



Task 3 Research issues 3
**Zero Trust architecture as a strategic
solution to protect corporate networks
against ransomware attacks**

Field:
Cybersecurity

Prepared by

ALI MMADI, PhD student-Midocean University



Research Issues(3)

Task 3

ALI MMADI

PhD student - Midocean University

www.midocean.ae

As part of assignment number 3 for the Research Issues course, I will critically analyze a recent study in the field of cybersecurity.

The study I have chosen focuses on the Zero Trust architecture as a strategic solution for protecting corporate networks against ransomware attacks.

This study takes place in a global context marked by an increase in sophisticated cyberattacks, particularly ransomware targeting critical infrastructure, businesses, and public institutions.



1. Study Objective

The main objective of this research is to evaluate the effectiveness of the Zero Trust model in preventing, detecting, and limiting the spread of ransomware in corporate networks.

The researchers aim to answer the following question:

Does the adoption of a Zero Trust architecture significantly reduce the risk of lateral infection and privilege escalation in an organizational environment?

2. Methodology used

The study adopts an experimental and analytical methodology.

First, the researchers simulated a traditional enterprise network environment based on the classic perimeter model.

Second, they implemented a Zero Trust model based on:

- ☐ Multi-factor authentication
- ☐ Network micro-segmentation
- ☐ Identity-based access control

Continuous user behavior monitoring

Then, ransomware attack scenarios were executed in both environments to compare:

- The propagation rate
- Detection time
- The level of impact on critical systems

The data were analyzed using risk indicators and quantitative security metrics.

3. Main results

The results show that:

- ❖ The traditional model allows rapid ransomware spread after initial compromise.
- ❖ The Zero Trust architecture significantly reduces lateral movement.
- ❖ Detection time is shorter thanks to behavioral monitoring.
- ❖ The overall impact on critical systems is noticeably reduced.

The authors conclude that Zero Trust is an effective approach to strengthening organizational resilience against modern attacks.

4. Critical Analysis – Strengths

This study presents several important strengths.

First, the comparative methodology is relevant because it allows a realistic evaluation between two security models.

Second, the use of simulated attack scenarios increases the practical validity of the study.

Third, the integration of measurable indicators makes the results objectively assessable.

Finally, the study fits within a cybersecurity risk management framework, which enhances its theoretical coherence.

5. Critical Analysis – Methodological Limitations

However, several limitations should be highlighted.

First, the experimental environment is controlled and does not fully reflect the complexity of real networks.

Second, the size of the organizational sample is limited, which reduces the generalizability of the results.

Third, the study does not sufficiently take into account the budgetary and organizational constraints related to the implementation of Zero Trust.

Fourth, there is a strong dependence on the specific technological tools used in the experiment.

6. Contradictions and discussion

Some recent research shows that Zero Trust can generate excessive operational complexity and administrative burden.

There is also a debate about the actual implementation cost compared to the benefits achieved.

Thus, although the study shows positive results, it does not sufficiently discuss the human and organizational challenges.

7. Positioning of my research project

In my professional context as a network and security manager, this study is very relevant.

However, I believe there is a significant gap:

Few studies analyze the adaptation of the Zero Trust model to hybrid infrastructures in developing countries, where resources are limited.

My future research project could therefore focus on:

A risk-based assessment of the gradual implementation of Zero Trust in resource-constrained hybrid environments.

Conclusion

In conclusion,

This study demonstrates the strategic effectiveness of the Zero Trust model against ransomware.

However, its methodological limitations and lack of contextual analysis pave the way for further research.

This critical analysis allowed me to better understand:

- ❖ How to structure a rigorous methodology
- ❖ How to analyze results scientifically
- ❖ And how to position my own project within a risk-based theoretical framework

Thank you for your attention.

رمضان مبارك

www.midocean.ae

KEY REFERENCES

- 1) Foundational Zero Trust Reference
John Kindervag (2010).
No More Chewy Centers: Introducing the Zero Trust Model of Information Security.
Forrester Research.
This is the original conceptual foundation of Zero Trust.
It introduced the principle: "Never trust, always verify."
- 2) **National Institute of Standards and Technology (NIST)** (2020).
Zero Trust Architecture (Special Publication 800-207).
Publication Date: August 2020
- 3) Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020).
Zero Trust Architecture.
NIST Special Publication 800-207.
National Institute of Standards and Technology.
- 4) Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019).
A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges.
IEEE Communications Surveys & Tutorials.
Publication Date: 2019.
- 5) Chen, L., et al. (2022).
Zero Trust: From Concept to Implementation in Modern Enterprise Networks.
IEEE Access.
Publication Date: 2022.
- 6) Scarfone, K., Souppaya, M., & Cody, A. (2023).
Guide to Zero Trust Implementation and Risk Management.
NIST Technical Report.
Publication Date: 2023.



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

