ZERO-TRUST ARCHITECTURE AND ITS COST-EFFECTIVENESS ON NETWORK SECURITY

A Paper
Submitted to the Graduate Faculty
of the
North Dakota State University
of Agriculture and Applied Science

By

Zillah Adahman

In Partial Fulfillment of the Requirements
for the Degree of
MASTER OF SCIENCE

Major Department:
Computer Science

April 2022

Fargo, North Dakota

NORTH DAKOTA STATE UNIVERSITY

Graduate School

Title

ZERO-TRUST ARCHITECTURE AND ITS COST-EFFECTIVENESS ON NETWORK SECURITY

By

Zillah Adahman

The supervisory committee certifies that this paper complies with North Dakota State University's regulations and meets the accepted standards for the degree of

MASTER OF SCIENCE

SUPERVISORY COMMITTEE:

Dr. Zahid Anwar
Chair

Dr. Kenneth Magel

Dr. Muhammad Malik

Dr. Maria Alfonseca Cubero

Approved:

05/09/2022
Date

Simone Ludwig
Department Chair

ABSTRACT

Zero-Trust Architecture (ZTA) is a ‘Never Trust, Always Verify’ concept to improve cybersecurity by eliminating trust and validating network requests continuously. ZTA replaces Virtual Private Networks (VPNs) and provides solitary access to applications and data. The growth of ZTA has spiked over the years, but organizations are reluctant to invest in this security approach. Previous studies cover ways to implement ZTA, its significance, and challenges but provide limited information on available tools, prices, and the success rate of ZTA.

This research shows the implementation of ZTA causes a reduction of $684K on average in risk impact over four years for small to medium-sized organizations. Organizations lack information on the quantitative evaluations of ZTA benefits and drawbacks. An in-depth analysis of ZTA to help security researchers better understand the costs and benefits of employing ZTA as a defense against cyber attacks is provided in this work.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

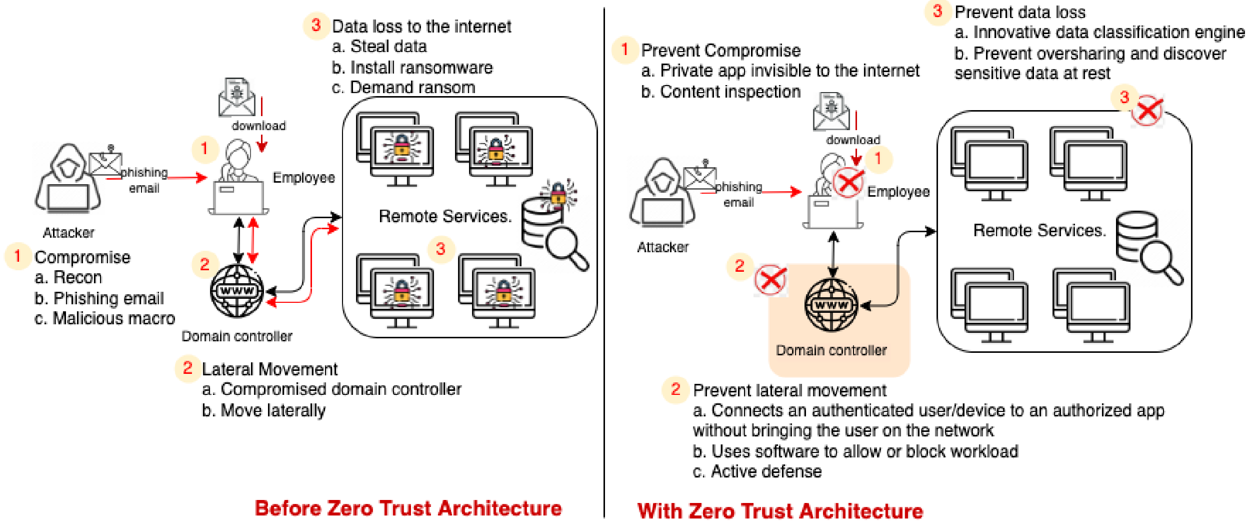
LIST OF ABBREVIATIONS

AI	Artificial Intelligence
BYOD	Bring Your Own Device
CAGR	Compound Annual Growth Rate
CPUC	California Public Utilities Commission
DE	Data Encryption
EP	Endpoint Protection
HVAC	Heating, Ventilation, and Air Conditioning
IAM	Identity Access Management
IoT	Internet of Things
IT	Information Technology
NIST	National Institute of Standards and Technology
OSI	Open Systems Interconnection
P	Policies
PA	Policy Administrators
PDP	Policy Decision Point
PE	Policy Engine
PEP	Policy Enforcement Point
SEC	Securities and Exchange Commission
SMBs	Small and Medium-Sized Businesses
US	United States
USD	United States Dollars
VPNs	Virtual Private Networks
ZTA	Zero-Trust Architecture
ZTNA	Zero-Trust Network Access

1. INTRODUCTION

As technology evolves, most employees work remotely (Mandal, Khan, & Jain, 2021). Unfortunately, many of these employees do not have a secure internet connection outside their work-office perimeter. As a result, organizations discover new ways to secure incoming requests to their assets using Virtual Private Networks (VPNs). VPNs are insecure and expensive to handle a large number of employees outside an organization's perimeter (Dhawan, 2021). Notably, amongst VPNs users in early 2021, about 21 million Android users utilizing Android VPNs like SuperVPN, GeckoVPN, and ChatVPN were targeted and breached (Melnic, 2021). The cyber-attackers retrieved sensitive user information and auctioned it on a popular hacker forum to the highest bidder. One issue with VPNs is the network groups users into one system, and if an attacker gains access, the entire system is compromised. Aside from VPNs insecurity, the utilization of cloud storage environments (Ferretti, Magnanini, Andreolini, & Colajanni, 2021) and Bring Your Own Devices (BYOD) policies have also evolved. Consider medical employees accessing an organization's Cloud environment (Ali, Gregory, & Li, 2021) using a not-so-secured BYOD - it provides an opening for malicious actors to attack an organization's network. Hence, a new approach to network security is needed.

Prospects of Zero-Trust Architecture (ZTA) introduced the framework as an inexpensive and secure replacement for VPNs. ZTA is a multi-layered approach to an organization's network security with the idea of never trusting and always verifying every access to a resource (Campbell, 2020). ZTA is used to secure employees' access to organizations' resources at a lower cost compared to VPNs (English, 2021). It also restricts full network access of any subject (users or devices) (Bertino, 2021). No one is trusted. Although the prospects of ZTA recognize it as an effective approach to strengthening an organization's network security (Al-Ruwaii & De Moura, 2021), 43% of organizations have no plans to implement ZTA (IBM, 2021). This lack of interest has a detrimental effect on the state of cybersecurity as technology evolves.



Before Zero Trust Architecture

With Zero Trust Architecture

Figure 1.1. ZTA for the Comprehensive Multi-Level Protection Against Sophisticated Attacks.

Fig. 1.1 depicts comprehensive multi-level protection of ZTA against attacks in an organization illustrating a scenario to cover the before and after-effects of the implementation of ZTA. An attacker uses social engineering to research, identify, and select their targets. The attacker sends a phishing email with a malicious macro to the target's employee. This scenario includes an employee working remotely through a VPNs connection, granting them full access to the organization's network system. When the employee opens the email, they undetectably install the malicious macro onto their system. The macro compromises the domain controller, moving laterally to the organization's network system. This malicious macro further leads to data loss where the attacker uses it to steal sensitive data, install ransomware, and demand ransom from the organization. As shown in Fig. 1.1, implementing ZTA strengthens the organization's network system against these attacks. It prevents malware compromise by inspecting email contents and protecting the user's device. It prevents lateral movement in the organization's network system by restricting access to only the requested resources and actively defending the domain controller. As a result, protecting the organization from data loss, ransom, and unwanted costs to recover or rebuild its network security.

This research work highlights the possible solutions to implement ZTA in an organization. A data-driven, quantitative analysis of the cost of ZTA tools and resources is conducted by providing the annual budget amount for each tool based on organization's employee headcounts and their business needs. These costs are also compared to different aspects of security incidents likely to occur. In this research work, modelling the reduced data breach risk is conducted based on recent breach events to portray ways ZTA reduces the chances of data breaches. This work can serve as basic guidelines for organizations, especially entrepreneurs, with the basic knowledge of the importance of ZTA, its budget estimates, and its cost with varying organization scales.

The salient features of this work are highlighted below:

- **The Cost and Budget Analysis of ZTA Tools and Resources.** – In a recent study, The National Institute of Standards and Technology (NIST) selected companies to demonstrate ZTA measures (Gunderman, 2021). Most of these companies are well-known, and have released ZTA tools for other organizations to implement. The prices of these tools are analyzed in this research. The cost of each tool is calculated and scenarios are provided to accompany the utilization of ZTA based on Small and Medium-sized Businesses (SMBs) with employee counts between 0 and 1000. ZTA solutions providing similar services are also analyzed to compare cost difference between different providers.

- **The Provision of Available ZTA Tools** – Information on available ZTA tools organizations can implement is provided in this research work. Some tools developed by different providers, like CylancePROTECT and Google Workspace, can be combined to work in parallel to establish a ZTA approach. Some ZTA providers offer all-in-one solutions with services for the complete implementation of ZTA like Perimeter81 (Perimeter81, 2022). There are also open-sourced and free ZTA software available for organizations to implement. In-depth information relating to these tools is provided in this work.

- **The Effects of Data Breaches on Organizations Without ZTA Implementation** – Factual data on recent breach events in organizations is provided to show the loss of capital and customers due to their inadequate security systems. This study explains the benefits of investing in ZTA to reduce recovery costs after a data breach event.

