

Policy Analysis Paper 1: The Development and Application of Zero Trust Architecture

Jacob Rivera

School of Cybersecurity, Old Dominion University

CYSE425W: Cybersecurity Strategy and Policy

Dr. Hamza Demirel

February 8, 2026

Introduction

As the digital world continues to grow and expand, cybersecurity has become a major concern for individuals, businesses, and governments around the world. Most of our everyday activities now rely on digital devices and a stable internet connection. This makes protecting our online information more of a priority than ever. To address these risks, governmental agencies, organizational agencies, and even private companies themselves create and rely on cybersecurity policies and strategies. Out of the many important frameworks, this paper will focus on Zero Trust Architecture (ZTA). This, of which, was developed by the National Institute of Standards and Technology (NIST) and outlined in their Special Publication 800-207. The following paragraphs will explain what ZTA is, why it was developed, how it can be applied, and how it can fit into a broader national policy.

What is Zero Trust Architecture?

According to NIST SP 800-207, the main principle of zero trust (ZT) implies that “...there is no implicit trust granted to assets or user accounts based solely on their physical or network location or based on asset ownership” (NIST, 2020). This means that no one should be trusted automatically just because you’re on a shared network or a company device. Instead, all users trying to access the data will have to prove they are authorized every time they try to access something. The maxim is “always verify, never trust”. Zero Trust Architecture is a more recent cybersecurity strategy that changes how organizations protect their digital systems. There are many definitions regarding ZTA, but in the same document, the operative definition is “...an enterprise’s cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies” (NIST, 2020). Therefore, ZTA can be

understood as an organization's overall approach for how its employees, devices, and systems are allowed to interact with one another, all while utilizing zero trust principles.

The Development of ZTA

Before the idea of ZT was brought to life, the most widely followed cybersecurity strategy was the perimeter security model. This model was heavily relied on from the 1980's through the 2010's, where multiple national security agencies such as NIST, Cybersecurity and Infrastructure Security Agency (CISA), and the Department of Homeland Security (DHS) endorsed the use of it (Poirrier et al., 2025). The model suggested that organizations could stay secure by operating within firewalls and internal network zones. According to the survey article by Poirrier and his peers at the Institute of Electrical and Electronics Engineers (IEEE), access privileges would be given based on the location of systems, grouping them into perimeters. However, this approach began to fail as cyber attacks developed within those walls. Insider threats, such as malicious and unauthorized users getting a hold of authorized devices presented a major risk to the perimeter security model. Additionally, technology continued to change. Throughout the years, and especially during the Covid-19 lockdown, remote work and bring-your-own-device policies meant employees didn't need to be connected to internal network zones in order to access company systems. Because of these weaknesses, the development of a new security strategy was needed. One that could protect systems even when users were not inside a clear defined network.

How ZTA can be applied and fit into a broader national policy

As the perimeter security model becomes more obsolete, organizations transitioning to ZTA can be challenging. Reported by a research article from IEEE, "One of the challenges is the lack of industry standards and concrete frameworks for effectively implementing ZTA... In

addition, migrating to ZTA requires IT system compatibility and interoperability” (Phiayura & Teerakanok, 2023). This statement suggests that since there is no universal set of rules that organizations can follow to apply ZT the same way, they would have to migrate to it slowly on their own. Another challenge they mention is system compatibility. If old systems can’t work well with newer security tools, the use of ZT wouldn’t function effectively. Because of the growth and emergence of cloud computing, traditional perimeter security forms many issues. This is where ZTA comes in, as it can address those problems. According to a scholarly article written by students at Xi’an University of Technology, ZT introduces fine-grained segmentation and requires that “each network session must be independently authenticated at the transport layer before any access to the network or protected servers is granted” (Kang et al., 2023). This means that every time data is requested by a user, they will need to be verified. One method to prove a user is authorized is multi-factor authentication (MFA). Here, the user needs to provide two or more forms of proof in order to be verified. Another method is microsegmentation. This suggests that the network will be broken up into smaller, isolated sections so that even if one section gets infiltrated, they will not be able to move freely onto other sections (Kang et al., 2023).

How ZTA can fit into a broader national policy

ZTA is not just a strategy suggested for individual organizations, but it is also utilized by the United States government. In fact, in early 2022, the office of management and budget mandated the use of ZTA in federal agencies. As a result, the adoption of ZT principles are in place to strengthen our cybersecurity defenses nationwide. By applying ZTA on national level agencies, organizations can better protect sensitive information and critical infrastructures. The

shift to this strategy also encourages good cybersecurity practices across the country, making sure that networks remain secure.

References:

- Kang, H., Liu, G., Wang, Q., Meng, L., & Liu, J. (2023). Theory and Application of Zero Trust Security: A Brief Survey. *Entropy*, 25(12), 1595. <https://doi.org/10.3390/e25121595>
- P. Phiyura and S. Teerakanok, "A Comprehensive Framework for Migrating to Zero Trust Architecture," in *IEEE Access*, vol. 11, pp. 19487-19511, 2023, doi: 10.1109/ACCESS.2023.3248622.
- Poirrier, A., Cailleux, L., & Heide Clausen, T. (2025). Is Trust Misplaced? A Zero-Trust Survey. *Proceedings of the IEEE*, 113(1), 5–39. <https://doi.org/10.1109/JPROC.2025.3555131>
- Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. *NIST Special Publication 800-207*, 1(800-207). <https://doi.org/10.6028/nist.sp.800-207>