CSIT302 Cybersecurity Assignment

Timothy Mah

8750634

txamah001@mymail.sim.edu.sg

# Zero Trust

## Contents



## References

GovTech Singapore. (May, 2023). Government Zero Trust Architecture (GovZTA). Singapore. Retrieved from https://www.developer.tech.gov.sg/guidelines/standards-and-best-practices/government-zero-trust-architecture

National Institute of Standards and Technology. (August, 2020). NIST Special Publication 800-207 Zero Trust Architecture. USA. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

## Summary

In the past, organisational security primarily focused on securing the perimeter of a network. However, with the evolution of technology and business practices, organisations today often adopt a hybrid or fully cloud-based approach to their operations. As a result, the traditional notion of an organization's "perimeter" has become more intricate and challenging to define, especially considering that data and users are dispersed across different geographical locations. Additionally, insider threats have emerged as a significant concern, circumventing conventional perimeter-based network security measures.

Recognizing the need for a more adaptable and robust security framework, the National Institute of Standards and Technology (NIST), an American organisation, introduced the NIST 800-207 standard[a]. This standard delineates the principles and specifications of Zero Trust network architecture, which fundamentally redefines the traditional security model by assuming that threats may exist both inside and outside the network perimeter.

The overarching objective of Zero Trust is to bolster an organisation's security posture by constraining lateral movement within its network infrastructure. This strategic shift aims to mitigate the risk of unauthorized access and data breaches, thereby enhancing overall cybersecurity resilience.

In response to a notable increase in cybersecurity incidents affecting prominent organizations in the United States, the Biden administration took decisive action by issuing an executive order in May 2021. This order mandates that all U.S. Federal Agencies adhere to the guidelines outlined in NIST 800-207 as a compulsory measure for implementing Zero Trust. This directive underscores the government's commitment to strengthening national cybersecurity defences and safeguarding critical assets against evolving threats.

Notably, the principles of Zero Trust are not confined to the United States alone but have also gained traction globally, including in countries like Singapore. The Government Technology Agency (GovTech) in Singapore has established its version of Zero Trust

[a] (National Institute of Standards and Technology, 2020)

architecture, known as the Government Zero Trust Architecture (GovZTA)[b].While GovZTA shares many similarities with NIST 800-207, this document will adopt GovZTA's definition of Zero Trust for clarity and alignment with local practices.

GovZTA emphasises the importance of layered defence mechanisms in enforcing Zero Trust principles, striving to strike a delicate balance between robust security measures and user accessibility. While tighter cybersecurity controls may initially result in reduced accessibility, the overarching goal is to enhance cyber resilience and expedite threat detection across government agencies.

## How Zero Trust works in detail

There are four main core principles that uphold Zero Trust[c].

- Implement least privilege and enforce access control
- Restrict lateral movement
- Incorporate security automation and orchestration
- Strengthen detection and response

### Implement least privilege and enforce access control

The concept of least privilege embodies the principle of providing users within an organisation with access to only the information and resources that are essential for performing their designated roles and responsibilities. This practice aims to minimise the potential for unauthorised access to sensitive data or critical systems, thereby reducing the risk of data breaches or malicious activities.

Implementing least privilege involves establishing granular access controls that govern the authentication and authorisation process for accessing organisational resources. Authentication verifies the identity of users seeking access to specific assets, ensuring that only authorised individuals are granted entry. This often involves the use of secure login credentials, such as usernames and passwords, biometric authentication, or multifactor authentication methods, to validate the user's identity.

Once authenticated, users must then be authorised to access specific resources based on their predefined permissions and privileges. This authorisation process evaluates the user's identity, role, and permissions against the access control policies established by the organisation. Access rights are granted on a per-request basis, meaning that users are only allowed access to resources that are necessary for fulfilling their job functions or completing authorised tasks.

By enforcing least privilege access controls, organisations can minimise the potential attack surface and limit the scope of potential security threats. Additionally, adopting a per-request authorisation model enhances security by ensuring that access rights are dynamically assigned and revoked based on changing user roles, responsibilities, and access requirements. This proactive approach to access management helps organisations mitigate the risk of insider threats, unauthorised access, and data breaches, ultimately bolstering overall cybersecurity posture.

### Restrict lateral movement

Network segmentation, air gaps, and isolation represent sophisticated system designs that serve multiple security purposes within an organisation's infrastructure. These architectural approaches not only enhance access control but also play a pivotal role in curbing lateral movement across the network, thereby mitigating the risks posed by insider threats.

Network segmentation involves dividing a larger network into smaller, distinct segments or zones, each with its own set of access controls and security measures. By compartmentalising the network in this manner, organisations can effectively restrict the flow of traffic between different segments, limiting the potential impact of security breaches or malicious activities. This strategy creates barriers that impede the lateral movement of attackers within the network, making it more difficult for them to traverse from one segment to another undetected.

