Zero Trust Network Access with Cybersecurity Challenges and Potential Solutions

MSc Research Project
M.Sc. in Cybersecurity

Aditya Talan
Student ID: x21152292

School of Computing
National College of Ireland

Supervisor: Dr. Arghir Moldovan

National College of Ireland
Project Submission Sheet
School of Computing

Student Name:	Aditya Talan
Student ID:	X21152292
Programme:	M.Sc. in Cybersecurity
Year:	2022-2023
Module:	MSc Research Project
Supervisor:	Dr. Arghir Moldovan
Submission Due Date:	20/12/2018
Project Title:	Zero Trust Network Access with Cybersecurity challenges and potential solutions
Word Count:	XXX
Page Count:	4

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	
Date:	14th December 2022

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	Q
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	Q
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	Q

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Zero Trust Network Access with Cybersecurity Challenges and Potential SOlutions

Aditya Talan
x21152292

Abstract

Major corporations' networks have migrated from conventional in-house platforms to third-party-managed cloud platforms, resulting in a hybrid structure. However, the network's security remains inactive, with less responsibility and supervision.

Multiple networks, each with its own set of zones, comprise the standard network security architecture. Each zone is surrounded by a perimeter defence consisting of one or more firewalls. Each zone gives a particular confidence level and offers access to a variety of resources. "Never trust, always verify" is the ethos of a burgeoning alternative architectural method. Everything inside and beyond the barrier is not immediately trusted under this viewpoint.

This study is primarily concerned with comparing the innovative requirement-specific characteristics employed by cutting-edge research models for zero-trust networks. In addition, the article focuses on selecting and implementing features required for future networks, as well as determining the areas covered by infosec standards (i.e.- ISO 27001:2013 and NIST SP-800). In addition, the research study included questionnaires to obtain information from both organizations and end consumers. Finally, a variety of ideas for future study are offered, which businesses might consider when determining implementation strategies for ZTNA, to develop trust-based enterprise networks.

Keywords – Zero Trust, ZTNA, Contributions, Crowdsource, Human Survey, Implementation, Traditional, architecture, standards, ISO 27001:2013, NIST SP-800.

1 Introduction

Participation in the vital discourse regarding cybersecurity is strongly encouraged for all businesses that work with sensitive data. There are many different circumstances that put vital data at risk of being lost in companies that are part of the private sector as well as the public sector. As a direct result of this, a great number of companies are actively trying to establish a network security infrastructure that will provide the best level of protection for their data. In the past, the company depended on in-house firewalls to prevent unauthorized users from accessing the network while still enabling employees to use their own laptops inside the confines of the security system (firewall). However, in recent months, this form of network security has grown increasingly challenging for the company because of new criteria that drive the company to transition to a workforce that is conducted remotely. In the early phases of COVID-19, governments adopted protocols with the goal of reducing the virus's ability to spread. The corporation made the decision to use work-from-home (WFH) solutions, which do not permit the installation of firewalls.

To satisfy the criteria while keeping business continuity management in mind, businesses have to devise a strategy to change their existing architecture into a Zero Trust Network Access architecture. The below table describes the cause for the modification.

Table 1: Currents State(VPN) vs Future State(ZTNA)

Current State vs Future State	Advantages	Disadvantages
Current state (VPN)	A VPN client encrypts the user's data and hides their location, preventing unauthorized access.	VPNs also fail to secure BYOD workforces, notably smartphones and tablets.
	Employees may securely access work computers remotely.	VPNs have always been frustratingly slow for remote workers.
	VPNs can protect data shared between branches.	SSL is needed. Network access requires username, password, and shared secret code.
	Cost-effective, by making users invisible on the network, they eliminate some of their features	Brute force attacks on VPNs might give compromised accounts access to more than they should.
Future State (ZTNA)	Advanced authentication underpins Zero Trust. It also uses the least privilege access (micro-segmentation).	Zero Trust security has no obvious drawbacks other than the imagined constraints of a new technological approach. However, a successful relocation requires a good migration strategy.
	ZTNA speeds up data center-to-cloud migration and reduces user impact. IT teams may align security with business policies.	
	ZTNA's easy user experience, quicker onboarding, more comprehensive offboarding, and application-specific regulations meet many compliance criteria.	
	ZTNA provides network-level access to many resources without extensive setup and maintenance.	

The above table also demonstrates the hypothesis i.e. on what basis why is it necessary to study about Zero-Trust Network Access.

Zero-trust network architecture ensures the security of all users, even those who are not listed on a private network (i.e.- third party and remote users). The figure below is the kind of building which is most suitable for usage.

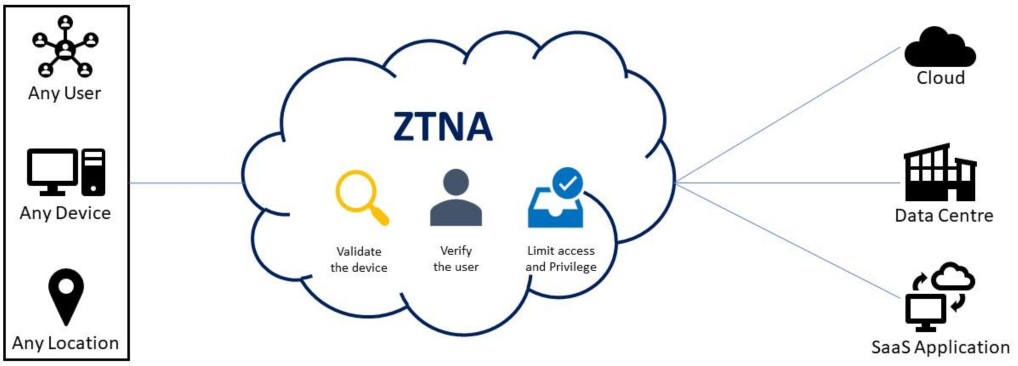


Figure 1: ZTNA Design

Until the infrastructure is completely functioning, organizations must address a number of difficulties, such as problems with hardware guidelines compliance, improper applications to control endpoint devices, and staff cyber awareness training. When an organization implements a hybrid on-prem/cloud platform, the risk of attacks increases. Numerous government organizations and business firms, including vendors, are making ongoing efforts to consolidate diverse norms and regulations (ISO 27001:2013, NIST SP-800, ISMS etc.) into flexible frameworks and models.