- **The Analysis of the Cost of Data Breaches** – The cost of data breaches in organizations with and without the implementation of ZTA is analyzed. Case studies are provided to showcase recent data breaches on SMBs and enterprise-level organizations. These organizations lost above 100,000 user records and disbursed hundreds of thousands to millions of United States (US) dollars towards data breaches. This research paper shows the cost-saving effect of ZTA when organizations invest in its approach.

The rest of the paper is structured as follows: Section 2 covers related work on ZTA. The background, benefits, and market share of ZTA are present in Section 3. Section 4 proposes the implementation of ZTA and ways to migrate to ZTA. Section 6 indicates the cost and budget analysis of tools and resources, Section 5 provides information on providers and other ZTA solutions, while Section 7 emphasizes the cost-effectiveness of ZTA. Finally, Section 8 presents the conclusion and future directions.

2. RELATED WORK

This section covers the recent contributions made to adopt ZTA within an organization. The subsections covers previous studies based on the implementation, best practices to overcome implementation challenges, cost and budget analysis, and ransomware activities. As per this research, areas like budget analysis, cost effectiveness, and ransomware government policies have been less explored.

ZTA Implementation Strategies

Kerman *et al.* (Kerman, Borchert, Rose, & Tan, 2020) illustrates the implementation of ZTA within an organization. They carried out different scenarios based on responses from organizations that agreed to participate in the implementation of ZTA. Buck *et al.* (Buck, Olenberger, Schweizer, Völter, & Eymann, 2021) focused on various related studies to provide gaps in ZTA. One of which is the Kindervag research paper. Kindervag *et al.* (Kindervag, 2010) implemented research for organizations and individuals to improve cybersecurity through a zero-trust model. The researchers explained ZTA changed the design of networks focusing on the increase in cyber threats. The authors advised organizations to build a networking architecture from the inside out by securing the data first before the networking part. Kindervag *et al.* research paper is more than a decade old; however, the implementation of ZTA within an organization has improved over time. This research paper provides the latest implementation tactics of ZTA.

Stafford *et al.* (Stafford, 2020) provides migration knowledge to ZTA with an overview of the logical components that make up the architecture. The authors provided variations to approach ZTA with use cases organizations can select from when searching for an approach to implement Zero-Trust Architecture. Nevertheless, some organizations implement multiple variations of ZTA based on the number of employees or their business needs. Table 6.1 of Section 6 provides different tools and resources organizations can utilize for various ZTA approaches. More into implementation, an article by Cavalancia (Cavalancia, 2020) focused on ZTA implementation by creating an outline of zero-trust in terms of authorization to resources both on-premises and the cloud. Cavalancia's article focused on implementing principles to only grant access to users after properly and heavily authenticating their identity.

Other related studies where ZTA was implemented include the following. Wylde *et al.* (Wylde, 2021) emphasized ZTA as a model based on no presumptive trust and a risk-based approach to trust along with continuous verification of trust. Luca *et al.* (Ferretti et al., 2021) utilized ZTA to guarantee security for cloud computing environments. Annamalai *et al.* (Alagappan, Venkatachary, & Andrews, 2022) demonstrates implementing ZTA in virtual power plants to enhance security in protecting its data and information privacy. Daniel *et al.* (D'Silva & Ambawade, 2021) focused on implementing ZTA using kubernetes to focus on security at every Open Systems Interconnection (OSI) model layer. Teerakanok *et al.* (Teerakanok, Uehara, & Inomata, 2021) paper also focused on the implementation and migration to ZTA due to the growth of cloud technologies and the IoT. The authors discuss the major components of ZTA and introduce steps for organizations with existing perimeter-based security to migrate to ZTA.

Lastly, Kindervag *et al.* built a case to improve network security by focusing on protecting data first. Teerakanok *et al.* provided steps on implementing and migrating to ZTA. Stafford *et al.* provided information on ZTA migration, models, and approaches. Kerman *et al.* (Kerman et al., 2020) also provided ZTA implementation scenarios for organizations. These studies are outdated and do not provide information on the tools or cost-effectiveness of implementing ZTA. This research paper discusses ways to implement ZTA within an organization while analyzing factual data to prove ZTA's cost-effectiveness. It also provides information on access authorization beyond legacy perimeter-based security.

Cost and Budget Analysis

Chase Cunningham (Cunningham, 2018) provided an overview of the tools to implement ZTA in a small-sized organization of roughly a hundred employees. He concluded that an organization needs to budget $45,000 to implement ZTA. Due to inflation and growth in cloud distribution technology, this amount calculated in Cunningham's article has changed. There exist limited studies on the cost and budget analysis of ZTA tools and resources. These research paper conducts a quantitative analysis of current and updated costs of tools and resources implemented regarding this new security approach.

Cost-Effectiveness

A study by Melanie English (English, 2021) focused on the cost-saving effects of ZTA. The article highlights that the importance of a precaution strategy to avoid malware attacks is more achievable than the money spent to save the organization when a breach occurs. The research conducted independently by the Ponemon Institute and reported by IBM provided information on the average costs organization spend and lost due to data breach events (IBM, 2021). IBM's report also provided financial information based on the number of records lost in data breaches. However, the studies on the cost-effectiveness of ZTA are limited. Melanie explained the cost-saving effect of ZTA under different implementation progress levels that organizations have carried out. IBM's report provided overall research of average costs spent on data breaches in previous years. This research paper calculates the reduced data breach risk by utilizing the average costs reported by IBM to focus on recent breach events of specific organizations and portray the cost-effectiveness of ZTA.

Ransomware Activities and Government Policies

The growth in cloud technology brings about an increase in its security and policies governing it (Ferretti et al., 2021). The introduction of ZTA occurred in 2010, but only recently have organizations begun looking for ways to implement the architecture. In terms of ransomware security through ZTA, there are limited studies available. This research provides insight into ZTA strengthening an organization's network security while aligning with government policies. The following are some related research on ZTA concerning ransomware activities and government policies.

Stafford *et al.* provided existing federal guidelines concerning ZTA plans, deployment, and operations. They emphasized ways ZTA would reinforce network security and protect organizations against common cyber threats. The President of Ericom presented ways for the implementation of Zero-Trust Network Access (ZTNA) to protect organizations against ransomware attacks (Canellos, 2021). The cybersecurity expert discussed that ZTNA defends organizations by preventing lateral movement in the event of a ransomware breach. Alevizos *et al.* (Alevizos, Ta, & Hashem Eiza, 2022) focused on reviewing ZTA augmented onto endpoints utilizing blockchain-based intrusion detection systems. Ali *et al.* (Ali et al., 2021) demonstrated ways ZTA mitigates cyber risks by implementing a multi-access edge computing architecture to uplift healthcare system. Sheng *et al.* (Liu, Zhuang, Huang, & Zhou, 2022) viewed ZTA as a way to ensure data security in cloud storage and demonstrated its efficiency by exploiting least significant bit embedded in pixels. Chen *et al.* (Chen et al., 2021) proposed a system which leveraged ZTA for a 5G-based smart medical platform to improve its security. The dark reading viewed ZTNA as a core component to protect organizations from ransomware attacks (Durbin, 2021). D'Angelo emphasized the benefits of public and private sectors partnering up and working together against sophisticated cyber-criminals (D'Angelo, 2021). Researchers in (Cunningham, 2020) presented ZTA as a means to reduce the risk of being victims of ransomware attacks but do not provide ways to reduce the risk.

Mistakes and Best Practices

Stafford's *et al.* paper described the threats that occur when implementing ZTA (Stafford, 2020). Threats like network disruption by an attacker or stolen credentials. Stafford's *et al.* paper does not provide any solutions to prevent or fix these threats. Kerman *et al.* discusses challenges occurring during the implementation of ZTA (Kerman et al., 2020). Kerman *et al.*

mentioned security issues, growth and change of vendor products supporting ZTA, and the unwillingness of employees to migrate to ZTA. Perez emphasized that some employees are not on the same page regarding ZTA implementation (Perez, 2021). These challenges are inevitable and correspond to some of the threats already listed in Stafford's *et al.* paper. Pietro *et al.* (Colombo, Ferrari, & Tümer, 2021) identified access control requirements in terms of internet of things (IoT), discussing significant challenges. Arntz briefly listed challenges organizations encounter during ZTA implementation (Arntz, 2020), and Fedor discusses that a breach is inevitable even with ZTA, but, at least, it prevents the breach from causing data loss or operation shut down (Fedor, 2021). Turner promoted a ZTA tool, StrongDM, by listing the obstacles that could occur when implementing ZTA (Turner, 2022). The article provided survey data of organizations struggling to implement ZTA even with the help of a third-party agency.

Furthermore, Teerakanok *et al.* (Teerakanok et al., 2021) introduced hindrances in the implementation of ZTA. Poremba (Poremba, 2021) penned that ZTA is untrustworthy, despite all its many benefits, and Craven (Craven, 2021) mentioned the primary challenge to ZTA's manageability. Tucker discussed the consistent increase in managing devices and users with ZTA. He mentions that some organizations currently employ the BYOD policy which restricts monitoring or controlling access to their network systems, thereby complicating the implementation of ZTA (Tucker, 2020). Notably, employees declare an invasion of privacy because BYOD is their private property. In such a case, organizations with the BYOD policy can implement policies and mechanisms governing BYOD (Mandal et al., 2021).

