LUND UNIVERSITY
School of Economics and Management

Department of Informatics

The Effect of Zero Trust Model on Organizations

Master thesis 15 HEC, course INFM10 in Information Systems

Authors: Can Lu
Umar Shahzad

Supervisor: Miranda Kajtazi

Grading Teachers: Soanee Sarker

Niki Chatzipanagiotou

The Effect of Zero Trust Model on Organizations

AUTHORS: Can Lu and Umar Shahzad

PUBLISHER: Department of Informatics, Lund School of Economics and Management, Lund University

PRESENTED: June 2023

DOCUMENT TYPE: Master Thesis

FORMAL EXAMINER: Osama Mansour, PhD

NUMBER OF PAGES: 124

Keywords: Zero Trust, Cybersecurity, Organization

ABSTRACT (MAX. 200 WORDS):

The increase in cyber threats has prompted organizations to adopt more robust cybersecurity frameworks, such as the Zero Trust model. This study investigates the effects of implementing the Zero Trust model on organizations. Based on qualitative analysis of expert views, it finds that Zero Trust enhances an organization's security posture, despite requiring significant changes in user habits and causing disruptions in workflow due to increased authentication and security measures. However, the benefits, including minimizing attack surface, reduced risk of security breaches, and heightened resilience against cyber threats, outweigh these challenges. The research also identifies the potential of integrating artificial intelligence and big data with the Zero Trust model, which could further improve the accuracy of threat prediction and informed security decision-making. Overall, this study underlines the transformative influence of the Zero Trust model on organizations, suggesting its vital role in fostering a secure, resilient future amidst an evolving cybersecurity landscape. However, it highlights the need for thoughtful implementation to balance security enhancements and user experience. Future research is recommended to explore the practical aspects of integrating AI and big data into the Zero Trust model.

Content

1 Introduction 6
1.1 Background 6
1.2 Problem Area 7
1.3 Objective and Purpose 8
1.4 Research Question 9
1.5 Delimitation 9
2 Theoretical Background 10
2.1 Vulnerabilities of traditional solutions 10
2.2 Zero Trust 11
2.2.1. History of Zero Trust 11
2.2.2. What is Zero Trust 11
2.2.3. What is Zero Trust Architecture (ZTA) 12
2.2.4 Zero Trust Logical Components in (ZTA). 13
2.2.5 Trust Algorithm 14
2.3 Organizational Impacts of Zero Trust 15
2.3.1 Enhanced Security and Risk Mitigation 15
2.3.2 Proactive Incident Response and Business Continuity 16
2.3.3 Complexity and Overhead 16
2.3.4 User Experience and Workflow Disruptions 17
2.4 Zero Trust Features 17
2.4.1 Authentication 17
2.4.1.1 Context-aware user authentication 17
2.4.1.2 Continuous Authentication 18
2.4.1.3 Device Authentication 19
2.4.2 Access Control 20
2.4.3 Micro-segmentation 21
2.4.4 Security Automation and Orchestration 22
2.4.4.1 Threat Intelligence 22
2.4.4.2 IoT and Networking in Zero Trust 23
2.4.4.3 Machine Learning for Security Automation 24
2.5 Summary of Literature Review 25
3. Methodology 28
3.1. Research Philosophy 28
3.2 Research Approach 29
3.2.1 Literature Review Approach 30

3.3 Data Collection Methods 31
3.3.1 Qualitative Research Model 31
3.3.2 Selection of Respondents 32
3.3.3 Interview guide 34
3.4 Data Analysis Method 36
3.5 Ethical Considerations 38
3.6 Scientific Quality 39
4 Findings 40
4.1 Transition to the Zero Trust Model 40
4.2 Enhanced security posture 43
4.3 Impact on users and usage habits 45
4.4 User Experience and Workflow Disruptions 47
4.4.1 Increased Authentication and Security Measures 48
4.5 Future Improvements 49
4.5.1 The Integration of Artificial Intelligence and Big Data 49
4.5.2 The Trustworthiness Assessment of Devices 49
5 Discussion 51
5.1 Transition to the Zero Trust Model 51
5.1.1 Advantage of Transition to the Zero Trust Model 52
5.1.2 Disadvantage of Transition to the Zero Trust Model 52
5.2 Enhanced Security Posture 53
5.5.2 Advantages of Enhanced Security Posture 53
5.5.3 Disadvantages of Enhanced Security Posture 54
5.3 User Experience and Workflow Disruptions 54
5.4 Future Improvements 55
6 Conclusion 59
6.1 Future Work 59
Appendix 1 - Interview Invitation Outline 61
Appendix 2 - Transcription - Respondent 1 62
Appendix 3 - Transcription - Participant 2 79
Appendix 4 - Transcription - Participant 3 85
Appendix 5 - Transcription - Participant 4 93
Appendix 6 - Transcription - Participant 5 101
Appendix 7 - Transcription - Participant 6 112
References 121

Figures

Figure 1: Zero Trust Architecture (Splunk., 2022) 12
Figure 2:Core components of Zero Trust (Rose et al., 2020) 14
Figure 3:Trust Algorithm (Syed et al., 2022) 14

Tables

Table 1: Overview of theoretical background 25
Table 2: Summary of Respondent Details 34
Table 3: Summary of Interview Details 34
Table 4: Summary of interview question details 35
Table 5: The coding interview 37
Table 6: Different phases of each company´s transition. 40
Table 7: Themes and Key Points from our Finding 57

1 Introduction

This chapter provides an overview of our study by covering it with a brief introduction to what is Zero Trust and its potential influence on large Information Technology (IT) organizations. The chapter starts with the background, followed by our research purpose, question, and specific delimitations related to the thesis are presented to specify the focus and scope of the research.

1.1 Background

In recent years, the number of cyberattacks on businesses and organizations has increased dramatically (Johns, 2021). Cybercriminals are continuously developing new tactics and technologies to exploit vulnerabilities in traditional security approaches, such as perimeter-based security (Dumitru, 2022). These attacks can result in significant financial losses, reputational damage, and legal consequences for organizations. To effectively counter these cybersecurity threats, organizations are compelled to adopt robust cybersecurity frameworks and uphold contemporary security best practices. This involves striking a delicate balance between enhancing security and maintaining productivity (Line, Tøndel & Jaatun, 2016). There are other frameworks, such as Information Security Framework ISO 270001, but none of them has gained enough attention in recent years as the emerging and valuable cybersecurity framework as the Zero Trust framework (Rose et al., 2020). It is due to its capability to provide continuous trust assessment and verification for the authenticity of users attempting to access organization resources that makes it potentially useful and also reduces the risk of unauthorized access to sensitive data or resources.

The concept of Zero Trust was first introduced by John Kindervag, a former Forrester Research analyst, in 2010 (Kindervag, 2010). This approach assumes that “never trust, always verify” (Wylde, 2021). The implementation of Zero Trust requires organizations to implement strict access controls and continuous monitoring of user behavior and security events. Access controls are implemented at multiple levels, including network, application, and data layers, and these are continuously monitored and updated based on user behavior and security events (Kindervag, 2010). Zero Trust has multiple benefits for organizations due to its ability to handle privileged and role-based access, which separates users, networks, and applications (Garbis & Chapman, 2021).

During the previous decade, there have been significant developments in the field of cybersecurity, particularly in the areas of access control and security architecture (Syed et al., 2022). In 2013, the International Cloud Security Alliance formed the Software Defined Perimeter (SDP) working group, which aimed to address the challenge of coarse-grained control posed by perimeter ambiguity in the age of mobile and cloud computing (Syed et al., 2022). The concept of SDP is based on identity-based access control, which provides a more granular approach to access control.

The implementation of a Zero Trust model fundamentally transforms network security by requiring continuous authentication and authorization, thereby minimizing unauthorized access, and reducing the attack surface. In 2017, Gartner introduced the Continuous Adaptive Risk and Trust Assessment (CARTA) model, which extends the Adaptive Security Architecture and combines zero trust and attack protection with a focus on continuous risk

and trust assessment to determine the state of security (Campbell, 2020). The CARTA model represents a shift away from traditional perimeter-based security approaches and acknowledges that not all users, devices, or workloads are equally trustworthy. Two years later, Kindervag (2010) presented the Zero Trust Extension (ZTX) study, which extends the view from the network to users, devices, and workloads (Cunningham, 2018). The study emphasizes the importance of identity, not only for users but also for IP addresses, MAC addresses, and operating systems. This view considers identity as a new perimeter and stresses the need for a continuous and comprehensive approach to security (Cunningham, 2018).

Nevertheless, the implementation of the Zero Trust model may also have a negative influence on the organization (Rose et al., 2020). For instance, users may experience delays in accessing resources or could have to repeatedly re-authenticate, which can be annoying and time-consuming. For optimization, organizations are advised to take a user-centered approach in order to improve the implementation of the Zero Trust Model. This approach takes into account the employees' needs and perspectives, along with the technical and organizational elements that can impact the efficacy of the security framework (Gasson, 2003).

While Zero Trust has been widely recognized as a promising framework to address the challenges of traditional perimeter-based security models, its adoption and effectiveness in real-world scenarios remain a challenge. Some organizations may face challenges in implementing the Zero Trust framework due to the complex and heterogeneous nature of their IT environments, the lack of skills and resources, and the potential disruption to existing workflows (Teerakanok, Uehara & Inomata, 2021). The impact of the Zero Trust Model on organizational dynamics needs further investigation. This is essential because the success of any cybersecurity solution hinges not only on its technical robustness but also on user acceptance and efficient performance that facilitates productivity. Understanding these facets in the context of the Zero Trust Model can provide valuable insights into optimizing its implementation within organizations (Buck et al., 2021).

1.2 Problem Area

According to the Zero Trust security model (ZTSM), no person or device may be trusted by default, and access to resources is only given to those who require it after rigorous authentication and permission procedures (Campbell, 2020). The framework is founded on the idea that only those with valid reasons should have access to sensitive information or systems. Zero Trust is a proactive security model that focuses on a more dynamic and risk-based approach rather than the more conventional perimeter-based security methods (He et al., 2022). In response to an escalating prevalence of security breaches and a call for intricate security mechanisms to counteract sophisticated cyber threats, the adoption of the Zero Trust model has noticeably surged in recent years. The Zero Trust Security Model (ZTSM), while offering a myriad of benefits in terms of data protection and risk management, carries potential implications for an organization's operational performance.

The complexity of the authentication and authorization procedure is one of the main issues with the Zero Trust security model as it affects implementation (Chuan et al., 2020). One of the core principles of Zero Trust is to ensure that all tangible and intangible assets in the organization are secure (Garbis and Chapman, 2021), which is why users may need to pass through several stages of authentication before they can access the essential resources due to Zero Trust security only allowing access to resources on a need-to-know basis (Chuan et al.,

2020). This procedure might take a while, especially if the user is using numerous devices or working remotely. Moreover, the necessity for constant monitoring and access verification might make it harder for employees in the organizations to focus on other activities by adding to their administrative workload (Buck et al., 2021). Burnout and dissatisfaction may emerge as consequences, nevertheless, Astakhova's (2022) article fails to pinpoint and identify the targeted companies. Rather, it gives a broad overview with a particular emphasis on the informational behavior of employees in an organizational context.

The deployment of a Zero Trust framework within an organization poses both potential advantages and disadvantages. Clear advantages, such as strengthened data security and improved risk management strategies, stand out prominently. However, these must be carefully weighed against potential difficulties, including the complexity of managing such a framework, potential disruptions to user experience, and the ongoing need for continuous monitoring and evaluation. Hence, it is essential for organizations to consider whether the advantage of adopting a Zero Trust model effectively counterbalances potential negative impacts on their overall structure and operation.

Furthermore, grapple with the challenge of implementing a Zero Trust framework that achieves an optimal balance between stringent cybersecurity requirements and operational considerations. This necessitates a thorough comprehension of the organization's particular requirements, a precise prediction of how a Zero Trust Model may affect its diverse operations, and the capacity to adjust continuously to the changing cyber threat scenario. A Zero Trust model has a wide-ranging impact on a business, having an impact on user experience, operational efficiency, and overall security posture. A comprehensive understanding of the organization's requirements, a readiness to change, and a dedication to striking a long-term balance between security and operational performance are therefore necessary before adopting a Zero Trust model.

The implementation of a Zero Trust security model may have an impact on organizations. However, organizations can effectively deploy such a model by balancing security demands with concerns related to organizational impact, through careful evaluation of their specific needs and measures taken to minimize possible problems.

1.3 Objective and Purpose

A thorough understanding of the potential advantages and disadvantages of implementing the Zero Trust framework necessitates an in-depth analysis of its impact on organizations. The aim of this study is to provide an in-depth understanding of the advantages and disadvantages tied to the adoption of the Zero Trust model, along with its consequential effects on organizational functioning. This research strives to offer valuable insights and practical recommendations to organizations contemplating the integration of the Zero Trust model into their security infrastructure, thereby fostering an informed decision-making process.

In addition, this study provides valuable insights and recommendations for large IT organizations that are considering or have embraced a zero-trust architecture framework. The study aims to help organizations understand how to utilize a zero-trust model to improve overall security while reducing the potential adverse impact on the user experience.

Further, this research is dedicated to providing organizations with strategies to avoid potential issues and ensure that the benefits of a Zero Trust model outweigh the disadvantages. This may involve making investing in user-friendly authentication and authorization processes, equipping staff with the necessary training and support, and ensuring that the organization receives sufficient management support to handle any increased administrative workload bought on by the adoption of Zero Trust.

The study also aims to investigate the potential effect of implementing a Zero Trust framework in organizations and provide recommendations on how to maintain a high level of cybersecurity best practices.

1.4 Research Question

- What effect does the implementation of the Zero Trust Model have on organizations?

1.5 Delimitation

The main topic of this research is the effect of the ZTSM on organizations. However, this study does not discuss the implications of zero trust on privacy or regulatory compliance. The study examines the effects of ZTM on organizations. It does not explore the implications of zero trust on privacy, regulatory compliance, or other peripheral aspects. The research concentrates on selected organizations' impact metrics relevant to the ZTM implementation. Other potentially related metrics, such as employee satisfaction or financial performance, are not included in this investigation.

The research includes organizations that have adopted or implemented ZTSM. The study utilizes both publicly available data and information, such as published reports and surveys, as sources of data. However, in cases where confidential or private documents may offer relevant and necessary information, such documents are included in the analysis. This study follows strict ethical guidelines regarding confidentiality and informed consent. This approach ensures that the study's findings are based on a comprehensive and diverse range of data sources while upholding the necessary ethical standards to protect the confidentiality and privacy of any sensitive information included. This research is grounded in six interviews conducted with organizations that currently use ZTSM, as the primary objective of the study is to examine the effects of Zero Trust implementation on organizations.

By delimiting the scope and boundaries of the study, the research can be more focused and targeted while also providing a clear understanding of its limitations and potential biases. This helps to ensure that the study provides valuable insights into the impact of the Zero Trust model on organizations, while also acknowledging its limitations and potential sources of error.

2 Theoretical Background

The theoretical underpinning of this thesis necessitates a comprehensive review of the scholarly literature related to the research topic to attain an in-depth understanding of the research subject. In addition to examining the various theoretical concepts that provide theoretical insights, the focus within this chapter is also on gaining insights into concepts that are used during the research.

2.1 Vulnerabilities of traditional solutions

Traditional computer networks have played an indispensable role in the expansion and growth of companies. These networks employ various topologies, such as stars, rings, buses, and meshes, meticulously designed to facilitate efficient communication pathways between nodes and ensure seamless data transmission across the network. A diverse array of hardware and protocols enable data transfer and communication between interconnected devices, with common network hardware including bridges, switches, hubs, and routers (Chen, Hu & Cheng, 2019).

In recent years, organizational operations have shifted due to the increasing popularity of working from home and trends such as Bring Your Own Device (BYOD). These changes, amplified by the Coronavirus pandemic, have resulted in users and devices needing dynamic access to data and applications from outside the internal corporate network (Chen, Hu & Cheng, 2019; Moubayed, Refaey & Shami, 2019). The integration of service providers and partners as well as the sharing of resources with third parties are examples of external connections that provide difficulties for an organization's network infrastructure. (DeCusatis et al., 2016).

Most organizations have enabled external access to internal resources to handle the dynamic changes in organizational operations. This works by creating an encrypted link between the external user or service and the internal network(Moubayed, Refaey & Shami, 2019). Users and services within the network are classified as trusted and have access to its resources (Chen, Hu & Cheng, 2019). However, current solutions, often consisting of static rule sets, firewalls, VPNs, and subnetworks, have difficulties responding to these dynamic changes (Chen, Hu & Cheng, 2019; DeCusatis et al., 2016).

There are significant disadvantages as a result of this architecture. First, the internal network has no controls or segmentation (Chen, Hu & Cheng, 2019). Once an external intruder or malicious insider gains access, they can access large areas of the network and potentially read, modify, and damage many organizational resources (Shlapentokh-Rothman, Hemberg & O'Reilly, 2020). Measures to restrict lateral movement through the network are scarce (Kumar et al., 2019). Second, the security level depends on the weakest protected device or application, allowing attackers to use poorly protected devices or applications as entry points into the internal network (Chen et al., 2019; Shlapentokh-Rothman et al., 2020). The security of the internal network depends on how well-protected the weakest device or application is.

Third, IP addresses for gadgets and services are publicly known. Existing solutions first establish a connection before confirming the user's access privileges, making them vulnerable to abuse via distributed denial-of-service (DDoS) assaults, for example (Kumar et al., 2019). Fourth, log files are stored on centralized log servers. Intruders can access the log files to disguise their activities and erase their tracks.

There is a pressing need to move to the Zero Trust model as the traditional computer network is no longer sufficient in addressing the complex and evolving cybersecurity challenges organizations face today. The Zero Trust model provides a more robust, adaptive security solution that eliminates the trust assumptions associated with traditional networks. Organizations can better protect their sensitive data and resources, mitigate insider threats, and adapt to the ever-changing cyber threat landscape.

2.2 Zero Trust

2.2.1. History of Zero Trust

The traditional security practices failed to meet the needs due to the increasing number of devices and their mobility requirements, as they did not consider the threat from within the network. As a result, late in 2004, the concept of de-perimeterization emerged, which strengthened the internal defenses of the organization and placed less emphasis on the external boundary. However, in 2007, the Jericho Forum and the Defense Information Systems Agency (DISA) introduced the principles and practices required for de-perimeterization, including the so-called "black core" security model, which focused on individual transactions instead of perimeter security. However, it was not until 2010 when John Kindervag from Forrester Research introduced the concept of zero trust and zero trust architecture (ZTA) that these ideas gained widespread recognition in both academia and industry.

2.2.2. What is Zero Trust

The Zero Trust model is a cybersecurity paradigm that advocates for a "never trust, always verify" principle, requiring continuous validation and verification of all entities attempting to access organizational resources (Kindervag, 2010). The National Institute of Standards and Technology (NIST) defines Zero Trust as a collection of concepts aimed at reducing ambiguity in access decisions by treating the network as potentially compromised (Kindervag, 2010). Zero Trust's main aim and mission were to stop and protect data from hackers and stop non-potential movements in a network (Rose et al., 2020). Zero Trust is not a specific architecture but rather a framework with guidelines on how to protect an organization's security at different layers. The primary concept underlying Zero Trust is the notion of withholding trust from all devices, as information may be inadvertently shared with unauthorized stakeholders without a secure verification process and proper identification of the recipient. This approach stems from the potential risk of external entities masquerading as employees within the organization to gain access to sensitive data (Buck et al., 2021). Rather than applying to the entire network, Zero Trust is activated on a per-user session basis, enhancing security measures (Rose et al., 2020). As a strategic framework, Zero Trust is founded upon a set of principles which are *Users, Devices, Network, Applications,*

Automation and Analytics as shown in Figure 1 that collectively contribute to the establishment of a comprehensive, holistic Zero Trust environment.

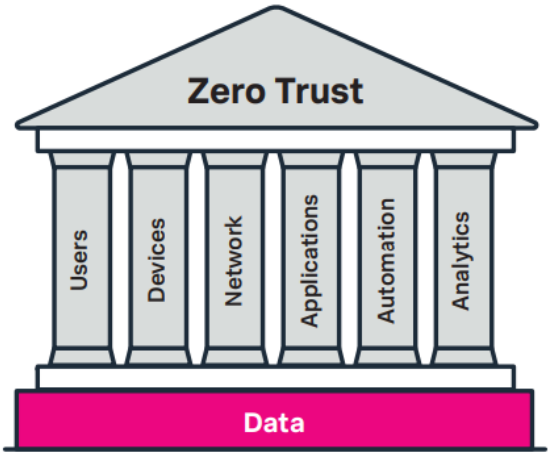

Figure 1: Zero Trust Architecture (Splunk., 2022)

2.2.3. What is Zero Trust Architecture (ZTA)

Zero Trust Architecture (ZTA) is the overall system design that supports this approach. Wu, Yan, and Wang (2021) emphasize in their work that ZTA is an end-to-end approach that seeks to transform network and data security paradigms. The ZTA approach emphasizes different dimensions connected to it such as identity access management, credential, users, application and infrastructure. Several dimensions in Zero Trust Architecture aim to prevent unauthorized access to a network and stop lateral movement within digital platforms and the web. This approach differs from traditional security methods that focus on surface-level security and interface monitoring to prevent and detect unauthorized communication channels passing through protected devices such as gateways, routers, firewalls, and encrypted tunnels.

Zero Trust Architecture prioritizes preventing risks and ensuring only authorized access to the network. On the other hand, Wu et al., (2021) highlight that ZTA is dynamic, and it requires identity-based and dynamic, trusted access control systems. This innovative approach serves as a mediator that facilitates interactions between subjects and objects within the context of a security framework (Wu, Yan & Wang, 2021). The approach is both transformational and linked to the ever-evolving environment, which is characterized by heightened levels of interconnectedness and complexity.

Wu et al., (2021) further mentioned there are numerous advantages to implementing Zero Trust Architecture (ZTA), including identity-based business security, continuous trust assessment, dynamic access control, encryption, and authentication measures. Additionally, ZTA challenges the conventional assumption of "trust by default" through mandate authentication. Moreover, other types of data sources are incorporated into ZTA for evaluating ongoing trust and dynamically assigning permissions through pattern recognition. This ultimately leads to the establishment of a trust ecosystem.

According to NIST (Rose et al., 2020), the ZTA is based on the following seven basic tenets:

- Resource: Any data source or computing service.

- Communication Security: Ensuring secure communication regardless of location.
- Session Security: Granting access to resources on a per-session basis, where authentication and authorization for one resource may not extend privileges to others.
- Access Control: Access to resources is determined by dynamic policies, taking into account the observable state of client identity, application, and requesting asset.
- Minimum Security Posture: Ensuring that all owned and associated devices maintain the highest level of security and continuously monitoring assets to enforce this.
- Continuous Authentication: Implementing dynamic and strict authentication and authorization for all resources.
- Information Logging: Collecting as much information as possible about the current state of the network infrastructure and communications to improve the organization's security posture.

2.2.4 Zero Trust Logical Components in (ZTA).

Zero Trust Architecture (ZTA) is composed of various logical components that work together to create a cohesive security model in an enterprise, which are displayed in Figure 2 below. The following sections outline the key logical components of a ZTA (Syed et al., 2022). Fu et al. (2022) emphasizes that ZTA is built upon two main components, often named as data plane and control plane. The data plane task is to handle network traffic and resource operations while the control plane is responsible for handling access and authorization access. The control plane consists of two critical and logical components: Policy Engine (PE) and Policy Enforcement Point (PEP) (Fu et al., 2022).

- Policy Engine (PE): The Policy Engine is responsible for determining access to resources based on enterprise policy and external input. As the PE makes decisions regarding access, the trust algorithm may introduce delays in resource access if the decision-making process is slow or requires additional validation. Furthermore, if the trust algorithm is overly restrictive, it may inadvertently block access to resources that employees need to perform their tasks.
- Policy Administrator (PA): The Policy Administrator component establishes and manages communication paths between subjects and resources. The efficiency of the PA in setting up and closing down communication paths can impact user productivity. If the PA is slow in generating session-specific authentication tokens or credentials, employees may experience delays in accessing resources, leading to frustration.
- Policy Enforcement Point (PEP): The Policy Enforcement Point monitors and manages connections between subjects and enterprise resources. In a Zero Trust environment, PEPs may need to enforce more stringent access controls, which can lead to increased latency and slower resource access times. Additionally, if PEPs are not optimally configured, they may create bottlenecks in the communication paths.

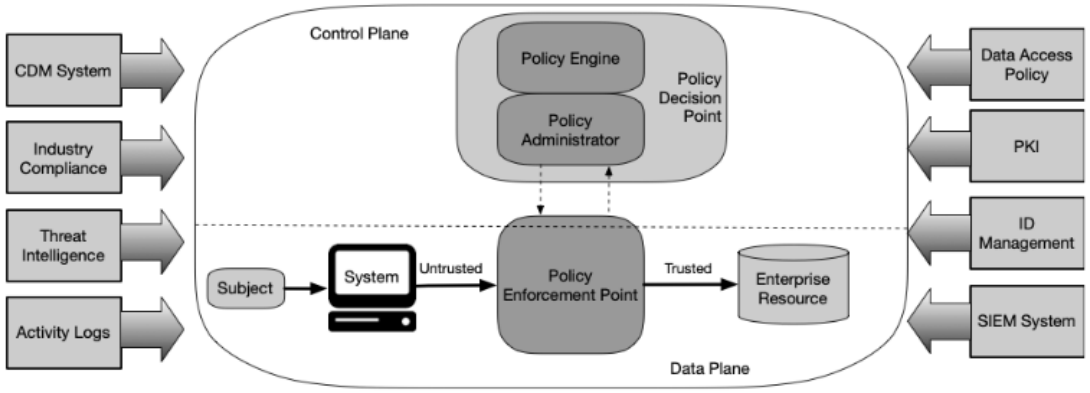

Figure 2:Core components of Zero Trust (Rose et al., 2020)

In addition to the core components mentioned earlier, several external components facilitate the implementation of Zero Trust security. These external components work with the core components, enhancing their capabilities and enabling a more effective Zero Trust environment. As described earlier, the Policy Engine (PE) makes access decisions by leveraging a Trust Algorithm (TA).

2.2.5 Trust Algorithm

The Trust Algorithm (TA) plays a vital role in determining the impact of Zero Trust implementation on user productivity in IT organizations. By analyzing various factors and data sources, the TA makes informed access decisions, affecting how users interact with resources and applications as shown in Figure 3.

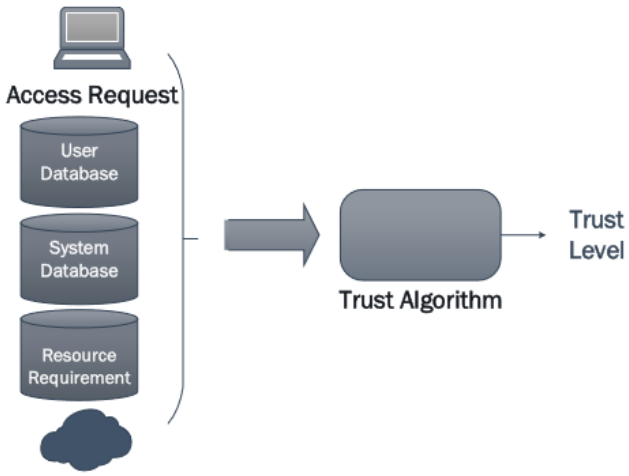

Figure 3:Trust Algorithm (Syed et al., 2022)

The TA considers the following data sources:

- Access Request: When a user makes an access request, the TA uses basic information about the resource and requester (e.g., operating system, patch level, and application used) to evaluate the legitimacy and appropriateness of the request.
- User Identification, Attributes, and Privileges: The TA considers user-related information, authentication methods, and attributes like time and location. User privileges, as encoded in the identity management and policy database, also contribute to the decision-making process.
- Asset Database and Observable Status: This database contains the status of all resources. The TA compares this information against the requester's observable status (e.g., operating system, patch level, location) to make an access decision.
- Resource Access Requirement: These policies specify the minimal requirements for accessing a resource, as set by the custodian (e.g., multi-factor authentication at a new location).
- Threat Intelligence: The TA uses information on potential threats, such as attack signatures or malware, from internal or external sources to make informed decisions.