Meanwhile, businesses who lack the staff, time, funds or interest to embrace such frameworks and technology have mostly passed on doing so. For this reason, it's crucial to conduct a comprehensive human-survey of existing network architectures that are built on zero-trust principles. The study will analyze how various trust-based networks authenticate identities and provide access to Zero-Trust services.

The purpose of our study is to provide guidance toward a state of Zero-Trust Maturity in network security for organizations across all levels of government, business, and education.

a. Below are the paper's contributions:

A. The article defines zero-trust architecture, lists the characteristics of the common network security architecture, and provides an overview of its implementation. Additionally, the cutting-edge ZTNA structure.

B. ZTA-based network criteria, crowdsourcing platform vendor shortlisting, and a ZTNA-based assessment methodology are all addressed in this article.

C. In particular, the document provides a mapping of the ZTNA requirements to the domains of ISO 27001:2013 and NIST SP-800 standards to help ensure conformity.

D. Using crowdsourcing platforms and human surveys (finalizing the subset of more relevant questionnaire) with different organizations and their Cybersecurity professionals, the report concludes by outlining continuing research and future plans for evaluating ZTNA using score plots and graphs.

E. Ultimately, the report outlines the step-by-step process for adopting ZTNA with the help of ZTNA vendors.

2 Related Work

There are several studies that conduct an examination of the structural and operational aspects of ZTA.

a. Analytic Overview

The results of previous polls relating to Zero Trust are summarized in Table 2. Buck et al.[20] conducted a study in which they assessed articles that were produced on ZTA using a search model that differentiated academic content from grey literature. Grey literature is defined as writing that is derived from non-academic sources, such as commercial or private ones. The concept of combining the immutability of blockchain technology with intrusion prevention and detection at network endpoints was discussed by Alevizos et al.[21] He et al.[22] provide a research that contrasts well-known approaches to trustworthiness assessment and discusses the benefits and drawbacks of various access control models and authentication protocols. Syed et al.[23] are also interested in access control mechanisms and authenticating protocols in networks, and their research focuses on these topics. They examine the difficulties associated with using such an architecture and broaden its use to include software-defined perimeters and micro-segmentation. The authors of the study, Pittman et al.[24], examine a unique concept in which the tenets and principles of zero-trust are applied to data objects rather than routes that enable users to access data. They come to the definitive conclusion that calculating trust in a complex system such as a network is a challenge that combines elements of classification and regression analysis.

Most studies concentrated their attention largely on the process of developing the design and administration of ZTA or on certain subjects that were generated from ZTA, such as micro-segmentation, software-defined perimeters, and intrusion prevention systems. The characteristics of the network, as well as certain distinguishing features that are often applied, are analyzed and compared in this research. The zero-trust architecture is not a monolithic design; rather, it makes use of a wide variety of established and developing technologies. Comparing different technologies is necessary to identify those that provide the greatest match for the design. In the publications that were analyzed, several of the writers made the claim that ZTNs have not been able to successfully replace traditional methods of network security.

b. Summary of Findings

Table 2: A comparison of previously conducted surveys and evaluations (discussed: Y ; never mentioned: X; partly mentioned: P) A: Methodology for Classifying the Works Examined, B: Individual statistic comparisons of several works, C: Examining Models with Different Features, D: Information about the issues of hybrid networks, and E: Highlights human surveys for further study

Writer(s)	Principal remark	A	B	C	D	E
Buck et al.	Analysis of industrial and academic knowledge gaps, as well as a compilation of works based on the Zero Trust principle	Y	X	X	P	X
Alevizos et al.	Boosting endpoint security using ZTA model analysis and blockchain-based IDS/IPS	P	X	Y	P	X
He et al.	The technologies at the heart of Zero Trust are dissected and weighed against one another.	Y	Y	Y	X	X
Syed et al.	The effects of ZT on authentication and access control in various contexts are discussed.	Y	Y	P	P	X
Pittman et al.	A method that applies Zero Trust concepts not to data access channels but to data objects	Y	X	X	P	X
This Article	ZTNA-based network criteria, crowdsourcing platform vendor shortlisting, and ZTNA-based evaluation. ZTNA mapping with ISO 27001:2013 and NIST SP-800 mapping. Human surveys complete the ZTNA evaluation's key topics. ZTNA vendor-assisted adoption completes the report.	Y	Y	Y	Y	Y

