Effectiveness of Zero Trust Architecture

Mehmet Cuce

Old Dominion University

CYSE425w

Prof. Hamza Demirel

12/9/25

Effectiveness of Zero Trust Architecture

Zero Trust Architecture has become one of the most widely incorporated security strategies in the world, as it is the answer to one the world's biggest security concerns. With the rapid technological growth that the world has experienced, older systems have started to show their age when presented with modern threats. These older systems often adopted parameter based security, meaning trust was assumed based on location rather than authority or status. While effective for its time, this assumed trust doesn't hold up to the tools that bad actors possess. Zero Trust Architecture solves this problem by verifying every user and device within a system, only granting limited access based on their role within the organization (Eijiofor et al., 2025) This method not only acts as a solution to limited capabilities of parameter based systems but also reduces the risk of the human factor.

To expand on the security effectiveness of ZTA, it's worth mentioning how and why ZTA acts as the solution to traditional parameter systems. Systems with zero trust architecture require a database on all authorized users that determines the level of access each user is able to obtain, this system of least privilege prevents unauthorized users from gaining access to restricted resources. Furthermore, by having a database with each user and device, it allows for organizations to monitor and enforce cyber policies within the network. This creates a level of individual accountability as all activities are recorded within the database, not only acting as a deterrent but also acting as insider threat detection. In the case that a threat were to arise, the real time monitoring that ZTA offers enables quick threat detection, preventing a possible attack before it even happens. Each layer of access is tied to a different segment of the system, meaning that if a bad actor were to gain access, it would be difficult to navigate the system and cause

further damage (Jain, 2025) . Overall the level of control that ZTA offers over systems is critical in managing the constant evolving threats in cyberspace, being able to quickly pinpoint and eliminate threats is critical to maintaining system security.

While ZTA has proven to be a good solution to outdated security architectures, it still comes with several notable implications that must be considered, these implications mainly being social, ethical and political. The political implications stem from the fact that ZTA requires lots of time, resources and collaboration between both the public and private sectors. Though ZTA can be challenging to implement, it creates a standard for the private and international sectors, overall improving security for everyone. Besides the political challenges that ZTA faces, the greatest points of discussion are within the social and ethical implications it has. In order for ZTA to be effective, it requires extensive monitoring of systems, constant verification and databases of all users/devices. These databases often contain personal information that allows for users to be identified for verification purposes, which brings us to the ethical dilemma. The main issue with having personal information on a system is that organizations can easily access and distribute this information which creates a concern for how user data is handled. Moreover the implicit lack of trust within ZTA might create issues in authority as everyone falls under the system's watch. While concerns for authority can be noted, the implementation of ZTA creates standards which allows the government to enforce policy within all sectors (Rose et al, 2023).

Overall, zero trust architecture is a proven strategy against the development of threats. While it presents challenges of its own, many of them can be circumvented through proper collaboration between the public and private sectors. Not only allowing organizational security

but creating better security for the individuals as well by promoting accountability and awareness to threats.

References

https://www.google.com/search?q=Zero+Trust+architecture+and+breach+containment+outcomes&rlz=1C1ONGR_enUS1146US1146&sourceid=chrome&ie=UTF-8

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture (NIST SP 800-207). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

Ejiofor, Oluomachi & Olusoga, Oluwafemi & Akinsola, Ahmed. (2025). Zero trust architecture: A paradigm shift in network security. Computer Science & IT Research Journal. 6. 104-124. 10.51594/csitrj.v6i3.1871.

Mushtaq S, Mohsin M, Mushtaq MM. A Systematic Literature Review on the Implementation and Challenges of Zero Trust Architecture Across Domains. Sensors (Basel). 2025 Oct 3;25(19):6118. doi: 10.3390/s25196118. PMID: 41094938; PMCID: PMC12526847.