

Policy Analysis Paper 5: The Effectiveness of ZTA

Jacob Rivera

School of Cybersecurity, Old Dominion University

CYSE425W: Cybersecurity Strategy and Policy

Dr. Hamza Demirel

April 28, 2026

Introduction

Throughout the previous four policy analysis papers, Zero Trust Architecture (ZTA) has been looked at from multiple different angles. The first paper covered what ZTA is, how it was developed and why it replaced the old perimeter based security models. The second paper looked at the political side of ZTA, covering how EO 14028 and Memorandum M-22-09 made it a requirement for federal agencies. In the third paper, ethical concerns that came with ZTA were addressed, particularly around workplace surveillance, financial inequality, and privacy. The fourth paper dove into the social factors that led to ZTA's creation and how its adoption has changed workplace culture. In this final paper, we will look into how effective ZTA has been as a cybersecurity strategy, drawing on expert evaluations and the policy implications that follow.

How experts have evaluated ZTA

Many experts have looked at how well ZTA performs in the work space, and their findings are helpful in understanding how successful the strategy is. One study that evaluated ZTA's effectiveness comes from an article written by Dotse et al. (2024), who analyzed ZTA adoption across three hundred enterprise environments in different industries including finance, healthcare, and technology. To do this, they measured key performance indicators before and after the implementation of ZTA. Their results found a “40% reduction in threat detection time, 39% improvement in incident response efficiency, and 63% decrease in successful breaches” compared to traditional security models (Dotse et al., 2024). These stats form a strong argument that ZTA is doing a great job in preventing attacks.

Another important evaluation comes from the literature review written by Gambo and Almulhem, which has been referenced throughout the previous papers. After reviewing ten years of ZTA research, they confirmed that the core core components of ZTA, such as continuous

authentication, least privilege access, and microsegmentation, work well in reducing both external and internal threats. However, they also talk about a big challenge with legacy systems, as it requires large financial investment and restructuring (Gambo & Almulhem, 2025). This would connect back to the ethical concerns discussed in my third paper, where smaller organizations were identified as being at a disadvantage when trying to meet the mandate set by M-22-09.

How evaluations lead to additional policy implications

The evaluations above can point to a few clear policy implications. First, the data from Dotse et al.'s study support more federal investing in ZTA. Because the improvements in security and response times are undeniable, it would justify the mandates set by Biden in 2022 and Trump's Cyber Strategy for America in 2026. Also, if ZTA continues to produce results like the ones recorded in Dotse et al.'s study, there is little reason for policymakers to move away from it anytime soon. Second, the challenges that Gambo and Almulhem identify about legacy systems and financial barriers would suggest that the current policy framework that is in place isn't doing enough for smaller businesses. If the federal government keeps setting high security standards without providing resources or guidance to those who cannot afford to meet them, then security levels across the country will remain uneven. This is something neither Biden or Trump has fully addressed, and it arguably is one of the most important areas for future policy development.

How the strategy would be assessed

Assessing ZTA's effectiveness requires looking at the measurable data and the experiences of people affected by it. On the data side, metrics such as mean time to detect (MTTD), mean time to respond (MTTR), breach incident rates, and financial impact measures are good indicators if ZTA is successful or not. These are the same indicators found in Dotse et

al.'s study. On the human side, surveys can get input from employees. In my fourth paper, we discuss the consequences for workplace culture and employee trust that ZTA brings. According to a journal article published by ISACA, employees feel uncomfortable having to constantly be monitored and verified, and the repetitive verification process creates friction in the workplace (Johnson, 2020). Surveying employees on their experience with this process would give policymakers a clearer picture of how the strategy is affecting the people it is supposed to protect. Beyond that, CISA's Zero Trust Maturity Model (ZTMM) could work as a useful benchmark to measure how far along agencies are in their ZTA adoption. The ZTMM breaks adoption into three stages across five pillars, which are identity, devices, networks, applications and data (CISA, 2026). They use the stages to track where each agency stands and what needs to be done in order for them to catch up. If we combine CISA's benchmark with the metrics and employee feedback mentioned above, assessing whether ZTA is actually successful can be easy.

Whether the assessment would demonstrate success

Based on the performance metric data, it would most likely show that ZTA has been successful in achieving its main mission. The numbers from Dotse et al.'s study suggest that ZTA significantly exceeds the previous perimeter based security model. Agencies have also made progress in meeting the mandates set by EO 14028 and M-22-09, which supports the argument that the strategy is working. However, there are gaps that still need to be filled in order for ZTA to be considered fully successful. As discussed in the third paper, smaller organizations continue to struggle with the financial burdens, and the ethical concerns in the workplace have not been completely resolved. Until these issues are addressed, ZTA will remain a strategy that only works well technically, but is inadequate for the people it affects the most.

References

CYBER STRATEGY for America. (2026).

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

Dotse, S. K., Sebuabe, S. Y., Obeng, A., Abudu, S. A., & Pappoe, E. A. (2025). Zero Trust Architecture Implementation in Enterprise Networks: Evaluating Effectiveness Against Cyber Threats. *International Journal of Computer Applications*, 187(45), 975–8887.

https://www.researchgate.net/publication/396143077_Zero_Trust_Architecture_Implementation_in_Enterprise_Networks_Evaluating_Effectiveness_Against_Cyber_Threats

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

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

Johnson, G. (2020, October 30). *The Unintended Consequences of Zero Trust on Enterprise Culture*. ISACA.

<https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/the-unintended-consequences-of-zero-trust-on-enterprise-culture>

NIST. (2021, April 9). *Executive Order 14028, Improving the Nation's Cybersecurity*. NIST.

<https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity>

Young, S. (2022). *EXECUTIVE OFFICE OF THE PRESIDENT OFFICE OF MANAGEMENT AND BUDGET MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES FROM*.

<https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf>

Zero Trust Maturity Model. (2023).

https://www.cisa.gov/sites/default/files/2023-04/CISA_Zero_Trust_Maturity_Model_Version_2_508c.pdf