The TA can be implemented in different ways, as described below:

- Criteria vs. Score-based TA: Criteria-based TA requires a combination of attributes to be fulfilled before allowing access. In contrast, score-based TA uses weighted values of input data to compute a confidence level, which is then compared against a threshold value (Rose et al., 2020).
- Singular vs. Contextual TA: Singular TA does not consider the user's historical information when making a decision, leading to faster decision-making but potentially missing some threats (Rose et al., 2020). Contextual TA, on the other hand, considers the user's historical behavioral patterns, increasing the likelihood of detecting potentially malicious requests.

2.3 Organizational Impacts of Zero Trust

Zero Trust is a cybersecurity Model that requires verification and authentication of every user, device, and network connection before granting access to an organization's resources. While this approach significantly improves security, it can also have implications within an organization and individual.

2.3.1 Enhanced Security and Risk Mitigation

The Zero Trust model's rigorous security measures, characterized by its "never trust, always verify" approach, provide a robust framework for protecting an organization's resources and sensitive data. By implementing strict access controls, multi-factor authentication, and

continuous monitoring, Organizations reduce the risk of unauthorized access, data breaches, and other security incidents significantly. In terms of productivity, a secure environment allows employees to work with confidence, knowing that their data and systems are well-protected. This sense of security can lead to increased focus, engagement, and commitment to their work, ultimately contributing to improved productivity (Morgan, 2020). Moreover, a secure environment helps ensure that critical systems remain operational and available, minimizing downtime and enabling employees to work without disruption (NIST, 2020).

2.3.2 Proactive Incident Response and Business Continuity

The Zero Trust model emphasizes continuous monitoring and real-time threat detection, enabling organizations to proactively identify and respond to security incidents. By adopting a proactive approach, IT teams can quickly detect, analyze, and remediate potential threats, minimizing the impact of security breaches on business operations (Kindervag, 2010). When organizations can promptly address security incidents, they reduce downtime, maintain business continuity, and ensure employees can continue working efficiently (SANS Institute, 2019). Additionally, proactive incident response strategies allow IT teams to learn from past incidents, refine their security measures and adapting to emerging threats. This ongoing learning process helps organizations stay ahead of evolving cybersecurity risks, ensuring the continued protection of their resources and maintaining a productive work environment.

2.3.3 Complexity and Overhead

While the Zero Trust Model offers significant advantages in terms of securing an organization's resources, it also introduces challenges related to increased complexity and overhead. These challenges can impact productivity and require additional investments in personnel, training, and technology (Teerakanok, Uehara & Inomata, 2021). Implementing a Zero Trust model necessitates continuous and context-aware authentication for users and devices, which can lead to increased complexity and overhead in the system. The Zero Trust model often necessitates the use of multifaceted authentication procedures, encompassing elements such as passwords, tokens, biometrics, and geolocation data. These added layers of security can inadvertently contribute to extended wait times and heightened cognitive load for users tasked with memorizing and managing diverse credentials (Nguyen et al., 2019). Tools such as Multi-Factor Authentication (MFA) and Single Sign-On (SSO) have been introduced to alleviate these complications. However, their efficiency is conditional, varying in accordance with the specificities of individual situations.

The Zero Trust model also requires strict access policies, continuous monitoring, and regular evaluation of user access rights, device compliance, and network traffic. This can lead to a significant increase in administrative tasks for IT teams, potentially diverting their focus from other essential duties. The additional workload might require hiring more IT staff or investing in automation tools, contributing to overall cost and complexity. Organizations must establish robust incident response plans and invest in employee training and awareness programs to ensure users understand the importance of following security procedures and adhering to access policies. However, these measures can increase the complexity and time required for successful implementation.

The successful deployment of a Zero Trust model demands a comprehensive understanding of an organization's resources, users, network architecture, and potential threats. Adaptive

authentication, which dynamically adjusts required authentication factors based on contextual information, further complicates the authentication process but enhances security by tailoring authentication requirements to the risk level of each access request (Nguyen et al., 2019). The need for specialized expertise in cybersecurity, networking, and cloud computing can further complicate implementation, necessitating collaboration among various teams within the organization and sharing of knowledge.

2.3.4 User Experience and Workflow Disruptions

As the Zero Trust model demands continuous and context-aware authentication for users and devices, the increased security measures often result in longer wait times and greater cognitive strain for users who must remember and manage various credentials. These delays may not only lead to reduced productivity but can also cause frustration among employees who perceive these additional authentication steps as impediments to their daily tasks. Organizations must carefully balance the need for robust security measures with the potential for negative impacts on employee morale and overall user experience.

User experience and workflow disruptions can have significant consequences on employees' efficiency within an organization (Adikari, McDonald & Campbell, 2011). When employees navigate complex systems and encounter obstacles while accessing resources or completing tasks, they may experience delays in their work processes, leading to reduced productivity (Brouwer et al., 2002). In the context of a Zero Trust model, which involves multiple authentication steps and increased cognitive strain, for example, employees might be required to enter their credentials multiple times throughout the day, causing delays and potential frustration. These disruptions can directly impact employees' ability to focus and efficiently perform their duties.

As employees face complex systems or cumbersome authentication processes, they must devote additional time to navigating these obstacles. This time could otherwise be spent on more productive tasks, contributing to the organization's overall efficiency. In a Zero Trust model, where continuous and context-aware authentication and trust assessment are required, employees often face longer wait times to access resources, significantly affecting their efficiency. In conclusion, user experience and workflow disruptions can have a direct and profound impact on employee efficiency within an organization.

2.4 Zero Trust Features

In this section, we will explore the various features of the Zero Trust model and examine how they affect an organization.

2.4.1 Authentication

2.4.1.1 Context-aware user authentication

Context-aware user authentication presents a sophisticated security methodology that contemplates a range of contextual elements during the decision-making process to grant or deny user access. This technique transcends conventional authentication mechanisms such as username-password combination or multi-factor authentication, by factoring in the extensive context surrounding a user's access request (Hayashi et al., 2013). Context-aware

authentication's inherent capability to analyze such contextual data enables it to deliver more discerning judgements regarding the approval, denial, or the necessity for supplemental authentication steps for a given user. This advanced approach strikes a balance between maintaining robust security controls and providing an efficient user experience.

Some common contextual factors considered in context-aware user authentication include:

- Location: The user's geographical location, ascertained from IP address or GPS data, emerges as a pivotal element in gauging the legitimacy of an access request. As an illustration, should a user who traditionally accesses resources from a specific location suddenly attempt to gain access from a different country, the system may interpret this anomaly as potentially suspicious. Subsequently, it may necessitate supplementary authentication measures as a response to this unexpected change in location patterns (Jakobsson et al., 2009).
- Time: The time of day or the time since the last successful login can be used to assess the risk associated with an access request. Access attempts outside of regular working hours or at unusual intervals may be deemed suspicious, prompting the system to request additional authentication or deny access.
- Device: The type of device and its security posture play a crucial role in context-aware authentication (Jakobsson et al., 2009). If a user attempts to access resources from an unrecognized or non-compliant device, the system may require additional authentication or deny access altogether.
- Behavior: Analyzing user behavior patterns, such as login frequency, resource access patterns, and typical data usage, can help identify anomalies that may indicate unauthorized access attempts. Unusual behavior may trigger additional authentication requirements or access restrictions.
- Risk Score: Combining various contextual factors, a risk score can be calculated to assess the overall risk associated with a particular access request. High-risk scores may result in additional authentication steps or access denial, while low-risk scores may allow for seamless access.

By incorporating context-aware user authentication into a security framework, organizations can strengthen their overall security posture and better protect their systems and data from unauthorized access (Kim et al., 2018). This strategy facilitates a more tailored and adaptive authentication procedure, diminishing resistance for verified users whilst upholding rigorous security standards. Context-aware user authentication forms a critical component of contemporary security frameworks, such as the Zero Trust model. This model underlines the significance of persistently verifying user identities and access rights, utilizing contextual data as a basis for decision-making. This approach integrates both user convenience and security, delivering a robust and user-friendly authentication experience.

2.4.1.2 Continuous Authentication

Traditional modes of authentication, such as passwords and biometrics, only provide entry-point security for establishing the identity of a subject (user, device, process) when accessing a secure service or device (Niinuma, Park & Jain, 2010). Once the subject is authenticated, there is typically no ongoing procedure to ensure continuous control of the session or device. As passwords are frequently leaked or hacked, continuous authentication methods are being explored to address these limitations(Niinuma, Park & Jain, 2010).

Continuous authentication, also known as active, transparent, or implicit authentication, employs various approaches to maintain ongoing control (Roth, Liu & Metaxas, 2014). One

approach uses the colors of a user's clothes and facial skin during a login session, but continuously capturing and sending photographs for authentication can be computationally expensive and raise privacy concerns. Another approach leverages the user's hand movement pattern while typing on a keyboard (Saevanee et al., 2015). However, continuously streaming video can be burdensome and degrade system performance, while requiring a webcam to remain pointed toward the keyboard limits its utility for other tasks (Frank et al., 2012).

Typing behavior-based continuous authentication using key hold-time and inter-key time features may only be effective when users are actively typing(Roth, Liu & Metaxas, 2014). Various methods have been proposed for continuous authentication on mobile devices, which incorporate numerous sensors such as touch sensors, accelerometers, and gyroscopes. Touch dynamics on the screen, the orientation of the finger, the pressure exerted, and the area occluded are examples of features that can be extracted for continuous authentication.

For devices without physical contact with humans, continuous authentication mechanisms using radio frequency signals and ambient parameters such as light, temperature, and sound have been proposed. Wireless channel parameters like channel state information and received signal strength can be used to continuously authenticate devices without human interaction. However, these continuous authentication approaches face limitations. Most are device-specific, working only on devices they were designed for, making their extension to online services accessed from various devices challenging.

2.4.1.3 Device Authentication

According to the NIST ZTA, all data-generating resources, including servers, workstations, mobile devices, IoT, and OT devices, are considered resources (Lam & Chi, 2016). Devices can be categorized as enterprise-owned or personal devices. Implementing zero trust for devices requires identifying all network-connected devices and their access points. Traditional authentication methods for humans may not be suitable for IoT and OT device identification and authentication. Key challenges include:

- IoT and OT devices often operate autonomously, rendering human-associated authentication factors irrelevant.
- Machine-to-Machine (M2M) communications in IoT and OT networks necessitate new authentication mechanisms, such as mutual authentication, for device authentication (Ali, Sabir & Ullah, 2019).
- Computational limitations of IoT devices can render existing identity verification methods impractical for device authentication.

In a ZTA context, devices must be authenticated before engaging in M2M communication. Popular authentication methods include symmetric key authentication, lightweight public key infrastructure (PKI), and Open Authorization 2.0 (Ali, Sabir & Ullah, 2019). The IoT device life-cycle comprises pre-deployment, ordering, deployment, functioning, and retirement (Ali, Sabir & Ullah, 2019). The proposed scheme is based on attribute-based access control, which is certificateless and reduces computation costs on constrained devices. It allows for seamless authentication across multiple domains throughout the device's life-cycle. In addition to the authentication schemes discussed, IoT devices require unique, tamper-proof identities that cannot be easily imitated. This aspect is crucial in ensuring the security and integrity of device authentication within a Zero Trust Model.

2.4.2 Access Control

In recent years, a multitude of scholars have concentrated their efforts on the elaboration of diverse typologies and theoretical frameworks about the Zero Trust Model. For example, Mehraj et al. (2020) proposed a compendium of methodologies and classifications centered around this notion. A salient approach encompasses the comprehensive automation of "Trusting Users," incorporating the deployment of a trust-based mechanism that amalgamates disparate systems responsible for data, user, and application management. By leveraging this integrated system, it may facilitate the determination of whether a user device warrants trust when establishing a connection to a specific network from an alternative network.

Access control, the foundational requirement for Zero Trust Architecture (ZTA), focuses on ascertaining a subject's privileges (either an authenticated user or a process executed on their behalf) and restricting access accordingly. Logical access control aims to protect resources (devices, data, applications, or objects) concerning the operations available to a subject (e.g., read, write, execute). Subjects must satisfy access control policies to perform a specific operation on a particular object. These policies are part of an organization's access control mechanism (ACM) and stem from its business and security requirements.

According to NIST's definition, the ACM is a logical component that assesses access requests and determines whether the subject is qualified to carry out the requested operation (Hu, 2014). ACMs can employ various methods to define and enforce access control policies. The logical progression from the trust mechanism to multi-factor authentication and access control within a Zero Trust Architecture ensures a comprehensive security approach. By effectively integrating these components, organizations can enhance their security posture, providing appropriate levels of access for each user while minimizing potential risks and vulnerabilities.

- **Identity-Based Access Control**: Identity-based access control (IBAC) is a straightforward and coarse-grained method for access control, where access authorization is directly linked to a subject's identifier. Using an Access Control List (ACL) is one way to implement IBAC, requiring system administrators to define access rights for objects concerning various recognizable subject identities. However, this approach is not scalable in dynamic environments with frequently changing subject and object groups, as it necessitates constant revisions to access authorizations.

- **Role-Based Access Control**: In contrast to IBAC, Role-Based Access Control (RBAC) relies on subjects' roles within an organization to manage access control. RBAC enables centralized management without cumbersome ACLs, but it can lead to "role explosion" or an accumulation of roles and privileges that persist beyond their justification. Although variations of RBAC have been proposed to improve the original scheme, their adoption has been limited due to factors such as deployment costs, infeasibility of certain assumptions, and limitations on achieving fine-grained access control when compared to more recent approaches like attribute-based access control.

- **Attribute-Based Access Control**: Attribute-Based Access Control (ABAC) is an access control mechanism that considers multiple attributes, with IBAC and RBAC as special cases. ABAC uses complex Boolean rule sets to evaluate access requests based on the attributes of the subject (Hu, 2014), object, and environment, along with defined policies. Environmental conditions include factors such as time, location, and risk level. Extensible Access Control Markup Language (XACML) and Next

Generation Access Control (NGAC) support and implement the ABAC model but differ in their approaches to defining and managing attributes and enforcing access decisions.

- **Risk-Based Access Control**: Risk-Based Access Control uses risk analysis to determine the risk associated with a specific access request, comparing it to access policies and acceptable risk levels to decide whether to grant access. Some approaches, such as using fuzzy inference systems to measure risk (Atlam et al., 2017), but face challenges in scalability and reliance on prior knowledge.

The article further discusses that access controls are fine-grained and are often in need of context-aware access control and different technologies which have emerged over the years amongst these are *smart homes, smart grids, healthcare IoT, and smart buildings,* These technologies have different requirements and access control which leads to same components can not be used in the aforementioned technologies leading to finding alternatives to protect IoT devices from cyberattacks (Syed et al., 2022).

2.4.3 Micro-segmentation

Micro-segmentation is a key security concept within Zero Trust Architecture, which aims to protect network resources by breaking the network infrastructure into smaller logical segments. This approach enables only authorized entities within the data center to access applications or data on protected resources, thereby preventing lateral movement by an attacker. Devices such as Next Generation Firewalls (NGFW) or security gateways act as Policy Enforcement Points (PEP) to enforce policies defined in the Policy Engine (PE) in line with the NIST ZTA proposal (Rose et al., 2020).

Traditional network segmentation techniques like Virtual LANs (VLAN), routers, and firewalls are often insufficient for providing granular security to workflows. To protect east-west traffic flowing in data centers, granular security controls are required to enforce strict security policies between individual resources. Micro-segmentation techniques can be applied using various deployment models, such as native micro-segmentation, third-party model, overlay model, and hybrid model (Syed et al., 2022):

- **Native Micro-segmentation**: In this model, micro-segmentation is achieved using the underlying infrastructure or operating system, allowing access policies to be deployed directly without the use of external hardware or software solutions. This model is limited to virtual environments where workloads operate.

- **Third-party model**: This model integrates virtual firewalls furnished by third-party vendors, enabling the structuring and execution of access policies between virtualized servers. However, this approach necessitates the virtual firewall to maintain visibility over workload traffic.

- **Overlay model**: This model capitalizes on agent software operative on servers in conjunction with a centralized controller or orchestration device to attain insight into workflow communications and enforce dynamic access policies. The merit of this strategy lies in the agents' superior visibility over individual workload communication patterns, thereby enabling the dynamic deployment of access policies via a centralized controller.

- **Hybrid model**: This model orchestrates a blend of native and auxiliary micro-segmentation strategies to effectively safeguard distinct communication layers.

The majority of micro-segmentation implementations hinge on network dependencies, necessitating programmable, software-based network equipment such as firewalls and switches. The administration of access policies in this context relies on centralized controllers (Kindervag, 2010). Conversely, network-independent implementations capitalize on virtual firewalls or overlay networks, demonstrating their capability to operate independently of the foundational network technologies.

The policies configured on micro-perimeters require understanding the complete life cycles of workflows and the complex interactions within the enterprise network. In network-dependent approaches, workflows are identified and granted access using their network identities, which can be spoofed or forged. Network-independent approaches, conversely, use workload identities to create fine-grained policies, providing a more secure method for enforcing access controls in a Zero Trust environment.

2.4.4 Security Automation and Orchestration

Security automation is a crucial aspect of achieving Zero Trust security. It can be broadly defined as the process of reducing frequent intervention by security professionals through automated threat detection and prevention. Traditional security logging approaches often generate a large volume of information, leading to alerts for security operation teams who then investigate potential threats (Syed et al., 2022).

However, these alerts can be repetitive and include numerous false positives, wasting time and resources on inconsequential analysis. Machine learning techniques can be employed in these scenarios to support the automatic detection of anomalies and determine appropriate actions in response to threats and vulnerabilities. This results in swift and efficient actions, allowing security teams to focus on significant threats as repetitive threats and false positives are automatically addressed (He et al., 2022).

Security automation focuses on automating access decisions, reassessing trust in current connections, and improving policy generation and enforcement using threat intelligence feeds, situational awareness, network activity logs, and system activity logs in the context of Zero Trust Architecture implementation.

2.4.4.1 Threat Intelligence

In today's highly connected world, where networks of IoT devices are prevalent, organizations must ensure quick and effective reactions to cyber threats. To achieve this, collecting and analyzing information from various internal and external sources is crucial. This information pertains to threats, vulnerabilities, and cyber attacks, providing the necessary data to enable Threat Intelligence (TI). TI equips organizations with up-to-date information on cyber threats and informs countermeasure techniques (Syed et al., 2022).

An efficient feedback system that automates security control is required considering the abundance of sources for this information in order to enable the necessary actions. To identify and prevent risks, threat intelligence entails gathering data on present and potential threats. To support decision-making regarding appropriate proactive security measures for effective threat management, it also entails sharing threat-related information.

Researchers have been developing novel approaches to address the challenges of gathering and utilizing threat intelligence in highly connected environments, such as IoT and CPS-based critical infrastructure (Tounsi & Rais, 2018; Zaheer et al., 2019). These advanced methods integrate information from different layers and sources, employing advanced models and frameworks to better understand and respond to potential cyber threats (Tounsi & Rais, 2018). By combining cyber and physical layer monitoring, these approaches can provide a more comprehensive understanding of the threat landscape and allow for the development of more effective countermeasures.

Moreover, researchers are working on refining the communication and collaboration between TI sources and security enforcement tools. By using standardized documentation and secure communication protocols, organizations can ensure that threat information is effectively shared and acted upon. This streamlined flow of information between various systems and components can lead to more efficient and timely threat response mechanisms (He et al., 2022).

As the IoT and CPS ecosystems continue to grow and become more complex (Tounsi & Rais, 2018), the need for effective threat intelligence and security automation will become increasingly critical. The advancements in threat intelligence and security automation are essential for organizations to manage and mitigate cyber threats in the context of Zero Trust Model. By leveraging the latest research findings and adopting state-of-the-art techniques, organizations can strengthen their security posture and better protect their networks and critical infrastructures from potential attacks.

2.4.4.2 IoT and Networking in Zero Trust

The widespread shift towards work-from-home arrangements during the COVID-19 pandemic has increased dependency on cloud resources, enabling businesses to maintain revenue growth and minimize financial losses (Mandal, Khan & Jain., 2021). This shift has led to heightened concerns regarding network security vulnerabilities, particularly for users connected to open networks. The lack of basic security measures on these networks can lead to heightened the risk of cybersecurity attacks, such as MAC spoofing and DDoS/DoS attacks, due to incoming traffic from untrusted networks. Wherein multiple devices connected to the network serve as potential attack vectors, causing significant damage and internal security threats (Mandal, Khan & Jain., 2021; Fu et al., 2022).

Moreover, this scenario can inadvertently facilitate unauthorized access to sensitive data, thereby underscoring the vulnerability inherent in static authentication methods. In light of our increasing dependence on networks, continuous authentication emerges as an indispensable security measure to effectively combat the risk of session hijacking. In the environment of Internet of Things (IoT) devices– many of which are intrinsically connected to networks – the lack of built-in biometric capabilities or password safeguards pose a substantial security concern. This emphasizes the urgency of integrating more robust and dynamic authentication methodologies, such as continuous or context-aware authentication, to ensure the protection of IoT devices and the data they hold.

To achieve a Zero Trust Architecture (ZTA) that incorporates edge and threat intelligence, the author proposes a multidimensional approach with two dimensions:

- **Subject of the satellite network**: This dimension encompasses the applications, users, and devices situated at the edge or within cloud solutions. Each entity possesses

varying trust levels, with higher-trust entities granted access to a wider array of resources.

- **Object of the satellite network**: In this context, the term "object" refers to resources exchanged during user sessions, such as video transmission, location data, or IoT streaming information. Vulnerable operations include uploading, downloading, exchanging, and modifying data, necessitating restrictions based on security levels. This dimension's features should account for resource value, demand degree, and threat level.

Due to the COVID-19 pandemic, Zero Trust networking has emerged as an essential approach for implementing access control policies that operate independently of VPN structures and micro-segmentation. The core principle involves verifying every incoming network request on both satellite and home-based networks, rather than simply trusting the network. The growing adoption of cloud environments and distributed cloud resources further underscores the importance of Zero Trust policies. The software-defined network (SDN) paradigm is a modern networking approach that decouples the network control plane from the data plane, enabling more flexible and centralized management of network resources. This decoupling allows network administrators to configure, manage, and optimize network resources more effectively and dynamically through software applications, without the need to manually configure individual every network device (Mandal, Khan & Jain., 2021). By integrating the software-defined network (SDN) paradigm into the network model, the Zero Trust concept becomes more flexible. In the realm of IoT and networking, access control policies based on Zero Trust principles can prevent MAC spoofing and ensure the security of hosts and cloud services remain protected and untouched. This proactive approach offers protection against both known and unknown attacks and can be adapted to support work-from-home scenarios while preventing unauthorized exposure of cloud resources. Ultimately, Zero Trust policies provide a dependable and secure means of protecting IoT devices and networking systems from cyber threats. This further leads to Machine Learning for Security Automation which plays a crucial role in identifying potential threats in the network.

2.4.4.3 Machine Learning for Security Automation

Machine learning (ML) has been instrumental in enhancing security automation by understanding the behavior of security threats and recognizing patterns to automatically take defensive actions. ML has significant potential to improve security automation procedures, especially in detecting and preventing threats in various critical scenarios, such as in Software-Defined Networks (SDNs) and Internet of Things (IoT) networks. For instance, researchers have used Support Vector Machines (SVM) to detect DDoS attacks in SDNs by classifying traffic as normal or anomalous based on extracted features (Elsayed et al., 2019; Myint Oo et al., 2019).

ML has also shown promise in intrusion detection. Researchers have demonstrated the efficacy of stacked autoencoders combined with SVM and Artificial Neural Networks (ANN) for detecting impersonation attacks in Wi-Fi networks (Aminanto et al., 2017). In social networks, deep learning can help identify novel cyber threats by leveraging their similarities to known attacks, as demonstrated by the successful use of long short-term memory recurrent neural networks for identifying anomalous traffic. In IoT networks, ML has been effective in detecting attacks. Moreover, deep learning has been employed to detect different types of attacks in IoT devices, such as DoS, DDoS, reconnaissance, and information theft (Myint Oo et al., 2019).

ML has significant potential to advance security automation, especially in critical scenarios like SDN and IoT networks. By understanding threat behavior and recognizing patterns, ML can automatically take defensive actions, reducing the need for human intervention. Deep learning techniques have shown promise in intrusion detection and identifying novel cyber threats.

2.5 Summary of Literature Review

The literature review chapter aims to provide a comprehensive overview of the existing research and knowledge related to the impact of the Zero Trust model on organizational. By examining various studies, articles, and reports, this chapter seeks to establish a foundation for understanding the key concepts, challenges, and opportunities associated with the adoption and implementation of a Zero Trust framework in organizations.

This chapter begins by exploring the vulnerabilities of traditional cybersecurity solutions, highlighting the limitations and challenges that have led to the development of the Zero Trust model. It then delves into the history, core principles, and architectural components of Zero Trust, providing a solid understanding of the framework and its underlying concepts.

Next, the literature review examines the relationship between Zero Trust and organizational impact, discussing both the positive and negative impacts that the adoption of a Zero Trust framework may have on an organization. The chapter then focuses on specific Zero Trust features, such as authentication, access control, micro-segmentation, and security automation, and their influence compared to traditional solutions. This analysis provides insights into the practical implications of implementing a Zero Trust model within an organization and helps identify best practices for balancing security and productivity.

Overall, the literature review chapter synthesizes existing knowledge and research on the Zero Trust model and its effect on organization, providing a foundation for further investigation and analysis. By identifying gaps in the current literature, this chapter also helps guide the direction of the study and informs the development of research questions and methodologies. In Table 1, we have systematically arranged the theoretical groundwork of this research into categorized themes, sub-themes, and their corresponding references.

Table 1: Overview of theoretical background

Theme	Sub-Theme	Reference
Foundational concepts		
Traditional network solution vulnerabilities	● Insufficient internal controls ● Weak device reliance ● Exposed IP addresses ● Vulnerable centralized logs	(Chen, Hu & Cheng, 2019), (DeCusatis et al., 2016), (Kumar et al., 2019), (Shlapentokh-Rothman, Hemberg & O'Reilly, 2020), (Moubayed, Refaey & Shami, 2019)

Zero Trust	• Zero Trust Architecture • Continuous- Trust-Assessment • Trust Algorithm	(Wylde, 2021), (Garbis & Chapman, 2021), (Bertino, 2021), (Cunningham, 2018), (Buck et al., 2021), (Campbell, 2020), (Fernandez & Brazhuk, 2022), (He et al., 2022), (Li, Iqbal & Saxena, 2022), (Chuan et al., 2020),, (Teerakanok, Uehara & Inomata, 2021)
Zero Trust and Organization	• Enhanced Security and Risk Mitigation • Proactive Incident Response and Business Continuity • Increased Complexity and Overhead • User Experience and Workflow Disruptions	(Morgan, 2020), (NIST, 2020), (Kindervag, 2010), (SANS Institute, 2019), (Teerakanok, Uehara & Inomata, 2021), (Nguyen et al., 2019), (Adikari, McDonald & Campbell, 2011), (Brouwer et al., 2002)
Zero Trust Feature		
Authentication	• Context-aware user authentication • Continuous Authentication • Device Authentication	(Hayashi et al., 2013), (Kim et al., 2018), (Jakobsson et al., 2009), (Abowd et al., 1999), (Saevanee et al., 2015), (Roth, Liu & Metaxas, 2014), (Niinuma, Park & Jain, 2010), (Frank et al., 2012)
Access Control	• Identity-Based Access Control • Role-Based Access Control • Attribute-Based Access Control • Risk-Based Access Control	(Mehraj & Banday, 2020), (Sarkar et al., 2022), (Hu, 2014), (Atlam et al., 2017)
Micro-segmentation	• Native Micro-segmentation • Third-party model • Hybrid model	(Syed et al., 2022), (Rose et al., 2020)
Security Automation and Orchestration	• Threat Intelligence • Machine Learning for Security Automation	(Tounsi & Rais, 2018; Zaheer et al., 2019), (Tounsi & Rais, 2018), (He et al., 2022), (Elsayed et al., 2019; Myint Oo

		et al., 2019), (Aminanto et al., 2017), (Myint Oo et al., 2019)

3. Methodology

This chapter outlines the research strategy in our study, including the design of our research, the research philosophy that underpins it, and the scientific approach we have taken. Additionally, this chapter gives detailed information about our data collection and analysis methods that have been chosen for this study. Finally, we give a comprehensive overview of the analytical procedures used to interpret the empirical data, as well as a discussion of ethical considerations and potential research limitations.