Although these previous studies mention mistakes, hindrances, or challenges occurring during ZTA implementation, they do not provide reasons to encourage organizations about the significance of investing in ZTA. Specifically, dealing with legacy systems is a big issue almost every organization will have to handle (Teerakanok et al., 2021). Most legacy systems do not support ZTA. Technology is dynamic and continues to grow every day. There are processes organizations can follow to migrate to ZTA. This research paper provides information on handling legacy systems when migrating to ZTA. No technology starts as perfect, and condemning the use of ZTA due to the lack of knowledge is unnecessary.

In conclusion, as ZTA continues to be recognized, organizations need information regarding ways ZTA strengthens its security system. Not only in terms of theoretical benefits but information on the types of attacks prevented by ZTA and the cost benefits. There are also limited studies regarding ZTA preventing ransomware or other cyber attacks. This research paper calculates updated prices for ZTA tools and resources, informing organizations of its availability in the market and an estimated cost to budget to invest in ZTA. It also provides a quantitative analysis showing the reduced data breach risk in organizations with ZTA built into their network system. More so, a data-driven analysis showing ZTA as a cost-effective approach to prevent cyber attacks is also conducted.

3. BACKGROUND

The concept of ZTA spiked when the Biden Administration signed an executive order to mandate the nation's cybersecurity (CISA, 2021). The term 'Zero-Trust' was introduced by John Kindervag in 2010 (Kindervag, 2010). John published a Forrester Research report to emphasize a zero-trust model promoting stricter cybersecurity efforts where no trust is given to anyone, inside or outside the organization's network (Kindervag, 2010). The ZTA is a form of security where identity is at the core. The identity refers to anything in need of authentication to access an organization's resources. Therefore, all traffic from inside or outside an organization is inspected and logged. Also, every identity is verified and authenticated continuously (DynamicCISO, 2020). The design of ZTA is to secure every aspect of an organization's digital footprint.

Benefits

ZTA provides numerous benefits. It improves the ability to quickly respond to any malicious attack, allowing fewer lateral movements (Craven, 2021). ZTA increases an organization's visibility on its network (Palo-Alto, 2022). Therefore, it promotes monitoring and detecting suspicious traffic more than other security strategies. ZTA introduces security across the entire digital attack surface and secures access to the organization's resources (Bertino, 2021). ZTA also allows organizations to adapt to remote work and cloud environments (Mandal et al., 2021). It secures every device and cloud environment listed as an asset in an organization. Organizations utilizing BYOD policies can also have secure access to resources with ZTA because each access point requires verification (Jack, 2021).

Market Share

The market size value of ZTA in 2021 was United States Dollars (USD) 22.06 billion (GrandViewResearch, 2021). ZTA prospects expect a revenue forecast of USD 59.43 billion by the end of 2028 if more organizations continue to adopt this architecture (Wood, 2021). The revenue forecast is a Compound Annual Growth Rate (CAGR) of 15.2% from 2021 to 2028 (Wood, 2021). The need to protect digital environments and prevent unauthorized access to critical data motivates the growth of ZTA's market. NIST selected 18 technology companies to demonstrate ZTA measures (Gunderman, 2021). The selected companies are major players in the market, offering ZTA security solutions to organizations. Some of these companies are Palo Alto Networks, IBM Corp., Microsoft Corp., McAfee Corp., and Cisco Systems, Inc. (Gunderman, 2021).

4. IMPLEMENTATION

ZTA relies on identity management, asset management, application authentication, network segmentation, policies, mechanisms, and threat intelligence factors (Cavalancia, 2020). In Fig. 4.1, the factors are divided across components defined by SMBs to show their interaction with one another (Stafford, 2020). The components are subject, resource, Policy Decision Point (PDP), Policy Enforcement Point (PEP), and supplement (Teerakanok et al., 2021). The working is explained below:

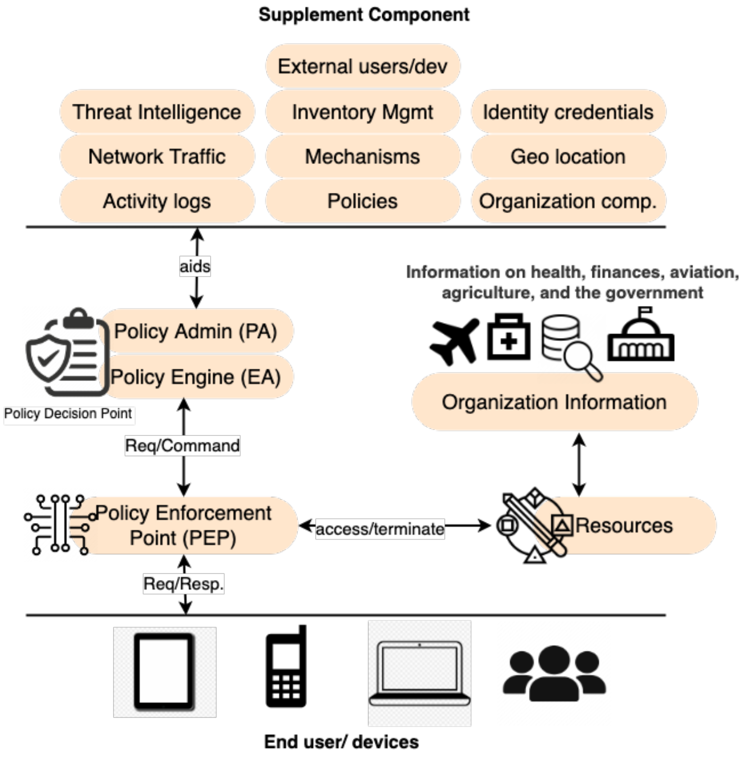


Figure 4.1. Detailed Architecture of ZTA Showing Components and Their Interactions.

- A subject is a user or any device that requests access to an enterprise resource. The devices include but are not limited to smartphones, laptops, smart TVs, and tablets (Teerakanok et al., 2021). The requests are sent from the subjects to the PEP.

- The PEP is a component on the organizations server enforcing policies for admission control and policy decisions in response to the requests. It forwards the request to the PDP and returns a response to the subject.
- The PDP decides on actions on the requests based on the application security policies (Teerakanok et al., 2021). It issues a command back to the PEP to either enable or terminate the communication between the subject and resource. Under the PDP component, the Policy Engine (PE) applies the applicable policies to the network security and the Policy Administrators (PA) administers and manages the organizations policies stored and received from the supplement component.
- The supplement component comprises of policies, activity logs and threat intelligence data to ensure decisions on requests are made according to the organizations safety (Teerakanok et al., 2021). In Fig. 4.1 the following supplements are mentioned:
  - Activity Logs – a detailed report on activities carried out on the organizations network.
  - Threat Intelligence – data to understand malicious actors techniques, motives, and targets.
  - Policies – laws and regulations to guide decisions and processes in the organization.
  - Organization Compliance – internal policies to comply with laws and sustain the organizations reputation.
  - Network Traffic – report of the amount of data accessing an organizations network at a period.
  - Mechanisms – report of data enforcing policies for organization's network system.
  - Geo Location – report of the location of users and devices accessing organization's network system.

  - Identity Credentials – usernames, emails , and passwords of users and devices accessing organization's network system.
  - Inventory Management – record of purchases and sales to help organization's keep track of assets and finances.
  - External Users and Devices – information of vendors, clients, third-party agencies, and partners with access to organizations network system.

- The resource component comprises of organizations assets, services, database, workflows and network accounts. This component includes information the subjects (users and devices) request access to access. Notably, information on finances, health, aviation and other sensitive data.

Implementation Guidelines

The implementation of ZTA is a strategic initiative supporting the component definitions in Fig. 4.1 (Cavalancia, 2020). Organizations should take different approaches to implement ZTA based on their needs, but the following steps are generic to serve as a basic guideline.

1. **Identify Devices and Users** – The identification of devices and users is a required step to implement ZTA. Organizations must manage inventory for their subjects and resources. ZTA involves identifying and controlling access to an organization's resource (Teerakanok et al., 2021). Organizations should identify resources and assets, including BYOD. Security Engineers or Policy Administrators should create inventories and user databases to help keep track of identified devices and users. Once created, organizations should put together policies and mechanisms to enforce continuous identification of devices and users requesting access to their resources (Kerman et al., 2020).
2. **Remove any Form of Trust** – ZTA focuses on zero-trust principles to achieve a state where every access request is verified (Cavalancia, 2020). This step removes implicit trust from all subjects. Every device and user located inside or outside corporate net-

works is treated the same by enforcing authentication before granting access to resources.

3. **Externalize Work flows** – In this step, the organization's PE performs service-level authorization to deny or grant access to resources using inputs from both internal and external sources. All communications are encrypted, and applications are externalized through an internet-facing PEP (Teerakanok et al., 2021). The PEP should receive inputs from external sources like threat intelligence feeds to improve its access to decision-making. Externalizing threat inputs will provide information about newly discovered attacks and vulnerabilities (Rose, Borchert, Mitchell, & Connelly, 2020).

These steps are performed in parts to reduce work clusters and allow organizations to continue utilizing legacy systems before fully migrating to ZTA. Once organizations have followed and completed the steps for implementing ZTA, they can customize a step-by-step approach to gradually move more data, devices, or assets from their legacy network to ZTA.

Migration Guidelines

Migrating an organization's network security to ZTA, an organization's security engineer should consider the following.

1. **Assess and Identify** – In this step, security engineers understand the organization's subject component. Specifically, users and devices. The engineers identify and monitor all related assets (hardware, software, and digital certificates) and build techniques to configure, manage, and observe their assets, such as inventories or databases (Teerakanok et al., 2021). If the organization enforces the BYOD policy, the security engineers and other stakeholders develop policies and mechanisms to govern personal devices used to access their resources (Jack, 2021).
2. **Risk Assessments and Prioritization** – In this step, the security engineers compile risk assessments to identify and rank the organization's operations based on importance (Teerakanok et al., 2021). The results show areas of the organization with less

impact on operations if migration to ZTA begins. Once a specific area of the organization is selected, policies and mechanisms developed in the first step can be improved to oversee the migration. This step allows employees to grasp the migration process and notice the impact of ZTA on their network security (ZPE, 2022).