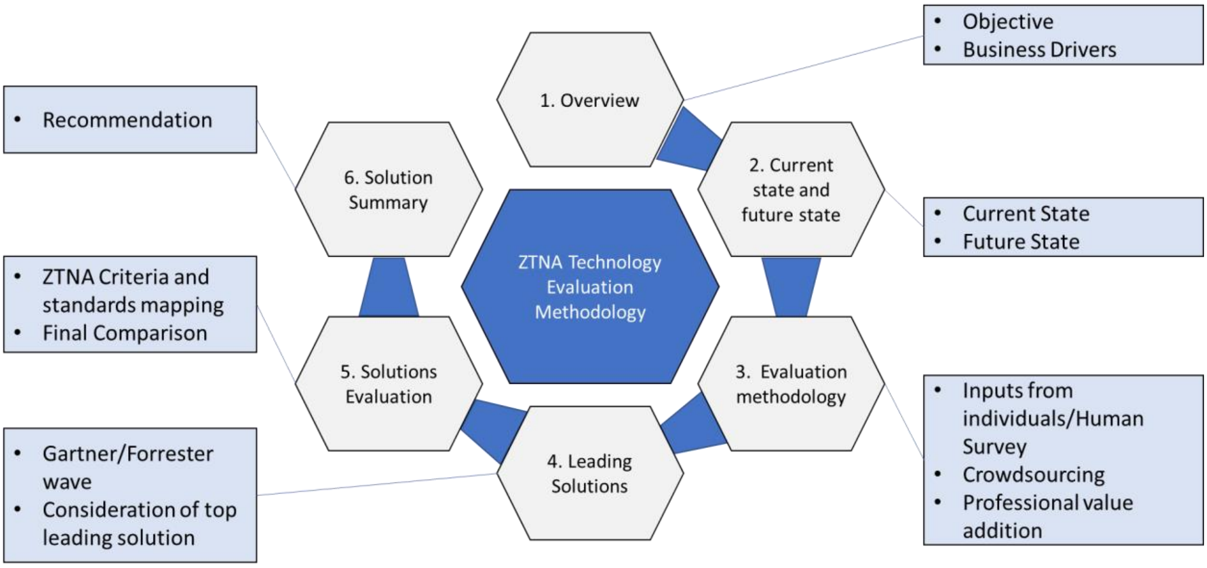
Many zero-trust on-prem/cloud (hybrid) network architectures are now in the formal development stages in both the organizational sector and academic institutions.

Most studies focused on the growth of ZTNA architecture and administration, or on its specialized offshoots such as micro segmentation, SaaS defined perimeters, and intrusion prevention systems. This study presents network criteria, vendor shortlisting from crowdsourcing platforms, and ZTNA-based assessment. The publication offers a mapping between the ZTNA requirements and the areas covered by ISO 27001:2013 and NIST SP-800 standards. The study finishes by discussing ongoing research and future plans for assessing ZTNA utilizing score plots and graphs. The article also utilized crowdsourcing platforms and human surveys (finalizing the subset of more relevant questions) with various corporations and their Cybersecurity specialists. The adoption of ZTNA with vendor support concludes the report.

3 Methodology

a. Research Methodology:

The research that was conducted to achieve these aims is presented in detail in this chapter. At the root of the research, two type of surveys were conducted: one for crowdsourcing platforms like Gartner and Forrester, and another for cybersecurity experts in corporations and organizations. The purpose of the business survey was to discover the opinions of businesses towards ZTNA. Below is a breakdown of the methods used:



Objective
Business Drivers
1. Overview
Recommendation
6. Solution Summary
2. Current state and future state
Current State
Future State
ZTNA Technology Evaluation Methodology
ZTNA Criteria and standards mapping
Final Comparison
5. Solutions Evaluation
3. Evaluation methodology
Inputs from individuals/Human Survey
Crowdsourcing
Professional value addition
Gartner/Forrester wave
Consideration of top leading solution
4. Leading Solutions

Figure 2: ZTNA Technology Evaluation Methodology

- Overview:
  To finalize the Zero Trust business driver, it is necessary to first have an understanding of the many different types of network environments and business requirements (objective).

- Current state and Future state:
  This method analyzes current corporate practices and pinpoints places where enhancements might be made. The adoption of these analyses improves efficiency and output.
  The as-is process analysis depicts how things now stand, whereas the future state process analysis illustrates how far you can take the business.
  Examining the current system and future goals of the business are the first steps in developing a process management framework.

- Evaluation Methodology:
  ZTNA evaluation methodology include the following:
  - Conduct research: Questionnaires or surveys were delivered to individuals to gather written form replies. With the use of surveys, we were able to probe into details we would have missed in the practice of personal observation.
  - Documentation: Following study and data collection, the gathered material from crowdsourced platform was documented in a standardized way.
  - Design: All companies evolve through time, which may be both beneficial and harmful. It has been common practice to employ current processes as inputs to future state diagrams (fig. 1) to guarantee a beneficial evolution.

- Leading Solutions:
  This procedure involves selecting two potential Vendors/OEMs from each segment of the Gartner/Forrester wave for further consideration. In addition, the top leaders from each dividend were selected based on the total number of feedbacks made by the industry experts who contributed to the Gartner/Forrester analysis.

- Solution Objectives:
  Solution objective includes the following:

  - Compliance: For the purpose of determining whether or not a compliance control is being adhered to, a compliance standard's representation of the control was mapped against a set of ZTNA criteria.
  - Final Comparison: The culmination of the findings obtained from questionnaires, human surveys, and platforms for crowdsourcing were combined in order to arrive at the ultimate conclusion, which was based on scoring presented in the form of graphs and plots.

- Solution Summary:
  Lastly, Recommendation was summed up with a collection of concepts, methodologies, and techniques/tools for accurately evaluating a technology's potential worth and its contribution to an organization, a geographic area, or an industrial sector in mind.

b. Data Collection:

In order to get as many replies as possible, the poll was made accessible online using Google Form for over 2 weeks. The participants' names and identifiers are kept confidential, but the questions and responses remain in plain text. Users were informed in a privacy statement that their responses to the poll and their identities would be kept private. In addition, the participant is given details about the study. A participant was under no obligation to stay in the study or answer any questions they are not comfortable with.

In our survey, we were able to gather information from two distinct groups of people. Ex-coworkers who responded to the global user survey made up one category. People from IT, consulting, healthcare, retail, and other industries. The second group was made up of executives, managers, chief information officers, security engineers, security architects, etc., who were actively engaged in rolling out ZTNA inside their respective companies. These are the LinkedIn-targeted businesspeople who completed the poll.

