LONDON METROPOLITAN UNIVERSITY

islington college
(इस्लिङ्टन कलेज)

CC5052NI Risk, Crisis & Security Management

50% Individual Coursework

on

{Zero Trust Architecture}

Semester 3

2024-25 Autumn

Student Name: Pradip Joshi

London Met ID: 23047485

College ID: np01nt4a230162

Assignment Due Date: Tuesday, December 3, 2024

Assignment Submission Date: Tuesday, December 3, 2024

Submitted To: Apil Chand

Count :

I confirm that I understand my coursework needs to be submitted online via MST Classroom under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

A Coursework Submitted

on

{ Zero Trust Architecture }

Semester 3

2024-25 Autumn

Student Name: Pradip Joshi

London Met ID: 23047485

College ID: np01nt4a230162

Assignment Due Date:

Assignment Submission Date:

Submitted To: Apil Chand

Count :

Abstract

The rapid development of digital world has made Zero Trust Architecture (ZTA) a critical security priority for all the organizations worldwide. This report explores the concept of Zero Trust Architecture in details, importance of Zero Trust in improving cybersecurity, especially considering the increasing shifting towards hybrid work environments post-pandemic. It explains the core principles of Zero Trust including verifying explicitly, enforcing least privileges access, and assuming breach, which collectively improves the defense of organization against the cyber threats. This report also talks about the Zero Trust Maturity model that provides a structured approach to implement Zero Trust across five key pillars: Identity, Devices, Networks, Applications and workloads, and Data. By using this model, organizations can gradually optimize their security posture. This report also examines the benefits of implementing Zero Trust in business environment. Such as improving compliance, reducing attack surfaces and enhancing employe productivity by enabling secure access from anywhere.

Additionally, this report evaluates a case of an organization that suffered a cyber-attack, evaluating how Zero Trust could have mitigated the attack and its impact. Overall, the report shows the significance of Zero Trust in enhancing defense of organization against evolving cyber threats.

It is suggested to have basic level of understanding on IT security to get the complete understanding on what the report is trying to present.

Contents

Table of Figures

1. Introduction

1.1. Background

Zero Trust strategy has become a top security across the industries, with **53%** of organizations considering it essential. It is kept in high priority in the **U.S. (56%)** and **Germany (53%)** where almost every security professional **(96%)** see it as critical strategy for their organization's success. Security professionals are looking to implement Zero Trust strategy to simplify security procedures for employees, to enhance overall security structure and to improve end-user experience (Microsoft, 2021).

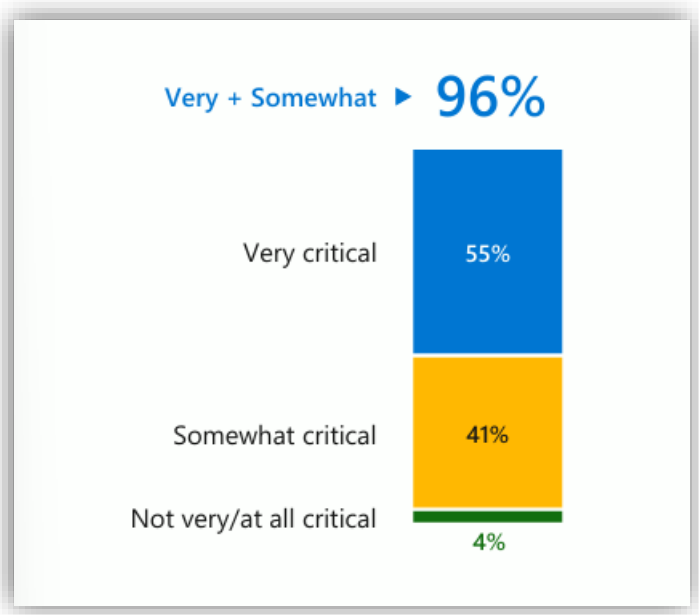

Figure 1 : Survey on criticality of Zero Trust (Microsoft, 2021).