3. **Utilization of Drafted Policies and Mechanisms** – In this step, the security engineers utilize drafted policies and mechanisms to begin the deployment of ZTA. They review the documents to detect mistakes to improve the next migration cycle. The security engineers document each process and result, jot down patterns, and monitor processes (Teerakanok et al., 2021).

This approach is a significant way to effectively migrate to ZTA without disrupting the organization's daily operations (Palo-Alto, 2022). The implementation and migration to ZTA require ongoing monitoring and analysis of established policies based on current activities and emerging threats (Cavalancia, 2020). There are available tools supplying services like identity access management, endpoint protection, monitoring and logging services, and data encryption necessary for ZTA implementation. Section 6 provides in-depth information relating to tools, resources, and estimated costs organizations expect to budget.

5. PROVIDERS AND OTHER SOLUTIONS

This section provides an analysis of various ZTA tool providers and solutions. It focuses on all-in-one solutions with features relating to all components of ZTA and open-source ZTA tools readily available for anyone to use.

Price Analysis of Google and Microsoft's Services

In this work, a study of Google (Prokopets, 2022) and Microsoft (Zelleke, 2021) shows that the providers offer similar services such as data storage, data and email encryption, and Identity Access Management (IAM). These providers are among the trusted and secured service providers in 2022 (Prokopets, 2022). Fig. 5.1 visualizes insights of the yearly budget organizations should expect. The cost in Table 6.2 is calculated based on the number of employees in an organization. Fig. 5.1 shows that although both tools offer similar services, the cost for Google Workspace is expensive compared to that of Microsoft OneDrive.

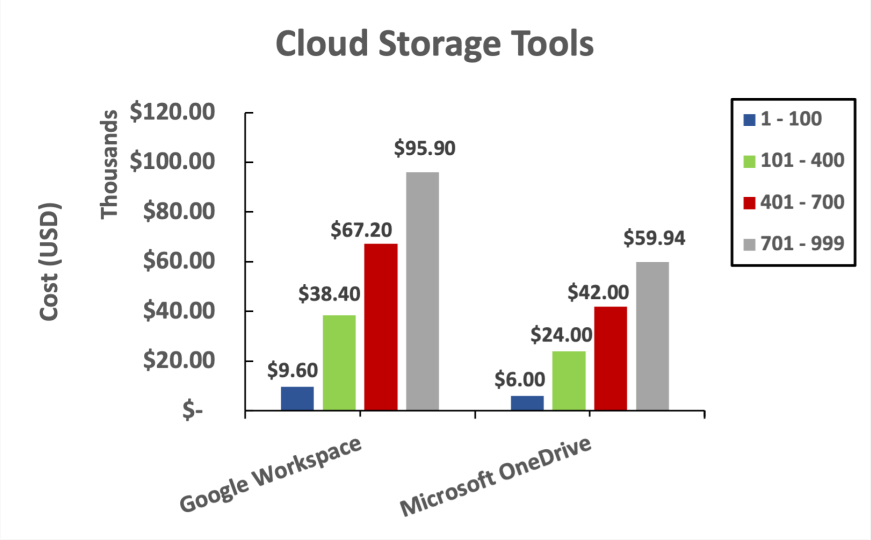


Figure 5.1. Comparing Google and Microsoft's Service Prices with Organization Sizes.

All-in-One Zero-Trust Solutions

There are all-in-one zero-trust solutions available to apply ZTA policies with minimal effort or cost (Sharma, 2021). Amongst the available zero-trust solutions, Perimeter81 offers features like activity audits and reports, unlimited data usage, cloud network management platform, web-based secure application access, user portal, device posture checks, dedicated solution architect, and zero-trust policy-based segmentation supporting each component of ZTA. The device posture checks protect the organizations' subjects. The cloud network management platform supports organization resources. A dedicated solution architect handles the PDP and web-based secure application access managing the PEP. Lastly, audits and reports are items of ZTA's supplement component necessary for decision making. Perimeter81 offers four different plans ranging from basic to enterprise (Perimeter81, 2022). This research provides detailed pricing information on the Enterprise Plan from an inquiry made to a Perimeter81 Cybersecurity advisor. The Enterprise plan starts at $25 monthly per user and $50 per month per gateway with an additional add-on of a $50 gateway per 50 users for latency reasons. It costs $78,000.00 to implement Perimeter81 solution in an organization with 250 member licenses and maximum five gateway licenses. Other Zero-trust solutions available in the market are Wandera, Okta, and Cloudflare Access providing organizations with a wide range of services (Sharma, 2021).

Open Source Software Tools

There are open-source ZTA tools available; however, organizations avoid implementing open-source ZTA tools because they are considered untrustworthy and lack software integrity (Schwartz, 2021). ZTA solution providers offer free trials to allow organizations, especially startups. The free trial is for a limited period, but organizations will be able to try out ZTA services before fully committing to purchasing their solution. ZTA solutions with free trials are Duo Security, Better Cloud, and NetMotion (G2, 2021b).

This research paper conducts a cost/budget analysis of ZTA to allow organizations to make more informed decisions of whether to invest in ZTA to improve their network security. Table 6.1 and 6.2 shows the cost/budget analysis and serves as a starting guide for organizations. The average budget for ZTA implementation is incomparable to the cost spent on data breaches. With the rise of technology, Artificial Intelligence (AI), and cloud storage, the cost of data breaches reached an all-time high of $4.24 million in 2021 (English, 2021). Cyberattacks have become consistent, but organizations can save tens of millions of dollars over a period by implementing ZTA (English, 2021).

6. COST AND BUDGET ANALYSIS

The implementation of ZTA depends on the number of employees in an organization and their business needs. An organization's budget changes from time to time. The cost/budget analysis of ZTA tools on an annual basis is depicted in Table 6.1. The costs shown in Table 6.1 are retrieved from distributors or ZTA services providers and select the employee counts based on the size of SMBs. These prices are current as of 2022 but may grow over time. As shown in Table 6.1, the calculations is for organizations with employee counts between 0 to 1000.

Table 6.1 displays tools selected from well known solution providers like Google, Kaspersky, and Microsoft. The costs are derived as shown in Table 6.1 by multiplying the employee count of the company with the unit cost of the tool per year. The base formula is eq. 6.1.

$$s \times u \tag{6.1}$$

where s represents the employee count of the organization and u represents the unit cost of each tool per user. As shown in Table 6.1, the unit cost of Virtru Encryption services is \$948 per 5 users (G2, 2022). In an SMB organization with 400 employee count, the cost to implement Virtru encryption is $400 \times \frac{948}{5} = \$75,840.00$. The cost for security engineers is calculated using \$60 per hour (Salary, 2022). The cost for one security engineer in each organization type is, $\$60 \times h \times avgWeekHours$, where \$60 is the average cost, h is the number of hours the employee works per week, and $avgWeekHours$ is the number of yearly work hours (4 weeks in 12 months $= 48$). Table 6.1 shows an organization with a size of 700 employees having a security engineer who maintains and modifies the ZTA tools work for an average of 20h/week. The average total cost for this security engineer is $60 \times 20 \times 48 = 57600$. Hence, the security engineer costs \$57,600.00 annually. Another selected tool is Microsoft OneDrive. Microsoft OneDrive offers 1TB for \$60 per user. For an SMB organization of 100 users with access to the organization's resources, the price for Microsoft OneDrive is $100 \times 60 = \$6,000$. Providers often offer discounts when organizations buy in bulk (Prokopets, 2022).

Table 6.1. ZTA Tools and Current Prices as of 2022

Tools and Resources	ZTA Component	Unit Cost (u) per Year	Cost Based on the Number of Employees in an Organization			
			1 - 100	101 - 400	401 - 700	701 - 999
CylancePROTECT for Endpoint Protection (Cylance, 2022)	Subject and Resources	$45 per endpoint for 1-250 endpoints. $41.75 per endpoint for 501 - 1000 endpoints	$4,500.00	$16,700.00	$29,225.00	$41,708.25
Kaspersky Security for Business with encryption services (G2, 2021a)	Data Encryption - Subject, Resources, and PEP Endpoint Protection - Subject and Resources	$45 per node	$4,500.00	$18,000.00	$31,500.00	$44,955.00
Google Workspace for Cloud-based Storage and Access Control (Prokopets, 2022)	Access Control - PE in PDP Data Encryption - Subject, Resources, and PEP Cloud Storage - Resources	2TB pooled cloud storage for $96 per user	$9,600.00	$38,400.00	$67,200.00	$95,904.00
Microsoft OneDrive (Prokopets, 2022)	Access Control - PE in PDP Data Encryption - Subject, Resources, and PEP Cloud Storage - Resources	1 TB for $60 per user	$6,000.00	$24,000.00	$42,000.00	$59,940.00
Virtru Encryption (G2, 2021c)	Subject, Resources, and PEP	$948 per 5 user	$18,960.00	$75,840.00	$132,720.00	$189,410.40
Microsoft Azure Active Directory for Access Control (Zelleke, 2021)	PE in PDP	Comes free with Microsoft OneDrive or $72 per user separately	$7,200.00	$28,800.00	$50,400.00	$71,928.00
Security Engineer (Salary, 2022)	PA in PDP	$60 per hour	5h/week $14,400.00	10h/week $28,800.00	20h/week $57,600.00	30h/week $86,400

Some of the tools listed provide multiple services for a cost. Microsoft OneDrive and Microsoft Azure Directory services are a package deal providing data encryption, identity access management, and cloud storage to organizations (Prokopets, 2022).