Air gaps represent an extreme form of network isolation; wherein critical systems or sensitive data repositories are physically or logically separated from the rest of the network. This isolation eliminates direct connectivity between the air-gapped system and external networks, significantly reducing the risk of unauthorised access or cyberattacks. While air-gapped systems offer unparalleled security benefits, they may also pose operational challenges due to the limitations imposed by their isolated nature.

Isolation techniques involve the implementation of virtual barriers or security boundaries within the network environment, segregating different components or assets to prevent unauthorised interactions. This could include isolating high-risk systems or sensitive data stores from less secure parts of the network, effectively containing any security incidents and limiting their impact on the overall infrastructure.

---

[b] (GovTech Singapore, 2023)
[c] (GovTech Singapore, 2023)

By incorporating these system designs into their security architecture, organisations can bolster their defence mechanisms against both external threats and insider attacks. Not only do these measures strengthen access control by enforcing strict boundaries and permissions, but they also act as deterrents against lateral movement within the network. By impeding the progress of attackers attempting to navigate through the network undetected, organisations can enhance their overall security posture and better safeguard their critical assets and sensitive information.

### Incorporate security automation and orchestration

Automated security systems integrated into continuous integration and continuous delivery (CI/CD) pipelines represent a proactive and dynamic approach to bolstering the security posture of software development and deployment processes. These automated security measures are seamlessly woven into the fabric of CI/CD pipelines, ensuring that security considerations are ingrained into every stage of the software development lifecycle.

### Strengthen detection and response

By consolidating logs from various layers of the OSI model, including the physical, data link, network, transport, session, presentation, and application layers, organisations can gain a comprehensive understanding of network activities and communications. This holistic approach allows for the detection of anomalous behaviour or deviations from normal patterns that may indicate malicious activities, such as unauthorized access attempts, data exfiltration, or unusual network traffic.

Analysing aggregated logs enables security teams to correlate information from different layers of the network stack, providing deeper insights into the root causes of security incidents and potential threats. For example, anomalies detected at the network layer, such as unusual spikes in traffic or suspicious IP addresses, may be correlated with application-layer logs to identify specific applications or services that are being targeted by attackers.

## Benefits that Zero Trust can bring

Apart from the general improvement of cyber defence, Zero Trust architecture has proven to be beneficial for businesses.

Cimpress is a large American company that offers mass multi-media customisation services. They rely on e-commerce and IT for their operations. During the COVID-19 pandemic, Zero Trust architecture played a crucial role in maintaining business continuity. As the pandemic forced enterprises worldwide to switch to remote work, many struggled with connectivity and more importantly, ensuring security. However, Cimpress faced no downtime or disruption due to their pre-existing zero trust, cloud-based setup. This allowed them to quickly transition to work from home[d], demonstrating the architecture's efficacy in providing secure and seamless connectivity for all employees, regardless of device or location.

Not only could their staff resume work, their IT team did not have to scramble to set up VPN and other work from home controls. This allowed their IT team to continue developing their Zero Trust Architecture. Results from their internal red team and penetration testing has shown that their network's mean time to detect (MTTD) has decreased. Both their internal testing and external consultants have responded with similar results.

This is one example of how Zero Trust not only improves cybersecurity posture but also business continuity and operations.

## My thoughts on Zero Trust approach

I have studied cybersecurity before. I have a cybersecurity diploma and I have the Certified Ethical Hacker certification. These are nothing much to boast about but they have taught me the general fundamentals of cybersecurity. Across my educational journey, working experience, and personal life, I actually have not heard of this Zero Trust term before. Although the semantic is foreign to me, the concepts are familiar. Least privilege, access controls, devops, these are concepts I've learnt before.

I think Zero Trust practices are great at improving cybersecurity. All the benefits are already highlighted in the previous sections. Then the question comes to mind, "why doesn't everyone adopt Zero Trust? Why was it not adopted earlier?". Like all other cybersecurity measures, cybersecurity is expensive. Businesses are meant to generate revenue. Although certain automation can improve throughput and performance, ultimately security systems are expensive. Not only are the tools, products, and services expensive, but the friction from staff having to incorporate an additional layer into their workflow would also reduce performance.

In an ideal world, everyone understands each other. Everyone can find a middle ground for whatever differences. Unfortunately, or perhaps even fortunately, we live in a big world with billions of minds, all with different opinions. As such, malicious intent cannot be avoided because of our differences. There will be hackers, threat actors, state spies etc.

We have established Zero Trust, or cybersecurity in general, is a must due to our diverse interconnected world. But how much Zero Trust systems should we implement? I think it boils down to the scope. What are the assets and what is their value? In our local context, we have GovZTA established for government agencies. There are many cybersecurity concepts. GovZTA highlights the more pertinent ones for government agencies. I think Zero Trust is a good step in the right direction for legacy organisations to improve their cybersecurity posture.

---

[d] (Teitler, 2021)