Figure 2 : Survey on reason to shift towards Zero Trust (Microsoft, 2021).

31% of security professionals see it Zero Trust as a critical tool to shift to hybrid workplace after pandemic, especially in **Australia/New Zealand (44%)**. **81% of the organizations** have started the shift towards hybrid model where **31%** have fully adopted it. However, adoption rates vary: **Australia/New Zealand leads at 37%**, while Germany **lags at 20%**. Even as global markets move toward a hybrid workplace at different rates, **91% of organizations** who haven't completed transition are planning to do so within five years. More importantly, **94% are concerned** about employee misuse, increased IT workloads, and increased risk of cyber-attacks (Microsoft, 2021).

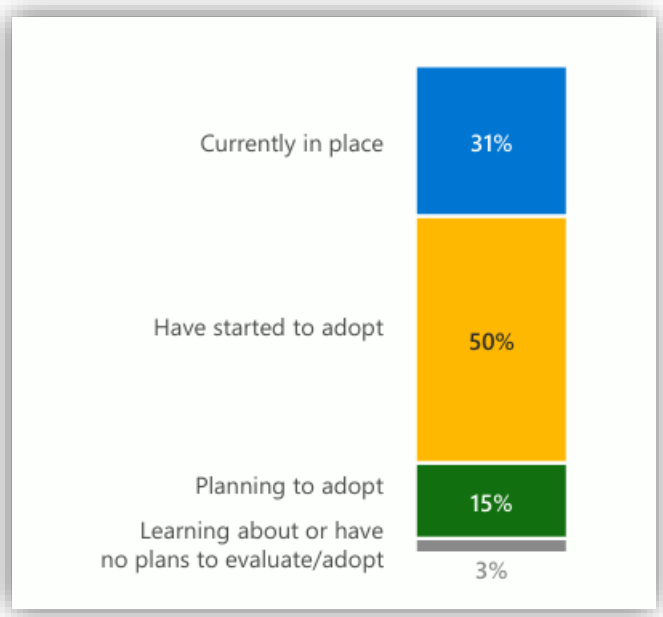

Figure 3 : Survey on intention to shift towards Hybrid workplace (Microsoft, 2021).

Figure 4 : Survey on concerns and challenges in the shift to a Hybrid workplace (Microsoft, 2021).

Therefore, this report focuses on exploring about Zero Trust architecture, its need in present context, its framework and maturity model of Zero Trust along. A case where a organization suffers from cyber-attack is taken to evaluate how Zero Trust architecture would have protected that organization from the attack and its consequences.

1.2. Aims and Objectives

The main of this report is to provide an in-depth understanding of the Zero-trust audit and the zero-trust architecture and the objectives are:

1. To gain comprehensive understanding of the zero-trust architecture.
2. To evaluate the need of zero-trust architecture.
3. To explore about the framework of zero-trust architecture.
4. To explore a case where an organization suffered a cyber-attack.
5. To analyze how zero-trust architecture could have protected that organization or minimized the impact.

1.3. What is Zero trust architecture?

Zero Trust Architecture is a security approach that focuses on the transition from a location-centric to a more data-centric approach to achieve enhanced security controls among users, systems, data and assets that might change over time (William Yeoh, 2023).

In Zero Trust Architecture, it is assumed that no users or devices that resides inside or outside the company network can be trusted. This contrasts with the traditional security methods, which usually need authentication for people outside the network and trust individuals and devices inside the network (SANS Cyber Defense, 2023).

2. Literature review

2.1. Why Zero Trust?

The rise in cloud apps, mobile devices, remote workers, and IOT (Internet of Things) connected devices have made the organizations to align their security policies based on business goals. Adopting Zero Trust means adopting procedures, technology, and policies that promotes business agility and improves security (CyberArk Blog Team, 2023).