Google Workspace provides cloud-based storage tools, encryption services, and identity access management(Prokopets, 2022). Kaspersky also offers multiple services, endpoint security and encryption services, at a cost.

The tools listed in Table 6.1 are utilized as follows based on the components of ZTA mentioned in Fig. 4.1.

1. The PA is the security engineer who continuously oversees regulating, monitoring, and modifying the PE in the PDP.
2. Google Workspace and Microsoft Azure Directory fall under the PE component. These tools allow the PA to manage access requests to the organization's resources. Google Workspace and Microsoft Azure Directory also fall under the supplement component of ZTA because they offer logging and monitoring services. The PA can utilize these tools to create documents and reports.
3. Data encryption is an important security measure during the implementation of ZTA (Teerakanok et al., 2021). Data encryption should encompass the devices and users requesting access to resources and the data flowing within the organization's network for both internal and external sources. Kaspersky Security for Business (G2, 2021a) and Virtru Encryption (G2, 2021c) tools provide this encryption service.
4. With the rise of cloud technology, organizations utilize cloud storage. In this study, The cost-effectiveness of Google Workspace and Microsoft OneDrive tools is analyzed to provide secured cloud storage (Prokopets, 2022). These tools are selected from two of the most trusted and secured cloud storage providers. These tools fall under the resource component of ZTA, where cloud storage holds the organization's assets. In addition to cloud storage, Google and Microsoft also provide email protection services.

5. Endpoint protection secures an organization's resources like services and Internet of Things (IoT) devices (Chandel, Yu, Yitian, Zhili, & Yusheng, 2019). In this study, CylanceProtect and Kaspersky Endpoint Protection for Business are selected to protect the subject and resource components of ZTA. CylancePROTECT utilizes Artificial Intelligence (AI)-based protection to stop cyberattacks and breaches before they occur, and Kaspersky combines multi-layered security with control tools for network security. The selection of these tools is because the ZTA approach is multi-layered and invests in the work of AI.

As mentioned in Section 4, organizations customize ZTA based on their needs and employee count. Table 6.2 shows a budget analysis based on select combinations of ZTA tools listed in Table 6.1. The combination of these tools changes depending on an organization's business needs. In this work, different scenarios are analyzed where organizations implement ZTA tools using various combination as shown in Table 6.2.

Scenario 1: Organizations offering remote work

An organization has employees seeking easy and secure access to their resources from any work location. The organization has 100 employees where 50% are working remotely. In this scenario, ZTA is implemented to secure access for both on and off-premises requests with Google Workspace and Kaspersky Endpoint Security for Business. Google Workspace provides a secure cloud storage space, email encryption, and identity access management, while Kaspersky is a multi-layered endpoint security system for small and large organizations. The implementation of these tools will strengthen their network security for an estimated budget of $28,500, which includes the salary of a security engineer, as calculated in Table 6.2.

Table 6.2. Budget Analysis of ZTA Tools

Tool Selections												
Cloud Storage		Access Control		Endpoint Protection		Data Encryption		Security Engineer	ZTA budget for an SMB based on the number of employees			
Google Workspace	Microsoft OneDrive	Google Workspace (comes with cloud storage)	Microsoft Azure Active Directory (comes with Microsoft OneDrive)	Cylance-PROTECT	Kaspersky Security	Kaspersky Security	Virtru Encryption		1 - 100	101 - 400	401 - 700	701 - 999
✗		✗		✗			✗	✗	$47,460.00	$159,740.00	$286,745.00	$413,422.65
	✗		✗		✗	✗		✗	$24,900.00	$70,800.00	$131,100.00	$191,295.00
	✗		✗	✗			✗	✗	$43,860.00	$145,340.00	$261,545.00	$377,458.65
✗		✗			✗	✗		✗	$28,500.00	$85,200.00	$156,300.00	$227,259.00

Scenario 2: Organizations collaborating with vendors across boundaries

There is a collaboration across organizational boundaries, where employees of two different organizations need access to each other resources. These employees are not on either organization's network but host their resources in the cloud. In this scenario, an organization with 400 employee headcounts implements tools where employees of the first organization installs a software agent on their device. CylanceProtect is an example of one such product that provides ZTA software agents. It encrypts and ensures access to the second organization's resources. Other tools that may be implemented are Microsoft One drive, Virtru, and Microsoft Azure Active Directory to track and monitor the activities of employees from the second organization. The estimated total cost to budget for these tools is $145,340.00, which includes the salary of a security engineer.

Table 6.2 shows the cost spent on ZTA tools and resources, ranging from $24,900.00 to $413,422.65. These costs recur yearly, depending on the number of employees in the SMBs. This table indicates a relatively economical budget that provides secure cloud storage, email and data encryption, identity and access management, endpoint protection, and a dedicated software engineer to maintain and modify the new network security.

7. COST-EFFECTIVENESS

A report released by IBM shows the global average cost of data breaches rising from $3.86 million to $4.24 million in the year 2021 (IBM, 2021). The cost is the highest average total recorded in IBM's history. The report shows remote work as one of the factors causing the increase in breaches to an average of $1.07 million. Organizations like Microsoft (Chik, 2022), Palo Alto Corporation, and IBM Corporation (Gunderman, 2021) with fully implemented ZTA approach, experienced a 42.3% savings on data breach costs (IBM, 2021). Specifically, the average cost of data breaches for organizations with fully implemented ZTA is $1.76 million lower than organizations with no ZTA, having an average cost of $5.04 million. Cyber attacks are detected and contained 27% slower in organizations with no ZTA than in organizations investing in a ZTA approach (IBM, 2021).

In IBM's report, it shows that ZTA helps to mitigate data breaches and reduce recovery time. The effectiveness of ZTA on mitigation, detection, and recovery time is analyzed in Table 7.1 which shows the effects of ZTA on incident response lifecycle an insider attacks. ZTA is a step-by-step process to give organizations, employees, and vendors enough time to grasp its approach. ZTA is effective within an organization, whether partially or fully deployed (IBM, 2021). Organizations can implement (IAM), Policies (P), Data Encryption (DE), and Endpoint Protection (EP) separately based on their needs.

Table 7.1. The Effects of ZTA on Incident Response Lifecycle and Insider Attacks

Data Breach Attributes	**IAM**	**P**	**DE**	**EP**	**Full**
Recovery Time	✓	✓	✓	✓	✓
Detection Time	✓	✗	✓	✓	✓
Insider Jobs	✗	✗	✗	✗	✓
Mitigation	✓	✓	✓	✓	✓

Table 7.2. Average Breach Costs Based on Organization's Employee Headcount (millions)

Years	Less Than 500	501 to 1000	1001 to 5000	5001 to 10000	10001 to 25000	More than 25000
2019	$2.74M	$2.65M	$3.63M	$4.41M	$4.35M	$5.11M
2020	$2.35M	$2.35M	$3.78M	$4.72M	$4.61M	$4.25M
2021	$2.98M	$2.63M	$4.09M	$5.15M	$5.52M	$5.33M

Table 7.3. Target's Financial History

	2015	2016	2017	2018	2019	2020	2021
Number of Employees	347000	341000	323000	345000	360000	368000	409000
Information Technology, Distribution & Other Costs	$773M	$587M	$620M	$568M	$811M	$917M	$600M
Data Breach Costs	$39M	-	$292M	-	-	-	-
Revenue	$74,494M	$70,271M	$72,714M	$75,356M	$78,112M	$93,561M	$103,328M

The Full-stack ZTA implementation provides the ability to limit users' access to the network resources preventing an attacker from freely moving laterally throughout the network's applications (Palo-Alto, 2022). Implementing only IAM tools reduces unauthorized access of malicious attackers from accessing restricted and critical resources. However, in the case of an insider job, IAM will not be enough to prevent an attack. Consider a scenario where the insider is a member of the administrative personnel in charge of monitoring and managing ZTA. The insider knows the details of ZTA deployment processes. It will be hard to detect the data breach through partially deployed ZTA.

DE and EP are other aspects of ZTA. Organizations and their vendors maintain high data protection standards and limit unauthorized decryption of critical files when using ZTA. After a data breach event, organizations spend less time and money reimaging their servers, rebuilding their network security, or implementing strong encryption algorithms. Table 7.1 shows that partially or fully deployed ZTA helps to mitigate, reduce detection and containment time, and speed up recovery time.

A quantitative evaluation of the reduced risk of data breaches is conducted due to the utilization of ZTA. The following case studies provide information on SMBs to enterprise-level organizations that recently experienced a data breach.

Case Study – 1: Target Data Breach

In 2013, a malicious actor accessed Target's servers with stolen credentials from a Heating, Ventilation, and Air Conditioning (HVAC) company (Vijayan, 2014). The HVAC employee had access rights to monitor energy consumption and temperatures at various Target stores through a remote network. The hackers used the credentials to gain access and planted data-stealing malware to steal 110 million records. Specifically, 40 million debit and credit card records and 70 million customer records (Vijayan, 2014). It took Target almost two weeks to detect the breach and more than three weeks to notify their customers (Sobers, 2020). Target declared in the US Securities and Exchange Commission (SEC) 2016 10-K report to incur $292 million on expenses relating to the data breach. The organization spent $90 million on insurance, recoveries and $202 million on other affected areas (Target, 2017). Notably, lost businesses and costs to rebuild their network security and infrastructure (Target, 2017). The expenses added up over the years from 2014 to 2016, as affected customers continued to pursue legal charges, and fines for privacy and compliance laws violations were issued (Target, 2017).