Table 3: Zero Trust Criteria Framework

S.No	ZT Criteria	Forrester Questions	Human Survey Questions
1	**Current Offering**		
1.1	Network Security	- How does the vendor support and enable segmenting and isolating crucial network areas? - How does the vendor enforce isolation or network segmentation? - What capacities does the vendor have that provide telemetry on data required for network security and allow visibility into encrypted tunnels and traffic within the network? I - How does the solution safeguard users who are on-premises vs those who are remote (are several products required to achieve this)? - What network protocols are supported (and which ones are not)? - Does the provider permit many, active tunnels to protected resources? - Can the solution handle a network infrastructure that is heterogeneous and multi-vendor? - How does the solution protect apps or resources against denial of service and other network-based attacks?	-Does the vendor support and enable segmenting and isolating crucial network areas? - Does the solution safeguard users who are on-premises and those who are remote? - Does the solution protect apps or resources against denial of service and other network-based attacks?

1.2	Data Security	- How does the solution improve data security in accordance with ZT principles? - Does the technology improve data management and security, data categorization and development, and data encryption both in transit and at rest? - How does the solution guard against malware/ransomware assaults and data exfiltration across various parts of the infrastructure? - How is data categorization made simpler and easier by the solution? - How does the proposed approach improve data inventory and knowledge? - Does the solution deal with mobile device technology, hybrid environments, or cloud data security? - How does the system provide data security through a setup of policies across various infrastructure parts?	- Does the technology improve data management and security, data categorization and development, and data encryption both in transit and at rest? -Is data categorization made simpler and easier by the solution? - Does the solution deal with mobile device technology, hybrid environments, or cloud data security?
1.3	Workload Security	- Does the solution allow for app-layer security controls to be implemented through the hypervisor? - Do virtual machines and containers fall under ZT controls? - How does the solution improve security from the apps via the OSI model? - Does the solution handle programs that run in virtual machines and containers? - How well does the solution integrate with workloads running on cloud platforms used by your organization? - Is app whitelisting a feature of the solution? - Does the solution allow for the micro-segmentation of workloads across various infrastructure components? - Does the solution quickly and effectively solve cloud workload vulnerability issues? - How does the solution handle dependable data security in cloud, hybrid, or mobile device environments? - The solution is for a specific cloud, or is it solely for on-prem and can operate on any cloud? - Do the policies of the solution adapt to the workload without changing?	- Does the solution integrate well with workloads running on cloud platforms used by your organization? - Does the solution handle programs that run in virtual machines and containers? - Does the solution allow for the micro-segmentation of workloads across various infrastructure components?
1.4	People/Workforce Security	- How does the technology apply ZT controls for user authentication, ongoing oversight of, and control over their access and privileges? - Does the technology adhere to NGA rules and principles? - How does the solution explain why what is being done important and who is doing it? - How does the solution provide light on the actions and motives of potential threat actors? - How can the solution address the scattered, mobile workforce of today and the perimeter's eradication? - What concerns with email, online gateways, and browser-based attacks does the solution address?	- Does the technology apply ZT controls for user authentication, ongoing oversight of, and control over their access and privileges? - Does the solution provide light on the actions and motives of potential threat actors? - Does the solution explain why what is being done important and who is doing it?

1.5	Device Security	- In relation to device restrictions, isolation, identification, and inventory, how does the solution use zero trust? - What features specifically enable administrators to remotely deactivate unrecognized or unknown devices using the solution? - How can the solution uphold ZT principles while allowing the incorporation of modern gadgets and technologies inside the network's confines? - How does the solution handle devices made by other companies? - How is the network security fabric expanded to include devices outside the network? - Is the device's context accessible for insights? - How can the solution's agentless (clientless) client security status reporting for access management function?	- Does the solution in relation to device restrictions, isolation, identification, and inventory? - Does the solution uphold ZT principles while allowing the incorporation of modern gadgets and technologies inside the network's confines? - Is the network security fabric expanded to include devices outside the network?
1.6	Visibility and Analytics	- Does the solution enhance or boost end user or administrator visibility and analytics? - Does it shed light on previously obscure or undiscovered network assets? - What about other programs that provide information about security measures? - How is the solution able to use such data, incorporate it for usage in the system, and apply it in response operations? - How do the system warnings encourage action? - What actions result from the tool's insights? - How can data and visibility make it simple to take action? - How does the solution explain why certain people were unable to log in?	- Do the system warnings encourage action? - Does the solution explain why you were unable to log in? - Does it shed light on previously obscure or undiscovered network assets of yours?
1.7	Automation and orchestration	- How is the automatic response and reaction to threats improved by the solution in terms of speed and scale? - How does the solution make it possible to integrate different technologies so that operators and administrators have more integrated capabilities? - How can automation allow operators to respond to threats with less administrative work? - How, regardless of whether they are on the enterprise-managed network, does the vendor solution enable detection and response to attacks on all common assets (email, endpoint, identity, cloud services, etc.)? - How do the vendor's capabilities (access control, threat detection, etc.) organically incorporate threat intelligence feeds? - How can users incorporate their own unique threat intelligence feeds into the system?	- Does the vendor solution enable detection and response to attacks on all common assets(email, endpoint, identity, cloud services, etc.)? - Are you able to incorporate your own unique threat intelligence feeds into the system? - Does the solution make it possible to integrate with a maximum number of different technologies so that operators and administrators have more integrated capabilities?