Based on context and identification, Zero Trust Architecture substitutes explicit trust for implicit trust. While restricting non-user to authorized resources exclusively, it safely links entities to resources, enabling users to access applications. Zero Trust follows the access principles of "just in time" and "just enough" by enforcing a dynamic and consistent approach to resource protection and visualizing which users are accessing particular apps. Through the alignment of authentication with risk, this method minimizes user friction while promoting a uniform security posture and access policies across users, devices and locations (Gartner, 2024).

2.2. Zero Trust Framework

Zero trust is security architecture that works on the three core principles. They are : Verify explicitly, Use Least privileges access and Assume breach.

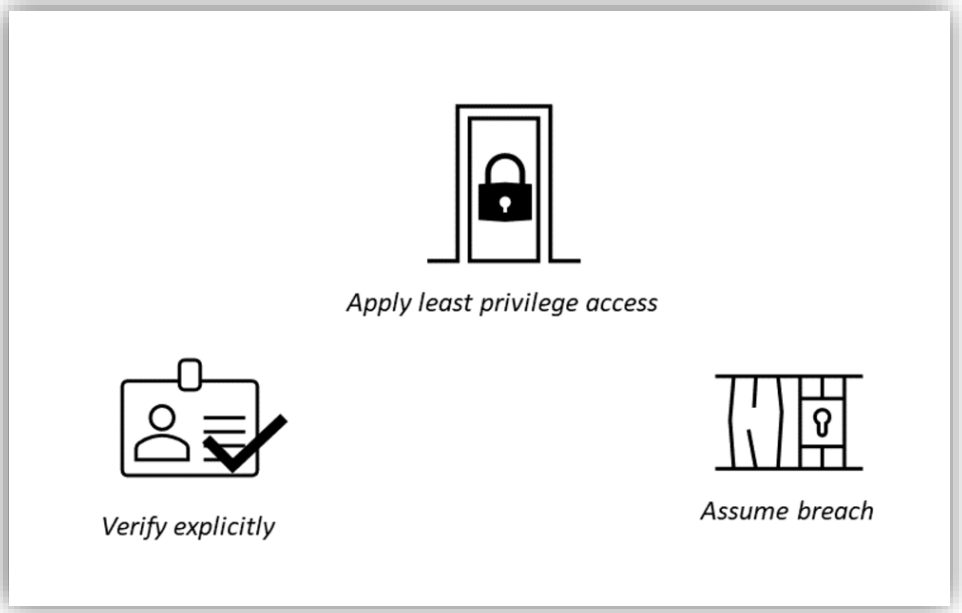

Figure 5 : Core principles of Zero Trust framework

Verify explicitly: It includes always authenticating and authorizing on all the available data points (microsoft, 2024). Standardized authentication protocols such as OIDC (OpenID Connect), SAML (Security Assertion Markup Language), Token-based authentication, multi-factor authentication are some techniques that can be used for authentication (frontegg, 2024).

Least privileges: It includes granting users only the access they require just like an army commander being provided with the information only they need to know. This allows us to reduce the exposure of the sensitive parts of the network (cloudflare, 2024) . Least privileges can be implemented by using the techniques like role-based access controls (RBAC) that gives permissions based on job roles and responsibilities (paloalto, 2024).

Assume breach: It means minimizing the Containment Zone and segment access. End-to-end encryption can be used, and proper analysis should be done to get visibility, drive threat detection, and improve defenses (microsoft, 2024).

2.3. Zero Trust Maturity Model

Zero Trust Maturity Model outlines a progressive approach to implement Zero Trust principles across five pillars in which little improvements can be done over time towards optimization. The pillars are Identity, Devices, Networks, Applications and Workloads, and Data. Each pillar gives the general information on the cross-cutting abilities. They are : Analytics and Visibility, Automation and Governance and Orchestration. The figure given below shows the pillars of Zero Trust Maturity Model (CISA (Cybersecurity and Infrastructure Security Agency), 2023).