3.1. Research Philosophy

For this research, we aimed to understand practitioners' perspectives on the impact of the Zero Trust model on organizational. The complex nature of human experiences, the social aspects of organizational environments, and the unique contexts within which the Zero Trust model is implemented make it necessary to adopt an interpretive research philosophy for this study. Interpretivism focuses on social constructs as a means of understanding reality (Myers, 2019), making it an ideal approach for exploring the nuanced experiences of practitioners in relation to the Zero Trust model.

By employing interpretivism and qualitative research methods, we sought to understand the aspects that influence organizational when implementing the Zero Trust model. We examined practitioners' perceptions of the benefits and challenges associated with the model, as well as the strategies and best practices they employ for its effective implementation. Myers (2013) argues that social researchers should examine problems from the inside, which, in this case, refers to understanding the Zero Trust model from the perspectives of those who interact with it daily.

Interpretative researchers adhere to the belief that the acquisition of knowledge is deeply rooted in the meanings that individuals assign to situations and experiences in order to rationalize the manner in which certain activities are performed (Klein & Myers, 1999; Orlikowski & Baroudi, 1991). The lenses through which individuals view the world are moulded by their experiences, which display a proclivity for transformation depending on varying circumstances. An in-depth exploration of practitioners' experiences with the Zero Trust model provides crucial insights into the elements influencing organizational, underlining the significance of this research in expanding the extant scholarly corpus.

The interpretive approach recognizes the importance of context and the subjective nature of human experiences. As a result, it emphasizes the value of in-depth, qualitative inquiry to gain a rich understanding of the phenomenon being studied (Denzin & Lincoln, 2011). In the case of our research, we focused on understanding the various factors that contribute to the success or failure of the Zero Trust model implementation and its impact on organizational. By using an interpretive lens, we sought to uncover the underlying reasons, motivations, and beliefs that shape practitioners' experiences and perspectives on the Zero Trust model.

3.2 Research Approach

There are three distinct research approaches to address the research question, namely qualitative, quantitative, and mixed methods. For this thesis, a qualitative method has been chosen due to the dynamic and complex nature of the research question (Patton, 2015), as how does Zero Trust implementation effect large organizations, which is an individual measure and can hold different meanings for each organization. By examining and contrasting the experiences of various organizations that have implemented Zero Trust, the research question can be effectively addressed (Patton, 2015). A qualitative research method, according to Patton (2015), entails the use of collecting detailed data and information from specific interviews which includes open-ended questions and in-depth responses about interviewees knowledge and experiences (Patton, 2015; Recker, 2013).

Using a qualitative research approach allows us to investigate how the implementation of Zero Trust impacts organizations (Schultze & Avital, 2011). Schulte and Avital (2011) emphasize the significance of providing in-depth details and descriptions from the data collected to guarantee the credibility of the information gathered. This is because it can enhance the researcher's work and it can identify different nuances from rich data and can also capture criticalities in the interviews. Therefore interviews providing comprehensive descriptions and overall high-quality research can also support the researchers arguments presented in the paper but also to ensure that the data is accurately interpreted (Schultze & Avital, 2011). Nonetheless, Patton (2015) contends that there is still a risk during the execution of qualitative research and emphasizes that it can occur in interviews where misunderstandings or misinterpretations may arise, or responses might be incorrectly interpreted due to the influence of researchers' own beliefs, values, and perspectives (Patton, 2015; Recker, 2013). Each researcher must prioritize ethical considerations and maintain a high standard of research quality, as this is crucial for providing assurance to readers that data collection and data analysis have been executed properly (Recker, 2013).

Marshall et al. (2013) elaborates on the intricate issues involved in ascertaining the sample size for qualitative studies, given the myriad factors that could potentially influence the research process. These factors necessitate conducting a sufficient number of interviews to ensure the acquisition of comprehensive data. The inherent ambiguity of qualitative research, stemming from the distinct characteristics of each study and the lack of prescriptive guidelines, further contributes to the complexity of determining an optimal sample size (Patton, 2015). Consequently, the researcher's judgment, coupled with the study's objectives and the depth of data required, plays a pivotal role in this determination.

Moreover, Bruce and Johnson (2006) emphasize the need to carefully consider the number of interviews to be conducted, as each research design is distinct and must be executed within the constraints of the available budget. Nevertheless, Marshall et al. (2013) proposes in its findings that a minimum of six interviews should be conducted, but the recommended range is between 15 to 30 interviews for grounded theory studies.

Considering that our study is based on a qualitative research approach, we have meticulously developed an interview guide that presents comprehensive information about the interview process. Conducting qualitative research necessitates a significant amount of time and resources, as the interviews must be prepared, executed, processed, and ultimately analyzed (Johnson & Onwuegbuzie, 2004). Consequently, we will conduct an optimal number of interviews, striking a balance between achieving a comprehensive understanding of the research subject and efficiently utilizing the available time and resources.

3.2.1 Literature Review Approach

In this part, we aim to establish a theoretical foundation for the concept of Zero Trust by conducting a literature review that supports our thesis. To achieve this, we conducted a systematic literature review process, which includes using the search and filtering strategies (Kitchenham & Charters, 2007). This technique was selected due to its efficacy in identifying relevant parts of the literature concerning the subject Zero Trust. As highlighted by Knopf (2006), a literature review comprises two essential components. First, it provides an in-depth analysis of the results obtained from prior research conducted within the chosen topic. Second, it offers a comprehensive understanding of the existing knowledge and identifies gaps within the current literature. The focus of literature review is on collective knowledge rather than individual contributions which sets the literature review apart from other methods. Undertaking a literature review approach offers several advantages, including:

A literature review gives a broad understanding of a research area that might be unfamiliar, allowing for more informed analysis and conclusions. It also identifies well-executed studies, preventing redundant efforts in exploring the same ground and facilitating a more efficient research process. Nevertheless, it stimulates innovative ideas that can be integrated into one's research, thus contributing to the development of novel concepts and theories. But it also assists in highlighting potential limitations or shortcomings in existing research, for researchers to address these gaps and enhance the overall quality for their research. To ensure a high-quality and well-considered theoretical background, specific keywords were used during the literature review process. These keywords were targeted search, enabling the identification of relevant sources and information to support the thesis theoretical background. Randolph (2005) asserts that the first step for data collection involves exploring relevant academic databases, which must be documented during the gathering process to enable traceability. According to Randolph (2005), keywords are crucial since information retrieval must be conducted using appropriate keywords, symbols and connectors to refine and optimize search results to filter out only relevant results. Therefore

In order to expand the scope of the search, we used both symbols and connectors such as “+”, AND and OR with the selected keywords, with the aim of capturing relevant information. The term OR was used to encompass words possessing similar or identical meanings, whereas AND was used to identify the terms and concepts (Timmins & McCabe, 2005). As a result, the following keywords were determined for the comprehensive search:

- Cybersecurity AND Zero Trust OR Zero Trust Model
- Zero Trust Model
- Zero Trust Security Model
- Zero Trust AND ZT
- Zero Trust Architecture
- Access Control AND Zero Trust
- Identity and access management (IAM) & Zero Trust
- Zero Trust over traditional security models
- Zero Trust vs perimeter-based security
- IoT AND Zero Trust

The research process involved the utilization of two digital academic databases, namely Google Scholar and Scopus were used, to gather relevant scientific literature. The primary aim was to explore the concept of 'Zero Trust' comprehensively and examine its impact and advantages and disadvantages for organizations. To gather more information about the Zero

Trust a logical statement is formulated, incorporating all the keywords, to provide a deeper understanding of the concept.

Zero Trust Model OR Zero Trust Security Model implementation in organization

While the abundance of available literature was significant, the search process encountered limitations in terms of Zero Trust. The search databases that were utilized for this theoretical background were Google Scholar and Scopus. These databases made it possible to find relevant literature such as academic journals, books, e-books, academic articles and conference papers. The study acknowledges the usage of non-peer-reviewed information such as white-papers in certain instances to explain and define certain terms but also usage of figures.

To facilitate the search and refine the number of search results in a comprehensive scientific literature review, we formulated a set of acceptance criteria. These criteria were devised in response to the rapid advancements and evolving nature of the field of cyber security and were intended to ensure the inclusion of relevant literature in our thesis. The first criteria which we used were to filter out search results dating back to 2010, since the databases will exclude any results and both databases offer different search and filtering options so we used only those criteria's which would match both databases.

3.3 Data Collection Methods

3.3.1 Qualitative Research Model

To gain a comprehensive understanding of the impact of the Zero Trust model on organizational, this study adopted a qualitative research model using interviews as the primary data collection method. Moreover, to comprehensively understand the impact of the Zero Trust model on organizational, this study strategically adopted a qualitative research model with semi-structured interviews as the primary method of data collection. The rationale behind choosing semi-structured interviews was to harvest in-depth insights and perspectives directly from practitioners and stakeholders involved in the implementation and daily operation of the Zero Trust model. The semi-structured nature of these interviews enabled us to explore the intricate and multifaceted experiences, challenges, and benefits associated with the adoption of the Zero Trust model within an organizational context. For this study, semi-structured interviews were chosen due to their flexible and interactive nature. They provide a guided conversation where the researcher has a list of predetermined questions (an interview guide), but the order can change based on how the conversation flows. The interviewer has the freedom to probe deeper into the topic, ask follow-up questions, and seek clarification as needed.

This flexibility allows the interviewers to adapt to the interviewee's knowledge and experience, leading to richer and more nuanced data. This is particularly important in our study, as we interviewed participants with varying degrees of familiarity and experience with the Zero Trust model. Furthermore, this approach allows the interviewer to explore new avenues and ideas that arise during the conversation.

The flexibility offered by semi-structured interviews in data collection and analysis creates a natural progression from the rich data obtained. This flexibility enables researchers to adapt their questions and focus as new insights and patterns emerge throughout the interview process, allowing for a more comprehensive understanding of the subject matter (Brooks, Horrocks & King, 2018). This adaptability is especially beneficial when examining a topic that lacks extensive research or comprehensive understanding, as it ensures researchers remain receptive to new discoveries and perspectives (Patton, 2014).

The in-depth data and flexible approach provided by interviews facilitate a deeper understanding of the contextual factors influencing the implementation of the Zero Trust model and its impact on organizational (Creswell & Poth, 2016). Acquiring context-specific knowledge is essential for developing effective strategies and recommendations for organizations seeking to adopt the Zero Trust model, thus ensuring a practical application of the research findings.

Interviews inherently promote a holistic perspective on the phenomenon being studied, observing the various factors, relationships, and dynamics involved (Denzin & Lincoln, 2011). In the context of this research, the logical connectivity between the rich data, flexible approach, and contextual understanding allows for a comprehensive examination of not only the technical aspects of the Zero Trust model but also the social, cultural, and organizational factors that shape its implementation and influence on productivity. This holistic understanding ultimately leads to more informed and effective recommendations for organizations adopting the Zero Trust model (Seidman, 2006).

3.3.2 Selection of Respondents

The careful choice of the right participants is an important part of this study (Recker, 2021). We began early to ensure the inclusion of a diverse range of organizations. The primary objective of the research is to investigate the impact of Zero Trust implementation on different businesses, particularly by examining similarities and patterns across various industries. By concentrating on large organizations, the study seeks to provide a comprehensive understanding of how adopting the Zero Trust framework affects these organizations.

To identify relevant participants and obtain insightful and in-depth responses, we specifically targeted roles in large organizations, such as cybersecurity officers, information security officers, managerial positions or CTOs. Various roles, such as executive-level positions or security strategists, provide a unique perspective because the diversity of roles leads to a range of different and mixed viewpoints. For example, some participants may discuss Zero Trust in more technical detail, while others may possess a broader technical understanding but have deeper knowledge of Zero Trust from an organizational perspective. This diversity also results in varied responses within our study. Furthermore, we focused on large multinational organizations, meaning they could have offices around the world, although it was not a requirement for these companies to have operations in Sweden. To maintain an appropriate sample size, we limited the number of interviews to 5 to 6, as these companies were a good fit and met the established criteria. Patton (2015) argues that choosing a scope and size of the study depends on various factors. These factors can be grouped into three main categories: research objectives, available resources, and the nature of the research itself. After identifying relevant companies for our research, we composed two email templates, one in English and one in Swedish, which were sent to the identified respondents. However, several of the

individuals we reached out to declined participation, prompting us to develop a cold-calling script used to contact the identified individuals on LinkedIn. Once interview appointments were scheduled, we sent each respondent a set of questions as well as a description of our research project. Prior to commencing each interview, we requested permission to record the conversation and to use their names, roles, and organizations in our research. All respondents agreed, thereby enhancing the credibility and reliability of our sources. Each interview lasted between 35 to 50 minutes and provided pertinent and valuable information. As a result, five interviews were sufficient for our data collection. The companies that chose to participate are: CloudDeep Technology, Industrial and Commercial Bank of China, China Everbright Bank, Combitech AB, JP - Morgan and Digital Hainan. Each organization is different and brings a unique perspective about Zero Trust to the table as some are working on an international, national, and local scale with Zero Trust. Table 2 gives a brief overview of each participating organization and information about the respondents. Meanwhile, Table 3 highlights the specifics aspects of the interviews, including the platform used for interviewing and date each interview took place.

CloudDeep Technology headquartered in Beijing, is a high-profile tech company, primarily operating within China but boasting a vast clientele, including international behemoths like Huawei and Microsoft, as well as prominent Chinese gaming corporations. Currently, CloudDeep Technology is committed to addressing comprehensive security issues at all levels, focusing particularly on network security and the integration and execution of the Zero Trust model.

The Industrial and Commercial Bank of China (ICBC) stands as the world's largest bank in terms of total assets. Founded in 1984, ICBC, a state-owned commercial entity situated in Beijing, furnishes a broad spectrum of financial services targeted at individuals, businesses, and government bodies. Services encompass personal and corporate banking, investment banking, asset management, and international banking. ICBC's product portfolio includes diverse offerings such as deposits, loans, credit cards, insurance, wealth management, and electronic banking solutions.

China Everbright Bank is a publicly traded commercial bank headquartered in Beijing, China. CEB provides a wide range of financial products and services to individuals, corporations, and government entities in China and globally. Its offerings include personal banking, corporate banking, investment banking, and asset management services.

Combitech AB is a renowned Scandinavian software development company which have expertise and specialization in the following sections: smart and secure industry, innovation, aftermarket services,

JP - Morgan is committed to formulating innovative solutions addressing the financial industry's monumental challenges. The firm's expansive skill set encompasses investment banking, asset management, private banking, treasury and securities services, and commercial banking. Operating in over 100 countries, J.P. Morgan utilizes its profound expertise and global insights to navigate the intricacies of the financial sector.

Digital Hainan
Digital Hainan is a ground-breaking initiative instituted by the Hainan Provincial Government, aimed at catapulting the province into a globally competitive digital economy. Concentrating on harnessing advanced technologies such as Artificial Intelligence, blockchain, cloud computing, and data analytics.

Table 2: Summary of Respondent Details

Respondent	Company	Country	Position	Appendix
R1	CloudDeep Technology	China	CIO	Appendix 1
R2	Industrial and Commercial Bank of China	China	Client Manager	Appendix 2
R3	China Everbright Bank	China	System Developer	Appendix 3
R4	Combitech AB	Sweden	CTO	Appendix 4
R5	JP - Morgan	USA	System Developer	Appendix 5
R6	Digital Hainan	China	System Developer	Appendix 6

Table 3: Summary of Interview Details

Respondent	Interview date	Communication Channel	Duration (record)	Appendix
R1	27-04	Zoom	55 minutes	Appendix 2
R2	03-05	Zoom	25 minutes	Appendix 3
R3	03-05	Zoom	35 minutes	Appendix 4
R4	04-05	Zoom	35 minutes	Appendix 5
R5	15-05	Zoom	28 minutes	Appendix 6
R6	17-05	Zoom	30 minutes	Appendix 7

3.3.3 Interview guide

The interview guide in Table 4 is designed to aid in our understanding of each organization's perspective and experience with the Zero Trust framework. The guide serves as a roadmap for the conversation, focusing on specific themes and areas of interest. By structuring our questions in this manner, we delve deeper into each company's unique experience, highlighting the challenges, successes, and insights obtained from their journey towards implementing Zero Trust.

Table 4: Summary of interview question details

Theme	Subtheme	Interview Questions
Introduction		1. Can you tell us about your background?
Traditional Solutions and Zero Trust Model Introduction	Understanding	2. Are you familiar with the Zero Trust Model?
		3. What is your understanding of traditional cybersecurity solutions?
	Transition	4. What led your organization to transition from traditional solutions to the Zero Trust Model?
Implementation and Adoption	Process	5. How was the Zero Trust Model implemented in your organization?
	Challenges	6. What challenges did you face during the implementation process, and how do they compare to the challenges faced with traditional solutions?
		7. How did your organization overcome these challenges?
Organizational and Zero Trust	Impact	8. In your opinion, what impact does the Zero Trust Model have on an organization's overall security posture?
		9. Were there any unexpected benefits or drawbacks to the Zero Trust Model in terms of your organization's performance?
	Enhanced Security and Risk Mitigation	10. Can you describe any improvements in security measures and the reduction of potential risks your organization has experienced since implementing the Zero Trust Model?
		11. How has the Zero Trust Model helped your organization detect and prevent security threats?
	Increased Complexity and Overhead	12. How has your organization managed the potential increase in complexity and resource requirements associated with implementing the Zero Trust Model?

	User Experience and Workflow Disruptions	13. Zero Trust Model has many advantages, however, you might have noticed that it also comes with an increased complexity at your organization?
		14.How has this affected the overall User Experience and Processes in your Organization?
		15. Could you mention and go through some of the processes which have changed during and after the implementation of Zero Trust.
		16. Have you noticed any changes in employee behavior or work habits due to the implementation of the Zero Trust Model?
Zero Trust Features	Features	17. How do the features of the Zero Trust Model (e.g., authentication, access control, micro-segmentation, security automation) affect your organization?
		18. Which features have had the greatest impact on productivity, either positively or negatively?
	Best Practices	19. What best practices have you identified for balancing security and impact within the Zero Trust Model?
Future Prospects and Improvements	Improvements	20. What further improvements or adjustments do you foresee for the Zero Trust Model in your organization?
	Evolution	21. Are there any new developments or technologies that you believe will have a significant impact on the future of the Zero Trust Model and traditional solutions?

3.4 Data Analysis Method

The analysis in this study is conducted using thematic analysis, a method that entails identifying common themes and patterns in the data, coding them, and interpreting their relevance to the research questions (Guest, MacQueen & Namey, 2011). This approach is particularly suited for examining the qualitative information gathered from the interviews conducted with organizations implementing the Zero Trust model.

The first stage in the analytical process involves transcribing the recorded interviews into written form. This requires listening to the recordings and converting the spoken words into verbatim written text, ensuring that the transcription accurately captures the participants' responses. Once the data has been transcribed, the coding process commences. This entails segmenting the data into smaller units or "codes," and identifying emerging themes and patterns. A combination of deductive and inductive coding is employed, which involves utilizing predefined codes based on the research questions and hypotheses, as well as allowing the data to reveal new themes that emerge organically.

Following the coding stage, the data analysis begins. This involves examining patterns or trends in the data and evaluating the findings in relation to the study's research questions. Additionally, the participants' backgrounds and other factors that may have influenced their responses are considered to ensure a comprehensive understanding of the data.

The analytical process culminates in interpreting the findings in light of the study objectives and drawing generalizations about the impact of Zero Trust characteristics on organizations. These insights are valuable for organizations contemplating the adoption of Zero Trust security measures or those already employing them but seeking to optimize their implementation. The identified themes and patterns in the data guide the interpretation and discussion of the results (Thomas, 2006).

In summary, the thematic analysis used in this study involves transcribing the interview data, coding the data using a combination of deductive and inductive approaches, analyzing the data for patterns and trends, and interpreting the findings in relation to the research objectives. This process allows for a comprehensive understanding of the impact of the Zero Trust model on organizations, providing valuable insights for those considering its implementation or seeking to enhance their existing Zero Trust security measures. The summary of thematic analysis can be seen in Table 5.

Table 5: The coding interview

Theme	**Code Description**	**Code**	**Sub Code Description**
TSZTM	Traditional Solutions and Zero Trust Model	TSS	Traditional security solutions
		TZTM	Transition to Zero Trust model
		ZTMA	Zero Trust model advantages
		ZTMD	Zero Trust model disadvantages
		CTSZTMA	Comparing traditional solutions and Zero Trust
ZTO	Zero Trust implementation for	ESRM	Enhanced Security and

	organizations		Risk Mitigation
		PIRBC	Proactive Incident Response and Business Continuity
		CO	Complexity and Overhead
		UEWD	User Experience and Workflow Disruptions
		ED	Security Education
ZTFO	Zero Trust feature related to organizational	AU	Authentication
		AC	Access Control
		ME	Micro-segmentation
		MLSA	Machine Learning for Security Automation
		IN	IoT and Networking in Zero Trust
FDZT	Future developments and improvements in Zero Trust		

3.5 Ethical Considerations

In conducting our study, we placed a strong emphasis on ethical considerations throughout the entire research process, as suggested by Patton (2015). Addressing ethical aspects is crucial to ensure that the research is developed properly and adheres to the principles of morality (Recker, 2013).

Interview processes can evoke emotions and memories in respondents (Patton, 2015). As interviewers, we remained focused on collecting relevant data and avoided straying from the intended research objectives. We were well-prepared and mindful of ethical issues when conducting the interviews, ensuring the protection of respondents' rights, prioritizing confidentiality, and maintaining their consent throughout the process (Patton, 2014; Ryan, Coughlan & Cronin, 2009). To preserve anonymity, we took measures to prevent respondent identification and securely stored the research data (Patton, 2014; Ryan, Coughlan & Cronin, 2009). Obtaining full consent from respondents was of utmost importance (Ryan, Coughlan & Cronin, 2009). We shared information about the study and the interview guide with

respondents before the interview and checked for consent during and after the interviews (Recker, 2013).

Recognizing that respondents could change their minds, we maintained a constant dialogue to ensure their continued willingness to participate (Recker, 2013). Given the potential sensitivity of company security information, we allowed respondents to review their interview transcriptions before using them in the study. Moreover, respondents received a copy of the thesis before its publication (Patton, 2014; Ryan, Coughlan & Cronin, 2009). Throughout the research process, we were consistently mindful of ethical aspects and prepared to address any related issues (Recker, 2013; Roig, 2006). We endeavored to maintain a high standard and relevance in the entire text, aiming to produce a unique contribution to the field (Recker, 2013; Roig, 2006).

3.6 Scientific Quality

Maintaining a high level of scientific quality throughout the research process to make a substantial contribution to the academic field was a top priority for the authors. It was crucial to identify a research topic that contributes to the existing corpus of knowledge. We carefully selected a relevant, stimulating, and innovative research topic that complied with ethical principles and addressed a gap in the literature (Recker, 2013). This approach ensured that our study was not only meaningful but also provided a solid foundation for further research in the field.

Ensuring that the entire research content remained unique and non-redundant was crucial in delivering high-quality work (Buchholz, 1995). Our literature review was developed using diverse, credible, and high-quality sources to establish a comprehensive and reliable foundation for the study (Efron & Ravid, 2019). This approach allowed us to provide readers with a well-rounded understanding of the topic, avoiding repetition, and redundancy. We prioritized transparency throughout the research process, providing clear explanations of our methods and reasoning, enabling readers to fully understand our approach and potentially replicate or expand upon our study (Bhattacherjee, 2012). In analyzing, discussing, and drawing conclusions from the collected data, we strived to remain objective and acknowledged the inherent difficulty in eliminating bias (Buchholz, 1995; Sica, 2006). By maintaining an awareness of our own potential biases, we aimed to minimize their impact on our findings and interpretations.

We rigorously analyzed the data obtained from interviews, ensuring that it was accurate, relevant, and useful for addressing our research aim and objectives (Patton, 2015). We also were able to derive valuable insights from this in-depth investigation and discover patterns, which helped us to better comprehend the research subject. In order to further enhance the caliber of our work, we also sought feedback from our peers and advisors frequently throughout the study process. This dedication to scientific excellence enabled us to conduct a study that not only adds to the body of knowledge but also lays the groundwork for further study and real-world applications in the subject.

4 Findings

In this section, we present the results of our qualitative research, obtained through the six in-depth interviews conducted with organizations that have implemented the Zero Trust Security Model (ZTSM). The findings are structured into three main categories: Transition to the Zero Trust Model, Enhanced security posture, Impact on users and usage habits, and User Experience and Workflow Disruptions.

4.1 Transition to the Zero Trust Model

When discussing with the respondents about their transition from traditional solutions to Zero Trust, it was revealed that the progress varied among the companies. Some were in the process of transitioning, adopting a hybrid approach and some had fully adopted Zero trust. Table (6) presents the different phases of each company's transition.

Table 6: Different phases of each company´s transition.

Maturity: Traditional, Initial, Advanced and Optimal		
Company	**Zero Trust Transition Process**	**Appendix**
CloudDeep Technology	Optimal	Appendix 2 (R1)
Industrial and Commercial Bank of China	Advanced	Appendix 3 (R2)
China Everbright Bank	Advanced	Appendix 4 (R3)
Combitech AB	Advanced + Hybrid Workplace	Appendix 5 (R4)
JP Morgan	Optimal	Appendix 6 (R5)
Digital Hainan	Initial + Hybrid Workplace	Appendix 7 (R6)

In the contemporary business landscape, the adoption of Zero Trust models remains a hybrid process, as organizations that have relied heavily on traditional IT departments during the pandemic are transitioning from their established modes of operation to more contemporary working environments. According to (R1:L6), the shift towards a Zero Trust model has become imperative as conventional network security solutions are increasingly unable to counter modern threats. Although the adoption of this novel approach presents challenges, strategies such as collaboration with cloud providers and the utilization of resource caching can facilitate businesses in overcoming these hurdles and augmenting their security measures. Both (R1:L8) and (R4:L6) concur that traditional networks rely on firewalls within local area networks (LANs) and the construction of VPNs for external connections when employees are

away from the office. This approach has engendered threats and vulnerabilities, as LANs cannot be adequately safeguarded. Consequently, transitioning to a cloud-based solution has become a necessity for enhanced security.

"In the transition to a Zero Trust framework, it becomes apparent that traditional concepts like LAN or intranet, typically found within IDC server rooms, present challenges. In a LAN, firewalls and defenses are employed to protect against external access. However, once services migrate to the cloud, they are directly connected to the Internet, rendering previous security measures insufficient. From this perspective, the only way to access these services is via the Internet, necessitating the adoption of a Zero Trust approach." (R1:L6)

The transition to a Zero Trust model also requires users to adapt to new security tools and procedures. This adaptation can entail a steep learning curve, as employees must familiarize themselves with novel technologies and practices. The need to master these tools can be particularly challenging for users who may have limited technical expertise or who are resistant to change. In turn, this can lead to a decline in productivity as employees struggle to navigate their new working environment.