Table 7.4. Target's Initial ZTA Implementation Cost

	2021
Number of Employees	409,000
Information Technology, Distribution & Other Costs	$ 600,000,000.00
IT budget	$ 90,000,000.00
ZTA costs	**$ 43,060,200.00**
Difference (IT Budget - ZTA Cost)	$ 46,939,800.00

The number of Target employees in 2021 is 409,000 (MacroTrends, 2022). This employee headcount places Target under the average cost of data breaches for organizations with more than 25,000 employee headcounts shown in Table 7.2. Table 7.3 shows the expenses by Target in building their network security and other infrastructures over the years. Table 7.4

shows $43,060,200 as the estimated cost Target spends to implement ZTA using the tools listed in Table 6.1. This cost is calculated using the formula postulated in Section 6. This ZTA cost is 14.75% of the cost spent towards the data breach.

Case Study – 2: Uber Data Breach

Table 7.5. Uber's Financial History

	2018	2019	2020	2021
Number of Employees	22263	26900	22800	29300
Information Technology, Distribution & Other Costs	$70M	$59M	$460M	$653M
Data Breach Costs	-	-	-	$158,750K
Revenue	$11,270M	$14,147M	$11,139M	$17,455M

In 2016, hackers gained access to 57 million records of Uber customers and drivers worldwide. The hackers breached Uber's network using an access key unintentionally posted on a code-sharing website, GitHub, by developers (Uber, 2022). Uber decided and paid the hackers $100,000 to delete the stolen data (Sobers, 2020). This action resulted in massive fines from government agencies. In 2021, Uber settled the data breach costs by agreeing with the attorney's general to pay $148 million for failure to report the breach on time, notably, a year. The UK, Dutch, and French regulators charged Uber $1.6 million. Uber is also required to pay $9.15 million to the California Public Utilities Commission (CPUC) for not producing information in their 2019 US safety report (Uber, 2022). These fines sum up to a total cost of $158,750,000 for the 2016 data breach.

The number of Uber employees in 2021 is 29,300 worldwide (Dean, 2021) placing the organization under the average cost of data breaches for organizations with more than 25,000 employee headcounts shown in Table 7.2. Uber's financial history in Table 7.5 shows an increase in the budget for technology and the number of employees over the years. Table

Table 7.6. Uber's Initial ZTA Implementation Cost

Uber ZTA Cost	**2021**
Number of Employees	29,300
Information Technology, Distribution & Other Costs	$ 653,000,000.00
IT budget	$ 97,950,000.00
ZTA costs	**$ 3,191,700.00**
Difference (IT Budget - ZTA Cost)	$ 94,758,300.00

7.6 shows $3,191,700 as the estimated cost Uber spends to implement ZTA using the tools listed in Table 6.1. This ZTA cost is 2.01% of the cost spent towards the data breach.

Case Study – 3: Utah Food Bank

Utah Food Bank is a non-profit organization with 51 – 200 employees (Utah Food Bank, 2022). In 2015, the organization experienced a security breach leading to the disclosure of 10,000 donors' personal information (Mckellar, 2015). The organization discovered a vulnerability allowing unauthorized access to donation data submitted by clients through their website. The breached data exposed names, addresses, emails, and financial details from a timeframe between Oct. 8, 2013, and July 16, 2015. The organization notified its donors (both the affected and unaffected), strengthened its network security, and hired security and legal experts. Although Utah Food Bank has not disclosed the data breach expenses, the average cost per record provided in IBM's report is utilized to calculate an estimated data breach cost the organization faces.

Table 7.7. Utah Food Bank's Initial ZTA Implementation Cost

	2021
Number of Employees	51 - 200
Development Costs	$ 2,035,900.00
IT budget	$ 305,385.00
ZTA costs	**$ 159,740.00**
Difference	$ 145,645.00

The average data breach cost per record in 2015 and 2021 is \$154 and \$161, respectively (IBM, 2021). The total estimated cost towards data breach is the average cost per record × the number of stolen records. That is, \$154 × 10000 = \$1,540,000 in 2015 and \$161 × 10000 = \$1,610,000 in 2021.

Utah Food Bank's employee headcount places the organization under the average cost of \$2.98 million on data breaches for organizations with less than 500 employees, as shown in Table 7.2. Table 6.2 shows a calculated average of at most \$159,740 to implement ZTA in an organization of fewer than 400 employees. This cost is further analyzed after calculating the reduced data breach risk.

Modeling Reduced Data Breach Risk

The aim of calculating the reduced data breach risk is to depict the cost-saving effect of ZTA as organizations invest in the approach for four years. ZTA prevents several risks introduced by several security threats like unauthorized access, phishing, and ransomware attacks (Forrester, 2021). Hence, ZTA reducing the likelihood of compromised accounts leads to the reduction of data breaches. Utilizing the information from the case studies earlier in this section, the reduced risk of data breaches for a 4-year projection is calculated with the following attributes.

- Average cost of a data breach through employee headcount (IBM, 2021).
- The average likelihood an organization will experience a data breach of 10,000 records or more is 29.6% in two years. Hence, 14.8% likelihood in a year.
- The average percentage of risk exposure with ZTA. By deploying ZTA within an organization, there's a reduction of risk exposure by an average of at least 37% (Reed, 2021).

The percentage of risk exposure from one to four years is calculated by incrementing the progress percentage for each stage of ZTA an organization acquires per year to 37%. The model used is stated below in eq. 7.1.

$$P_n = \frac{Y_n}{Y_{n-1}} + P_{n-1} \tag{7.1}$$

where P_n is the percentage of ZTA progress in the current year, Y_n is the average cost of data breaches with ZTA in the current year, Y_{n-1} is the average cost of data breaches with ZTA in the previous year, and P_{n-1} is the percentage of ZTA progress in the previous year.

The model to calculate the reduced data breach risk is

$$R_B = (\mathscr{X}' \times AL - \mathscr{X}) \times (AL \times (1 - RL)) \tag{7.2}$$

Where $\mathscr{X}'$ represent the no ZTA average cost of data breaches, AL is the average likelihood of a data breach occurring, $\mathscr{X}$ is the average cost of data breach with ZTA, and RL is the reduced likelihood a data breach will occur with ZTA.

A downward risk adjustment of 20% (Forrester, 2021) is accounted for in this analysis due to changes in the average cost of data breaches, inflation, inaccurate ZTA implementation, or loss of employees resulting from the renunciation of ZTA. Tables 7.8 and 7.9 show the calculated values of risk exposure, the total reduced data breach risk, and the adjusted total reduced data breach risk of four years.

Analysis and Discussion

The case studies are analyzed to compare the cost of implementing ZTA to the cost spent on their network security without ZTA. Organizations spend 10% to 15% of their Information Technology (IT) budget on cybersecurity and related infrastructure (Gatefy, 2021). The costs to implement ZTA for each case study is calculated using the tools listed in Table 6.1 and the formula postulated in Section 6. Specifically, to calculate the initial ZTA cost, the average cost for endpoint protection, \$45 per node, the average cost for access control and data encryption services, \$60 per user, and the average cost for a security engineer, \$60 per hour in a 40 work hours per week system is collected. Lastly, the benefit of ZTA based on the reduced data breach risks in Tables 7.8 and 7.9 is analyzed.

Target budgets \$43,060,200 to implement ZTA using the tools mentioned in Table 6.1. The current network security budget is \$90,000,000, achieved by computing 15% of their Information Technology, Distribution, and others cost of \$600,000,000.

Table 7.8. Reduced Data Breach Risk Analysis for Organizations with More Than 25,000 Employee Headcount

Attributes	Source	Year 1	Year 2	Year 3	Year 4
Average cost of data breach without ZTA ($\mathscr{X}'$)	IBM & Ponemon Institute	\$ 5,330,000.00	\$ 5,330,000.00	\$ 5,330,000.00	\$ 5,330,000.00
Average cost of data breach with ZTA ($\mathscr{X}$)	IBM & Ponemon Institute	\$ 4,380,000	\$ 3,710,000	\$ 3,280,000	\$ 3,075,410
Difference in average costs	$= (\mathscr{X}' - \mathscr{X})$	\$ 950,000	\$ 1,620,000	\$ 2,050,000	\$ 2,254,590
Average Likelihood of Data Breach (AL)	Forrester Research (%)	0.148	0.148	0.148	0.148
Reduced Likelihood of Data Breach (RL)	Forrester Research (%)	0.37	0.52	0.64	0.75
Reduced data breach risk	$= (\mathscr{X}' \times AL - \mathscr{X}) \times (AL \times (1 - RL))$	**\$ 380,448.80**	**\$ 526,928.84**	**\$ 613,547.62**	**\$ 676,096.70**
Risk Adjustment	Forrester Research by 20%	0.20	0.20	0.20	0.20
Reduced data breach risk (adjusted)		**\$ 304,359.04**	**\$ 421,543.07**	**\$ 490,838.09**	**\$ 540,877.36**
	Total Reduced Data Breach Risk	\$ 2,197,021.96		**Total Adjusted Reduced Data Breach Risk (Present Value)**	\$ 1,757,617.56

Table 7.9. Reduced Data Breach Analysis for Organizations with Less Than 500 Employee Headcount