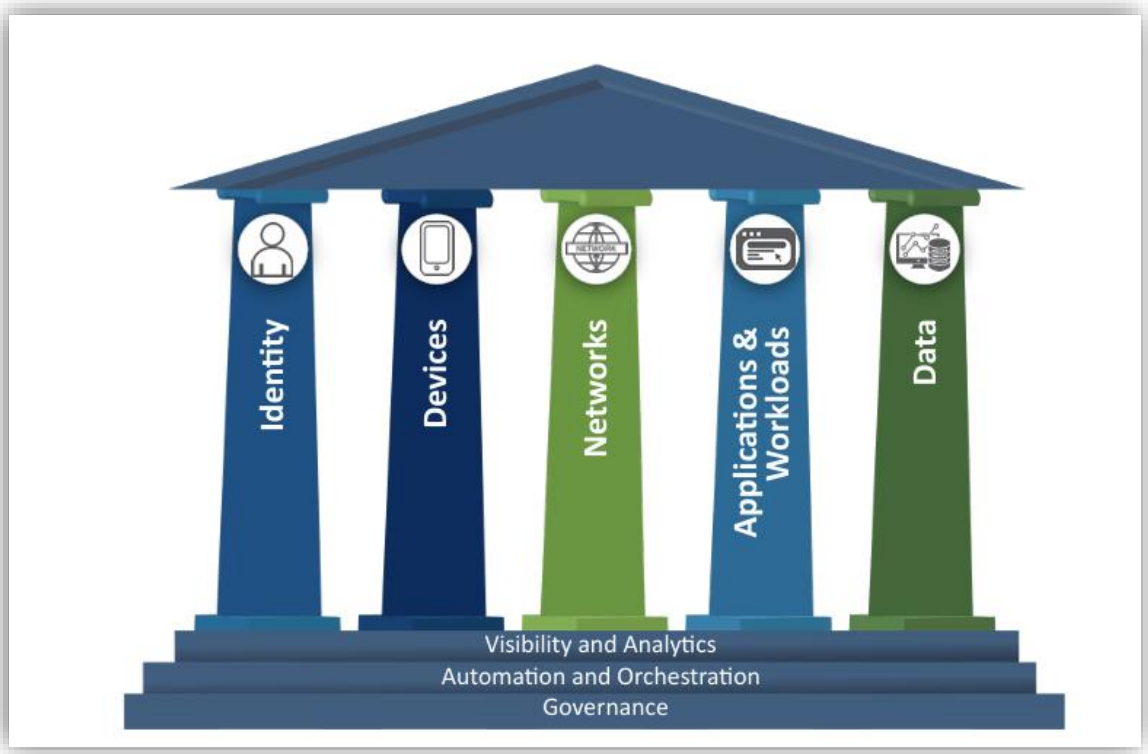

Figure 6 : Zero Trust Maturity Model Pillars (CISA (Cybersecurity and Infrastructure Security Agency), 2023)

The pillars of Zero Trust Maturity Model are described below:

1. Identity

   Users and entities have access to the authorized resources only when necessary and for the appropriate purpose. To enforce robust authentication, customized context-based authorization, and to evaluate identity risk for agency users and entities, identity, credential

and access management solutions should be combined across their whole organization. Integration of the identity stores and management systems should be done across the enterprise to increase awareness of enterprise identities and their duties and authorities (CISA (Cybersecurity and Infrastructure Security Agency), 2023).

2. Devices

In Zero-Trust environment, it's important to consider who has access to the resources along with from where and how it is being accessed. Device pillar suggests that access to resources of the organizations should only be granted to trusted devices that have right security posture. Device authentication, ongoing health monitoring, and confirming that devices adhere to company security guidelines are included in it (Rotlevi, 2023).

3. Networks

ZTA facilitate a shift from conventional perimeter-focused security strategies and allows to control internal and external traffic flows, isolate hosts, enforce encryption, segment activities and improve network visibility across the enterprise. It strengthens defense-in-depth and complement conventional network security by enabling the implementation of security controls closer to applications, data and other resources (CISA (Cybersecurity and Infrastructure Security Agency), 2023).

