CISC 3392 Research Paper

Audrey Finerfrock

Eastern Florida State College

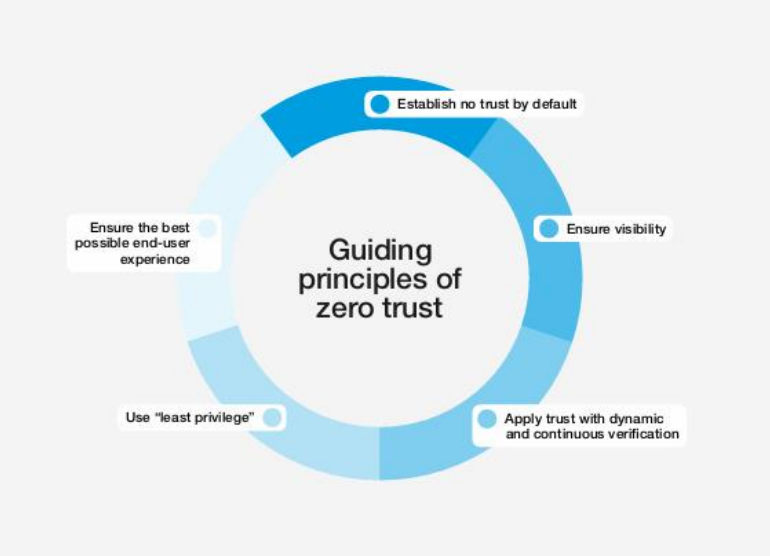
Spring 2025 CISC 3392 Windows Forensics

Table Of Contents

Introduction to Zero Trust

Zero Trust security is a comprehensive approach that assumes no entity whether inside or outside the network can be trusted. Security within an organization is important. As technology advances there are more security risks with devices being used and the privileges on those devices. With proper policies in place, organizations can remain safe along with their employees.

Attacks are always happening, specifically more than 100,000 each day, within a medium sized business (Saini, Gulzar, Turaey, 2024). The goal of these attacks is to compromise the network and to obtain sensitive information. Due to these kinds of attacks, there is a growing need to reinforce the network security within these organizations. The goal of zero trust security is to assume that threats always exist inside and outside of the network. Therefore, requiring continuous verification of identities of devices and users, even remotely. It also encompasses a persons, "...credentials, access management, operations, endpoints, hosting environments" (Rose, Borchert, Mitchell, Connelly, 2020).



Essentially, granting the minimum privileges needed. In 2021, 21% of surveyed organizations have zero trust architecture in place. 25% have made it a plan to adopt one within that same year. Zero-trust is continuing to grow from $27.4 billion to $60.7 by 2027 (World Economic Forum, 2022). Throughout the next few years, organizations will make implementing zero trust a priority to better secure their networks.

Before the use of zero trust, organizations relied on the perimeter-based security model. With this model, it focused on building a perimeter around the network. It did not focus on if there were threats within the network. Therefore, this model relied heavily on firewalls (Souza, 2025). Once users were authenticated, they had access to the internal systems. This method made room for cyberattacks like phishing or malware. In 2023, over 2,365 cyberattacks occurred globally which affected more than 343 million people. This was based on perimeter-based models (Souza, 2025). According to Electroiq, "By 2025, 60% of companies are expected to adopt Zero Trust...". Zero trust will be the greatest current way to prevent breaches, which cost organizations millions.

There are multiple benefits in implementing zero trust for organizations. Security events will be less frequent or be stopped completely compared to current perimeter-based security models. It minimizes the risk of unauthorized access by verifying permissions of the users and devices on a network. Data is then therefore protected from any breaches and leaks. Zero trust is also scalable due to the quick growth of technology and security risks that appear (World Economic Forum, 2022). Reputation can also be damaged if an organization does not have a proper security policy in place (AL, Kabir, 2018). If a security breach occurs of user data, such as credit card information or social security, those people cannot trust that organization anymore. If a security breach happens, it also leads to downtime which then leads to financial losses.