Combitech highlighted that previously, several consultants needed to travel to clients or work internally to carry out tasks (R4: L4). These were referred to as "legacy systems" by Johan because their ongoing efforts to implement a Zero Trust model in organizations meant they could not rely on systems used before. Consequently, the company had to choose new systems from scratch, primarily because the traditional systems and infrastructure were outdated. One example provided by (R4:L34) is the computers that needed to be sent and then returned via mail, which was not efficient. However, with the implementation of Zero Trust and a secure cloud environment, computers can now be installed on-site without needing to be shipped.

Transitioning from traditional networks and IT departments to implementing a Zero Trust model within an organization necessitates both technical expertise and a paradigm shift in security thinking. This new mindset is essential in embracing the fundamental principles of Zero Trust, which prioritize continuous monitoring and verification to ensure optimal security. One key aspect of implementing the Zero Trust model is the adoption of least-privilege access, where users are granted access based on their roles and daily tasks, with permissions updated regularly to ensure alignment with employees' responsibilities. This approach is mentioned both by (R2:L8,L4; R3:L10, R4:L10 and R5:L11) which helps to automatically detect unauthorized access attempts and sends alerts to the responsible department for further investigation.

(R2:L10,L12) emphasizes that the adoption of the Zero Trust framework in banks has marked a significant departure from traditional security practices. Previously, access to systems was often granted by using of an employee card or a standard username and password.

“It usually takes…an employee card, including…those who use that kind of card and then swipes it to log in like the access card. Later, it is ready to gradually change to password login.” (R2:L6)

With the transition to the Zero Trust model, even departments such as the helpdesk have adopted advanced authentication techniques such as fingerprint authentication. (R2:L22) suggests that the traditional method of accessing the system is significantly affected since authorization can no longer be granted by one party to another using their credentials. In the context of the Zero Trust model, (R2:24) explains that every action, task, and system access necessitate fingerprint authentication. This method has enhanced authorization processes and

enabled task assignments in a significant manner that wasn't achievable through traditional methods. However, changes in access control because of the implementation of the Zero Trust model have both advantages and disadvantages.

On the other hand, (R4:L8) illustrates that, upon implementing Zero Trust in their organization, network segmentation was used, making the network more manageable by setting limitations and narrowing the potential scope of security breaches. (R3:L4, L6) agreed with this perspective, highlighting during the interview that network segmentation not only facilitates management but also helps to contain threats and minimize damage in the event of an attack. (R1, R3 and R4) mentioned during the interview that implementing least-privilege access and strong authentication helps secure the data and makes it easier to collaborate with external users outside the organization and internally.

"In fact, for the risk of an outsourced worker, because no matter which industry, there may be some outsourced worker involved, in order to improve the efficiency of development, so our management of outsourced workers is relatively strict. All the office computers of the outsourcing personnel are actually used to access the office data in the form of a bastion machine. The bastion machine is used to access the exclusive virtual office desktop of the outsourcing personnel to carry out the corresponding development and office work." (R3:20)

(R3), a system developer in the banking industry, emphasizes the pivotal role of the Zero Trust transition in enhancing the security of the banking industry. The financial sector has been dedicating substantial efforts to network and information security, especially as cyber-attacks have been escalating over the years. (R3:L4, L6) characterizes security measures as a first line of defense that shields the network using firewalls and VPN. Nonetheless, with the increased frequency and severity of financial cyber-attacks, there is an amplified necessity for more sophisticated security and network protection against external threats. There are multiple factors, according to (R3), that led the banking industry to transition from traditional security mechanisms to Zero Trust. The primary factor is the escalating external threats. Secondly, the advent of the Internet era 3.0 and the surge in cloud solution utilization have resulted in an increased dependency on mobile banking applications. These applications, unfortunately, are subject to numerous invasion attempts. (R3:L8) cites platforms like WeChat and open APIs, accessible to all, as a source of increased threats.

The views of R5, R2, and R3, all associated with the banking industry, are congruent. They clarify that the banking sector handles a substantial amount of personal information and operates a multitude of interconnected systems to monitor the financial information of both individuals and corporations. Consequently, any data breach could result in significant damage, with far-reaching implications for bank data security and privacy. The impact of such breaches on the banking sector is considerably more detrimental compared to other industries. Hence, the implementation of Zero Trust in the banking industry is deemed vital. Moreover, (R3:L18: L24) elaborates on the various challenges that surfaced during the implementation of Zero Trust. These involve addressing multiple security obstacles prevalent in the banking sector, including "physical security, network security, access control, intrusion prevention, operating system security, application security, business insecurity, and privacy protection" (R3:L8).

"The foremost of these was the escalating number of security breaches and vulnerabilities that traditional security models failed to address adequately. With the growing sophistication of cyber threats and the increasing complexity of the IT environment, we found the traditional 'trust but verify' security model inadequate." (R5)

"The need to enhance security was the primary driver for transitioning from traditional security measures to the Zero Trust model" (R6).

Conventional methods that emphasized border defense were increasingly found to be ineffective against sophisticated attackers who managed to infiltrate the network. The organization realized that *"without additional security mechanisms inside the network, intruders could easily launch a broad, horizontal attack"* (R1:L6). Further it has been stated that *"The balance between development investment and security implementation presented a significant challenge"* (R6:L23). An overemphasis on security measures led to inflated costs of business development and subsequent project delays. "The dilemma of managing this trade-off was a significant hurdle to overcome" (R6:L23).

"The Zero Trust model's implementation had major implications on resource access, inter-service communication, and data protection" (R6). All resources demanded authorization, and data protection followed the principle of least privilege, ensuring that *"permissions for data resources were restricted to the absolute minimum"* (R6:L26). Intriguingly, the Zero Trust model also impacted the organization's client-end products. "The incorporation of dynamic risk control strategies required a careful redesign of product interfaces, emphasizing user experience" (R6:). Despite these challenges, the organization noticed a substantial benefit such as *"The Zero Trust model's focus on real-time monitoring and logging provided the ability to trace security incidents and understand their origins, significantly enhancing the organization's security posture"* (R6:L18).

4.2 Enhanced security posture

By enforcing strict access controls and limiting access to sensitive resources based on user roles and responsibilities, the Zero Trust model minimizes the potential attack surface for cybercriminals. This approach ensures that users and devices can only access the minimum necessary resources required to complete their tasks, reducing the risk of unauthorized access and lateral movement within the network. The Zero Trust model extends beyond simple authentication, verifying the trustworthiness of users, devices, and applications throughout the entire session. This includes monitoring user behavior, access patterns, and device health to detect and respond to anomalies in real-time. Continuous monitoring allows organizations to identify potential threats and respond accordingly, mitigating the risk of successful attacks. According to the interview respondents, implementing the Zero Trust model within their organization possesses numerous advantages (R1:L26; R2:28; R3:L16; R4:L12; R5:L11). One of the respondents, R1 claimed that first it was very easy to access a computer through LAN and when you install something on a computer you can also start accessing and see other information are not to be seen as they are classified. Johan Gunnarsson (R4) from Combitech AB explains that users inside the organization are now able to collaborate and work on different projects from their internal laptop without the need for a new laptop.

“As soon as we access the cloud we understand the problem that there must be a traditional concept called LAN, or intranet, inside the IDC server room. Within my LAN I make a firewall, or you access my LAN from the Internet, and I can defend this process. But once my service is on the cloud, it is directly connected to the Internet. It does not exist even if the intranet is an intranet of the cloud's IDC center, but from my point of view, it is already connected to the Internet, because I can only access it through the Internet." (R1:L8)

Implementing the Zero Trust model requires a strong identity and access management (IAM) framework, incorporating multi-factor authentication (MFA), role-based access control (RBAC), and the principle of least privilege (POLP). These measures ensure proper authentication and access to resources based on job roles and responsibilities, reducing the likelihood of unauthorized access and the potential damage resulting from compromised credentials. The Zero Trust model's emphasis on continuous monitoring and verification promotes proactive threat hunting. This involves actively searching for signs of malicious activity within the network, rather than waiting for alerts from security tools. By adopting a proactive stance, organizations can identify and remediate threats before they cause significant damage.

The implementation of the Zero Trust model significantly enhances an organization's security posture by reducing the attack surface, mitigating the risk of unauthorized access and data breaches, and promoting proactive threat hunting. This comprehensive approach to security enables organizations to adapt to the ever-evolving cyber threat landscape and safeguard their critical assets. (R3:L16) mentions that one of the crucial elements of this enhanced security posture is the early intervention of security measures in the project cycle, which calls for an increase in dedicated security personnel such as security designers and security measures personnel. This further requires specialized skills and internal education inside the organization to empower the employees to identify potential security threats and formulate advanced preventive measures accordingly. This is an essential step in ensuring that organizations can adequately safeguard their networks in an increasingly complex and dynamic digital landscape.

Organizations face a rapidly evolving cyber threat landscape, and the need for scalable and adaptable security solutions has become increasingly apparent. Traditional perimeter-based security approaches have proven insufficient in addressing the complex challenges posed by new technologies, remote workforces, and cloud-based services. The Zero Trust Model offers a modular and flexible approach to security, allowing organizations to adapt to these challenges effectively. This approach enables organizations to tailor their security infrastructure to their specific needs and requirements, facilitating efficient resource allocation and streamlined security operations. The Zero Trust model provides a framework that allows organizations to seamlessly integrate new technologies, such as artificial intelligence, machine learning, and blockchain, into their security infrastructure. This adaptability ensures that organizations can leverage cutting-edge solutions to stay ahead of emerging threats and enhance their overall security posture.

They knew about a lot of threats. They had a lot of threats that were detected through the system. It's a bank. So like it was more of all the beginning level threats that were already taken care of. It was APTS that were the real threats that required manual work. So the system worked almost flawlessly to the degree it needed to for beginner level. (R6:L25)

The Zero Trust model supports the secure integration of remote workforces by enforcing strict access controls and continuously verifying the trustworthiness of users, devices, and applications (R4:L10, L18). This approach enables organizations to maintain a strong security posture while accommodating the growing trend of remote work and distributed teams. The Zero Trust model facilitates the secure adoption of cloud-based services by enforcing granular access controls, monitoring user activities, and ensuring data protection. This enables organizations to take advantage of the benefits of cloud computing, such as cost savings, increased agility, and improved scalability, while maintaining robust security measures.

Another aspect of enhanced security posture lies within the potential of the Zero Trust model to be integrated with Machine Learning (ML) and Artificial Intelligence (AI) (R5:L46). This integration is argued on a very foundational level by (R5), enabling the ZT model to employ ML in enhancing its architectural defense against incoming threats. This perspective is also expressed in a similar way by (R3) concerning the necessity of simulations and tests for optimizing the implementation of the Zero Trust model. By leveraging ML capabilities, the Zero Trust model could be implemented within an organizational network architecture in a way that allows for superior threat detection (R1; R2; R5:L27). Furthermore, the self-learning nature of ML algorithms means that the system can recognize patterns indicative of potential threats (R1:L38). This pattern recognition subsequently improves the system's ability to anticipate and counteract such threats, reinforcing the overall cybersecurity posture (R3). These insights underline the capacity for the Zero Trust model to evolve and adapt to the dynamic threat landscape, particularly when integrated with advanced technologies such as ML (R5, R1). This fusion could potentially enable a more proactive and intelligent network defense mechanism, as it is both important and is the 1st line of defense in today's increasingly interconnected and digitized world.

Let's see. I think the biggest development was cloud…. Artificial Intelligence and machine learning…the rate of a machine learning model being successful is 95 %.... And the next AI I think that it will be used for to detect,..It would be your detection instead of your what zero trust is like, anticipate, setting up for something the ideas is in reaction to something. (R6: L46)

R5 highlights how the Zero Trust model can help organizations grow and adjust over time. This model introduces a flexible approach to security that can change and adapt as needed, making it effective in managing unpredictable and ever-changing digital threats. Given the quick pace of technological changes today, having such flexibility in security is crucial.

4.3 Impact on users and usage habits

The implementation of the Zero Trust model within an organization necessitates the introduction of more stringent data protection measures, which can elicit a spectrum of impacts on users (R2:L26; R3:L21). For instance, the implementation of a sandbox system, allowing users to access the organization's resources within a secure and controlled environment, introduces a dual-faceted impact (R1:L34). On one hand, it fortifies the defense against data breaches and unauthorized access, which can enhance user confidence in the organization's data protection capabilities (R2:L10). On the flip side, the sandbox solution may also impose certain inconveniences for users, potentially disrupting their work experience (R2:L30; R3:L20).

"This time we will have a solution, is that I in his own computer above to it to do a sandbox, sandbox is and its original system isolated a system, in the sandbox inside is access to our is sdp, but his computer itself is not access to sdp, the user will actually be more comfortable, comfortable is that he did not, in fact, this is my personal computer, I can still use the sandbox I can still use the sandbox to deploy into it, because as long as I enter the sandbox, I will enter the company environment, but it will have more restrictions, which means that there is a lot of a lot of is in the sandbox and your personal computer is not quite the same, this process, your security control will not be able to do absolute control. It also increases the learning costs for certain users to a certain extent. And then there is a real increase in the load on your own computer as well." (R1:L34)

The necessity for users to adapt to new processes or find alternative methods to complete tasks can lead to an increase in learning costs (R1:L34). Additionally, the sandbox system may exert additional load on the users' personal computers, which could affect their overall computing performance (R1:L10; R4:L20). Furthermore, the enforcement of stricter security protocols within the Zero Trust model may change user behavior within the organization (R2: L24), potentially increasing the burden on users in terms of vigilance and adaptability to new security tools (R4: L10).

> *With the Zero Trust Model, employees start with minimal access rights and must request additional access as needed. This change was initially challenging for some employees, who found themselves suddenly unable to access resources they were accustomed to using (R6:L35)*

The incorporation of the Zero Trust model within an organization brings with it a series of implications that can alter the existing workflow significantly (R4: L30; R5: L15; R6: L21). These changes are primarily driven by the necessity to introduce more robust security measures to limit unauthorized access to sensitive data (R2: L32; R5: L11; R5: L13). The transition to a Zero Trust model could translate into the introduction of additional steps in the daily tasks of employees. These tasks, which previously could have been accomplished in a straightforward manner, might now require extra stages of authentication or verification before access is granted. This shift may increase the time taken to accomplish tasks, contributing to delays and potentially impacting the overall efficiency within the organization (R2: L24).

Moreover, the Zero Trust model could result in an increased need for approvals at multiple levels. This added layer of scrutiny, although beneficial for maintaining data security, could potentially create bottlenecks in the workflow, leading to longer turnaround times (R2: L24). In fast-paced business environments, such delays might have far-reaching implications on the organization's ability to deliver timely results, thereby affecting its competitive advantage. These potential challenges need not be insurmountable. One of the key strategies to manage these issues effectively is to foster a collaborative environment within the organization (R5: L30). Communication channels between various stakeholders - IT departments, management, and end-users - should be kept open and active. This will not only ensure that the potential issues are identified at an early stage but also that the proposed solutions are aligned with the needs and capabilities of all parties involved (R5: L30).

Moreover, leveraging advanced technologies such as machine learning and artificial intelligence can help minimize disruptions to the user experience while maintaining stringent security measures (R1: L24; R2: L24; R5: L30; R6: L18). These adaptive security systems can respond to user behavior patterns, allowing for more seamless and personalized security measures without compromising data protection.

The successful implementation of a Zero Trust model within an organization requires a delicate balance between strong security measures and the maintenance of a positive user experience (R1: L24; R5: L30; R6: L18). Through careful consideration of user needs, investment in appropriate technologies and tools, and fostering a communicative, collaborative environment, organizations can create a secure and user-friendly environment that aligns with their overall business objectives (R3: L20; R4: L30; R5: L38).

4.4 User Experience and Workflow Disruptions

The implementation of the Zero Trust model within an organization brings about numerous changes that impact on the user experience and cause disruptions to established workflows. These changes include the introduction of stricter data protection measures, and the need to adapt to new security protocols, which are associated with the adoption of new technologies and processes.

The Zero Trust model enforces strict data protection measures to reduce the risk of data breaches and unauthorized access (R1: L32; R5: L38). While these measures contribute to a safer environment for users and enhance user confidence in the organization's ability to protect sensitive information, they may also lead to inconveniences affecting the overall user experience (R6: L25). For instance, users might face unpredictable issues with peripherals, the need to use specialized testing equipment when working with certain tasks, and constant vigilance in handling confidential information (R3: L22). These challenges can cause delays or frustration for users, as they might need to adapt to new processes or find alternative ways to accomplish their tasks (R3: L22).

Furthermore, the Zero Trust model requires users to adhere to stricter security protocols and guidelines (R5: L38). These changes may impose additional burdens on users, such as adapting to new security tools and procedures, which can affect their overall workflow and efficiency within the organization (R2: L24; R6: L18). One example of this is the increased number of authorization levels, which may slow down the work process as tasks now require more layers of review and approval (R6: L18). This can lead to longer customer waiting times and a less satisfying user experience for employees of the organization (R2: L24; R4: L30; LR6: L18).

"Originally, one or two people finished the work, and one person handled the review. Now it may be necessary to submit the review and approval layer by layer, and then handle the review and approval. Finally, there may be several levels of approval." (R2: L24)

Another aspect that affects user experience and workflow disruptions is the adaptation and learning curve associated with the introduction of new security measures and technologies (R1, L34; R2: L24). The use of isolation environments, for example, provides an isolated system for users to access secured resources (R1: L34). Although these isolated systems offer a more secure environment, they also present differences in functionality compared to users' personal computers, which may require employees to adjust their workflows.

The use of isolated systems can also increase the learning costs for some users, as they must become familiar with the new environment and its restrictions. This learning curve might be challenging for some users, potentially leading to slower adoption of the Zero Trust model within the organization. Moreover, the increased workload on users' computers due to the implementation of isolation environments can affect their overall user experience, potentially causing performance issues and further disruptions to their workflows.

"There must be a big change in work habits, because in the past, people may not pay much attention to some aspects of security at work. You just use each other's cards, use each other's login cards and operating systems, and you use yours more frequently, but now you have changed your fingerprints. Everyone may have an improvement in safety awareness." (R2: L26)

The Zero Trust model may also bring about a change in employees' work habits, as they now need to pay more attention to security aspects in their daily tasks (R2: L26). This change may lead to improvements in employees' safety awareness but also requires users to adapt to new security measures. Organizations adopting the Zero Trust model should be aware of the potential user experience and workflow disruptions and provide adequate support and resources to facilitate the transition for their employees. This includes offering training and guidance on new security measures, technologies, and processes, as well as establishing clear communication channels for users to voice their concerns and receive assistance (R6: L20, R5: L21, R5: L11).

"Alongside these technical measures, we also invested heavily in training our staff on the principles of Zero Trust and how to operate under this new model. This helped foster a more security-conscious culture within the organization and ensured that everyone understood their role in maintaining our network's security." (R5: L11)

The implementation of the Zero Trust model within an organization has significant implications for user experience and workflow disruptions. While the model offers enhanced security and data protection, it also presents challenges in terms of adaptation, and changes in established work habits. Organizations should take these factors into consideration when adopting the Zero Trust model and provide the necessary support and resources to ensure a smooth transition and minimize disruptions to user experience and workflows.

4.4.1 Increased Authentication and Security Measures

One aspect of the Zero Trust model involves an increase in authentication and security measures, which can lead to disruptions in the user experience. For example, users may be required to enter their passwords more frequently or go through multi-factor authentication processes. This can lead to potential inconveniences and frustrations for users as they adapt to these additional security requirements. The following transaction text exemplifies this problem:

"Because of his authentication, I am always asked to enter my password. When I go into a system, I will enter my password again. If I leave the computer for about 20 minutes, I also have to continue entering my password as well as various verifications when I return" (R2: L16)

Furthermore, users may also need to undergo multi-factor authentication processes, which require the presence of multiple pieces of evidence to verify their identity. These processes can include providing a fingerprint, using a physical security token, or receiving a one-time code through an authenticator app. While these measures significantly enhance security, they can also create additional burdens for users, who must remember and manage multiple authentication factors.

Another challenge associated with increased authentication measures is the potential for users to experience "authentication fatigue." With constant demands for verification, users may become desensitized to the importance of security and begin to view these measures as a hindrance rather than a necessary safeguard. This fatigue could lead to users adopting unsafe practices, such as reusing passwords across multiple systems or sharing login credentials with colleagues, undermining the overall security of the organization.

Moreover, the implementation of stringent security measures may impact users' ability to collaborate effectively. In a Zero Trust environment, users may be required to request and obtain permissions before accessing shared resources or collaborating on projects. This process can be cumbersome and slow, potentially hindering the pace of work and stifling innovation. Additionally, it can lead to frustration among team members, who may perceive these measures as bureaucratic obstacles rather than essential security precautions.

In conclusion, the introduction of increased authentication and security measures associated with the Zero Trust model can lead to significant disruptions in the user experience. Users may face inconveniences, frustrations, and delays as they adapt to new security requirements and protocols. Moreover, these measures may impact collaboration and productivity within the organization. It is essential for organizations adopting a Zero Trust model to carefully consider these potential challenges and develop strategies to minimize their impact on users, ensuring a smooth transition to this new security model.

4.5 Future Improvements

4.5.1 The Integration of Artificial Intelligence and Big Data

The amalgamation of Artificial Intelligence (AI) and Big Data into the Zero Trust model emerges as a critical future development avenue for organizations, significantly enhancing their security posture (R5; R6). AI, known for its robust data analysis capabilities and pattern recognition, can augment the predictive power of the Zero Trust model, enabling organizations to identify anomalous behaviors and threats more efficiently (R2, R4,). This fusion not only streamlines security operations but also supports decision-making processes by providing timely and actionable insights, thus leading to more efficient threat responses and a reduced risk exposure (R3).

In the realm of big data, its integration with the Zero Trust model brings an unprecedented level of sophistication to organizational security architectures (R2). Big data's ability to process and analyze large data sets in real-time significantly enhances the Zero Trust model's efficiency, providing robust tools for detecting unusual activity and potential security breaches (R6). Moreover, the principles of Zero Trust, when applied to other organizational domains such as user behavior analytics and supply chain risk management, provide comprehensive security coverage, further strengthening the organization's defenses (R5).

Therefore, integrating AI and Big Data into the Zero Trust model can lead to a more robust, adaptive, and comprehensive security framework, dramatically enhancing organizational resilience against evolving cyber threats (R3, R6,). This promising development avenue is critical for future improvements and the successful implementation of the Zero Trust model in organizations.

4.5.2 The Trustworthiness Assessment of Devices

Ensuring the trustworthiness of devices accessing the system is crucial. R3 suggests assessing device trustworthiness by collecting information about the network connection and location. Unusual device behavior, such as logging in from a different location, can raise alerts and

trigger manual interventions to prevent potential security risks. R4 suggests the use of Micro-segmentation and hybrid workplace and R5 elaborates on it by explaining on risk scoring, which means ML can assist in creating adaptive risk scoring models that consider a range of factors such as for user behavior, devices, network behavior, and historical data. This allows the security system to react dynamically to threats, and to allow which device should get access and depending on their previous record history, authorization requests and access. The second future improvement which R5 mentioned during the interview is the automated access control which will reduce the administration burden of manually controlling access and will likely improve the security as it minimizes human errors.

5 Discussion

This chapter delves into a detailed discussion of our research findings on the Zero Trust model's implementation and impact in organizations. We will explore how the model enhances security, the challenges it presents to user experience and workflows, and compare our findings with previous research. Furthermore, we will identify gaps in existing research. By the end of this chapter, readers will gain a deeper understanding of the Zero Trust model's benefits, challenges, and implications for organizational cybersecurity strategies.

5.1 Transition to the Zero Trust Model

The shift to the Zero Trust model transcends mere technological modification, representing a comprehensive organizational transformation (Chen, Hu & Cheng, 2019; Moubayed, Refaey & Shami, 2019). This paradigm challenges conventional perimeter-based defenses, preferring a "never trust, always verify" strategy focused on protecting resources rather than network (Campbell, 2020). It necessitates a reimagining of existing security strategies and policies, requiring the involvement of stakeholders across the organization, from top management to frontline employees. The transition to the Zero Trust model, as revealed by the findings of this research, is a complex process that varies significantly among organizations. This process necessitates the ongoing evaluation and development of both novel and existing procedures within the organization, with a view to identifying where Zero Trust can be applied and pinpointing those components within the system that may be vulnerable to security breaches (He et al., 2022). This diversity in adoption stages underscores the complexity of the transition process and the need for a tailored approach that considers the unique needs and circumstances of each organization. The research also highlights the advantages associated with the transition to the Zero Trust model in which traditional network security solutions, such as firewalls and VPNs, are unable to encounter such modern threats. This limitation of traditional security solutions has necessitated the shift towards more robust security frameworks like the Zero Trust model.

Our research findings indicate that some organizations we have studied have fully adopted the Zero Trust model, while others are in the process of transitioning or adopting a hybrid approach. This is attributable to the organizational bureaucracy and the intricacies involved in initially establishing a Zero Trust (ZT) model and subsequently implementing it. Transitioning to a Zero Trust model has its disadvantages. One primary concern is the elongated decision-making process in organizations, which employees find time-consuming. Furthermore, the initial setup of the Zero Trust architecture can be burdensome. Another disadvantage which R3 mentioned is that, everybody needs to be in the office to do the authorization, and nobody can lend their credentials to anybody.

It has been evident through numerous interviews that the transition from a traditional security structure to the Zero Trust model has not been straightforward. According to Moubayed, Refaey & Shami (2019), this is due to organizations needing external access to resources that they must securely and reliably connect to in order to retrieve information. Companies like Combitech and CloudDeep Technology, which collaborate with other market players and have consultants working with other organizations, are impacted by this situation. They

require an optimized and secure network that allows their consultants to use the same computer for both consulting work and internal company tasks.

5.1.1 Advantage of Transition to the Zero Trust Model

One of the main reasons these companies are transitioning to Zero Trust, according to Kumar et al. (2019), is the need to strengthen and protect their network so that even if a virus is introduced from a client's computer, it can't affect the network because it is shielded by Zero Trust. Consequently, the virus cannot access and alter the resources and information. Both Combitech (R4) and CloudDeep Technology (R1) place great emphasis on computers and their environments. According to Chen et al. (2019) and Shlapentokh-Rothman et al. (2020), devices are the second weakest link in the security architecture and therefore need protection. An attacker can exploit an application with a weak link and use it as an entry point into the network, potentially causing significant damage. Instead of protecting the entire network, the user and their devices are the focus of protection, as suggested by Rose et al. (2020).

Our research also reveals the importance of collaboration with cloud providers and the utilization of resource caching in facilitating the transition to the Zero Trust model. These strategies can help organizations overcome the hurdles associated with the transition and augment their security measures. Nevertheless, the effectiveness of these strategies may be contingent on the organization's unique circumstances, such as its size, industry, and nature of operations. The implementation of the Zero Trust model significantly enhances an organization's security posture. By assuming no trust, organizations aim to minimize their attack surface, reducing the risk of both internal and external security breaches (Kindervag, 2010).

5.1.2 Disadvantage of Transition to the Zero Trust Model

It has been evident through numerous interviews that the transition from a traditional security structure to the Zero Trust model has not been straightforward. According to Moubayed, Refaey & Shami (2019), this is due to organizations needing external access to resources that they must securely and reliably connect to retrieve information. Companies like Combitech and CloudDeep Technology, which collaborate with other market players and have consultants working with other organizations, are impacted by this situation. They require an optimized and secure network that allows their consultants to use the same computer for both consulting work and internal company tasks.