Attributes	Source	Year 1	Year 2	Year 3	Year 4
Average cost of data breach without ZTA ($\mathscr{X}'$)	IBM & Ponemon Institute	\$ 2,980,000.00	\$ 2,980,000.00	\$ 2,980,000.00	\$ 2,980,000.00
Average cost of data breach with ZTA ($\mathscr{X}$)	IBM & Ponemon Institute	\$ 4,380,000	\$ 3,710,000	\$ 3,280,000	\$ 1,719,460
Difference in average costs	$= (\mathscr{X}' - \mathscr{X})$	\$ (1,400,000)	\$ (730,000)	\$ (300,000)	\$ 1,260,540
Average Likelihood of Data Breach (AL)	Forrester Research (%)	0.148	0.148	0.148	0.148
Reduced Likelihood of Data Breach (RL)	Forrester Research (%)	0.37	0.52	0.64	0.75
Reduced data breach risk	$= (\mathscr{X}' \times AL - \mathscr{X}) \times (AL \times (1 - RL))$	**\$ 32,648.80**	**\$ 179,128.84**	**\$ 265,747.62**	**\$ 378,005.28**
Risk Adjustment	Forrester Research by 20%	0.20	0.20	0.20	0.20
Reduced data breach risk (adjusted)		**\$ 26,119.04**	**\$ 143,303.07**	**\$ 212,598.09**	**\$ 302,404.23**
	Total Reduced Data Breach Risk	\$ 855,530.54		**Total Adjusted Reduced Data Breach Risk (Present Value)**	\$ 684,424.43

The budget to implement ZTA is 7.18% of the current information technology costs. Specifically, $46,939,800 less than the current network security budget as shown in Table 7.4. Table 7.2 shows an average data breach cost of $5.33 million for organizations with more than 25,000 employees. Target houses 409,000 employees, which results in an adjusted total reduced data breach risk of $2,197,021.96 in a span of 4-year as shown in Table 7.8.

Uber budgets $3,191,700 to implement ZTA using the tools mentioned in Table 6.1. Their current network security budget is $97,950,000, achieved by computing 15% of their Information Technology, Distribution, and other costs of $653,000,000 in Table 7.6. The budget to implement ZTA is 0.49% of the current information technology costs. Specifically, $94,758,300 less than the current network security budget as shown in Table 7.6. Similar to the target case study, the adjusted total reduced data breach risk for Uber, housing 29,300 employees, is $2,197,021.96 in a span of 4-year as shown in Table 7.8 and depicted in Fig. 7.2.

Utah Food Bank budgets at most $159,740 to implement ZTA using the tools mentioned in Table 6.1. Their current network security budget is $305,385, achieved by computing 15% of their development costs of $2,035,900 (Utah Food Bank, 2021) in Table 7.7. The budget to implement ZTA is 7.85% of the development cost. Specifically, $145,645 less than the current network security budget as shown in Table 7.7. Table 7.2 shows an average data breach cost of $2.98 million for organizations with less than 500 employees. Utah Food Bank has 51 - 200 employees, resulting in an adjusted total reduced data breach risk of $684,424.43 in a span of 4-year as shown in Table 7.9 and depicted in fig 7.1.

These findings demonstrate that ZTA implementation costs less and reduces the risk of data breaches, contrary to the current network security infrastructure without ZTA. Fig. 7.3 shows the 4-year projection estimate of reduced data breach risks (adjusted and unadjusted) of organizations per employee headcount of 0 to more than 25000.

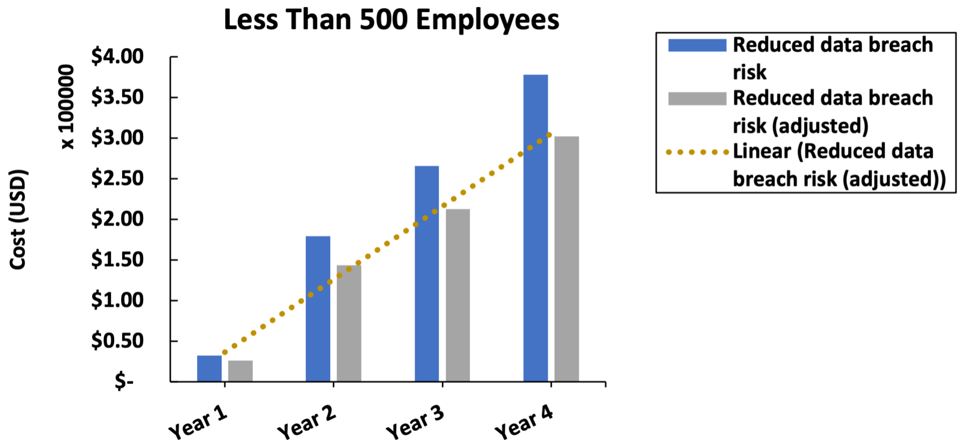


Figure 7.1. Reduced Breach Risk Analysis for Organizations with Less Than 500 Employees

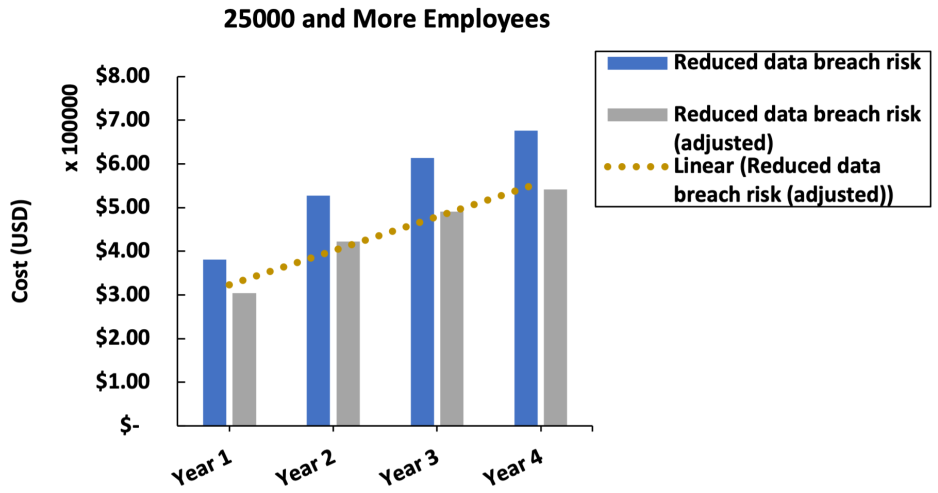


Figure 7.2. Reduced Breach Risk Analysis for Organizations with More Than 25000 Employees

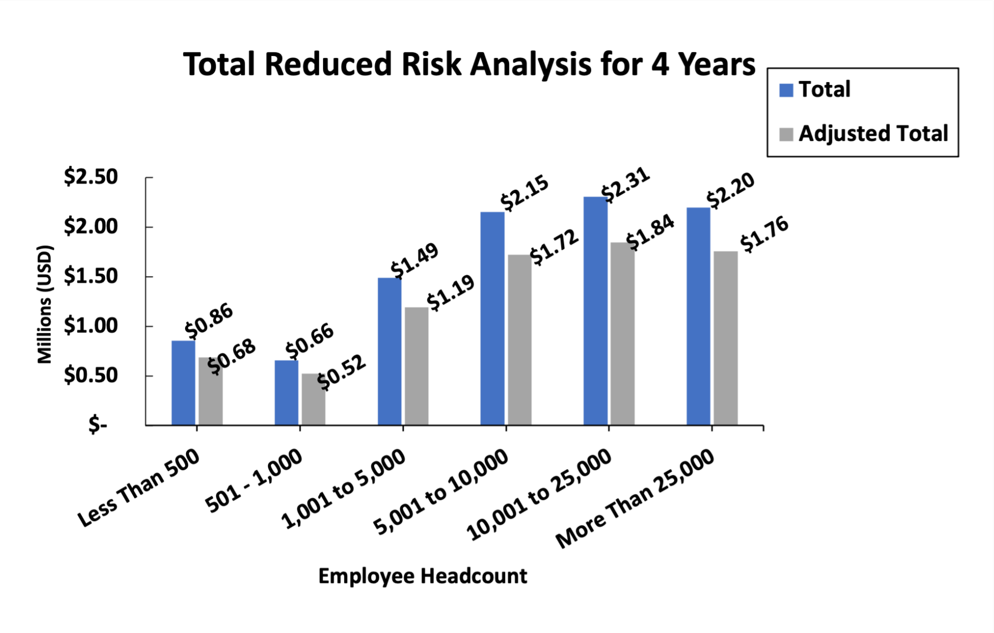


Figure 7.3. Reduced Breach Risk Analysis for Organizations Per Employee Headcount

8. CONCLUSION AND FUTURE DIRECTIONS

This research aimed to showcase a cost and budget analysis of ZTA tools and resources. The prices of available ZTA tools, including all-in-one solutions like Perimeter81 and tools with free trial plans are provided in this work. The research also aimed to demonstrate the cost-effectiveness of investing in ZTA. The costs of implementing ZTA and the reduced data breach risk of investing in ZTA is computed in this work. Based on the quantitative analysis in Section 7, implementing ZTA proposes a significant effect on both SMBs and enterprise-level organizations.

ZTA is not a simple cybersecurity measure. It is a collection of actions used to reinforce an organization's network security and save them from excessive financial loss during data breach events. As technology grows and changes in economy occurs, costs become outdated. The growth in technology also impacts ZTA. Its implementation processes may change or improve. More all-in-one solutions may become available, making it easier to implement within organizations. Hence, to better understand the implications of this work findings, future studies could be conducted to update the financial values relating to the implementation of ZTA and address the changes and improvements in ZTA.

REFERENCES

Alagappan, A., Venkatachary, S. K., & Andrews, L. J. B. (2022). Augmenting zero trust network architecture to enhance security in virtual power plants. *Energy Reports*, *8*, 1309–1320.