With that there are some challenges that come with zero trust. It can be complicated and time consuming to completely change current infrastructures and policies within an organization. This can also be costly to set up, specifically for smaller organizations. Employees would also need to be trained, which is another cost factor and part of this change. However, the benefits outweigh the challenges and organizations will benefit from implementing a more robust security architecture (World Economic Forum, 2022).

Zero Trust Secuity represents a significant shift in cybersecurity where nothing internal or external is trusted. Given the increase of cyber threats, it is essential that organizations continuously verify users and devices within a network to ensure data remains protected. Although the transition into zero-trust architecture is time consuming and costly, the benefits outweigh the challenges in the long term as cyber threats continue to evolve. Adopting a zero-trust framework will lead to a more secure and resilient security infrastructure.

History of zero trust

Zero trust existed in cybersecurity before it officially was called “Zero-Trust”. The earliest ideas were found in the early 2000s. In 2004, the Jericho Forum introduced the concept of “de-parameterization”. This focused on strengthening security within the internal network instead of just focusing on what attacks may be entering from the outside. In 2007, they officially created principles to steer away from the traditional firewalls, intrusion detection systems, and antiviruses.

In 2010, John Kindervag introduced zero trust. He emphasized that all perimeter-based security models should not be used and to take a more dynamic approach to security. Then now, more recently, in 2020, NIST published an official outline providing guidance on implementing zero trust (Bush, Mashatan, 2022).

Throughout the past few years as mentioned above, zero trust has gained more popularity, and more organizations have planned to implement this security plan. In 2017, there was a security breach at Equifax, and in 2019, at Capital One. Those two significant security breaches led those companies to implement zero trust principles.

Design of zero trust policy

It is important to cover all bases when creating a security policy. All requests should be verified-incoming and outgoing, using multi-factor authentication (MFA). This means that once a user logs into the network, there should be another form of authentication other than their password to ensure that it is them that is logging in. This could be as simple as a numbered passcode or using an app on another device to confirm their login and identity. Least privilege access must be implemented at all times. This means giving the user the minimum amount of privilege needed to do their job, which is managed by an administrator.

Just In Time (JIT) can also be implemented to only give a specified amount of time with a certain privilege. Let's say a user needs to have an elevated privilege to do something. You would not want them to always have access to do this, therefore only implementing an allotted time would be more secure.

Below is a comparison of traditional and zero trust security models.