1.8	Manageability and usability	- How well does the solution integrate with existing technologies and capacities? - Does it improve or impair user function and capability? - Does it reduce or adversely affect the operators' workload? - How quickly can this be implemented in order to provide Zero Trust? - What conditions must be met to get more assistance? - How close to zero trust does the proposed approach come? - Does the solution allow for item-level policy control? - If so, what kinds of laws are put into effect? - How many UIs must be used by a user before the solution is useful? - How does this solution facilitate the use of legacy and hybrid systems in the context of security operations and Zero Trust? - Is it possible to apply access restrictions consistently across all surfaces, including the admiNIST SP-800rative interfaces (such as cloud consoles, SSH to the workloads, online access to applications, service perimeters, etc.)?	- Was the implementation quick enough to provide zero trust while not affecting the work delivery? - Does the solution integrate well with existing technologies and capacities? - Does the solution facilitate the use of legacy and hybrid systems in the context of security operations and Zero Trust?
1.9	APIs	- What API use documentation is offered? - Do the APIs need complex technical knowledge unique to that vendor to utilize, or are they simple to use? - How do the APIs provide functionality, or do they even exist at all? - How many of the accessible API hooks are really being used by customers to provide greater control or uses?	- API use documentation is offered to users? - The APIs provide functionality, or do they even exist at all? - The accessible API hooks are really being used by customers to provide greater control or uses?
1.10	Future State of ZTA	- How can the vendor's solution support a future workforce that is more mobile, BYOD, and less reliant on infrastructure components built around perimeters? - How does the vendor's solution get rid of concerns like password removal, VPN removal, end-user device security, patch management, etc. with security postures in a future ZT infrastructure? - How does the vendor provide measurement and score of security hygiene concerns (unpatched machines and permissive access control on storage/network/etc.) that might jeopardize ZT security assurances? - How does the solution support both on-premises and cloud environments?	- Does the solution support a future workforce that is more mobile, BYOD, and less reliant on infrastructure components built around perimeters? - Does the solution get rid of concerns like password removal, VPN removal, end-user device security, patch management, etc? - Does the solution support both on-premises and cloud environments?

The above mentioned Human Survey Questions were released after a process of finalizing a subset of the most relevant questions, i.e.- the survey of all questions might have resulted in delay and time required with each participant, therefore a smaller, more manageable collection of three questions from each ZT criteria was chosen instead.

c. Data Analysis:

The survey data was analyzed using some basic plotting and graphing.

This procedure was used because the data has a normal distribution across the two sources (crowdsourcing platform scores and human survey scores), with each source carrying equal weight (50%). Each business survey question is connected to a specific hypothesis, thus we wrote a script to help us come up with the right response.

All of the responses from the respondents were used as a vector in the script to check each hypothesis. Due to the ordinal nature of the data, each answer to the questions has been converted to an integer between 1 and 6, with 1 representing no understanding and 6 representing full agreement. There will be a subsequent section where the survey data and its analysis are provided in detail.

d. Ethical Consideration:

Ethical permission from the appropriate Study Ethics Committee was sought and received because of the sensitive nature of the research and the inclusion of human subjects. Due to the lack of therapeutic intervention, novel research methods, disadvantaged populations, participant deceit, and other physical, social, or psychological risks to participants, the research posed minimal ethical concerns. Children, persons with learning or intellectual disabilities, subordinates of the person conducting the study, and other people who may not have comprehended the research were excluded from participation. No external sources of money were approached for this study, nor was any kind of financing solicited. There was no danger to the participants, they may quit at any moment, and no unlawful information was gathered. The survey's data was protected and anonymous.

4 Design Specification

a. Architectural Design:

When comparing zero-trust with virtual private networks, the latter is far more focused on individual devices (VPNs). In order to ensure that only authorized users have access to a network, zero trust network access (ZTNA) performs constant authentication of users in real time using identity, time, and device posture checks. On the other hand, a classic VPN would simply provide authorized users access to anything on the company's network. The following designs are the example of hypothetical architecture derived from different organisations. The following layouts are taken from various organizational network and derived to a speculative architecture.

