 and NIST SP 800-207"***

Auteurs : Schmidt, R. et al. (2024)

Revue : *IEEE Transactions on Cloud Computing*

INTRODUCTION

92% of companies use multi-cloud, but 78% suffer breaches related to configuration errors. For this 9th task, I am analyzing a revolutionary Zero Trust framework that meets ISO 27001 and NIST SP 800-207 standards to secure multi-cloud environments.

Title and variables

The title is technical but comprehensive:

Independent:

Type of cloud deployment (AWS/Azure/GCP)

Dependent: Number of data breaches

Moderator: Maturity of Zero Trust policies

A crucial issue: sensitive data is spread across an average of 4 clouds!



Central issue

The major challenge: traditional perimeter security is ineffective in dynamic cloud architectures. Vital question: 'How to apply the principle "Never Trust, Always Verify" in heterogeneous multi-cloud environments while adhering to international standards?'

Innovative framework

The solution: a unified framework with:

- 1) **Intelligent micro-segmentation:** Isolation of workloads via SD-WAN
- 2) **Continuous access control:** Contextual verification (identity + behavior)
- 3) **Unified telemetry:** Centralized monitoring with inter-cloud SIEM Result: 94% fewer breaches among early adopters!

Conceptual model

- 1) **Workloads are encapsulated** in trust zones.
- 2) **The policy engine** applies ISO/NIST rules.
- 3) **The risk analyzer** calculates scores in real-time. Equation:
$$\text{Trust_score} = (\text{Identity_verification} \times \text{Device_security}) / \text{Context_risk}.$$

Normative implementation

Guaranteed compliance:

- ❑ **ISO 27001:2022:** Controls A.8.25 (cloud security) implemented
- ❑ **NIST SP 800-207:** 7 Zero Trust pillars operationalized
- ❑ **GDPR:** Homomorphic encryption for sensitive dataReal case: Secure migration of SAP to AWS/Azure in 3 months!

Best practices

The 5 commandments:

- 1) Map ALL inter-cloud flows
- 2) Enforce E2E encryption (even for data at rest)
- 3) Automate weekly compliance audits
- 4) Adopt machine identities (non-human)
- 5) Test recovery plans monthly

CONCLUSION

This framework makes multi-cloud Zero Trust an operational reality. Next frontier: Integrating post-quantum. Compliance is no longer an obstacle but a security accelerator!

Bibliographic References

Main Article

Schmidt, R. et al. (2024). *IEEE Transactions on Cloud Computing*

↗ DOI: [10.1109/TCC.2024.3389220](https://doi.org/10.1109/TCC.2024.3389220)

International Standards

ISO/IEC 27001:2022 : ↗ [iso.org/standard/27001](https://www.iso.org/standard/27001)

NIST SP 800-207 : ↗ nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Tools

Zero Trust Automation Toolkit : ↗ github.com/cloud-security-alliance/zero-trust-toolkit



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