This multifaceted need calls for a security infrastructure that is not only robust enough to fend off cyber threats but is also capable of handling diverse tasks across different environments without compromising operational efficiency. The adoption of a Zero Trust model, while providing enhanced security, necessitates careful orchestration to prevent disruptions to work processes or unwarranted complexity in daily tasks.

However, the shift to the Zero Trust model also impacts users and their usage habits. Increased authentication requests and stringent security measures potentially cause friction for end-users (He et al., 2022). Users might have to adapt to new processes, leading to temporary drops in productivity. The Zero Trust model significantly alters users' interaction with organizational resources, pushing them to be more vigilant about data access, sharing, and security (Herath & Rao, 2009).

Despite these challenges, the findings suggest that the Zero Trust model provides a more proactive approach to cybersecurity, enabling organizations to minimize their attack surface and reduce their susceptibility to unauthorized access. Risk to data or resources. This enhanced security posture can enhance an organization's resilience against cyber threats and improve its reputation and credibility in the eyes of customers, partners, and regulators.

The model encourages security controls like multi-factor authentication, least-privilege access, and micro-segmentation to safeguard sensitive data and systems. Such measures bolster the organization's resilience against cyber threats, enhancing its reputation among clients, partners, and regulatory bodies.

5.2 Enhanced Security Posture

The transition to the Zero Trust model has been found to significantly enhance an organization's security posture. This model offers a more proactive approach to cybersecurity. By continuously verifying the authenticity of users and devices, organizations can minimize their attack surface and reduce the risk of unauthorized access to sensitive data or resources.

Our research findings align with the work of previous scholars who have emphasized the potential security benefits of the Zero Trust model. For instance, Kindervag (2010) argued that the Zero Trust model could significantly reduce the risk of internal and external security breaches by eliminating the concept of trust from organizational networks.

5.5.2 Advantages of Enhanced Security Posture

The Zero Trust model offers a robust alternative to conventional network security solutions, embodying a shift in focus from securing network perimeters to securing individual resources. As pointed out by Boville (2020), the vulnerabilities of perimeter-centric security solutions like firewalls and VPNs often result from their lack of attention to internal threats. They function on the assumption that any activity within the network perimeter is trustworthy, leaving internal resources exposed to insider threats and malware that breach the perimeter. In contrast, the Zero Trust model eliminates the notion of implicit trust for any entity, whether inside or outside the network perimeter. This model can considerably minimize the attack surface, as it secures each resource individually to prevent lateral movement of threats within the network. By requiring consistent verification of identity and access permissions, the Zero Trust model provides an enhanced level of protection for resources and limits the potential for unauthorized access, thereby enhancing the organization's overall security posture.

Another significant security benefit of the Zero Trust model is its emphasis on continuous authentication and verification. Unlike traditional security models, which typically operate on the assumption of trust, the Zero Trust model assumes no trust. This means that every user and device must be continuously authenticated and verified, regardless of their location or network status. This continuous verification process can significantly reduce the risk of unauthorized access and data breaches.

5.5.3 Disadvantages of Enhanced Security Posture

Adopting the Zero Trust model necessitates a substantial organizational transformation, presenting intricate complexities and formidable challenges. A fundamental requirement is the introduction of advanced security measures inherent to the Zero Trust model, which demands considerable technical alterations. Essential investments in cutting-edge technologies, such as identity and access management (IAM) systems, network segmentation tools, and security analytics platforms, become unavoidable (Campbell, 2020).

Additionally, the vital aspect of employee training emerges in the transition process. The implementation of the Zero Trust model alters the interaction dynamics between users and organizational resources, thereby emphasizing the indispensability of user education and awareness (Cunningham, 2018). Employees must comprehend the principles underpinning the Zero Trust model and their respective roles in fortifying cybersecurity.

Moreover, the plausible disruptions to workflow and user experience form another significant apprehension. Enhanced authentication procedures may extend resource accessibility durations and consequently evoke user frustration. Furthermore, the task of securing stakeholder assent for the transition process is arduous. Leaders necessitate understanding the intrinsic value and indispensability of a Zero Trust model and committing adequate resources and backing for its execution. Embedding a culture epitomizing 'never trust, always verify' within the organization requires an all-encompassing shift in mindset across organizational tiers (Chuan et al., 2020).

While considering these potential challenges, the importance of a meticulously formulated transition strategy is critical. Striking an optimal balance between security enhancements and usability is quintessential, alongside adequate organizational preparedness for imminent changes.

5.3 User Experience and Workflow Disruptions

The Zero Trust model's rigorous data protection measures are designed to fortify the organization's defenses against data breaches and unauthorized access. While these measures provide a safer environment for users and bolster their confidence in the organization's commitment to safeguarding sensitive information, they may inadvertently introduce inconveniences that impact the overall user experience. For instance, users may encounter unpredictable issues with peripherals, need to use specialized testing equipment for certain tasks and exercise constant vigilance in handling confidential information. These challenges can cause delays and frustration, as users grapple with new processes and seek alternative ways to accomplish their tasks.

Previous research on the topic of user experience and workflow disruptions in the context of the Zero Trust model has primarily focused on the technical aspects of the model, such as its ability to enhance the security posture and reduce the risk of data breaches (Teerakanok, Uehara & Inomata, 2021). However, there has been less emphasis on the human aspects of the model, such as its impact on user experience and workflows. For instance, studies have highlighted the potential for increased security measures to cause inconveniences for users, such as unpredictable issues with peripherals and the need for constant vigilance in handling

confidential information. However, these studies often do not delve into the specific ways in which these inconveniences impact the user experience and disrupt workflows.

Our research addresses this gap by providing a more comprehensive understanding of the human aspects of the Zero Trust model. We explore the specific ways in which the implementation of the model impacts user experience and disrupts workflows, and we provide empirical evidence of these impacts. For instance, we found that the increased need for approvals at multiple levels, a key feature of the Zero Trust model, can create bottlenecks in the workflow and lead to longer turnaround times. This finding builds on previous research by providing a more nuanced understanding of the potential disruptions caused by the Zero Trust model.

However, it's important to note that the transition to the Zero Trust model is not without its challenges. Organizations must grapple with the complexities of implementing new security measures, training employees, and managing potential disruptions to workflows and user experience. The successful implementation of a Zero Trust model within an organization requires a delicate balancing act between implementing robust security measures and maintaining a positive user experience. Through careful consideration of user needs, investment in appropriate technologies and tools, and fostering a communicative, collaborative environment, organizations can create a secure and user-friendly environment that aligns with their overall business objectives.

5.4 Future Improvements

During the Interviews (R1) mentioned about the increasing data volume and intelligence of the system increase, there will be automatic matching rules and adaptation capabilities. This means that the system can dynamically adjust permissions based on individual circumstances, such as granting temporary permissions to employees who have special circumstances. The adoption of more intelligent strategies in determining the level of security, as opposed to strict adherence to inflexible rules, is gaining interest in the field of cybersecurity. This movement aligns with the research conducted by Elsayed et al. (2019) and Myint Oo et al. (2019) on the application of machine learning (ML) in Zero Trust Networks (ZTN). The studies suggest that ML can potentially enhance security by not only detecting intrusions but also identifying threats within social networks and pinpointing attacks on Internet of Things (IoT) networks. Prominent ML models such as Support Vector Machines (SVM), Artificial Neural Networks (ANN), and deep learning structures like Long Short-Term Memory Recurrent Neural Networks (LSTM) are used for these purposes. These machine learning algorithms have shown promising results in the given contexts, indicating their effectiveness in implementing ZTNs.

One of the most significant benefits of incorporating ML into ZTNs lies in its capacity to recognize patterns related to user behavior, particularly regarding login frequency and locations. For example, if a user typically logs in during daytime hours from their office location, an unusual login attempt in the evening from an unfamiliar location would raise a red flag. The system would then deny the request, or necessitate additional user authentication and verification to ensure the integrity of the login attempt.This enables the system to dynamically adjust permissions and security measures based on individual circumstances. This results in more intelligent and adaptive security policies where permissions are continuously evaluated and revised, based on the ongoing assessment of the system's security

posture. This indicates a shift towards more personalized and adaptive cybersecurity strategies, as empowered by machine learning within Zero Trust Networks.

Integration of AI and Big Data: The respondents agree that the future improvements should involve a more organic combination of AI and big data. This integration can help in building more mature models and rule setters within the industry. By leveraging AI and Big data, the system can accumulate and analyze large amounts of data, making the models more valuable and effective. The study by Mandal, Khan, and Jain (2021) and Fu et al. (2022) highlights the significance of addressing data security concerns arising from potential eavesdropping on device or network traffic, which may compromise the confidentiality of the transmitted data. Integrating AI into Zero Trust can be beneficial in minimizing the risk of unauthorized access by hackers. Deep Learning (DL) and Network Segmentation (NS) are two areas that can contribute to enhancing the security of the overall network. Deep Learning (DL) techniques are used to analyze the incoming network traffic, patterns, detect suspicious activities, and identify potential security breaches. By leveraging AI algorithms, DL models can learn from historical data and detect suspicious activities or any unauthorized access attempts. These unauthorized access attempts can be traced back to the device using MAC and IP address (Aminanto et al., 2017); Mandal, Khan & Jain., 2021; Fu et al., 2022). This can help in proactively identifying and mitigating security threats. Network Segmentation (NS) is also mentioned by R4 and according to (Rose et al., 2020)) it involves dividing the network into smaller, isolated segments or containers. This approach limits the lateral movement of hackers within the network, as each segment has its own security controls and access permissions. Another strategy, as per R6, focuses on is the concept of containerization. By establishing small, independent networks within a broader context, it could potentially lower the likelihood of unauthorized entry into crucial resources. R3 also highlights the essentiality of the need to improve artificial intelligence (AI) algorithms. Particularly, AI algorithms play an integral role in the functioning of an intelligent trust engine, a key component of the Zero Trust model. As stated by Syed et al., (2022), the trust engine considers several data sources including access requests, identification, and threat intelligence.

R6, R3, and R1 collectively imply that these algorithms should be developed further to be more adaptable and able to learn. This will enable a better understanding of user and employee behaviors, which, in turn, allows for improved security decision-making. It's crucial that these algorithms should be implemented in the future, yet flexible, in order to most effectively protect the network.

5.5 Summary

Our research has revealed that several organizations have made a complete shift to Zero-Trust architecture. This decision, according to academic literature, is primarily driven by inadequate internal control systems prevalent in conventional solutions, which often lead to ineffective management and increased risk of data breaches. Furthermore, the dependence of these organizations on unreliable hardware and devices poses substantial threats, potentially causing both physical damage to servers and system malfunctions that could result in data loss.

However, the literature also highlights several challenges associated with transitioning to the Zero Trust model. One of the significant barriers is the considerable time and financial investments involved, which vary based on the organization's size and this also came forwards in our findings. Additionally, a thorough evaluation of the existing solutions is essential before initiating the transformation. From our literature findings, the future of Zero Trust will involve a combination of advanced authentication methods, continuous monitoring, intelligent risk assessment, and the integration of emerging technologies. By adopting these advanced technologies which improve continuously using deep-learning models, organizations can strengthen their security posture and better protect their critical assets from evolving threats.

Table 7: Themes and Key Points from our Finding

Theme	Key Points
Transition to the Zero Trust Model	• The transition to the Zero Trust model varies among companies, with some adopting a hybrid approach and others fully adopting Zero Trust. • The transition necessitates both technical expertise and a paradigm shift in security thinking. • The diversity in adoption stages underscores the complexity of the transition process and the need for a tailored approach that considers the unique needs and circumstances of each organization. • The implementation of the Zero Trust model can introduce complexity and overhead to an organization's IT infrastructure. • It requires a substantial organizational transformation, presenting intricate complexities and formidable challenges. • The shift to the Zero Trust model also impacts users and their usage habits. Increased authentication requests and stringent security measures potentially cause friction for end-users. • The Zero Trust model significantly alters users' interaction with organizational resources, pushing them to be more vigilant about data access, sharing, and security.
Enhanced Security Posture	• The Zero Trust model offers a robust alternative to conventional network security solutions, focusing on securing individual resources rather than securing network perimeters.

	• The Zero Trust model provides a more proactive approach to cybersecurity by continuously verifying the authenticity of users and devices, thereby reducing the risk of unauthorized access to sensitive data or resources. • The Zero Trust model offers a dynamic risk control strategy that is more adaptable to the dynamic network environment. • The implementation of an enhanced security posture can introduce complexity and overhead to an organization's IT infrastructure. • The shift to an enhanced security posture impacts users and their usage habits. Increased authentication requests and stringent security measures potentially cause friction for end-users. • Early risk detection increases awareness of suspicious behavior but at the same time it is time-consuming and enhances user experience.
User Experience and Workflow Disruptions	• The Zero Trust model introduces more robust security measures, which can result in longer wait times. • Users may need to remember and manage various credentials, leading to potential frustration and reduced productivity. • The transition to a Zero Trust model can significantly alter existing workflows within an organization. • The Zero Trust model could result in an increased need for approvals at multiple levels, potentially creating bottlenecks in the workflow and leading to longer times.
Future Developments	• The study suggests that advancements in areas like artificial intelligence and machine learning can further enhance the effectiveness of the Zero Trust model in managing security in an ever-evolving digital landscape. • These technologies can improve the accuracy of threat prediction and informed security decision-making, providing a more proactive and efficient approach to cybersecurity.

6 Conclusion

This research has embarked on an in-depth exploration of the impact of the Zero Trust model on organizations. While the Zero Trust model has been recognized for its potent ability to fortify an organization's security posture, the full extent of its implications on an organization warrants thorough examination.

The study has revealed that the adoption of the Zero Trust model offers significant advantages, particularly in enhancing data security and streamlining risk management processes. However, these gains should not overshadow potential challenges that may arise, such as increased complexity in security management, possible disruptions to user experience, and the necessity for persistent monitoring and evaluation. It is, therefore, incumbent upon organizations to assess whether the advantages of implementing a Zero Trust framework effectively offset any potential negative impacts on their overall operations.

Moreover, the challenge of successfully implementing a Zero Trust model lies in striking a delicate balance between the robust cybersecurity requirements it demands and the operational considerations of the organization. This necessitates a profound understanding of the organization's unique needs, a clear foresight on the potential impact of a Zero Trust approach on its various operations, and a readiness to adapt to an ever-evolving cyber threat landscape. The future of cybersecurity, the Zero Trust model holds significant promise.

As cyber threats grow increasingly sophisticated, a shift towards a trust-nothing, verify-everything approach could prove to be the most effective line of defense. However, the model's successful implementation requires more than just a shift in technological solutions; it demands a change in organizational culture, mindset, and workflows. The impact of the Zero Trust model on organizations is profound, influencing not just productivity but also operational efficiency, user experience, and the organization's overall security posture. Therefore, the adoption of a Zero Trust model requires a holistic view of an organization's needs, a readiness to adapt, and a commitment to striking a sustainable balance between security and operational effectiveness.

In conclusion, the Zero Trust model represents a major paradigm shift in the field of cybersecurity. As with any significant change, it carries both opportunities and challenges. By understanding its impact on organizational structures, operations, and culture, organizations will be better equipped to navigate this new landscape and harness the potential of the Zero Trust model for a more secure future.

6.1 Future Work

Future research in this area could focus on quantitative studies that measure the specific impacts of Zero Trust on productivity, security, and other key performance indicators within organizations. This would enable a more precise understanding of the trade-offs involved and help organizations make more informed decisions when considering Zero Trust. Additionally, longitudinal studies could provide insights into the long-term effects of Zero Trust implementation. For instance, does user productivity eventually increase as employees

become more accustomed to the new security measures? How does the model impact the organization's resilience against cyber-attacks over time?

Finally, as technology continues to evolve, so will the Zero Trust model. Future work could also explore how advancements in areas like artificial intelligence and machine learning can further enhance the effectiveness of Zero Trust in managing security in an ever-evolving digital landscape. While the scope of our research provides valuable insights into the impact of the Zero Trust model on organizational productivity, it is not without its delimitations. Primarily, our study focused on qualitative insights gathered from a limited number of practitioners and stakeholders. This means the findings may not fully represent the diverse experiences and perspectives of all those working with Zero Trust across different industries and scales of operation.

Appendix 1 - Interview Invitation Outline

Thesis: The Impact of Zero Trust Model on Organizational

Thank you for your time and interest in participating in our research study for our master's thesis. Your insights will be invaluable in understanding and improving the implementation of Zero Trust Model and its impact on organization. The interview will cover different topics related to your experience with the Zero Trust Model, their influence on your organization. The topics are as follows. Some of the questions are presented so you can be prepared in case you don't have an immediate memory of your interaction during some cybersecurity events.

1. Traditional Solutions and Zero Trust Model

- Are you familiar with theZero Trust Model?
- What is your understanding of the differences between traditional cybersecurity solutions and the Zero Trust Model?

2. Implementation and Adoption

- How was the Zero Trust Model implemented in your organization?

3. Organizational impact and Zero Trust

- In your experience, what impact does the Zero Trust Model have on an organization's overall security posture?
- Zero Trust Model has many advantages, however, you might have noticed that it also comes with an increased complexity at your organization?
- Have you noticed any changes in employee behavior or work habits due to the implementation of the Zero Trust Model?

4. Zero Trust Features

- How do the features of the Zero Trust Model (e.g., authentication, access control, micro-segmentation, security automation) influence your organization in general?

5. Future Prospects and Improvements

- What further improvements or adjustments do you foresee for the Zero Trust Model in your organization?

While answering these questions, you can provide different details related to your experience. This will enrich our study. We ensure that all this information will be managed anonymously and confidentially. A transcript of the interview will be shared with you after the session so you can confirm that the content is aligned with what you answered.

Appendix 2 - Transcription - Respondent 1

Num	Person	Question & Answer	Code
1	CL	Ok, briefly introduce your own background.	
2	R1	I am mainly engaged in the Internet work, and then I have been working for about 8 years, and then I have been switching back and forth between the two directions of product and technology. My job, the core is mainly committed to developing China's leading market, and then my boss is Chen Benfeng, who is the leader of zero trust in China's CST region, and is also one of the creators of the Sdp protocol, so we are an initiator and a promoter of zero trust in China.Then we have been hoping to use zero trust as a mature product to cover all Chinese enterprises, including some overseas enterprises in China.	
3	CL	According to my understanding, you actually have a better understanding of Zero Trust	
4	R1	Yes, it is.	
5	CL	What is your understanding of traditional network security solutions?	

6	R1	In fact, the traditional we can actually understand the entire Internet era, it is actually experienced several cycles, the first cycle is called software. I remember when I was very young, we saw the so-called security defense is to use antivirus floppy disk, there is a very small square disk, and then there is antivirus software, which may only a few KB or a few MB of antivirus software, at that time we think it is point to point. When we entered the era of 2.0, which is often referred to as the firewall era, I think this is more like a point to line process, in essence, is to link a server and a host of home host to a piece, then in fact, our core defense is not the home personal computer, or home personal computer, is not the focus of defense in the Internet, but more The so-called firewall concept is actually a layer of defense at your port, all the entrants and exits in this port, on top of the port I allow, to identify your identity to identify and determine whether you allow. ***But when we enter the so-called 3.0 era of the Internet era, the biggest difference in this era is that all the hardware servers or services we think are on the cloud. The so-called on the cloud means that it will no longer be a host, such as a large IDs server room such a place, and then a broadband center such a place, but has become a larger is everything is connected together.*** ***And we started to use a lot of distributed technology, that is, between the point and the point it is a breakpoint, you understand it? That is, all the information it is actually a mesh structure of the process of a single point of breakthrough, and then to do a horizontal attack on this thing has become very scary, because once you invade a point, it's a horizontal attack on all your points it all breakthrough.*** ***So this process to deal with the entire cloud era, we believe that sporadic awareness based on the background of this era generated a defense characteristics, this is my understanding.***	TSS
7	CL	Is it causing an organisation to transition from a traditional solution that is to a Zero Trust solution,	

		for example, where there are a lot of these attacks on the cloud happening, is this a more typical example?	
8	R1	Yes, let me give you an example, in fac***t we can break down some of the defence industries and look at them, for example, let's just say manufacturing, one very typical feature of manufacturing is that it has a particularly high number of distributors and suppliers.*** He has a lot of such customers, this time it is inevitable that it has to open up part of their own, for example, CM rights or ERP rights to these sellers, and because a large number of its services are arranged on the cloud, of course, there is a large part of it is placed in their own traditional server room inside, but because it for the whole increase in efficiency, it will still be a large number of cloud. ***As soon as we access the cloud we understand the problem that there must be a traditional concept called LAN, or intranet, inside the IDC server room. Within my LAN I make a firewall, or you access my LAN from the Internet, and I can defend this process. But once my service is on the cloud, it is directly connected to the Internet. It does not exist even if the intranet is an intranet of the cloud's IDC centre, but from my point of view, it is already connected to the Internet, because I can only access it through the Internet, right?*** As a service provider, I can only go through the Internet open, but this process, once one of my suppliers he is very arbitrary, because I have hundreds of suppliers, there is a supplier, for example, his account is lost and left behind, or was transferred out, or he holds some not good mentality resold, no matter what kind of way, this time will create a new problem.	TZTM, AC
9	CL	Ok has actually encountered any difficulties or challenges in implementing such a Zero Trust service, and such challenges are not often seen in the traditional model.	ZTMA

10	R1	In fact, there is, ***first of all, because you think because our data transmission is encrypted***, right? ***This process is inevitably a large volume of business, and there will be some performance loss in this process, which is one of them. Another big problem is that many enterprises are concerned about the cost.*** I give a simple example, because the traditional is point to point, I go over the direct access on it, and sdp this process to produce a thing, that is, I want to always on your data encryption, and then decryption, and then transmitted over, on the channel itself process are to go through my server to do a plus or minus password, that is, I want to do on your security to do a authentication, that is, your traffic On double up. This process for the enterprise to speak it must understand, because all of the cloud it speaks of cost, the first thing is talking about bandwidth, to speak of traffic, right? Because this is the way to calculate, so the cost will be a relatively large threshold for enterprises to choose us, for them to consider this issue.	
11	CL	Are there any particular examples of how you have overcome such a limiting situation?	
12	R1	In fact, we are solving this problem through two angles. The first angle is that we will solve it through the enterprises themselves, first of all, the developers of cloud computing welcome us, because in itself they are willing to help us sell because it can greatly help him consume his resources, which is very practical. Because that's what they're in the business of selling, and if he can push a customer's resource consumption up twice as much, he's still very happy to do that. Again, it helps them with some of the security issues. ***Then we also put a reverse pressure on him, that is to say you have to push the price down if you want to go through my traffic, because our traffic is bigger, we get more customers, we can help them to push the price down, this is one of them, we were working with something like Huizhou Mobile or Unicom, and also Hebei Telecom which, because our core cooperation is actually Microsoft, we are with Microsoft We have done a big cooperation there, but we later found that in***	ZTMA ZTMD

		fact Microsoft they can accept such a bandwidth strength is also very limited, so we later is directly with them in the domestic some broadband we can even talk about we can not help our cloud service providers to lower their traffic prices, because his traffic is large, we can then reverse the price, so then we can also actively This is part of what we can do for our customers. The other is that we do a technology called resource caching in the process of computing, I do not decrypt the case of all your encrypted data to do a logo, when I find this logo is similar, some static resources such as pictures and so on, in the cache cycle, in the cache cycle, we can greatly reduce the loss of traffic.	
13	CL	How does this zero trust model affect an organisation's overall security posture?	
14	R1	I think this may be an inevitable trend, because in fact we know that many traditional enterprises, including manufacturing, finance, and the Internet, the Internet is fine, in fact, like finance and manufacturing, these two relatively traditional industries, they will have some natural desire to say that my services are deployed in my local, that is, I have my own IDC server room, all things are me so that I can be safe and responsible for myself. I can be responsible for my own security. But because of the current form of business, for example, banks also need to use a lot of business, especially for cryptocurrencies and so on, and there is no way for them to say that they can include all the Idc rooms, they can't say that I can make a cryptocurrency by myself and then I can put all the books of the currency in me. This is not in line with its technical logic, and this time a new situation arises, the new situation is that he has to accept the cloud, even now a lot of traditional business he is already accepting the cloud, he has to accept the process of the cloud, he has to consider a new problem, which is compliance, because the traditional way to the traditional security situation, it can only do a part of the defense, because it can not do a complete defense of the process This time we will be a	ESRM, ZTMA

		better solution provider if we consider compliance for the financial sector, for example. If it's a manufacturing industry like ThyssenKrupp, a very famous lift company in Germany and the second largest in the world, they have a concept, because their manufacturing industry has many distributors and many production plants. For example, if my motor breaks down, I have to go there at any time. I can't say that everyone is concentrated in Shanghai, and then if there is a problem in Anhui, I can't send someone from Shanghai. So this leads to a new problem: its staff are too dispersed, but it wants to keep all its safety, all its rules and regulations, all its safety and defence system, its operation and maintenance system in line with the head office. Like ThyssenKrupp, they call the tradition follow sun, that is, all things follow my head office, in this process, it must enable the cloud, and it must enable the cloud process, and there is no way to say that all things are unified management, then the best solution is to use such a security trust method like zero trust, so that everything is in a node, because I am SaaS, you use the cloud, you can use the cloud to protect the security. Because I am SaaS, you use me as a centralized node, I do your sun.	
15	CL	Have there been any unexpected benefits or drawbacks to the Zero Trust model in your organisation, especially in your experience?	

16	R1	In fact, both of these points are actually there, on the unexpected benefit is that to a large extent he helped many many operations and maintenance personnel and security personnel to solve security problems, because it is so, you think I as a security service provider, in fact, I am a security node for all my service users or my customers, and I will receive itself I will have a very powerful is a virus database, right? I will tell all for example you use me, ***you use my set of products when I will determine a lot of security problems, I will constantly do a security upgrade themselves, including the patch and so on.*** I will tell all for example when you use me, you use my set of products, I will come to determine a lot of security issues, I will constantly do a security upgrade themselves, including my patches and so on, such as vulnerabilities and so on, including scanning and so on this series of security issues, I will do self-improvement, because I am after all a security company, I am both professional, and I every day my server My big data are doing, and all companies receive security issues are centralized point, like I certainly do not mean to centralize me a shop, because we are also distributed in each node, but these data belong to us, then the equivalent is to say that I will act as a very powerful brain, for all users to solve all security problems, and this process when my data volume is bigger, my security capabilities The more data I have, the stronger my security capabilities will be, which all these companies cannot do on their own, because when any company solves its own security problems, it can only solve a single problem within its own scope, and its security engineers cannot even play an absolute role. ***When using us, we have two advantages, the first is that we are more professional than they are in doing security themselves, and the second thing is that we can also help him save some of the manpower costs, and make it easier for their security engineers, and then also save some of the simpler, or some of the security personnel.*** In fact, I just mentioned, because in fact, zero trust is after all a newborn industry, this process will have a part of the traditional industry originally in the process of change, you dare not easily replace, or	ZTMA, ESRM, MLSA, CO

		in this process, you are after all a relatively young business at the business level, when going to contact the replacement of the old business, is bound to produce some problems, we all We all know that. As an example, for example, we were talking to Tieta, the largest technology service provider in China, including telecommunications and these are all through him to go to his service is a very large state-owned enterprises in China, we then to his service when a problem will arise. He put forward a concept, that is, I carry my staff every day is about more than 4 million, my staff a day will be in the morning of the punctual 8:00 more than 4 million at the same time logged into their computers, while logging into their business server to solve their own problems to solve. When you deploy your service over, more than 4 million people log in at the same time every morning at one point, you can't carry it. It is a very detailed business process, so when we find that SaaS cannot solve all the problems of all the customers in a point-to-point manner, and when the problems are concentrated in a single point, I think this is a problem that no new business can imagine or avoid facing.	
17	CL	In your experience you have this kind of growth in complexity and this kind of resource consumption, there is actually a more significant growth, for example, maybe the user needs more procedures when he accesses, and then he has more overheads especially in terms of, for example, traffic and bandwidth, which exists, but have you noticed that in this kind of organisation with the involvement of zero trust, this kind of complexity of the organisation is not only the complexity of the organisation's structure, but also the complexity of his employees, for example, the complexity of their daily work, without encountering this kind of additional overheads.	