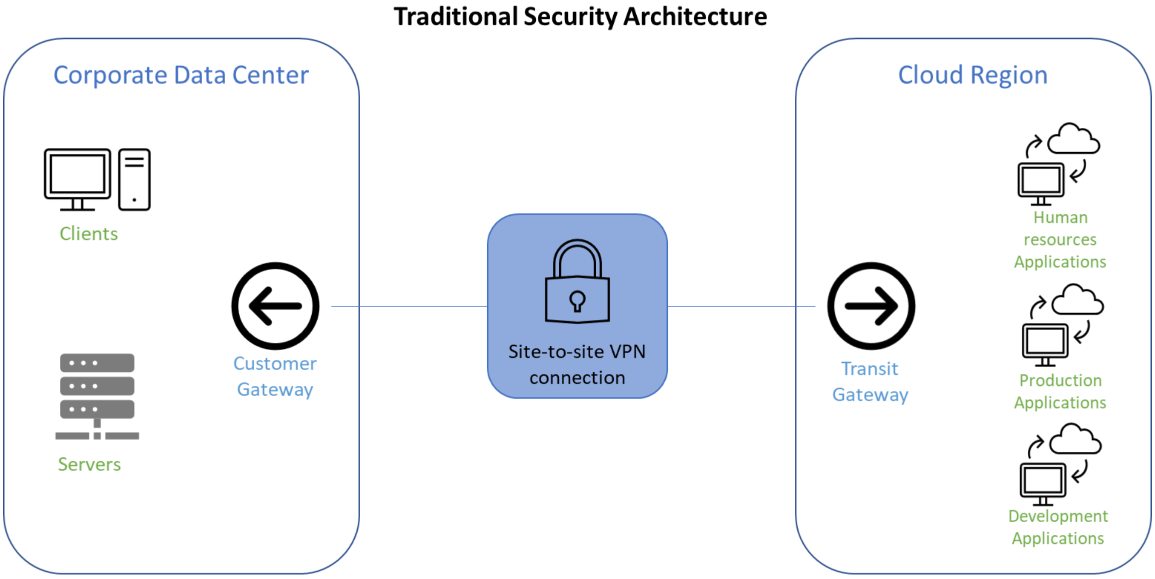


Figure 3: Traditional Architecture

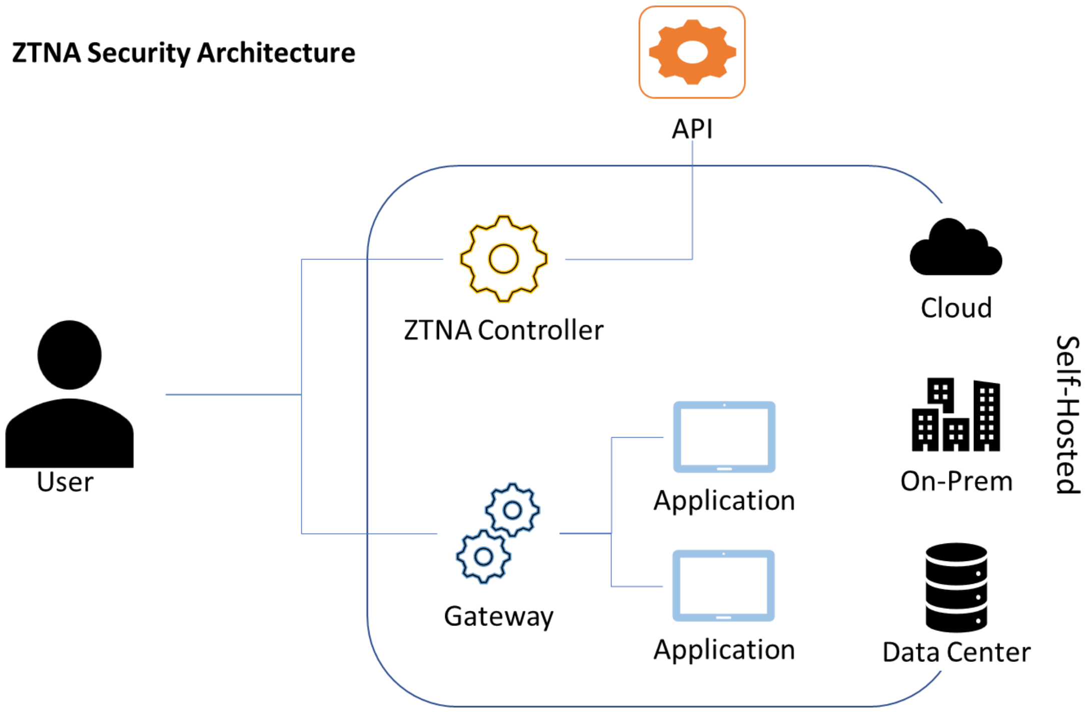


Figure 4: ZTNA Proposed Design

Table 4: Traditional architecture vs ZTNA Architecture Design

	Traditional Security Architecture	ZTNA Security Architecture
Defence	The focus is on the network	The focus is on Identity and Data
	Emphasize competing offensive and defense strategies	The emphasis will be on applications and resources
Safety Net	Safeguards based on Boundaries	Isolation Limits in Software
	Construct reliance	No presumption of confidence, restricted access by design
Security Principle	Single-use passwords and a method that doesn't change	Verification is ongoing, and so is dynamic approach.
	Lethargic, immobile defense	Automated, preventative defense

b. ZTNA Framework Analysis Design

An illustrative of the framework that was built for the ZTNA analysis can be seen in the table below. This includes completing the subset of questionnaire and mapping ZT Criteria and existing offering with ISO 27001:2013 and NIST SP-800 standards.

Table 5: ZTNA Framework Design

S. No.	ZT Criteria	Forrester Questions	Human Survey Questions	NIST SP-800-SP 800-53 Rev.5	ISO 27001:2013
1	**Current Offering**			**Compliance mapping**	
1.1	Network Security	- How does the vendor support and enable segmenting and isolating crucial network areas? - How does the vendor enforce isolation or network segmentation? - What capacities does the vendor have that provide telemetry on data required for network security and allow visibility into encrypted tunnels and traffic within the network? l - How does the solution safeguard users who are on-premises vs those who are remote (are several products required to achieve this)? - What network protocols are supported (and which ones are not)? - Does the provider permit many, active tunnels to protected resources? - Can the solution handle a network infrastructure that is heterogeneous and multi-vendor? - How does the solution protect apps or resources against denial of service and other network-based attacks?	-Does the vendor support and enable segmenting and isolating crucial network areas? - Does the solution safeguard users who are on-premises and those who are remote? - Does the solution protect apps or resources against denial of service and other network-based attacks?	-CM-8 -AC-4, -AC-17, -AC-18, -CP-8, -SC-7.	- A.8.1.1 - A.8.1.2, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3, A.6.2.1, A.6.2.2, A.13.1.1, A.11.2.2, A.17.1.2, A.14.1.3

*****To access the whole workbook of ZTNA Framework Design click on the excel sheet attached below:*

ZTNA Criteria and
Standards Mapping.xl

c. Techniques used to conclude Crowdsourcing result and Human Survey Scoring:
The scoring was done using two different sets of findings, namely, one score obtained through crowdsourcing (x), and another score obtained from a human survey (y). The ultimate score, out of a possible two, was determined by taking the average of the scores from each of the separate outcomes ((x+y)/2). The

findings will be presented in the section that follows.

5 Implementation

After these preliminary stages, there are two more before ZTNA may be used in the real world. This may occur with the vendor's assistance after the vendor has been chosen.

a. Deployment in User Acceptance Test Environment:

User acceptance testing (UAT) environments, also known as staging environments, are used to let the application's primary users try out new features before they are made available to everyone. In order to avoid having users associate poor functionality with bad server performance, it's important that the UAT environment closely mirror the production environment in terms of specs.

The vendor is responsible for setting up the UAT setup with the necessary management servers and components:

Table 6: Deployment in UAT environment

S.No.	*Deployment in UAT Environment*
1	The vendor and the customer have a conversation about a use case.
2	The UAT setting is where the vendor should configure any standard or customized policies.
3	The agent/service at the endpoint will be deployed on test systems/servers by the vendor.
4	The supplier will demonstrate the UAT login and logout process.
5	The UAT and report will be managed by the vendor.
6	The client must examine the test results and provide their final verdict.
7	Keeping an eye on the infrastructure for a reasonable amount of time.
8	Client approval is required.
9	Be sure to follow up on any concerns.

b. Deployment in Production Environment:

When software or other products are released to the end users for their intended use, professionals refer to this setting as the "production environment," where unforeseen defects and issues might be discovered and reported.