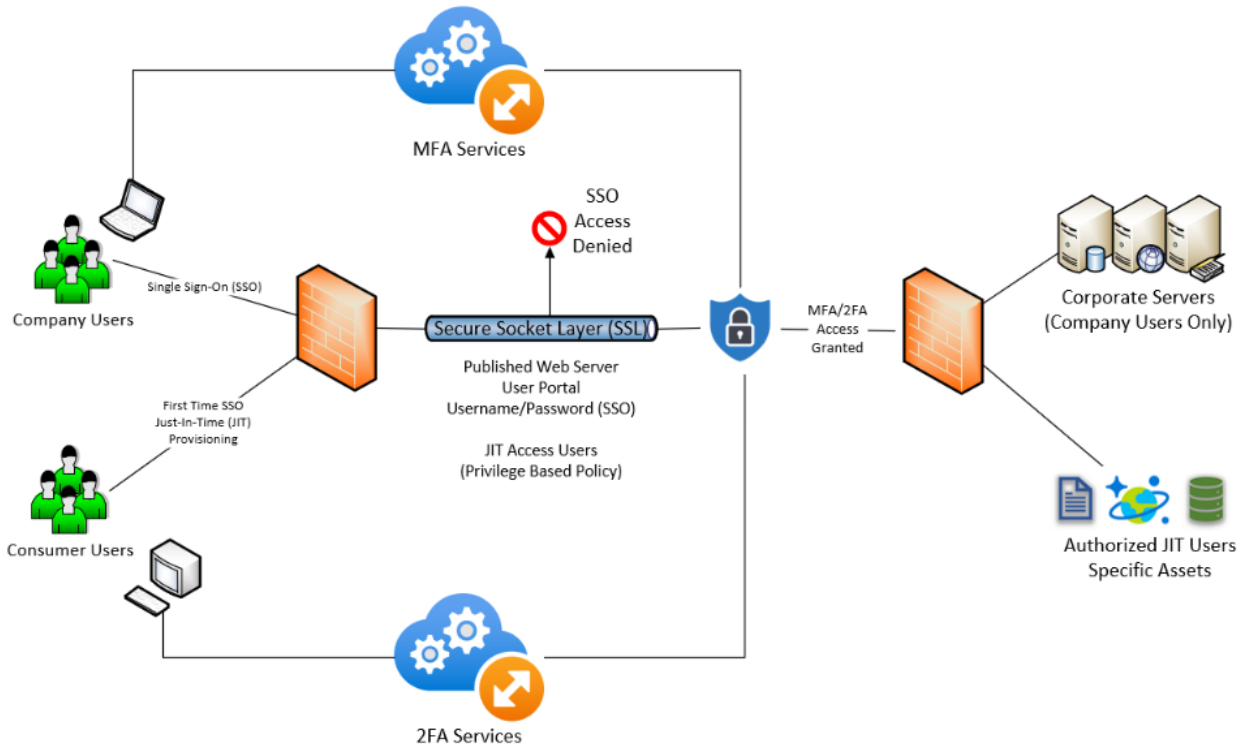
Aspect	Traditional security	Zero trust security
Security perimeter	Relies on network boundaries	Focuses on identity and resource access
Trust model	Implicit trust within the network	No trust; verify every request
Threat mitigation	Limited to perimeter-based attacks	Addresses both internal and external threats
Scalability	Difficult with modern could and remote setups	Designed for distributed environments
Monitoring	Periodic or reactive	Continuous and proactive

Source: ESP International Journal of Advancements in Computational Technology

Zero trust security is stricter on not trusting just any device and user. This creates a stronger more secure network.

Below I have created a zero-trust policy in the form of a diagram to show the connections to how a network should be protected. I have implemented multiple techniques in creating a stronger more secure network.

In the diagram below there are company users and consumer users. They are separated based on which servers they need to connect to. Company users do need a higher level of security/authentication due to the data they will be accessing. Company users will login using SSO (Single Sign-On) which is an authentication method that allows them to log in once with one set of credentials. Following that is MFA (Multi-Factor Authentication) for an extra layer of precaution. Once they validate their SSO login and go through MFA, they gain access to the



corporate servers. There is a firewall at the entrance of the network after SSO and after MFA. Secure socket Layer (SSL) protocol is used to establish an encrypted connection.

Consumer users go through a similar login process, but with Just-In-Time access (JIT). Just in time access is where a certain privilege is implemented to a user for a specified amount of time. This helps to minimize the risk of standing privileges that attackers can exploit. Consumer users will login using SSO then following 2FA. Then JIT will be implemented. 2FA (2-Factor Authentication) is used instead of MFA because users should not have as hard of a time logging in due to them not having access to critical data.

Results

The results of the implemented zero trust diagram demonstrates a clear distinction between access protocols for company and consumer users. Company users use multi-layered authentication systems including SSO, MFA, and SSL encryption which ensures secure access to corporate servers. These measures, reinforced by firewalls, effectively protect sensitive company

data. Consumer users utilize a similar login process such as SSO, JIT access and 2FA. This minimizes security risks while maintaining convenience as consumer users do not require access to critical data. Overall, this diagram shows a balanced framework that upholds zero trust security standards.

Recommendations

There are many ways to enhance a zero-trust policy and different standards to adopt to strengthen overall security within an organization. It is important to include as many as necessary, without overcomplicating the policy. It also must be trainable and understandable to employees.