18	R1	I think this is actually okay, as far as we are dealing with the actual process, we have a security concept called fencing, fencing means that we can do some restrictions on the device based on some conditions or some information, for example, I stipulate that you can only access the company's website in this location, right? You can only access it during this time, right? In fact, for many security officials, or security staff, the reason they prefer zero trust is that all computers will be centrally controlled by their rules. It's a benefit to the security staff that they don't have to think about the complexity of their own business, like we do now with many products, or it will have ready-made templates, right? Security templates we are actually researching the rules of other companies or the rules of the industry to provide more templates to our these, he is based on the template to make changes to make adjustments, although the line between the company and the company is different, but there are many commonalities between the industry, and then this process largely reduces it to lay out the rules of a process. So I think that in terms of complexity, we are reducing the difficulty of using it.	CO, AC
19	CL	From my understanding, for example, if you popularise this business, it is no longer necessary for front-line staff to have such a concept of security in their minds. It may be concentrated in a single point of complexity, but if it is not divided out, its overall complexity may be reduced and reduced.	

20	R1	Yes, I'll give you a very realistic scenario, which is ThyssenKrupp. ThyssenKrupp is like this, because their company uses Microsoft, and all the computers are controlled by a LAN controller from the head office, which means that I can install whatever I want on your computer, and I can download whatever I want on it, but you can't download if you're not allowed to. So it's very simple for us to work with him, because I am a client, right? So he only needs to go to the user as long as the computer is turned on, this computer is online, automatically in the background will it this program to it installed, after the installation also do not need to go to the registration, also do not need to go to the registration, because his computer information is his administrator computer administrator information, the user information is actually already itself is registered, in Microsoft, he is there is a Microsoft has a What's it called? A secure account system, we directly a docking, docking over, ***its entire account information including the organization structure is all inverted, and then this time we will recommend him a management template, management template may be such as this industry or that direction, and then they go on this basis to make changes, after the modification is actually on the fence or some information to do some, such as This point to this point is not to allow employees to access the Internet, and then for example, the boss is not to open, workers which level of staff will get higher, itself is a whitelist of settings, this process in fact it alleviates a lot.***	ESRM, AC, ME
21	C L	Does it have any impact on the overall user experience process as this zero trust is applied to such companies?	

22	R1	In fact, there is, in itself, we feel that more and more enterprises are asking for zero trust. From their point of view, when the entire business of security is centralized or shrunk to a point, they hope to put more of their existing security capabilities into our system, because you inevitably have a problem is the process of the old and the new, the new is not all old can not do it, for example, it may have used a security device for 10 years, said today The next day he deleted the whole equipment, because you know a lot of traditional security it is box, it hardware facilities directly thrown into the server room, and then in the local area intranet to do a security protection, but the first of these things it has paid the cost. ***The second thing it he also dare not say to solve this thing on the solution, and there are some have some company it's even no way to use security is zero credit security, including sdp this way, I give an example, is China very have a quite famous company Miho You, in fact they are very inclined to use zero trust, but for the game industry has a very important problem.*** ***The original words and video of a transmission, they move a resource may be very large traffic transmission, with zero trust encryption after the completion of the transmission back, decryption and then passed, and then the traffic double these things, and this process it has a very fast transmission, encryption process, when I put a thing to expand, the time consuming enhancements with the original completely different, as an employee or I as an original As an employee or as an original artist, a 3D max model that I have to transfer, the feeling is completely different.*** Ok, so these obstacles are actually inevitable.	CO, UEWD, ESRM
23	CL	In your experience, for example, have there been any significant changes, for example before and after the implementation, in terms of changes in this process or the overall user experience?	

24	R1	There are some companies because they are relatively new, like Little Red Book, for example, one of the companies we work with, they are relatively new to the internet and their business is relatively new, right? It can actually be new all of a sudden, because I'm all on the cloud, I can be brand new all of a sudden, and then this process is actually a very good experience, including it has branches in various places and so on, when he wants to deploy his own security, in fact, it is very similar to the experience we are using Zoom. ***The security guy just needs to put his organisational information and structure, and enter his email into our system, and then he will send a link to all the emails, which means that you need to download the program and install it, and then in the process, log in through your own company email, and log in to the program with your original email account password, but then it will have become the default boot-up. After you agree to this, you end your original access to all the things, or according to the original you just do a download, an automatic installation, and finished all, and then for the security practitioners his feeling is very good, because this instant all the original people are not controlled by the things, all in your control, you do not allow him to access, you have a completely legitimate reason You have every reason to deny him access.*** I can do that during the work of his computer, I do not allow you to access anything, I can do that during the work of what you access me what people are not allowed to access my company's internal things, I can do that. In this process, its security is greatly protected.	ESRM, AC, CO
25	CL	Sdp in fact we all know it is zero trust, it has many models, it has many features, for example it has many such features, or it has continuous authentication, and access control, it's micro segregation as well as security of this automation, in fact in your organization, how does all this affect, is there this affect to your organization?	

26	R1	***For my organization, it actually has a great impact, because we ourselves, in addition to the stp itself micro-segregation , we are also is also in use, but this service in our process and did not try to open to our users, because micro-segregation it is a very need with your business content.***	ME
27	CL	What are the benefits?	
28	R1	What are the benefits? The benefit is that when we use the Zero Trust system, our overall security on the cloud is very high after the deployment of this mechanism.	ESRM
29	CL	For example, we talked about authentication prevention and control, and micro-isolation, and security automation and which of these features do you think have had the greatest impact on the organisation, both positively and negatively.	
30	R1	We think there are still some industries that we have had some very positive impacts on. As an example, we had a partnership with Huawei at the time. ***We know that car networking is a thing that electric cars will do now, including cars, automatic flameout, fire network control start and so on, including now automatic driving, although not fully automatic driving, but semi-automatic driving has begun to slowly spread in all can not say all vehicles in most of the advanced vehicles, including Mercedes-Benz BMW and so on.*** So at that time we went to do this as a solution to the traditional service providers, it is very high cost, it may need to go in all the IDC nodes to lay a box, even if you are a cloud service provider, I also have to go to your cloud side to do a cooperation, on the whole thing will be very complicated around.	IN
31	CL	In the organisation. Is there anything that your experience has involved that makes a difference to the impact he has had compared to the traditional ones?	

32	R1	I give an example, because I myself, in addition to being a product designer, I am also a manager, because I am actually the company's Cto, that is, the R & D team and the product team are in me, and then there will be a problem, even when we go to use zero trust within the company, still inevitably a problem. Because your head of security or your head of operations and maintenance, who may not actually understand your company's organisational structure, may still do some very in our view stupid rules in the process. This kind of problem although I as a person in charge, I still even if he is the person in charge below me, ***I will also have some arguments with him, there is no way out, but because there is zero trust he is all general, especially when our data is not perfect now, of course we actually think it is good that when these stupid rules come up, we can improve these stupid rules on our template, so that when there is a smarter not smart enough security head inside our other customers to do This is what we call the security brain.*** ***We actually know that the first stage of zero trust is triangular architecture, the second stage is intelligent control, we can have enough data to solve, but in the early stage you in the data accumulation stage, including we know ait also have stup, it is not smart enough, so we are also trying to include trying to do our own big model, can we see better in the security level to say, let it become more intelligent. Make it smarter. Yes, that's one of them.*** ***Another one that might have a bigger impact is that it's very painful to share the old with the new and we've had quite a few customers, their employees, complain to us that they have to use two security products at the same time, one is dumb enough, surprisingly there's another one, although that one might not affect him as much, but the process is in the middle.***	ZTMD,TZTM,MLSA, IN, CO, UEWD
33	CL	What are some of the practices or adjustments that you have found that balance security and organisational impact?	

34	R1	I'll give you an example of a new solution that we've actually tried, called a sandbox plus what we call a domain. Essentially, when I go to a company that already has a set of security measures in place and I want to replace them with their old security measures, there is no way to do that directly. This is not only because of the cost, but also because of the company's business organisation or internal politics, whatever the reason, and in the process it has decided to replace them all, but it may take two or three years to do so. At this time we will have a solution, that is, I will make a sandbox for it on top of my own computer, the sandbox is a system isolated from its original system, inside the sandbox is possible to access our is sdp, but his computer itself is not able to access the sdp, the user will actually be more comfortable, because as long as I enter the sandbox, I will enter the company's environment, but it will be more restricted. That is to say there are many, many are not quite the same as your personal computer inside the sandbox, a process where you can't have absolute control over your security controls. This also increases the learning costs for some users to a certain extent. And then it also does increase the load on your own computer. This is not only because of the cost, but also because of the organizationorganisation of the company's business or internal political issues, whatever the reason, in the process it has decided to replace all of them, but it may take two or three years to replace them. ***This time we will have a solution, is that I in his own computer above to it to do a sandbox, sandbox is and its original system isolated a system, in the sandbox inside is access to our is sdp, but his computer itself is not access to sdp, the user will actually be more comfortable, comfortable is that he did not, in fact, this is my personal computer, I can still use the sandbox I can still use the sandbox to deploy into it, because as long as I enter the sandbox, I will enter the company environment, but it will have more restrictions, which means that there is a lot of a lot of is in the sandbox and your personal***	TZTM, UEWD, CO

		computer is not quite the same, this process, your security control will not be able to do absolute control. It also increases the learning costs for certain users to a certain extent. And then there is a real increase in the load on your own computer as well.	
35	CL	In your organisation, especially in the environment you use, what improvements or adjustments do you think would make your experience or the experience of your employees better?	
36	R1	I actually think there will be more adjustments in the data. ***When it becomes more intelligent, that is, when its data volume is large enough to our brain, it can we will do some automatic matching rules, including some automatic adaptation, and then based on the enterprise to us itself to say that the brain open permissions, for example, there are some employees have some special temporary circumstances, and there is no way in charge of the audit situation, then this situation, we We will not give him a temporary permission adjustment, the degree of security, we can not more intelligent determination, it is not a safe state, because we in the early days, probably in the year before last, there will often be a problem, the employee may he did do something, slightly on a little sensitive behavior, but we will think that this thing is not safe, instantly kicked down his account to the .***	MLSA, UEWD
37	CL	Our next question, there aren't any new technological developments that you see at the moment either that could have a big impact on the future of this model of zero trust?Because I'm now getting feedback from you that it needs to possibly be combined with AI or big data a lot more organically in the future.	

38	R1	Yes, this one is also recognized as being the recognized go-to breakthrough point within our entire industry, in fact we do a lot of business that is not actually exactly. ***The goal is to target towards the interests of the business to do, Isenkrupp, there are some very large enterprises, I may not be too convenient to disclose the name, because these are authorized I can say some enterprises, and then in this process, we are actually more is also to accumulate, write, because when his number of employees is large enough, his data before instead will seem more valuable, and who can be inside this industry earlier to build up these AI models more mature? I think even if you rely on this model, it amounts to a rule setter inside this industry.***	MLSA, FDZT

Appendix 3 - Transcription - Participant 2

Num	Person	Question& Answer	Code
1	C L	Ok, let's get started. Can you please give us a brief background on you?	
2	R2	After I work in the Industrial and Commercial Bank of China now, my main job responsibility is in the branch of the Industrial and Commercial Bank of China, that is, the branch of external business. The main content of the work is marketing, mainly responsible for the customers of government agencies, as well as the marketing of some large and medium-sized public customers.	
3	C L	Ok, are you familiar with the framework that we're going to talk about today called the zero trust model.	
4	R2	In fact, the Zero trust model has always been used in banks. Whether it is the system used by our external members at the front desk, or the system used by our customer managers in marketing, including their login methods, as well as their handling of business.	
5	C L	What kind of understanding do you have about the traditional network security solution? If you don't understand the tradition?	
6	R2	Traditionally, in fact, at the beginning of our bank, in order to solve the security problems of these outlets, including because the security of bank funds is more important, ***it usually takes this kind of employee card, including the teller, who uses that kind of card and then swipes it to log in like the access card. Later, it was ready to gradually change to password login.Later, the staff at front desk are basically driven by fingerprints.***	TSS
7	C L	Ok, how do you understand how this Zero Trust model is implemented and deployed in your organization?	
8	R2	One line is the front desk teller I just mentioned, ***they are now using fingerprints to log in, and another line is the account manager, they do not have direct contact with the business, but they will have access to some information about the customer, such as how much money the customer has, after the customer's money transactions or whatever, they are still using this password method for the time being.***	CTSZTMA, AU, AC

		After that, in addition to these login measures, there are also some rules for sending out emails and so on, which I don't know specifically.	
9	C L	Ok, in your work experience, he has zero trust in the implementation. Compared with the traditional scheme, it will certainly face some challenges. What do you think is the main aspect of this challenge?	
10	R2	Certainly, I think it is mainly for us, for employee, ***it is mainly a matter of convenience.In the past, they could swipe their card and log in, or enter a password and log in, so that if they were not in, or if they were late or whatever, they could have someone else take their place. Or this business, which only he can handle, but now he can only use his own fingerprint, the convenience will definitely be affected.***	ZTMA, CTSZTMA, AU, CO
11	C L	do you have any relevant experience? How do you overcome such inconvenience or some inconvenient conditions in your organization?	
12	R2	To overcome this challenge, the current fingerprint login mode can only increase the number of authorized people. For example, in this business, I may give them three or four people to increase authorization at the same time. In this case, he will at least not say that because this person is not here, I can't do this business.	AU
13	C L	In your opinion, what kind of impact does this Zero Trust model have on the overall security situation of your organization?	
14	R2	If you start with the employees***, you can feel that this must be the security of our entire system, or the protection of our customers' capital, it must improve security, there is no doubt about that.***	ESRM
15	C L	In the process of implementing this, have you noticed any unexpected advantages or disadvantages?	
16	R2	***Because of his authentication, I am always asked to enter my password. When I go into a system I will enter my password again. If I leave the computer for about 20 minutes, I also have to continue entering my password as well as various verifications when I return.***	ZTMD,CO, UEWD, AU
17	C L	In fact, its validation may still be a bit much for the staff.	

18	R2	Yes. The frequency of its verification is too high, and I think it is a little too high for me.	
19	C L	have you noticed an improvement in the security measures of this mode	
20	R2	***There should be a potential risk, because in the past, we used that kind of access card, and others can also use my Card to operate, so in case something happens, right? To make it clear, at least the responsibility can be sorted out now.***	ESRM
21	C L	Have you noticed the related complexity and resource requirements? What are the specific areas of growth?	
22	R2	Apart from this complexity, in fact, as you said earlier, the level of delegation has increased, because I may not mean that one person cannot operate, ***I may need to give him what was one person to operate, and now it is divided into three people to operate, which I think is actually a waste of resources. In a way, it's an increase in complexity.***	AU,CO
23	C L	In your work experience, what changes or impacts does he have on the overall user experience and process?	
24	R2	***The process is like the gradual increase of authorization levels I just mentioned, and this will certainly lead to slower efficiency. Originally, one or two people finished the work, and one person handled the review. Now it may be necessary to submit the review and approval layer by layer, and then handle the review and approval.*** ***Finally, there may be several levels of approval.This is the impact of the process, the user experience, our bank is definitely the window of external business, customer waiting time, whether personal business or public business, its waiting time will be very long, the user experience is relatively bad***.	CO, UEWD
25	C L	Ok, in fact, you can see from your description that there are still many such changes. Have you noticed the behavior and working habits of employees? With the improvement of safety measures, for example, has there been any obvious change.	
26	R2	***There must be a big change in work habits, because in the past, people may not pay much attention to some aspects of security at work. You just use each other's cards, use each other's login cards and operating systems, and you use yours more frequently, but now you have changed your***	UEWD

		fingerprints.Everyone may have an improvement in safety awareness.	
27	C L	we all know that this mode actually has many features, such as authentication access control, segmentation and security automation, and then what functions are mainly used in your organization, and what aspects of your organization are specifically affected by these functions?	
28	R2	***Authentication is the change from cards to passwords to fingerprints as I mentioned earlier. Access control may not be particularly obvious at my workplace, but at my workplace, for example, they have established that you are a personal act. You can only deal with some personal systems and personal business. If it is determined that you are a corporate act, he may only be able to deal with corporate business. It will have such controls that it will not allow you to access personal business systems.*** Here's a very obvious example. When it comes to military business, it is very obvious that if military information is involved, it is more sensitive. It is handled by a separate computer and requires separate permissions.	AU, AC
29	C L	Ok, in your work experience, have you found that the deployment of this new framework has had a greater impact on Organization?	
30	R2	I don't think I need to say more about the negative aspects. ***The convenience mentioned before, as well as the experience of employees,*** including the experience of customers, are negative aspects. ***On the one hand, I think it's definitely because your overall safety is improving, so relatively speaking, for banks, their capital risk and credit risk is decreasing, and this kind of thing should be a positive impact for banks as a whole.***	CO, ESRM
31	C L	You think it's still a balanced process, and the overall security has been improved, which is certainly good for the overall system.But now, when it falls to the implementation staff, there is still an increase in complexity. Then in your workplace, have you found any cases or practices with better balance.	
32	R2	Relatively speaking, for example, in our account manager system, after it uses password authentication, permissions may not be adjusted because of the account manager, it is not particularly complex business, for some uncomplicated business, it may be relatively relaxed."	CO

		This type of secure authentication would be slightly relaxed." For some data that is not so sensitive, it actually has the same permissions as the original method, and then for some sensitive data it may be improved in certain aspects of authentication or access control.	
33	C L	In your experience, what do you think will be the next step of improvement or adjustment?	
34	R2	***I think for people who don't know much about this, I hope that it will be more automatically identified by a system, rather than by adding authorization links, including this way to the system.*** For example, I'm talking nonsense now. ***For example, if this kind of AI is added now, will it make these systems more intelligent?I think it is mainly in this respect.***	MLSA
35	C L	Have you noticed that this new technology or development, as you just mentioned some AI or big data, will have a significant impact on the future of this security framework?	
36	R2	***I feel that the development of this technology is a double-edged sword. On the one hand, it may make our security system more intelligent, and then make it more convenient for our employees at the bottom, but on the other hand, it will also deepen this potential threat, such as the threat of system intrusion?***	FDZT
37	C L	let's talk about the parallelism of the two systems again. Especially in your work experience, have you found that many employees are more resistant to these two systems? Have you found that some employees do not accept the parallelism of the two security frameworks.	
38	R2	***Of course, employees feel that the more convenient the better, the smoother the work, but for security reasons, it is a kind of rules and regulations for employees to increase the access restrictions of these authorizations, and it will not be said that they are particularly unwilling, but they will feel that there will be complaints.***	UEWD
39	C L	do you think this kind of training on the system security framework will greatly improve employees' acceptance and understanding of the security of such a system.	
40	R2	***I think the staff will generally improve their safety awareness.And as I said just now, I think it's safer for them to say something about operating habits and working habits, right? Maybe there will be more improvements in the system.***	ED

41	C L	Ok, even if your company's security awareness is already very good, and it's already very high, and then you still face a lot of complex verification and complex permission management, which still exists, right?	
42	R2	Yes, and then y***ou may still want to make it more intelligent, or to reduce the interference of some employees in their work processes and reduce their impact on the business.***	UEWD, MLSA
43	C L	Ok, in fact, inside the system, security is still the priority, convenience is the second priority, and the impact is still the second priority. Yes. Have you noticed that there are some trends that are actually designed to slow down its impact?	
44	R2	I think there should be a trend. However, it may not be obvious when it is reflected to employees.Yes, in fact, it is not very obvious, and in recent years, because of security problems, there may be more external risk events, so the security is actually increased.	
45	C L	It is still a growing trend?	
46	R2	Yes, maybe the focus now is not on the control of our login access, but on some of our information leaks, including some on our mobile phones, because now mobile is also very common, and some of the risks of information leaks on mobile phones are controlled, for example, our work software does not allow screenshots and so on. Compared with login access, it is not bad. There has been no change in recent years	

Appendix 4 - Transcription - Participant 3

Num		Question& Answer	Code
1	C L	Let's start with the first question and give you a brief introduction of your background.	
2	R3	I am now in the financial industry, and then more specifically belong to the banking industry.At present, in the technology department of the bank, and then is mainly responsible for the research and development of software.	
3	C L	Do you know anything about the zero trust model before?	
4	R3	I have learned about it before, and now I also pay attention to my own industry. ***At present, the banking industry also attaches great importance to the field of network security and information security.***	TSS
5	C L	What is your understanding of the traditional network security solution?	
6	R3	***The traditional security scheme is more likely to be a mode of network intrusion prevention, which may be more inclined to a passive upgrade and passive learning mechanism. In the process of continuous attack and defense, we should improve our network protection ability.*** As the saying goes, the road is one foot higher, the devil is ten feet higher, the means of network attack are increasingly abundant, and then the measures of network protection are increasingly sound, so the traditional solution is more likely to take a role of self-entertainment to do this work.	TSS
7	C L	how do you make the transition from the traditional scheme to the Zero Trust model?	

8	R3	***I think it can only be related to the whole background environment, one is that the banking industry is also becoming the focus of many attacks, and with the popularity of mobile intelligence of Internet technology, the access of banking applications exposed to the Internet has become more and more, including applications of Wechat, and some possible open APIs.*** ***As a direct entrance to the Internet 3.0, it actually increases the possibility of being attacked by the Internet. The other is the particularity of this industry, because after all, the banking industry involves all ordinary customers, whether private or public customers personal privacy information, as well as some financial information are very sensitive. From the perspective of data security, in fact, the consequences of this kind of information security, including the leakage of personal information, are greater than those of other industries.***Therefore, based on the above aspects, the urgency of this transformation may still be needed.	TZTM
9	C L	How does this Zero trust model work in your organization and how does it work in your organization?	
10	R3	In fact, now is also a stage of exploration. In fact, according to the current development trend of the banking industry, including mobile, digital and intelligent, we may summarize some security aspects facing challenges, and then make a division. ***It can be roughly divided into the following aspects. One is physical security, which mainly includes computer facilities and venues, as well as network security, access control, intrusion prevention, and so on. There is also the security operating system at the system level, as well as the security at the application level. Then you may have business insecurity and some privacy protection.Maybe we have done some different security measures from these levels, which is probably such an unfolding model.***	ZTMA, ESRM
11	C L	What are the challenges it faces compared to traditional solutions of this kind?	

12	R3	In fact, whether it is to study or demonstrate safety separately, the scope may be wider now than in the past. ***The whole scope involved is from what I just said, because it involves more levels, because the division is more detailed, so the challenge it brings is that it may involve a wider range. Another is that the time of safety intervention will be earlier, because from the perspective of research and development, the whole safety design may run through the whole project cycle, which will lead to more personnel, equipment and manpower investment in the whole project than before.*** These may be some challenges.	ESRM, CO
13	C L	That is, how do you face such challenges and difficulties in your work?	
14	R3	One is to institutionalize and standardize this safety-related theory and form a clear regulatory system to guide it.On the other hand, it has increased the input of a person, because now in addition to this kind of ordinary R & D personnel and testing personnel, ***there may be a new kind of person, called this kind of security designer or security measures personnel, who has increased the input of this part.***	CO
15	C L	what is the impact of its model on the organizational structure, system structure and its overall security situation?	
16	R3	***Security situation, I think on the one hand, it provides a good development idea for the future security design or security precautions, and on the other hand, in this more complex network environment, it may be more confident about the development or promotion of this Internet application, which may be because of all this***. In fact, it is all for better business development, so the whole business security situation actually plays a supporting role in the development of the whole business.	ESRM, CO
17	C L	your work experience, how this model helps you, how it detects or prevents safety.	

18	R3	***In terms of detection or prevention, at this stage of prevention, it can be said that in the process of doing all the scientific and technological research and development, it has specially added such a process of safety design. In fact, it is aimed at the application security level, to do a survey of some hidden dangers related to safety, and to do a preventive design in advance.*** This may have done some work at the level of prevention. As for the detection, there may be two parts, one is the security test, and the other is the simulated attack and defense drill. For simulated attacks, some functions that have been launched may be verified or detected one by one by means of simulated attacks, and then in order to verify whether the current security design is reasonable and whether it can effectively resist these external attacks.	ESRM
19	C L	Is there any impact on their users, their usage habits and their development process?	
20	R3	This is definitely there, to give a simple example, in fact, for the risk of an outsourced worker, because no matter which industry, there may be some outsourced worker involved, in order to improve the efficiency of development, so our management of outsourced workers is relatively strict. ***All the office computers of the outsourcing personnel are actually used to access the office data in the form of a bastion machine. The bastion machine is used to access the exclusive virtual office desktop of the outsourcing personnel to carry out the corresponding development and office work.this is to achieve the protection of office data, and then there is an impact on employee behavior in the big environment.*** ***In fact, for employee behavior, there is a security for the use of office computers, including Keys, as well as the storage of some confidential documents. After scanning confidential documents, they are scanned regularly, and then they are deleted and recorded.*** There are also the use of some secure USB disks and so on, which may be derived from this model and have such an impact on employee behavior.	CO, UEWD
21	C L	Are there any changes in their behavior?	

22	R3	In fact, this is where data protection and ease of use are two opposite directions. If you strengthen this security, it will inevitably lead to inconvenience in use, for example if you do some tests that require peripherals, such as when you need to connect an IC card reader for ID cards, or when I connect a printer via this virtual desktop. ***There may be some unpredictable problems that cause the whole technical testing process to fail. At this time, he may need to resort to the industry's specialized testers for office equipment to complete their corresponding tests.*** This possible inconvenience to your work is also an impact.	CO, UEWD
23	C L	we all know that its Zero Trust model has many features, such as authentication permission control, access control, and micro-block automation. Can you give us some examples of how these functions are deployed in your organization and how they affect your organization.	
24	R3	In terms of impact, I think from the perspective of employees within the enterprise, one is the establishment of this system, the establishment of security-related systems, and some information, including the promulgation of some laws at the national level, including data protection laws. ***Personal information, personal privacy information protection law and so on actually require enterprises to do this function, and then there are more security considerations from the application security, including some security design, security testing and so on.*** ***Another simple example is the use of identification means, in order to identify the customer is not his own such a function, in fact, now through this so-called zero trust model, in fact, is also established some mechanisms, including may do artificial intelligence before the line, now with this artificial intelligence, may be through biometric means to do identity verification, in fact, these are some and the customer for business may not be very relevant, but are as a non-business operation of a necessary means, I think this is the impact of this part of the customer.***	ESRM, MLSA
25	C L	Can you give me an example of the functions that have the greatest impact on your organisation?	

26	R3	I think it may still be this kind of authentication and identification. In fact, especially the application of artificial intelligence biometrics technology, it actually has a greater impact on productivity, because the banking industry actually depends on the difference between deposits and loans. In fact, if you want to make more profits, banks should try their best to make loans. ***You also know that in China, some of the hottest loans are credit loans, and every bank is now trying to acquire this customer, and the one that can really take the lead actually depends mostly on the response rate of its system, especially in the approval of loans, because if you don't have this set of artificial intelligence algorithm or biometric technology to support, it may depend on the previous manual But now, through this biometric technology, or the intervention of this access algorithm, from this identity authentication to the access control, the synchronization can achieve this second approval and second release by relying on this system capability.*** One is to enhance the experience of two customers, and the other is to be able to quickly issue their own loans, so as to enhance the profitability of enterprises. So I think this has a great impact on the overall productivity.	MLSA, AU
27	C L	So in your work experience, have you been exposed to other security measures?	
28	R3	I think I have come into contact with some of these before. In fact, I think the authentication is actually a more interesting direction, that is, as the means of attack become more and more advanced, some people may be able to simulate customers. ***He may not be the customer himself, he just may pass on the information through some other such fake pictures or motion pictures, in fact, this stage for this kind of live detection is actually a more important link, is to ensure that the customer himself in front of my mobile phone is a live person.Yes, so this piece of verification technology I think is also a very important aspect of this Zero Trust model.***	AU
29	C L	In your work experience, have you found any good practical examples of the impact of balancing safety and balance on the organization.	