Alevizos, L., Ta, V. T., & Hashem Eiza, M. (2022). Augmenting zero trust architecture to endpoints using blockchain: A state-of-the-art review. *Security and Privacy*, *5*(1), e191.

Ali, B., Gregory, M. A., & Li, S. (2021). Uplifting healthcare cyber resilience with a multi-access edge computing zero-trust security model. In *2021 31st international telecommunication networks and applications conference (itnac)* (pp. 192–197).

Al-Ruwaii, B., & De Moura, G. (2021). Why the time has come to embrace the zero-trust model of cybersecurity. *WE Forum*.

Arntz, P. (2020). Explained: the strengths and weaknesses of the zero trust model. *Malware Bytes Lab*.

Bertino, E. (2021). Zero trust architecture: Does it help? *IEEE Security & Privacy*, *19*(05), 95–96.

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*, *110*, 102436.

Campbell, M. (2020). Beyond zero trust: Trust is a vulnerability. *Computer*, *53*(10), 110-113. doi: 10.1109/MC.2020.3011081

Canellos, D. (2021). Midsize organizations implementing zero trust security: Simple equals smart. *Forbes Technology Council*.

Cavalancia, N. (2020). Zero trust architecture explained. *AT & T CyberSecurity*.

Chandel, S., Yu, S., Yitian, T., Zhili, Z., & Yusheng, H. (2019). Endpoint protection: Measuring the effectiveness of remediation technologies and methodologies for insider threat.

In *2019 international conference on cyber-enabled distributed computing and knowledge discovery (cyberc)* (p. 81-89). doi: 10.1109/CyberC.2019.00023

Chen, B., Qiao, S., Zhao, J., Liu, D., Shi, X., Lyu, M., ... Zhai, Y. (2021). A security awareness and protection system for 5g smart healthcare based on zero-trust architecture. *IEEE Internet of Things Journal*, *8*(13), 10248-10263. doi: 10.1109/JIOT.2020.3041042

Chik, J. (2022). Us government sets forth zero trust architecture strategy and requirements. *Microsoft*.

CISA. (2021). Executive order on improving the nation's cybersecurity. *Cybersecurity & Infrastructure Security Agency*. Retrieved from `https://www.cisa.gov/executive-order-improving-nations-cybersecurity`

Colombo, P., Ferrari, E., & Tümer, E. D. (2021). Access control enforcement in iot: state of the art and open challenges in the zero trust era. In *2021 third ieee international conference on trust, privacy and security in intelligent systems and applications (tps-isa)* (pp. 159–166).

Craven, C. (2021). What are zero-trust benefits and challenges? *SDxCentral*.

Cunningham, C. (2018). Zero trust on a beer budget. *Forbes*.

Cunningham, C. (2020). A look back at zero trust: Never trust, always verify. *Forrester*.

Cylance. (2022). Cylanceprotect. *Cylance*. Retrieved from `https://www.blackberry.com/us/en/products/unified-endpoint-security/blackberry-protect`

D'Angelo, T. (2021). The challenge of zero trust compliance. *Security Infowatch*.

Dean, B. (2021). Uber statistics 2022: How many people ride with uber? *BackLinko*.

Dhawan, A. (2021). Zero trust network access (ztna) vs. vpn: How they differ. *Citrix*.

D'Silva, D., & Ambawade, D. D. (2021). Building a zero trust architecture using kubernetes. In *2021 6th international conference for convergence in technology (i2ct)* (p. 1-8). doi: 10.1109/I2CT51068.2021.9418203

Durbin, S. (2021). Zero trust: An answer to the ransomware menace? *Dark Reading*.

DynamicCISO. (2020). 30% of apps being protected in a zero trust architecture are saas apps: Akamai. *DynamicCiso*.

English, M. (2021). 5 stats that show the cost saving effect of zero trust. *Teramind*.

Fedor, J. (2021). 5 mistakes companies make in their zero-trust journey. *Presidio*.

Ferretti, L., Magnanini, F., Andreolini, M., & Colajanni, M. (2021). Survivable zero trust for cloud computing environments. *Computers & Security*, *110*, 102419.

Forrester. (2021). The total economic impact of zero trust solutions from microsoft. *Forrester*. Retrieved from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWRIEi

G2. (2021a). Kaspersky endpoint security. *G2*. Retrieved from https://www.g2.com/products/kaspersky-kaspersky-endpoint-security-for-business/features

G2. (2021b). Top free zero trust networking software. *Cyberpedia*. Retrieved from https://www.g2.com/categories/zero-trust-networking/free

G2. (2021c). Virtru. *G2*. Retrieved from https://www.g2.com/products/virtru/reviews

G2. (2022). Best encryption software for small businesses. *G2*. Retrieved from https://www.g2.com/categories/encryption/small-business

Gatefy. (2021). How much should i spend on cybersecurity to protect my business? *Gatefy*. Retrieved from https://gatefy.com/blog/how-much-should-i-spend-cybersecurity-protect-my-b/

GrandViewResearch. (2021). Zero trust security market size, share & trends analysis report by deployment (cloud, on-premises), by security type (network, endpoint), by application area, by organization size, by authentication, by region, and segment forecasts, 2021 - 2028. *Grand View Research*, 140. Retrieved from https://www.grandviewresearch.com/industry-analysis/zero-trust-security-market-report

Gunderman, D. (2021). 18 companies to participate in nist ’zero trust’ project. *Banking Info Security*.

IBM. (2021). Cost of a data breach report 2021. *IBM Corporation*.

Jack, S. (2021). Implementing zero trust architecture in byod environments. *Federal News Network*.

Kerman, A., Borchert, O., Rose, S., & Tan, A. (2020). Implementing a zero trust architecture. *National Institute of Standards and Technology (NIST)*.

Kindervag, J. (2010). Build security into your network’s dna: The zero trust network architecture. *Forrester Research Inc*, *27*.

Liu, S., Zhuang, Y., Huang, L., & Zhou, X. (2022). Exploiting lsb self-quantization for plaintext-related image encryption in the zero-trust cloud. *Journal of Information Security and Applications*, *66*, 103138.

MacroTrends. (2022). Target revenue and number of employees 2010-2021 | tgt. *Macro Trends*. Retrieved from `https://www.macrotrends.net/stocks/charts/TGT/target/number-of-employees`

Mandal, S., Khan, D. A., & Jain, S. (2021). Cloud-based zero trust access control policy: an approach to support work-from-home driven by covid-19 pandemic. *New Generation Computing*, *39*(3), 599+.

Mckellar, K. (2015). Utah food bank security breach exposes 10,000 donors’ personal info. *Deseret News*.

Melnic, V. (2021). Can your vpn be hacked? yes. here’s how you stay safe in 2022. *Privacy Hub*.

Palo-Alto. (2022). What is a zero trust architecture. *Cyberpedia*. Retrieved from `https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture`

Perez, L. (2021). Communication remains major challenge in zero trust journey for sba. *Meritalk*.

Perimeter81. (2022). Perimeter pricing plans. *Perimeter81*. Retrieved from https://www.perimeter81.com/pricing

Poremba, S. (2021). When not to trust zero-trust. *Security Boulevard*.

Prokopets, M. (2022). The 5 best cloud storage tools and how to decide. *NIRA Blog*. Retrieved from https://nira.com/best-cloud-storage/

Reed, A. (2021). 5 reasons to use zero trust architecture. *Red River*.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (Tech. Rep.). 100 Bureau Dr, Gaithersburg, MD 20899: National Institute of Standards and Technology.

Salary. (2022). Hourly wage for senior security engineer salary. *Salary*. Retrieved from https://www.salary.com/research/salary/posting/senior-security-engineer-hourly-wages

Schwartz, S. (2021). Beware open source when going zero trust, expert says. *Cybersecurity Dive*.

Sharma, L. (2021). 6 zero trust application and network solutions for business. *geekflare*.

Sobers, R. (2020). Data breach response times: Trends and tips. *Varonis*.

Stafford, V. (2020). Zero trust architecture. *NIST Special Publication, 800,* 207.

Target. (2017). Target corporation, form 10-k for the year ended january 28, 2017. *SEC*.

Teerakanok, S., Uehara, T., & Inomata, A. (2021). Migrating to zero trust architecture: reviews and challenges. *Security and Communication Networks, 2021*.

Tucker, K. (2020). Pros and cons of the zero trust model. *Infused Innovations*.

Turner, J. (2022). Zero trust explained: The ultimate guide to zero trust security. *StrongDM*.

Uber. (2022). Uber technologies, inc., form 10-k for the year ended january 28, 2017. *SEC*.

Utah Food Bank, U. (2021). Utah food bank annual report 2021. *Utah Food Bank*. Retrieved from `https://www.utahfoodbank.org/wp-content/uploads/2022/03/Utah-Food-Bank-2021-Financial-Statements-Final.pdf`

Utah Food Bank, U. (2022). Utah food bank. *LinkedIn*.

Vijayan, J. (2014). Target breach happened because of a basic network segmentation error. *Computer World*.

Wood, L. (2021). Zero trust security market size, share & trends analysis report 2021-2028 by deployment, security type, application area, organization size, authentication, & region - researchandmarkets.com. *Business Wire*.

Wylde, A. (2021). Zero trust: Never trust, always verify. In *2021 international conference on cyber situational awareness, data analytics and assessment (cybersa)* (pp. 1–4).

Zelleke, L. (2021). The 6 best identity access management tools. *Comparitech*.

ZPE. (2022). How to overcome 5 challenges of zero trust security. *ZPE Solutions*. Retrieved from `https://www.zpesystems.com/how-to-overcome-5-challenges-of-zero-trust-security/`