4. Applications and Workloads

Application security refers to protecting application by preventing exceptions to the application or underline information system's security policies. By combining features from the user, device, network and environment pillars, the application and workload pillar aims in securing access at the application layer to stop data collection, illegal access, and interference with vital operations or services. Users firmly authenticate into applications and underlying networks in sophisticated ZT systems. By adhering to the DoD CS RA (Department of Defense Cybersecurity Reference Architecture) concept, which demands that least privilege should be implemented by setting systems to give just necessary capabilities, applications are further secured with a smaller attack surface ((NSA) National Security Agency , 2024).

5. Data

The data of a business is very useful and significant. Data kept in any form is targeted by malicious attackers. An organization's critical element includes customer records, user credentials, proprietary data, employee personally identifiable information (PII), intellectual property, private emails, etc. whether the organization's data resides inside or outside the network, the ZT (Zero Trust) architecture is built as a data-centric security model that leverages each connected pillar to guarantee the availability, confidentiality and integrity of that data.

Data loss Prevention (DLP) techniques, encryption, tagging and labelling, and the application of data rights management (DRM) technologies are some of the techniques used to secure and enforce access to data both in transit and at rest ((NSA) National Security Agency, 2024).

3. Case study

References

(NSA) National Security Agency , 2024. *Advancing Zero Trust Maturity Throughout the Application and Workload Pillar.* [Online]
Available at: https://media.defense.gov/2024/May/22/2003470825/-1/-1/0/CSI-APPLICATION-AND-WORKLOAD-PILLAR.PDF
[Accessed 26 November 2024].

(NSA) National Security Agency, 2024. *Advancing Zero Trust Maturity Throughout the Data.* [Online]
Available at: https://media.defense.gov/2024/Apr/09/2003434442/-1/-1/0/CSI_DATA_PILLAR_ZT.PDF
[Accessed 26 November 2024].

CISA (Cybersecurity and Infrastructure Security Agency), 2023. *Zero Trust Maturity Model* , Washington, D.C.: CISA (Cybersecurity and Infrastructure Security Agency).

cloudflare, 2024. *Zero Trust security | What is a Zero Trust network?*. [Online]
Available at: https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/
[Accessed 11 november 2024].

CyberArk Blog Team, 2023. *What Is Zero Trust and Why Is it So Important?*. [Online]
Available at: https://www.cyberark.com/resources/blog/what-is-zero-trust-and-why-is-it-so-important
[Accessed 26 November 2024].

frontegg, 2024. *Complete Guide to Authentication in 2024.* [Online]
Available at: https://frontegg.com/blog/authentication
[Accessed 27 November 2024].

Gartner, 2024. *Implement Zero-Trust Architecture to Adapt to a Shifting Threat Landscape.* [Online]
Available at: https://www.gartner.com/en/cybersecurity/topics/zero-trust-architecture
[Accessed 26 November 2024].

Microsoft, 2021. *Zero Trust Adoption Report,* Redmond, Washington: Microsoft.

microsoft, 2024. *What is Zero Trust?*. [Online] Available at: https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview [Accessed 27 november 2024].

paloalto, 2024. *What Is the Principle of Least Privilege?*. [Online] Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-the-principle-of-least-privilege
[Accessed 27 November 2024].

Rotlevi, S., 2023. *How to Implement Zero Trust: A Simplified Guide.* [Online] Available at: https://www.wiz.io/academy/how-to-implement-zero-trust [Accessed 26 November 2024].

SANS Cyber Defense, 2023. *What is Zero Trust Architecture?*. [Online] Available at: https://www.sans.org/blog/what-is-zero-trust-architecture/ [Accessed 26 November 2024].

William Yeoh, M. L. M. S. F. J., 2023. Zero trust cybersecurity: Critical success factors and A maturity. *Computers & Security* , 133(1), p. 13.