**Evaluating the Effectiveness of Zero Trust Architectures in Hybrid Work Environments**

Manikanta Puttoj

23249889

Programme Code – Research in Computing CA1

National College of Ireland

# Research Problem Background

The shift toward hybrid offices, where employees spend time in the office and at home alternately, has drastically changed how organisations should secure their IT system. The traditional perimeter-based security models have been unable to fulfill the security requirements of the organizations due to the ability of the users to access company resources in various locations, networks, and devices. In response, the Zero Trust Architecture (ZTA) has emerged as a hot security framework, working under the slogan of "never trust, always verify."

ZTA creates the need to continuously authenticate identity, device posture, and access context, which reduces the attack surface; thus, mitigating risks, such as threat lateral movement. A report by McKinsey & Co. released in 2023 found that organisations which have implemented ZTA frameworks saw a 50 per cent reduction in the number of data breach incidents in hybrid work environments. However, it is difficult to put into practice. The majority of organisations have to cope with the issue of reconciling ZTA principles and legacy systems, managing the impact of user experience and optimisation of authentication and monitoring mechanisms. Moreover, empirical evidence on the effectiveness of ZTA in production hybrid environments is also lacking (Gartner, 2024).

The proposed study will address these gaps by conducting an applied study of ZTA deployments in hybrid work environments, their security effects, usability versus and organisational preparedness (NIST, 2022) ...

# Research Question

How can Zero Trust Architectures be effectively implemented and evaluated to enhance security in hybrid work environments, while balancing user experience and operational efficiency?

# Justification

It is a topical and practically important field of research. The hybrid work model has become a staple of most industries and it is critical to adjust the security models to it. Even though Zero Trust is a critical approach which is being promoted by the leading security frameworks (NIST SP 800-207), empirical advice on how ZTA functions in hybrid environment, and what effects it has on operational processes is scanty.

The research will represent a useful piece of work, as it will conduct a comparative analysis of various ZTA elements, such as identity verification, micro-segmentation, endpoint compliance checks, and monitoring in hybrid work environments. It will also delve into user-based result like authentication friction and perceived usability. Such a twin stance on security efficiency and user experience is under-documented in available literature (Forrester, 2024).

The project is repeatable: Zero Trust elements may be tested with the help of the security platforms and hybrid work testbeds that are available commonly. This research question is measurable since all of the security outcomes (reduction in attack surface, breach attempts), as well as usability indicators (login success rates, user satisfaction) can be quantified. Ethical guidelines of IT security research will be followed closely, and the study will not authorise any monitoring of user behaviour or misuse of personal data.

# Specific Items to be Addressed

Item #1: Baseline scan of the security vulnerabilities in hybrid work environments.  
Item #2: Deploy and set up Zero Trust essentials in a hybrid test environment.  
Item #3: Quantify security posture enhancements (e.g., decreasing lateral movement opportunities, authentication bypass attempts).  
Item #4: Measure the effects of user experience through usability testing and feedback.  
Item #5: Examine the obstacles to ZTA adoption and organizational preparedness factors.

# Bibliography

Forrester (2024). The State of Zero Trust Adoption in Hybrid Enterprises. [online] Available at: https://go.forrester.com/research/zero-trust-adoption-2024 [Accessed 14 Jun. 2025].

Gartner (2024). Implementing Zero Trust Security in Hybrid Work Environments: Best Practices and Pitfalls. [online] Available at: https://www.gartner.com/en/documents/zero-trust-hybrid-work [Accessed 14 Jun. 2025].

McKinsey & Company (2023). Securing the Hybrid Workplace: The Case for Zero Trust. [online] Available at: https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/securing-the-hybrid-workplace [Accessed 14 Jun. 2025].

NIST (2022). Zero Trust Architecture. Special Publication 800-207. National Institute of Standards and Technology. [online] Available at: <https://csrc.nist.gov/publications/detail/sp/800-207/final> [Accessed 14 Jun. 2025].