While the methods for implementing the UAT environment stay the same depending on the organization's server count.

Table 7: Deployment in Production environment

S.No.	*Deployment in Production Environment*
1	The vendor and the customer have a conversation about a use case.
2	The UAT setting is where the vendor should configure any standard or customized policies.
3	The agent/service at the endpoint will be deployed on

	test systems/servers (Secondary Server) by the vendor.
4	The supplier will demonstrate the UAT login and logout process.
5	The UAT and report will be managed by the vendor.
6	The client must examine the test results and provide their final verdict.
7	The agent/service at the endpoint will be deployed on test systems/servers (Primary Server) by the vendor.
8	The supplier will demonstrate the UAT login and logout process.
9	The UAT and report will be managed by the vendor.
10	The client must examine the test results and provide their final verdict.
11	Keeping an eye on the infrastructure for a reasonable amount of time.
12	Client approval is required.
13	Be sure to follow up on any concerns.

6 Evaluation

The following are the vendors shortlisted from three dividends – Contenders, Strong Performers, and Leaders. Additionally, the product solution for ZTNA by the vendors was identified:

Table 8: Vendors shortlist

S. No.	Vendors	Solutions
1	Palo Alto	Prisma Access
2	Zscaler	Private Access
3	Akamai	Enterprise Application Access
4	Netskope	Netskope Private Access
5	Cloudflare	Cloudflare Access
6	Cisco	Duo Beyond

Furthermore, on the basis of crowdsourcing and human survey the results are displayed below:

a. **Case Study 1: Statistically significant outcome based on crowdsourced data:** This case study refers to the practice of calculating the outcome from soliciting contributions of labor, data, or ideas from a large number of individuals using electronic means, including the Web, social media platforms, and mobile applications.

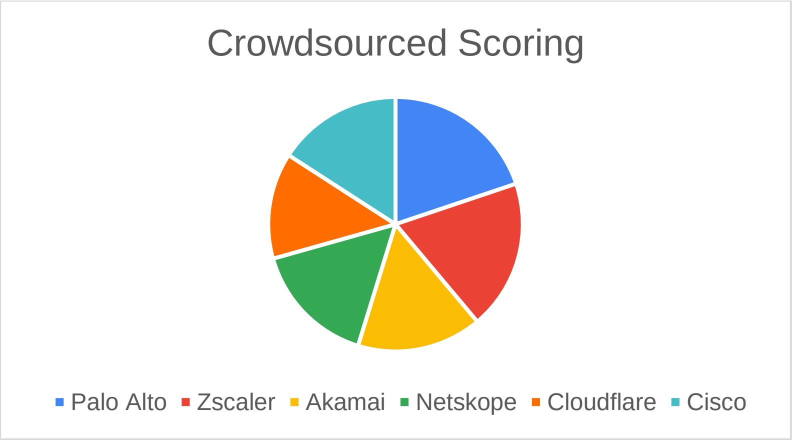


Figure 5: Scoring from crowdsourced data

b. **Case Study 2: Statistically significant outcome based on human survey data:** In this context, it refers to what can be learned about a group's characteristics when researchers gather data from a representative sample of that population and apply statistical methods to make educated guesses about those traits.

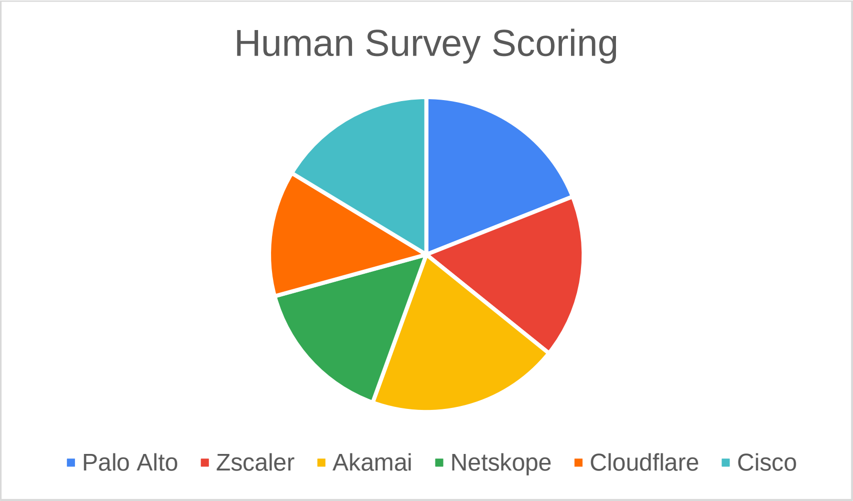


Figure 6: Scoring from Human Survey

c. **Case Study 3: Consolidated findings from the previous two:** The total score in this section is determined by aggregating the previous two responses.

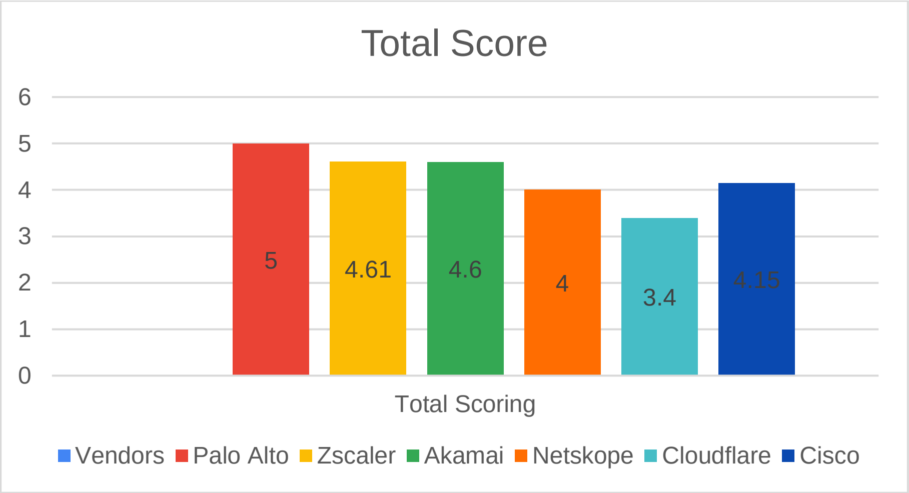


Figure 7: Final Score of shortlisted vendors

7 Conclusion and Future Work

a. **Conclusion:**

The benefits and drawbacks of existing zero-trust cloud network technologies were laid out in detail in this article.