Adopting a zero-trust framework that integrates device, network, application, and data level security can take current security policies to a greater level. Simply increasing complexity of traditional security models have been deemed insufficient (NIST, Bellamkonda 2022). Modern concepts of securing a networks perimeter between the internal and external network can more easily be bypassed with threats such as Advanced Persistent Threats (APTs). With the use of cloud computing and IoT devices (Internet of Things), there is more risk in that alone (NIST, Bellamkonda 2022). Cybercriminals are continuing to exploit vulnerabilities in traditional security frameworks, making it challenging to mitigate (Kumar, Rachamalla, Vatti 2024). Therefore, not trusting incoming and outgoing will serve as the best protection against attacks in the long run.

Ensuring a strong identity and access management is a useful recommendation to follow by such as enforcing multi-factor authentication (MFA) for all users and devices. This could be something you know (a password), something you have (a phone or token), or something you are

(biometric data). Implementing least privilege access principles and granting users the minimum permissions needed to perform their roles. Admins should also monitor users' behaviors on their systems, and the entire network as well. Implementing micro-segmentation can also make this easier for admins to control and manage and also minimizes the impact of a breach. Each part of the segmented network should be secured individually. If an attacker reaches one part, they may not be able to reach other parts of the network, making this system more secure (Kumar, Rachamalla, Vatti, 2024).

Employing real time continuous monitoring tools to monitor and overseeing network traffic, user behavior, and system performance is also beneficial for security. With machine learning and artificial intelligence evolving, it can be utilized in security analytic tools and find patterns that could indicate threats (Kumar, Rachamalla, Vatti, 2024). This would allow for a quicker reaction to an attacker attempting to access the network.

Zero trust is the new standard of network security and overall security in organizations. Trusting the least number of users and devices can prevent and reduce the number of attacks that occur on organizations. These attacks lead to data loss, a loss of trust, and loss of finances.

As technology advances, attackers are able to change the way they implement their attacks and are continuing to find ways to obtain protected information. Steering away from traditional perimeter-based models, which affected over 343 million people in 2023, will help lessen the amount of cyberattacks that occur yearly.

References

AL, B., & Kabir, H. (2018, April 17). *Information security policy: Need, development and implementation*. Journal of Emerging Technologies and Innovative Research. https://www.academia.edu/42767339/Information_Security_policy_Need_Development_and_Implementation

Ashfaq, et al. S. (2024). *Zero trust security paradigm: A comprehensive survey and research analysis*. Journal of Electrical Systems. https://doi.org/10.52783/jes.688

Bush, M., & Mashatan, A. (n.d.). The ACM Digital Library | Communications of the ACM. https://dl.acm.org/doi/10.1145/374308.374363

Dhiman, P., Saini, N., Gulzar, Y., Turaev, S., Kaur, A., Nisa, K. U., & Hamid, Y. (2024, February 19). *A review and comparative analysis of relevant approaches of Zero trust network model*. MDPI. https://doi.org/10.3390/s24041328

D'Souza, J. (2025, January 31). *Zero trust security statistics by adoption, issues faced and market size*. Electro IQ. https://electroiq.com/stats/zero-trust-security-statistics/

Kang, H., Liu, G., Wang, Q., Meng, L., & Liu, J. (2023, November 28). *Theory and application of Zero trust security: A brief survey*. MDPI. https://www.mdpi.com/1099-4300/25/12/1595

Kumar, R., Rachamalla, D., & Vatti, P. (2024). *Zero-Trust Architectures: Decoding the Future of Enterprise Cyber Resilience*, *3*(1).

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020, August 11). *Zero trust architecture*. CSRC. https://csrc.nist.gov/pubs/sp/800/207/final

The “zero trust” model in Cybersecurity. (2022). https://www3.weforum.org/docs/WEF_The_Zero_Trust_Model_in_Cybersecurity_2022.pdf