30	R3	Take the example of verification, which you will often use when using a banking app. ***In fact, you can find that there are many details in the in authentication, one is the action of your in authentication, you should find that he will sometimes ask you to shake your head, or sometimes ask you to blink your eyes, and open your mouth, through this action to verify your identity, this point is actually in the balance of security and practice, the business is also made a proof. Of course you have like three actions, and then for this kind of security designer, the more actions you design, the more you can guarantee the accuracy of your live detection results, but the impact of your more actions is that the customer experience is very poor.*** So by balancing the accuracy of the security and the customer experience, the business set out to choose two actions that were easier to complete as the final collection rules. So I think this is an example of balancing security and best practice, in terms of the number and choice of security actions.	AU, CO
31	C L	What further adjustments or improvements do you think there are in the Zero Trust model?	
32	R3	In fact, I think that when it comes to adjustment and improvement, ***I think it is actually the rational use of some cutting-edge technology, including this kind of artificial intelligence machine learning, I think this ability is still lacking, including in the use of some good artificial intelligence algorithms, its algorithm exercise and enhance, I think it still does not do enough.*** Because this is in the zero trust model there is a concept called trust engine. In fact, I just mentioned that it should be combined with artificial intelligence AI, because the intelligent trust engine is also a very important part of it. You think that the trust engine needs to be more advanced and more flexible, and then it needs to learn more about the behaviour of these users and the behaviour of the employees.	MLSA, FDZT
33	C L	I actually have a question, because you actually just mentioned that a lot of what is involved is such authentication of users on the mobile side, identity verification, which is actually part of zero trust?	

34	R3	Yes, because it is not protected either, and it can also be used as an intruder if it is. The trustworthiness of the device is also an issue, which means that when the device accesses the app, it is able to collect information about the device it is accessing, and in fact the trustworthiness of the device is assessed by collecting information about the IPv4 or IPv6 address of the network it is connected to, and the range of the base station. For example, if the person is usually logged in Beijing, but suddenly the device appears in Xinjiang, this may be a danger signal for the system.	
35	C L	if your system receives a danger signal, will it have further warning in security measures?	
36	R3	On the one hand, it provides SMS alerts to customers that you have logged in in a very useful area, please pay attention to this, and at the same time, this information will be registered in our own so-called intrusion prevention logs, and then the business staff will receive this alert information to do a manual intervention.	
37	C L	So we're done for the day, and this thanks you for joining us	

Appendix 5 - Transcription - Participant 4

Num	People	Question & Answer	Code
1	U	Let's start this interview and my name is Umar, and I'm studying information systems at Lund University.	
2	C L	My name is Can lu. I'm working with Umar on our thesis about Zero trust. So happy you can come to join us	
3	U	Could you tell us about your background?	
4	R4	Before this role at Combitech! I'm a Phd in automatic control. A longtime ago and I have also been involved in startups. That's and then recently I've been acting in different kinds of software development products such as simulation. My background is in modeling and simulation and software development. Modeling people present modeling language at the time was involved in. And it's very famous and learned it, actually. And then said 2012, I was part of Combitech in particular. Now I have the role since the another person left of due to being in another city, it was 5 years back.	
5	U	Are you familiar with Zero trust and what is your understanding about it?	
6	R4	My understanding about the idea is to not to build a local area network, go in behind the fire walls, but instead assume that only on ***it should be connected and secured constantly and do that by using advanced encryption and identity access management.***I usually explain it like this for all. It's like to have the ***units always connected via a vpn connection***. If we now take the the classical computer networking problem in the company.	TSS, CTSZTMA
7	U	What is your understanding of traditional cyber security solutions?	

8	R4	My understanding from the background that I have experienced is that security is typically something that is needed and for more cloud based services, when you do, the business model is to get more like software as a service (SaaS) or platform as a service (PaaS) kind of then. So it just becomes the traditional way to run your service in the house to to have all the different operations. And in house, it's quite expensive and it's very hard, but you have control over it. But you might also think that you get some you have control, but you have also the sole responsibility to actually keep the security completely on your own. And the question is, can you really do that? Do you have and can you achieve that amount of security that the cloud providers can provide instead for? Or will it be actually a higher risk being. But the fact that you need to take care of the security completely on your own, you step into a big debate with a different, so it's a debate with a lot of different fellows. It's a political discussion sometimes even what is the best? So definitely, that's my understanding.	
9	U	What led your organization to transition from traditional solutions to Zero Trust Model?	
10	R4	We didn't care really about the Zero trust itself. What we cared about is that we needed to be able to have more sort of modern set up for our employees since they are consultants. And they need to be able to have computers that can and be used in consultant assignments, being used for software development, perhaps being engaged in different customers, using the same computer and so on so that it wasn't really possible with them. ***The traditional that we had before, because the traditional idea was not suited for consent of business. It was more suited for more classical internal product development where you don't need to interact this much with external parties.*** So when you are a consultant company, you need to be able to collaborate. You need to have things like microsoft teams, you need to. So it was a need for our business to have more modern tools and features for collaboration and for development.	TSS, CTSZTMA
11	U	That's great to hear that. So how was that Zero trust model implemented in Organizations?	

12	R4	In our session, we did green field strategy. Could that be? Is that established term? I don't know. We were forced to not transfer anything from the old. So we were forced to build something completely new, completely empty at start, and then making our employees being the one that sort of brought. There's stuff manually from the all the it department to the new one that so it was a very poor strategy, but we were forced to do it. ***Normally, you would that was for security aspects, because it's it was decided that we couldn't, it was not possible to find any automatic ways of transferring systems and information, because you need to have someone being for everything you need to make an assessment, what information is possible to bring and what should stay behind the fireworks and so on.*** So a greenfield implementation, and that is also the situation that we actually I use the old pill that is very important to keep that because we need to we built a completely new house, but we haven't moved into the new house completely. We still need to to sleep some days in the old house. So we are a lot of moving back and forth right now.	CTSZTMA
13	U	What challenges did you face during the implementation process? And how do they compare to the challenges faced with traditional solutions?	
14	R4	There were no specific challenges, just from the from a different philosophers. It's the challenges is more into what I say. ***The organization and the processes and the people that are governing the old stuff and the competence and processes and covering that in the people that should handle their new stuff in.*** ***So the challenge was people and not technology, I would say.***	ZTMD
15	U	And how did your organization overcome these challenges?	
16	R4	And it's a classical recipes when it comes to leading change transitions. T***here is in, I think this matter, this case, it's it is also a matter of education, a matter of explaining that the zero trust stuff is safe and is accepted. The people are extremely skeptic when they are.*** But when we're working in related to defense aspects as well, they typically, they don't understand how it can be safer in the cloud, which is a contradiction. Right?	ED

17	U	In your opinion, what impact does the uterus model have on an organization? Overall security posture?	
18	R4	The impact is that the first of all, I would say that you can create the security perimeter that involves them complete life of a consultant and enables the mobile phones and everything. ***So you can have more footprints and more sensors to actually detect. Not only what is happening inside behind the fire walls, but in the hole that the whole it lifespan that what is one thing? The other thing that I would mention is that security policies is and very dependent on the iti don't know, the identity management. And you need to have good solutions there. The third thing is the information security classification, which is that you need to be able to, it must be very easy to do the right thing. If you're a user. Not, everyone can be a next security experts. So it must have extremely good usability. And it must be very easy to do the right thing. And that means also, it must be easy to also set the appropriate and security classification on documents and all kinds of information, emails, because otherwise, you cannot really take the right measures on how to control the information.*** The fact is that from the previous traditional idea that you don't have as many information classification structures that means it's very basic in the new world, you can do a lot more, but that means that you also need to educate more, and they need to be explained. You need to have more. People are engaged in defining and working with information structure, because then you can ideally, you should be able to separate very, very efficiently, what is actually secret and what is not so secret. And you can should be easy to distinguish between these things. I think in the traditional idea, then everything is blended and mixed, and you cannot really distinguish between different classification. And that is a risk. I haven't seen the full implementation of these things. I don't know. Even though Microsoft tries to do a good job and different services from that, I still would like to see a good and automatic and smart and easy way to use them. How can I make a separate information in all these different aspects, in an easy way? That is a challenge, but also hope, I think absolutely.	ESRM, CO
19	U	Were there any unexpected benefits or drawbacks to the zero trust model in terms of your organization performance?	

20	R4	Not really, I think it's not it or again, it doesn't have a specific relation to the Zero trust it. It's more about what is good and what is bad with Microsoft and their stuff. And because you typically work very intimate with the cloud provider for these things. And Microsoft is good in certain things and perhaps not so good in other things. But the Zero trust itself is, for instance, one thing that we happen to be there. The idea is that you should have local breakouts when it comes to getting access to the internet and all different places and that we don't tell. We are using it. An internet provider from the classical, traditional way. ***And that is so you can't really, it's sometimes we are forced to do things not in the most optimal way that create some gaps and some less performance. It creates the possibility that perhaps the team doesn't work and when we have meetings like this and so on.*** But I can stop there. So the next question.	ZTMA
21	U	Can you describe any improvements in security measures and a reduction of potential risk? Your organization experienced implementing Zero trust models?	
22	R4	I can't really comment on that. Surely, what I know, though, is that and again, it's you get a richer set of sensors to detect things. You get quicker updates on everything from spam victors to actually being able to get insights whether a software is good or bad, because your microsoft provides data with all the different applications and whether it has been proven to be useful for someone else, probably in other countries. So there is a lot for everything you do. There is a lot of experience already generated. You are not alone in figuring out if something is good or bad in the same way as the other way.	
23	U	So your cloud and software provider is Microsoft? Or are they also your partner?	
24	R5	Microsoft is just one cloud provider we are using for IAM and secure collaboration. On our own we are using Microsoft, but we also have other important cloud and software providers when it comes to development and together they build a secure Zero Trust Model, but yes we do collaborate and we have other solution providers. But right now we're talking about our own environment inside the organisation and that is Microsoft 365 solution.	

25	U	I think you have already answered some of it, but how has the zero trust model helped your organization detect and prevent security threats?	
26	R5	I cannot directly comment on that at the moment. Its security threats is also another thing that I cannot comment on, ***but the important takeaway is that we get better possibilities to actually act to be more efficient in our business and with that we can do multiple things at the same time such as having stronger and more flexible security features and mechanisms.*** So we know what we are doing, we have the same level of security, but we also have the flexibility to actually help our consultants to do a good job with the customers.	ESRM, PIRBC
27	U	How has your organization managed a potential increase in complexity and resource requirement associated with implementing the zero trust model?	
28	R5	We cannot really answer that, either because the old operation was taken care of by our other company. This new environment, we are doing ourselves when it comes to operation and maintenance and so on. Because that is also a way to do it. And for us , the new environment is sort of cheaper than the old one. So I don't really agree that ***there are increasing resources, but it can be very complex. It requires a lot more knowledge. We need to have expertise in a different way. Yes.***	CO, ED
29	U	You have mentioned a bit about the user experience and workflow disruption. So in that, I have a question regarding whether the zero trust model has many advantages. However, you might notice that it also comes with an increased complexity at your organizations. How has this affected the overall user experience and processes in your organizations?	
30	R5	You need to focus on being very informative, being very having a lot of guides, trainings, and people, but we can take how to learn to use markets of teams when it comes to collaboration that that is a very complicated. ***People still want to convince people to stop using Outlook, but instead trying to move to a more collaborative environment on only that little simple thing is very hard.*** ***And it takes time. But you need to sort of market and educate and give it time. And eventually, people will learn and inspire themselves in different ways.***	ED

31	U	Did you noticed any field increased complexity in your organization after implementing Zero trust like the employees giving their views on how you feel about it.	
32	R5	***We experience that it was mainly the major complexity for us is the mixture that we have both the old one and the new one. We are living in two houses. And so that creates a lot of complexity for people that are starting to work a compact. They don't understand why.*** All right.	CO, UEWD
33	U	Could you mention and go through some of the processes which have changed your rings? And after the implementation of Zero trust.	
34	R5	I know I cannot really, one thing is we can know how to and the management of our computers are completely changed, because before there, each computer needs to have an installation performed on the hard drive by a certain apartment. ***You have to send the computer back and forth in the country. And now everything is downloaded dramatically and you get the computer ready to go in a much quicker way. So that has been a great advantage.***	ZTMA
35	U	Have you noticed any changes in employee's behavior or work habits due to the implementation of the zero trust model?	
36	R5	***When it comes to collaboration, it will last in different communities, tools and things like being able to come in contact with your colleagues in a much easier way than before***. That's clear to see.	PIRBC
37	U	How do you feel the features of the Zero Trust model, for example, authentication, access control, Micro segmentation, security, automation, affect your organizations.	
38	R5	That's the need to understand it and to have it. ***The authentication process is done with multifactor authentication all the time. So that 's a convenient solution. So people are happy about it.***	AU
39	U	which features have had the greatest impact on productivity. You can mention either positively or negatively.	

40	R5	Positive is the use of Microsoft teams when it comes to collaboration, not just the meeting feature, and it's the collaboration part of it. ***The negative side is that we are living in two. I did an environment at the same time. There's the downside of it, and that we are not for different reasons, we are not able to completely move into the zero trust.***	CO
41	U	What best practices have you identified? Identified for balancing security and impact within Zero trust model.	
42	R5	I just want an example. We are able now to have a security philosophy when it comes to our computers. So we can have a secure environment on the computer. And they are managed and still be able to be useful for software developers. It wasn't possible before. ***That means that there has been also a change in the way you're thinking, also for software developers, software developers tended to to really knock it on the streets claiming that they can only use completely unmanaged computers where they are of their local ADMIN in every aspect. And that has changed.*** ***So also, how software developers become more concerned about security. Thanks to the fact that now it's possible to actually give them things that actually work also for their daily business.***	ERSM, ED
43	U	What further improvements or adjustments do you foresee for the Zero Trust Model in your organization?	
44	R5	Cannot read a comment on that. Let's move to the next one.	
45	U	Are there new developments or technologies that you believe will have a significant impact on the future of the zero trust model? Answer the traditional solutions.	
46	R5	***Micro-segmentation, and also a hybrid, and that you can subdivide things that are of high importance.***	FDZT

Appendix 6 - Transcription - Participant 5

Num	Person	Question & Answer	Code
1	Umar	Can you tell us about your background?	
3	R5	I have a bachelors in computer science from UTD university of texas and dallas. And then after that, I worked 1 year in a software developer role at jp morgan.Now i'm about to have another job at lockheed martin as a cyber systems security specialist.	
4	Umar	Are you familiar with the zero trust models?	
5	R5	Yes, through work and being in jp morgan. There was the zero trust of whenever you were given access to anything, it basically had nothing, no access. We requested it. So their whole enterprise is based around zero trust.	
6	Umar	What is your understanding of traditional cybersecurity solutions?	
7	R5	I don't know what the traditional one is, because that's the only one I have experienced is the Zero Trust not the traditional ones in an organizational context	
8	Umar	What led your organization to transition from traditional solutions to the Zero Trust Model?	
9	R5	***As a software developer at JP Morgan, the transition to the Zero Trust Model was driven by a combination of factors. The foremost of these was the escalating number of security breaches and vulnerabilities that traditional security models failed to address adequately. I was told by one of our managers that the old systems operated on a verify approach, which, while functional, left too much room for potential misuse and misconfiguration. With the growing sophistication of cyber threats and the increasing complexity of the IT environment, we found the traditional 'trust but verify' security model inadequate.*** ***The Zero Trust Model, on the other hand, assumes no implicit trust. Every request is thoroughly validated, irrespective of its origin. This was particularly appealing to us because it significantly reduced the potential for unauthorized access and data breaches.***	ZTMA, CTSZTMA, ERSM

		Moreover, this model provided us a way to manage access more granularly. It allowed us to ensure that each individual only had access to the resources that were necessary for their job, minimizing the risk of misuse and unnecessary accessing information which you are not allowed to see.	
10	Umar	How was the zero trust model implemented in your organization ?	
11	R5	Implementing the Zero Trust Model at JP Morgan was a multi-step process that required significant changes to our existing infrastructure and processes. Here's a broad overview of how we approached it: First, we had to identify sensitive data and systems within our network and define micro-perimeters around them. This step is crucial in the Zero Trust Model, as it helps reduce the attack surface by segmenting the network into smaller, more manageable parts. ***Access Control Management: We shifted from a traditional access control system to a more granular, role-based access control (RBAC) system. In this system, every access request must be approved based on the confidentiality and sensitivity of the data or system in question. We used an upgraded ticket system for this purpose. If an employee needed access to a certain resource, they would have to submit a ticket. The ticket would then be reviewed by the relevant authorities (like the team lead or project manager), who would approve or reject the request based on the individual's role and the sensitivity of the data.*** ***Secure Access for BYOD: We also had a Bring Your Own Device (BYOD) policy at JP Morgan. To ensure secure access for these devices, we required each user to register their device's MAC address with our network. In addition, each user had to log in using their unique username and password.*** ***Multi-Factor Authentication (MFA): To further secure access, we implemented multi-factor authentication across our systems. This meant that a user's identity had to be verified through multiple means before they could gain access to our systems.*** ***Continuous Monitoring and Analytics: Finally, we deployed advanced analytics and monitoring solutions to continuously***	ERSM, AC, AU, ED

		track and analyze network traffic. This allowed us to quickly detect and respond to any abnormal activities or potential threats. ***Education and Training: Alongside these technical measures, we also invested heavily in training our staff on the principles of Zero Trust and how to operate under this new model. This helped foster a more security-conscious culture within the organization and ensured that everyone understood their role in maintaining our network's security.*** ***This is a simplified overview, and the actual implementation process was much more complex and involved. However, despite the challenges, the transition to the Zero Trust Model has significantly enhanced our security posture and reduced the risk of data breaches.***	
12	Umar	You mentioned about bring your own device at JP-Morgan and how does that impact the organization	

13	R5	The Bring Your Own Device (BYOD) policy is indeed a significant aspect of our network architecture at JP Morgan. While it offers numerous benefits in terms of flexibility and convenience, it also poses certain risks, as you rightly pointed out. To manage these risks, we have a stringent set of security measures in place. Here's how we address some of the concerns you raised: ***Device Verification and Security Scans: Before a device is allowed to connect to our network, it undergoes a full security scan. This helps us ensure that the device is free from any known vulnerabilities or malware. Devices with outdated security patches or any signs of being compromised (like jailbroken phones) are not permitted access.*** ***Network Segmentation: Devices connecting through the BYOD policy are placed on a separate network segment with limited access. This means that even if a device is compromised, the potential damage can be contained within that segment.*** Intrusion Detection Systems (IDS): We have robust IDS systems in place that continuously monitor network traffic. These systems can detect unusual activities or patterns that may indicate a cyber threat, allowing us to respond swiftly. ***Virtual Desktop Infrastructure (VDI): For certain sensitive tasks, employees are required to use a Virtual Desktop Infrastructure (VDI). This provides an additional layer of security by ensuring that sensitive data is processed in a controlled and secure environment***. VPN and Firewall Policies: We have strict policies around the use of VPNs. Certain VPN protocols are blocked outright, while others are allowed under specific circumstances. This is a delicate balance, as we also want to ensure that our employees can securely access our network from remote locations.	ERSM, ME, AU
14	Umar	What challenges did you face during the implementation process, and how do they compare to the challenges faced with traditional solutions?	

15	R5	I can't mention traditional solutions since it happened before I started! However Zero Trust, It is fully implemented, but I would say it's fully being upgraded constantly. It's not a one set done sort of thing they're constantly having more people hired on to knowledge of the software development and what is current team need such as to monitor the traffic and containerize networks to improve it. I would say when I came onboard, it was almost fully up to date. They're just trying to keep it up to date on the other security aspects of it. So more of I would say there, they've put in a great baseline, but new things are coming out and they're trying to stay up to date. ***Despite being constantly updated and upgraded. I would say the biggest problem was the automation that they had tried to build automation into the workflow. And that would fail a lot of the times. So you'd have to contact customer support.*** And i'm not a fan of that. That's one of the biggest frustrations I would say what I had with. It was their failure to automate correctly. Other than that, I much preferred, though it over having breakings, because those were much more critical in the workplace.	ERSM, UEWD, CO
16	Umar	How did your organization overcome these challenges?	
17	R5	***Streamlined Approval Process: We recognized early on that the new, granular access control system could potentially slow down operations if not managed efficiently. To mitigate this, we streamlined our approval process. Employees were encouraged to build relationships with their team leads and other individuals who could expedite their access requests. This not only helped to speed up the approval process but also ensured that the individuals responsible for granting access had a clear understanding of the employee's role and responsibilities.*** ***Establishing Points of Contact: To simplify the process and make it more user-friendly, we established designated points of contact within each team who were responsible for managing access requests. This helped to ensure that employees always knew who to go to when they needed access to a particular resource.***	PIRBC
18	Umar	In your opinion, what impact does the Zero Trust Model have on an organization's overall security posture?	

19	R5	In my view, adopting the Zero Trust Model can greatly enhance an organization's overall security posture. The first one is such as it reduces Trust Assumptions: Zero Trust is based on "never trust, always verify". This means we no longer make the assumption that everything inside our network can be trusted. Instead, every request is treated as a potential threat and must be verified before access is granted. This reduces the risk of insider threats and lateral movement within our network. With the Zero Trust Model, we gain more visibility into our network traffic and have granular control over who can access what and when. This increased visibility allows us to detect anomalies or suspicious activities more quickly and accurately, thereby improving our ability to respond to potential security incidents. ***The Zero Trust Model enforces the principle of least privilege, meaning each user is given the minimum level of access necessary to perform their job. This minimizes the potential damage in case of a security breach, as an attacker can only access the resources that the compromised account has permissions for. And the amount of security that had to be implemented after was lower, like you didn't have to constantly be monitoring everything. You just monitor the device whenever it is connected. I can't go into too much detail on the software, because I don't know, because I didn't actually build it, but I would say it was very beneficial in preventing easily, easily mistaken problems of people, not knowing consequences of some actions.***	ERSM
20	Umar	Were there any unexpected benefits or drawbacks to the Zero Trust Model in terms of your organization's performance?	
21	R5	Additionally, the continuous monitoring and verification practices under the Zero Trust Model have improved our ability to detect and respond to security threats. We're now able to identify suspicious activities more swiftly and act upon them, limiting the potential damage. ***Despite our efforts to automate many processes, the increased volume of access requests and the need for thorough verification can slow down response times***. We've observed that certain Service Level Agreements (SLAs) aren't being met as promptly as they should be, with processes sometimes taking a day or two longer than expected. This is something we're actively working on – we're investing in	CO

		additional training and resources to streamline our processes and improve our response times.	
22	Umar	Can you describe any improvements in security measures and the reduction of potential risks your organization has experienced since implementing the Zero Trust Model?	
23	R5	Only a year at JP-Morgan its really hard to say anything about that.	
24	Umar	How has the Zero Trust Model helped your organization detect and prevent security threats?	
25	R5	***They knew about a lot of threats. They had a lot of threats that were detected through the system.*** It's a bank. So like it was more of all the beginning level threats were already taken care of. It was APTS that were the real threats that required manual work. So the system worked almost flawlessly to the degree it needed to for beginner level.	ERSM
26	Umar	How has your organization managed the potential increase in complexity and resource requirements associated with implementing the Zero Trust Model?	
27	Jacob	I would day JP-Morgan invest heavily in Technology: We have invested in advanced technologies that enable the implementation of the Zero Trust Model. ***Since I'm working in the Software Development team, we used such Identity and Access Management (IAM) systems, micro-segmentation tools, and advanced threat detection and response solutions, help manage the increased complexity and reduce the manual workload.*** ***Automation: We've leveraged automation to handle repetitive tasks, such as access request processing, security patching, and continuous monitoring. Automation not only reduces the workload on our staff but also helps minimize human error, which can be a significant source of security risk. But there's still a lot of automation which is left to do and could be fixed for a seamless experience***	CO, ME, MLSA
28	Umar	Zero Trust Model has many advantages, however, you might have noticed that it also comes with an increased complexity at your organization?	

29	Jacob	If you say, mentioning it complexity? Definitely. ***You don't notice it until you notice how long you've been doing it. It took like probably 3 months to get used to how things work. I would say.***	CO
30	Umar	How has this affected the overall User Experience and Processes in your Organization?	
31	Jacob	***I would say for a normal person, it would be. All right. For me, I just didn't need all of the things, so I didn't actually use all of it. I wish I could have like they had where you can integrate your devices onto their network and like actually go into something and like use it. I never actually got to use that stuff. I it took too much time and so much complexity and processing time and I just found it not worth it.***	CO
32	Umar	So how long does it take to actually get into the system? For example, if you don't have those security measures in place two factor authentication	
33	Jacob	I think if they were, if they had people for any shorter amount of time, it would not be worth it. But the people there were there for years. ***So even if you had like 2 to 3 months of getting used to the technology and factor authentication and stuff like that, it was still worth it because people were gonna be there for years.*** ***It took me. I would say if you wanted to talk about most people there, it was about 6 months. At that point, you either thought it was too much, and you didn't get it and you just left. By that point, you already had the technology down where it was like secondhand. So for their organization, it was very useful.*** I could see it very being not as useful for other organizations that don't have longer-staying employees. People don't leave the organization before at least 1 to 2 years	CO,ED
34	Umar	Could you mention and go through some of the processes which have changed during the and after the implementation?	

