

Policy Analysis Paper 3: The Ethical Implications of ZTA

Jacob Rivera

School of Cybersecurity, Old Dominion University

CYSE425W: Cybersecurity Strategy and Policy

Dr. Hamza Demirel

March 29, 2026

Introduction

Zero Trust Architecture (ZTA) is a cybersecurity strategy that goes by the saying “never trust, always verify”. This means that it requires validation of every user, device, and request that goes on inside a network. By order 14028 in 2021 and the Office of Management and Budget’s Memorandum M-22-09, ZTA was instated into several agencies so it became a nationwide practice. It was introduced because of the increase of high profile cyber attacks on the country’s critical infrastructure systems and the inefficiency of the older, perimeter based security models. Although ZTA does present better advancements in cybersecurity compared to perimeter based security models, its broad implementation introduces ethical concerns as well. More specifically, privacy, equity, and individual rights. This paper will go over the costs and benefits of ZTA, the rights it protects and potentially limits, and whether the strategy appropriately addresses individuals’ rights.

Costs and Benefits of ZTA

According to cybersecurity policy expert Vladimir Tsakanyan, “Cybersecurity threats are one of the main national security, public safety, and economic challenges every nation faces in the 21st century” (Tsakanyan, 2017). This goes for both governments and individuals. The benefits of implementing Zero Trust to our security models includes getting rid of built in trust in a digital network, which makes it significantly harder for external or even internal malicious parties to access sensitive information. Of course, the main function of ZTA is to prevent and reduce cyber attacks and while that happens, it indirectly protects citizens by making sure that their digital footprints, banking information, and other personal data are also protected. Additionally, because ZTA greatly decreases the likelihood of an attack happening in the first place, it also decreases the occurrence in which organizations deal with economic consequences that follow after the attack. This can be system recovery costs, legal liability, and the possibility of reputational damage.

However, ZTA also has many costs. In the article written by Gambo and Almulhem (2025), they point out that the main challenge this framework presents is integrating it to legacy systems.

Implementing ZTA to existing security infrastructure can already be a hassle for organizations as it needs

many reconfigurations. If implemented to legacy systems, or outdated computer systems that are still in use, it might require a large financial investment and organizational restructuring if they're expected to meet modern security needs. Because of this, smaller businesses may be unable to meet standards mandated in M-22-09. This can cause the security levels in the nation to be uneven. Beyond financial costs, introducing ZTA can negatively impact user experience and the work culture (Amos, 2024). With constant verification processes, such as repetitive authentication requests, it can slow down productivity and cause frustration among employees.

Rights Protected and Potentially Limited

ZTA protects many crucial rights. Mainly, the right of privacy is supported because it greatly reduces the chances that an unauthorized party accesses personal data stored inside an organization's system. If a company successfully keeps sensitive information protected for a long period of time, customers can trust that their privacy is protected. One obvious right that is protected is security. The purpose of the government suggesting Zero Trust was to better protect the public from threats in the cyber space. At the same time, ZTA can potentially limit rights. As I mentioned before, ZTA can involve constant verification processes. This means that there will be continuous monitoring and with this, employees can be subject to surveillance. Although the right to privacy is protected from external threats, the organization itself can become a source of privacy violations if the monitoring systems are not governed properly.

Whether ZTA Appropriately Addresses Individuals' Rights

Two versions of Zero Trust strategies have been created under the past two administrations. Under the Biden administration, Executive Order 14028 and M-22-09 was established and pushed a strong technical foundation for ZTA throughout all federal agencies. The policy focused on mandating Zero Trust, but ultimately lacked the discussion of ethical implications, such as transparency with organization employees. Under the current administration, President Trump's Cyber Strategy for America was introduced. However the focus shifts towards efficiency and building "Talent and Capacity" through "great investments". While this just works to improve on the previous cyber strategy, it can raise concerns

for individual rights protection. Tigranovich's article reminds us that cybersecurity threats greatly impact public safety and employee wellbeing (Tigranovich, 2017). This suggests that cybersecurity strategies like ZTA should also consider the rights of the individuals working within these systems, not just the technical goals.

Conclusion/Ethical Implications

ZTA presents many benefits and some ethical concerns. While it's mainly supposed to protect the privacy and security of our nation's citizens by preventing unauthorized access to sensitive data, it can also introduce issues like workplace surveillance and unequal financial problems for smaller organizations. Both administrations have pushed for stronger cybersecurity standards, but neither framework has fully addressed the ethical concerns that come with implementing ZTA. To become truly ethical, the policy should include clear guidelines that at least addresses those that are affected. As we know, ZTA is overall a fairly new strategy that is still developing. As it continues to improve, however, the protection of individual rights needs to grow with it.

References

Amos, Z. (2024, October 7). *Overcoming 8 Challenges of Implementing Zero Trust - Risk and Resilience Hub*. Risk and Resilience Hub.

<https://riskandresiliencehub.com/overcoming-8-challenges-of-implementing-zero-trust/>

CYBER STRATEGY for America. (2026).

<https://www.whitehouse.gov/wp-content/uploads/2026/03/President-Trumps-Cyber-Strategy-for-America.pdf>

Easley, M. (2025, December 9). *Pentagon plans to publish zero trust strategy 2.0 in early 2026*. DefenseScoop.

<https://defensescoop.com/2025/12/09/dod-zero-trust-strategy-2-0-expected-early-2026/>

Gambo, M., & Almulhem, A. (2025). *Zero Trust Architecture: A Systematic Literature Review*.

<https://arxiv.org/pdf/2503.11659>

Tsakanyan, V. T. (2017). The role of cybersecurity in world politics. *Vestnik RUDN. International Relations*, 17(2), 339–348.

<https://doi.org/10.22363/2313-0660-2017-17-2-339-348>