35	Jacob	Give me 3 minutes and let me think about it: ***Access Request Process: Previously, employees had broad access rights based on their roles, and additional access could be granted quite easily. With the Zero Trust Model, employees start with minimal access rights and must request additional access as needed. This change was initially challenging for some employees, who found themselves suddenly unable to access resources they were accustomed to using. However, with time, employees adapted to the new process and the organization benefited from a reduction in unnecessary access rights, which decreased our overall risk.*** ***Authentication Process: The Zero Trust Model introduced more stringent authentication processes. Employees now use multi-factor authentication methods, such as biometrics or OTPs, in addition to their usernames and passwords. This change enhances security but was an adjustment for employees who were used to simpler login methods.*** ***Software Development Process: In the past, developers had wide-ranging access to development environments, code repositories, and other resources. Now, access is granted based on the principle of least privilege, meaning developers only get access to the resources they need for their current tasks. This change was implemented to prevent potential misuse of access rights and protect our codebases and data.***	ERSM,AU,AC
36	Jacob	Let me give you a concrete example: System would give you no warning. ***It would just say, hey, you cannot connect to the VPN you can't push (to the github repo) Access denied, and you ask what happened.*** ***So then you have to go to your manager.*** You have to go, hey, my visual studio isn't working, and he'd go to somebody else. And they'd go, hey, I think it's not working for us either. And then they'd go higher up. And somebody else would figure out they just pushed an SLA request for us. And then they'd be like, okay, and here's the fix. And then they send you the documentation and you have to go through and you have to submit the ticket. But like, that's the one downside of a big organization. I can't say that was necessarily the zero trust architecture. That was the fault point because it was such a massive organization. I don't think they planned on having any notifications for everybody that uses the software. No, nothing in place for that.	CO, AC
37	Umar	Have you noticed any changes in employee behavior or work habits due to the implementation of the Zero Trust Model? Zero Trust Features	

38	Jacob	***At the outset, there was a certain level of frustration and resistance, which is quite common when any new system or process is introduced. Employees, especially those fresh out of college like you mentioned, were used to a more open environment and found the stringent controls and increased oversight to be a bit overwhelming.*** For them, it felt like an extra layer of bureaucracy, slowing down their work and making tasks more complicated. They had to adapt to new processes, such as requesting access to resources they previously had at their fingertips, which could be seen as a disruption to their work habits. ***On the other hand, seasoned employees who had experienced security incidents in the past understood the need for such measures. They were more accepting of the new protocols, recognizing the benefits of the Zero Trust Model in terms of preventing unauthorized access and protecting sensitive data.***	ED
39	Umar	How do the features of the Zero Trust Model (e.g., authentication, access control, micro-segmentation, security automation) affect your organization?	
40	Jacob	There were too many documents you learned on the job, and the job paid you to learn it. So you don't really go around it to go and try and read it, even though it did provide beneficial to read documentation when they released updates, but it's only because I was interested in it. ***When it comes to the features I think it is access control and security automation features of the organization and a reason why they're still in the market today. Without that, I think they would have become one of the banks that fall fell through to cyber attacks.***	AC, MLSA
41	Umar	Which features have had the greatest impact on productivity, either positively or negatively?	
42	Jacob	If we want to talk personally, the biggest productivity thing is bring your own device because I liked working on a laptop negatively, it would be the amount of access that you need to get something done in the amount of requests. Anything else? No, it was most background stuff which was very nice. I can't tell you, though, from my friend, he's now working for a company and that ***access control is much different. And he probably has a different, on the amount of access he's given from some things.So the access control is a negative***	CO, AC

43	Umar	Are there any new developments or technologies that you believe will have a significant impact on the future of Zero trust models?	
44	Jacob	Let's see. I think the biggest development was cloud, which was the biggest with cloud, and I am security other than that. I don't think there's anything that's going to be new in the next few years. Do you? Sorry. Do you have anything that you think will be impacting it in the next few years?	
45	Jacob	***Artificial Intelligence and machine learning, for example, in cyber security.***	MLSA
46	Jacob	thinking from a standpoint of a percentage of success. The rate of a machine learning model being successful is 95 % and no machine. No code can be written with that % of accuracy. So I don't think they can implement that into the automation segment. And the next AI thinks that what they will write will be something to detect, but the IDs systems are something different than zero trust. ***It would be your detection instead of your what zero trust is like, anticipate, setting up for something the ideas is in reaction to something.***	FDZT
47	Umar	Thank you for the Interview	

Appendix 7 - Transcription - Participant 6

Num	People	Question & Answer	Code
1	C L	To start our interview today, can you tell me a little bit about your background?	
2	R6	I am currently a team of software developers doing information technology in the government sector. I myself am engaged in software development work, I am an engineer, and then we have engaged in some information technology services, such as software development, system development related work.	
3	C L	Are you familiar with the Zero Trust model we'll be talking about today?	
4	R6	We are also basically familiar with the Zero Trust model. We may know less about this concept, but we have used this Zero Trust model in our own work. We are also currently exploring and learning from this solution, and we are currently trying to solve the problem of data security and communication security between microservices, especially in the public cloud, or to improve the security of our services.	
5	C L	What is your understanding of this traditional solution of cyber security?	
6	R6	***My understanding is that perhaps traditional network security solutions, which more often rely on border defense, such as the newcomer's intranet, for example, I have a dedicated intranet, the network of the external network may be more skeptical of such traditional network security solutions, it may be some physical rooms or network segment isolation, there are such means, for example, they will be through this kind of fortress machine Vpn Firewalls and other such means to carry out such security protection.*** I am a software development IT service provider in the government sector, so we may serve some government IT sector, there will be some proprietary clouds, such as the government cloud, they will have some network segments, and our public network is separate, for example, I just said the government extranet or even higher is the government intranet, when we want to When we want to access these resources, we	TSS

		may have to go through a fortress and then a VPN to access these special network segments.	
7	C L	What led your organization to transition from this traditional cyber security solution to a zero trust model.	
8	R6	***The primary reason is to improve security, because the previous traditional security policy, which still emphasizes border defense, sometimes cannot stop hackers or attackers, once they enter the intranet, if you do not have another security mechanism to protect your data security or service security between the intranet, then once they enter the intranet If you don't have another security mechanism to protect your data security or service security, then once it enters the intranet, it can attack horizontally at once, and it will be a straightforward one.*** Why should we explore zero trust? In fact, zero trust has a better mechanism, he has a minimum of a resource principle, and a mechanism called dynamic risk risk control, for example, when all my requests come, I can dynamically analyze whether your request is a trusted request, but at present we are also belonging to a preliminary transition to zero trust in an early stage, still in the We are still exploring.	ZTMA ,ESRM
9	C L	What are the challenges in this implementation and how do they compare to traditional solutions, traditional network solutions?	

10	R6	The traditional solution is still the same as the border problem, that is, the problem of border defense, which has just been mentioned. However, it may not be so demanding on the management of business development rights, and the granularity of resources is not so demanding. But his emphasis on mechanisms such as authentication and authorisation or minimal privileges is still somewhat intrusive to the business. So our challenge is how to weigh the investment ratio and cost ratio of development and security implementation, in fact, we are also considering that excessive security investment will often increase the cost of our business development, which will also lead to the delay of our project development. It's still a big challenge for us.	ZTMA ,ESRM ,CO
11	C L	What are your experiences of how you have overcome such challenges?	
12	R6	***I can actually go back to our current implementation, including the Zero trust model, which we are actually exploring, for example, the single point of authorization we use for risk control, and this kind of security gateway or resource permission control, are all things that we are currently exploring and are adding to our security architecture step by step.*** ***All requests have to be authenticated and authorized before they can be accessed by each other, and the maintenance and services can be accessed by each other, as well as the identification of malicious attacks, such as the protection and decryption of sensitive information in our risk control and some gateways, and even the registration and discovery of routes, as well as the monitoring of logs and the tracking of behavior, the challenge is actually in the implementation process.*** For example, we have just discussed the issue of cost, that is, the cost of security policy investment, it is indeed very difficult to control, for example, I in the process of rapid business iteration, how to pick out which business or which scenario we think is suitable for the highest priority to find the implementation of security policy of this priority. ***Our current challenge is that our implementation experience, for example, payment user information and other services, such scenarios or resources, we may feel relatively sensitive, and then we may give priority to ensuring that a few scenarios, or a few services, or a few resources to ensure the security of the most core resources.***	ESRM, AU

13	C L	This means that we are now in the process of improving our cyber security solutions, but there are still many challenges in this process and it is difficult to find a balance, so it is necessary to implement them step by step.	
14	R6	***Yes, because the real business development of a team is sometimes really uncontrollable, and the investment in security brings with it the investment in technology, including the investment in professionals and professionals, as well as the investment in personnel, which often still has a certain impact on the business and is still quite challenging.***	CO
15	C L	How does the zero trust model affect the overall security posture of an organisation like yours?	
16	R6	***For example, for all our resource access and communication between services, we will have an authorized, right? In fact, there is a security posture, another is our current data protection.In fact, our data protection will be the lowest possible principle for users or our developers and our data protection, for example, to ensure that our data permissions are at the lowest possible level for our data resources.*** Because even if this thing is leaked, then I will not affect a big impact. There is also a security posture, that is, we currently feel better is a dynamic risk control strategy, it is more adaptable to the dynamic network environment. For example, we are working on the c-end users, we may have some c-end products, it is possible to combine the real-time environment and user information, such as your access IP, your device, and even your mobile phone some basic information, and then go closer to do some dynamic such wind control strategy, and then closer to the scene and business, can more improve our security. So combined with these aspects, I think from improving security or enhancing data protection these aspects to think that zero trust has a great impact on the overall security posture.	ERSM
17	C L	From your work experience, have you found any unexpected benefits or drawbacks to implementing the Zero Trust model?	

18	R6	In the early stages of our implementation, the focus of our team was probably not so much on security issues, but on the progress of business development. So the unexpected downside is that we are currently lengthening our development process. ***For example, when we implement zero trust, then there will be more complex process such review meeting, for example, when we do a business system, there will be a lot of security review, because zero trust it needs to build a reliable authentication, so that requires us to invest a lot of work resources or even meetings, so that it is very expensive to implement.*** ***Another aspect is the impact of this model on our c-terminal products, but also experience is also some of the impact. For example, the dynamic network mentioned just now, such as the wind control strategy I mentioned, may require more consideration in product design and more consideration from the user experience, because it will bring some, for example, your login process of this more. It also means that when the user identifies risks in the process of operating the business, it will lead the user to do some secondary verification, so this also increases the complexity of the user experience.*** But there is a benefit for our internal system, because it focuses on the monitoring of logs, the monitoring of behaviors, it is possible for each behavior to be traced for our team or even for our developers, so that they can trace our security incidents, for example, I found this incident, I have some logging behavior, recording behavior Which person and which incident came from where, so that's probably one of the benefits. So that's probably one of the benefits of having a model for this, and then having a real-time monitoring and logging.	CO, AU,
19	C L	From your feedback, it seems that the development schedule is still the primary goal, and do you think it would be better to train developers on, for example, the Zero Trust model and the related system security in the process to get this model implemented?	
20	R6	***In fact, according to my personal understanding, all security issues are in fact largely related to the security awareness of the internal staff organisation. That is to say, I go through this kind of security policy or my security structure internally, in fact, it can improve the security of your organization.*** I think what you are saying is that it is very useful to train and to implement this internally, and it is very useful.	ED

21	C L	In your work experience of managing the implementation of the Zero Trust model, have you noticed any increase in the complexity and resource requirements associated with this?	
22	R6	***In the beginning, when we implemented Zero Trust, we did some workflow, first we did an overall review of our internal technical architecture and security architecture, then we also sorted out some important resource priorities, and we also developed a phased implementation of Zero Trust, where we prioritised some data that was of high risk to the organisation, and then gradually spread it to the rest of the business.*** ***We prioritised some of the data in the sensitive parts of the organisation, and then gradually spread it to other business, other systems or other data resources, we are similar to an implementation process, picking a few key parts to implement the leading model first, and then expanding from important modules to other areas. To sum up, we need to set a target, then sort out our priorities for data resources and even systems, and then slowly move from the important to the universal stage.***	ESRM, CO, ED
23	C L	We've just talked about how it has a lot of advantages, and you mentioned that it actually comes with a certain amount of organisational complexity, do you have any experience of this?	

24	R6	In particular, first of all, the most intuitive feedback is definitely on our c-end products, for example, the most intuitive user experience, probably the user experience will be more clear more quickly, more obvious. Zero trust is definitely the authorization of each step of the request, as well as the identification of the risk of the request. ***So in terms of the product team, for example, if we are logging in, or if we are dealing with information about user operations, it has a more complex authentication process, or even more complex authentication steps. So also in the product form, that is to say, also increased this kind of secondary user authentication guidance, which is to lead to the complexity of the user's use.*** ***Secondly, as I said just now, from the development point of view, it does increase the cost of each business development, that is, each business development we have to consider the issue of security, have to open security meetings, have to open security reviews, and even have to open this kind of risk control strategy.*** This protection for business scenarios, or risk control strategies have to take into account this step, whether there are security risks	AU, CO
25	C L	In this process, has the overall user experience process changed compared to the previous one?	
26	R6	The user experience process is still very complex, so there will be more authentication steps in the whole user experience. Let me give you an example, even though it may improve security, it may also cause a certain degree of disruption to the user's login experience. For example, when I go to do a login operation on another device that I don't use very often, or when I go to do a login operation on an off-site network. ***Then my authentication , or the dynamic risk control strategy just mentioned, it will trigger my secondary verification, for example, you have to guide the user to carry out a biological authentication, or even a mobile phone SMS verification, or more complex, such as the verification of the previous login history, so it is to the user It adds complexity to the user experience, but it increases security.***	AC, AU, ERSM

27	C L	We also talked about the fact that in Zero Trust, it has a lot of features, such as authentication rights control and dynamic monitoring, can you give us some examples of these features that have the most impact in your organisation.	
28	R 6	The main focus is on authentication and access control. ***At present, we have an internal platform called unified authentication, that is, all services or all micro-services are to enter the unified authentication of such a set of platform, or such a product inside, it is still to a large extent to ensure that all our services, all technology development system or service, to ensure the security of such services.*** ***Then there is the issue of access control. In fact, our access control is mainly to better reduce our data leakage.*** ***In fact, we have a similar product called data resource control system, our database is actually a separate block of data, so I for each user or for each organization's personnel, we try to ensure the principle of data minimization, this way you can fully ensure the security of data, but also to improve data security.*** ***We have not yet implemented the rest of the micro-segmentation or security automation you just mentioned. Maybe we need to learn more about these two features again.***	AC, AU, ME
29	C L	How do you balance security and this impact on your organisation in your work experience?	
30	R6	We are still in the process of learning how to implement security measures in different stages, starting with pre-review sessions, such as security education sessions, or the review of our final objectives, which are broken down into multiple phases.	
31	CL	What developments or technologies are available and which technologies or directions do you think will have a significant impact on the Zero Trust model or on traditional security solutions.	

32	R6	The latest thing I can think of is artificial intelligence. It's still a very powerful technology or trend for the moment. These technologies are able to, for example, use self-learning capabilities, are these technologies able to, for example, use artificial intelligence to analyse my large amount of security event data or logs in real time. ***Or use artificial intelligence to do some detection, or automatic scanning or automatic learning of this ability, so that artificial intelligence to go through intelligent analysis is not faster to find to deal with security threats, that is, do not wait for the threat to come and then we go to deal with, but that the use of artificial intelligence to make security intervention earlier, so faster to solve this problem.*** Can artificial intelligence subsequently also help us to warn safely, it just keeps on learning and keeps on detecting for you, right?	MLSA, ERSM, FDZT
33	C L	Okay thanks. That's all we have for today and we thank you very much for taking part in our survey.	

References

Abowd, G. D., Dey, A. K., Brown, P. J., Davies, N., Smith, M. & Steggles, P. (1999). Towards a Better Understanding of Context and Context-Awareness, in *Handheld and Ubiquitous Computing: First International Symposium, HUC'99 Karlsruhe, Germany, September 27–29, 1999 Proceedings 1*, 1999, pp.304–307

Adikari, S., McDonald, C. & Campbell, J. (2011). A Design Science Framework for Designing and Assessing User Experience, in *Human-Computer Interaction. Design and Development Approaches: 14th International Conference, HCI International 2011, Orlando, FL, USA, July 9-14, 2011, Proceedings, Part I 14*, 2011, pp.25–34

Ali, I., Sabir, S. & Ullah, Z. (2019). Internet of Things Security, Device Authentication and Access Control: A Review, *arXiv preprint arXiv:1901.07309*

Aminanto, M. E., Choi, R., Tanuwidjaja, H. C., Yoo, P. D. & Kim, K. (2017). Deep Abstraction and Weighted Feature Selection for Wi-Fi Impersonation Detection, *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 3, pp.621–636

Atlam, H. F., Alenezi, A., Walters, R. J., Wills, G. B. & Daniel, J. (2017). Developing an Adaptive Risk-Based Access Control Model for the Internet of Things, in *2017 IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and Ieee Smart Data (SmartData)*, 2017, pp.655–661

Bertino, E. (2021). Zero Trust Architecture: Does It Help?, *IEEE Security & Privacy*, vol. 19, no. 05, pp.95–96

Bhattacherjee, A. (2012). Social Science Research: Principles, Methods, and Practices

Brooks, J., Horrocks, C. & King, N. (2018). Interviews in Qualitative Research, *Interviews in qualitative research*, pp.1–360

Brouwer, W., Van Exel, N., Koopmanschap, M. A. & Rutten, F. F. (2002). Productivity Costs before and after Absence from Work: As Important as Common?, *Health policy (Amsterdam, Netherlands)*, vol. 61, no. 2, pp.173–187

Buchholz, K. (1995). Criteria for the Analysis of Scientific Quality, *Scientometrics*, vol. 32, no. 2, pp.195–218

Buck, C., Olenberger, C., Schweizer, A., Völter, F. & Eymann, T. (2021). Never Trust, Always Verify: A Multivocal Literature Review on Current Knowledge and Research Gaps of Zero-Trust, *Computers & Security*, vol. 110, p.102436

Campbell, M. (2020). Beyond Zero Trust: Trust Is a Vulnerability, *Computer*, vol. 53, no. 10, pp.110–113

Chen, Y., Hu, H. & Cheng, G. (2019). Design and Implementation of a Novel Enterprise Network Defense System Bymaneuveringmulti-Dimensional Network Properties, *Frontiers of Information Technology & Electronic Engineering*, vol. 20, no. 2, pp.238–252

Chuan, T., Lv, Y., Qi, Z., Xie, L. & Guo, W. (2020). An Implementation Method of Zero-Trust Architecture, *Journal of Physics: Conference Series*, vol. 1651, no. 1, p.012010

Creswell, J. W. & Poth, C. N. (2016). Qualitative Inquiry and Research Design: Choosing among Five Approaches, Sage publications

Cunningham, C. (2018). The Zero Trust EXtended (ZTX) Ecosystem, *Forrester, Cambridge*,

MA

DeCusatis, C., Liengtiraphan, P., Sager, A. & Pinelli, M. (2016). Implementing Zero Trust Cloud Networks with Transport Access Control and First Packet Authentication, in *2016 IEEE International Conference on Smart Cloud (SmartCloud)*, 2016, pp.5–10

Denzin, N. K. & Lincoln, Y. S. (2011). The Sage Handbook of Qualitative Research, sage

Dumitru, I.-A. (2022). Zero Trust Security, in *Proceedings of the International Conference on Cybersecurity and Cybercrime (IC3)*, International Conference on Cybersecurity and Cybercrime, 30 April 2022, Romanian Association for Information Security Assurance, pp.99–104, Available Online: https://proceedings.cybercon.ro/index.php/ic3/article/view/2022-13 [Accessed 9 March 2023]

Efron, S. E. & Ravid, R. (2019). Action Research in Education: A Practical Guide, Guilford Publications

Elsayed, M. S., Le-Khac, N.-A., Dev, S. & Jurcut, A. D. (2019). Machine-Learning Techniques for Detecting Attacks in SDN, in *2019 IEEE 7th International Conference on Computer Science and Network Technology (ICCSNT)*, 2019, pp.277–281

Fernandez, E. B. & Brazhuk, A. (2022). A Critical Analysis of Zero Trust Architecture (Zta), *SSRN Electronic Journal*, [e-journal], Available Online: https://www.ssrn.com/abstract=4210104 [Accessed 11 December 2022]

Frank, M., Biedert, R., Ma, E., Martinovic, I. & Song, D. (2012). Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication, *IEEE transactions on information forensics and security*, vol. 8, no. 1, pp.136–148

Fu, P., Wu, J., Lin, X. & Shen, A. (2022). ZTEI: Zero-Trust and Edge Intelligence Empowered Continuous Authentication for Satellite Networks, in *GLOBECOM 2022-2022 IEEE Global Communications Conference*, 2022, pp.2376–2381

Garbis, J. & Chapman, J. W. (2021). Zero Trust Security: An Enterprise Guide, Springer

Gasson, S. (2003). Human-Centered vs. User-Centered Approaches to Information System Design, *Journal of Information Technology Theory and Application (JITTA)*, vol. 5, no. 2, p.5

Guest, G., Bunce, A. & Johnson, L. (2006). How Many Interviews Are Enough? An Experiment with Data Saturation and Variability, *Field methods*, vol. 18, no. 1, pp.59–82

Guest, G., MacQueen, K. M. & Namey, E. E. (2011). Applied Thematic Analysis, sage publications

Hayashi, E., Das, S., Amini, S., Hong, J. & Oakley, I. (2013). Casa: Context-Aware Scalable Authentication, in *Proceedings of the Ninth Symposium on Usable Privacy and Security*, 2013, pp.1–10

He, Y., Huang, D., Chen, L., Ni, Y. & Ma, X. (2022). A Survey on Zero Trust Architecture: Challenges and Future Trends, *Wireless Communications and Mobile Computing*, vol. 2022, pp.1–13

Hu, C. T. (2014). Attribute Based Access Control (ABAC) Definition and Considerations

Jakobsson, M., Shi, E., Golle, P., Chow, R., & others. (2009). Implicit Authentication for Mobile Devices, in *Proceedings of the 4th USENIX Conference on Hot Topics in Security*, Vol. 1, 2009, pp.25–27

Johns, I. (2021). Role of AI in Tackling Cybercrime, *Jus Corpus LJ*, vol. 2, p.1233

Johnson, R. B. & Onwuegbuzie, A. J. (2004). Mixed Methods Research: A Research Paradigm Whose Time Has Come, *Educational researcher*, vol. 33, no. 7, pp.14–26

Kim, S.-H., Choi, D., Kim, S.-H., Cho, S. & Lim, K.-S. (2018). Context-Aware Multimodal FIDO Authenticator for Sustainable IT Services, *Sustainability*, vol. 10, no. 5, p.1656

Kindervag, J. (2010). Build Security Into Your Network's DNA: The Zero Trust Network Architecture

Klein, H. K. & Myers, M. D. (1999). A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems, *MIS quarterly*, pp.67–93

Kumar, P., Moubayed, A., Refaey, A., Shami, A. & Koilpillai, J. (2019). Performance Analysis of Sdp for Secure Internal Enterprises, in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, 2019, pp.1–6

Lam, K.-Y. & Chi, C.-H. (2016). Identity in the Internet-of-Things (IoT): New Challenges and Opportunities, in *Information and Communications Security: 18th International Conference, ICICS 2016, Singapore, Singapore, November 29–December 2, 2016, Proceedings 18*, 2016, pp.18–26

Li, S., Iqbal, M. & Saxena, N. (2022). Future Industry Internet of Things with Zero-Trust Security, *Information Systems Frontiers*, [e-journal], Available Online: https://link.springer.com/10.1007/s10796-021-10199-5 [Accessed 11 December 2022]

Line, M. B., Tøndel, I. A. & Jaatun, M. G. (2016). Current Practices and Challenges in Industrial Control Organizations Regarding Information Security Incident Management–Does Size Matter? Information Security Incident Management in Large and Small Industrial Control Organizations, *International Journal of Critical Infrastructure Protection*, vol. 12, pp.12–26

Marshall, B., Cardon, P., Poddar, A. & Fontenot, R. (2013). Does Sample Size Matter in Qualitative Research?: A Review of Qualitative Interviews in IS Research, *Journal of computer information systems*, vol. 54, no. 1, pp.11–22

Mehraj, S. & Banday, M. T. (2020). Establishing a Zero Trust Strategy in Cloud Computing Environment, in *2020 International Conference on Computer Communication and Informatics (ICCCI)*, 2020 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, January 2020, Coimbatore, India: IEEE, pp.1–6, Available Online: https://ieeexplore.ieee.org/document/9104214/ [Accessed 27 December 2022]

Moubayed, A., Refaey, A. & Shami, A. (2019). Software-Defined Perimeter (Sdp): State of the Art Secure Solution for Modern Networks, *IEEE network*, vol. 33, no. 5, pp.226–233

Myers, M. D. (2019). Qualitative Research in Business and Management, *Qualitative research in business and management*, pp.1–364

Myint Oo, M., Kamolphiwong, S., Kamolphiwong, T. & Vasupongayya, S. (2019). Advanced Support Vector Machine-(ASVM-) Based Detection for Distributed Denial of Service (DDoS) Attack on Software Defined Networking (SDN), *Journal of Computer Networks and Communications*, vol. 2019

Nguyen, L. D., Le-Hoai, L., Tran, D. Q., Dang, C. N. & Nguyen, C. V. (2019). Effect of Project Complexity on Cost and Schedule Performance in Transportation Projects, *Construction Management and Economics*, vol. 37, no. 7, pp.384–399

Niinuma, K., Park, U. & Jain, A. K. (2010). Soft Biometric Traits for Continuous User Authentication, *IEEE Transactions on information forensics and security*, vol. 5, no. 4, pp.771–780

Orlikowski, W. J. & Baroudi, J. J. (1991). Studying Information Technology in Organizations: Research Approaches and Assumptions, *Information systems research*, vol. 2, no. 1, pp.1–28

Patton, M. Q. (2014). Qualitative Research & Evaluation Methods: Integrating Theory and Practice, Sage publications

Patton, M. Q. (2015). Qualitative Research & Evaluation Methods: Integrating Theory and Practice, Fourth edition., Thousand Oaks, California: SAGE Publications, Inc

Recker, J. (2013). Scientific Research in Information Systems: A Beginner's Guide, Springer
Roig, M. (2006). Ethical Writing Should Be Taught, *BMJ (Clinical research ed.)*, vol. 333, no. 7568, pp.596–597
Rose, S., Borchert, O., Mitchell, S. & Connelly, S. (2020). Zero Trust Architecture, National Institute of Standards and Technology, Available Online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf [Accessed 9 March 2023]
Roth, J., Liu, X. & Metaxas, D. (2014). On Continuous User Authentication via Typing Behavior, *IEEE Transactions on Image Processing*, vol. 23, no. 10, pp.4611–4624
Ryan, F., Coughlan, M. & Cronin, P. (2009). Interviewing in Qualitative Research: The One-to-One Interview, *International Journal of Therapy and Rehabilitation*, vol. 16, no. 6, pp.309–314
Saevanee, H., Clarke, N., Furnell, S. & Biscione, V. (2015). Continuous User Authentication Using Multi-Modal Biometrics, *Computers & Security*, vol. 53, pp.234–246
Sarkar, S., Choudhary, G., Shandilya, S. K., Hussain, A. & Kim, H. (2022). Security of Zero Trust Networks in Cloud Computing: A Comparative Review, *Sustainability*, vol. 14, no. 18, p.11213
Schultze, U. & Avital, M. (2011). Designing Interviews to Generate Rich Data for Information Systems Research, *Information and organization*, vol. 21, no. 1, pp.1–16
Seidman, I. (2006). Interviewing as Qualitative Research: A Guide for Researchers in Education and the Social Sciences, Teachers college press
Shlapentokh-Rothman, M., Hemberg, E. & O'Reilly, U.-M. (2020). Securing the Software Defined Perimeter with Evolutionary Co-Optimization, in *Proceedings of the 2020 Genetic and Evolutionary Computation Conference Companion*, 2020, pp.1528–1536
Sica, G. T. (2006). Bias in Research Studies, *Radiology*, vol. 238, no. 3, pp.780–789
Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z. & Doss, R. (2022). Zero Trust Architecture (ZTA): A Comprehensive Survey, *IEEE Access*, vol. 10, pp.57143–57179
Teerakanok, S., Uehara, T. & Inomata, A. (2021). Migrating to Zero Trust Architecture: Reviews and Challenges, *Security and Communication Networks*, vol. 2021, pp.1–10
Thomas, D. R. (2006). A General Inductive Approach for Analyzing Qualitative Evaluation Data, *American journal of evaluation*, vol. 27, no. 2, pp.237–246
Tounsi, W. & Rais, H. (2018). A Survey on Technical Threat Intelligence in the Age of Sophisticated Cyber Attacks, *Computers & security*, vol. 72, pp.212–233
Wu, Y. G., Yan, W. H. & Wang, J. Z. (2021). Real Identity Based Access Control Technology under Zero Trust Architecture, in *2021 International Conference on Wireless Communications and Smart Grid (ICWCSG)*, 2021, pp.18–22
Wylde, A. (2021). Zero Trust: Never Trust, Always Verify, in *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, 14 June 2021, Dublin, Ireland: IEEE, pp.1–4, Available Online: https://ieeexplore.ieee.org/document/9478244/ [Accessed 11 December 2022]
Zaheer, Z., Chang, H., Mukherjee, S. & Van der Merwe, J. (2019). Eztrust: Network-Independent Zero-Trust Perimeterization for Microservices, in *Proceedings of the 2019 ACM Symposium on SDN Research*, 2019, pp.49–61