Recently released zero-trust network models, frameworks, and ideas are compared and contrasted in this research. Future researchers will be better able to narrow in on security flaws and oversights in today's network architecture if they can compare and contrast the various models and frameworks utilized in zero-trust networks. The ability to orchestrate, automate, and respond to security threats in a zero-trust cloud environment is made possible to achieve 'Never Trust Always Verify' statement. Existing Zero-Trust Architecture solutions for on-premises and cloud deployments may benefit from more research into their scalability.

The paper's scope is broad enough that it might be used by experts in the future to monitor the network's actual capabilities and operating requirements in real time. It would prevent them from adding unnecessary features to their design while also making their network more responsive, automated, and transparent.

b. **Future Work:**

Numbers of applications might easily approach the thousands, depending on the size of the company. On top of that, they battle with imperfect information from their users. It may be difficult to establish the controls and rules needed to guarantee least-privileged access at scale when dealing with thousands of users and hundreds of apps. Our most recent development provides a solution to this issue by enabling teams to make more rapid and informed security choices by supplementing human skill with AI-powered application segmentation.

Artificial intelligence (AI)-powered application segmentation removes the complexity of traditional network segmentation, making it easier for network and security teams to identify the appropriate application segments, develop the appropriate zero trust access policies, and minimize the internal attack surface.

References

1. Alagappan, A., Venkatachary, S.K. and Andrews, L.J.B. (2022). Augmenting Zero Trust Network Architecture to enhance security in virtual power plants. *Energy Reports*, 8, pp.1309–1320. doi:10.1016/j.egyr.2021.11.272.

2. Anon, (2021). *ZTNA vs. VPN: How Zero Trust Network Access Differs | Citrix Blogs*. [online] Available at: https://www.citrix.com/blogs/2021/12/02/zero-trust-vs-vpn-comparison/.

3. Appgate. (n.d.). *Appgate | ZTNA Architecture - Zero Trust Architecture - ZTNA Guide:…*. [online] Available at: https://www.appgate.com/blog/ztna-architecture-zero-trust-architecture-guide.

4. Duo Security. (n.d.). *A VPN-Less Future for Hybrid Work - Duo Blog*. [online] Available at: https://duo.com/blog/modernizing-secure-remote-access-vpn-less-future-hybrid-work [Accessed 15 Dec. 2022].

5. Gartner.com. (2022). [online] Available at: https://www.gartner.com/doc/reprints?id=1-29XM6YV7&ct=220502&st=sb.

6. getstarted.awsworkshop.io. (n.d.). *Review Site-to-Site VPN Architecture :: Get Started with AWS for Production Workloads*. [online] Available at: https://getstarted.awsworkshop.io/05-extend/01-hybrid-networking/03-review-site-to-site-vpn-architecture.html [Accessed 15 Dec. 2022].

7. Gwilliam, A. (2022). *ZTNA vs. VPN: What's the Difference?* [online] JumpCloud. Available at: https://jumpcloud.com/blog/ztna-vs-vpn [Accessed 15 Dec. 2022].

8. Networking. (n.d.). *VPN vs. zero trust vs. SDP: What's the difference? | TechTarget*. [online] Available at: https://www.techtarget.com/searchnetworking/feature/SDP-vs-VPN-vs-zero-trust-networks-Whats-the-difference [Accessed 15 Dec. 2022].

9. NSFOCUS, Inc., a global network and cyber security leader, protects enterprises and carriers from advanced cyber attacks. (2022). *Zero Trust Network Access (ZTNA): Never Trust, Always Verify*. [online] Available at: https://nsfocusglobal.com/zero-trust-network-access-ztna-never-trust-always-verify/ [Accessed 15 Dec. 2022].

10. Palo Alto Networks. (n.d.). *Unit 42 Cloud Threat Report, 2H 2021*. [online] Available at: https://www.paloaltonetworks.com/prisma/unit42-cloud-threat-research-2h21 [Accessed 15 Dec. 2022].

11. Ramezanpour, K. and Jagannath, J. (2022). Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN. *Computer Networks*, p.109358. doi:10.1016/j.comnet.2022.109358.

12. reprints2.forrester.com. (n.d.). *Forrester Reprint*. [online] Available at: https://reprints2.forrester.com/#/assets/2/82/RES176124/report [Accessed 15 Dec. 2022].

13. Sarkar, S., Choudhary, G., Shandilya, S.K., Hussain, A. and Kim, H. (2022). Security of Zero Trust Networks in Cloud Computing: A Comparative Review. *Sustainability*, [online] 14(18), p.11213. doi:10.3390/su141811213.

14. Teerakanok, S., Uehara, T. and Inomata, A. (2021). *Migrating to Zero Trust Architecture: Reviews and Challenges*. [online] Security and Communication Networks. Available at: https://www.hindawi.com/journals/scn/2021/9947347/.

15. Tyler, D. and Viana, T. (2021). Trust No One? A Framework for Assisting Healthcare Organisations in Transitioning to a Zero-Trust Network Architecture. *Applied Sciences*, 11(16), p.7499. doi:10.3390/app11167499.

16. VMware. (2022). *The Forrester New Wave^{TM}: Zero Trust Network Access, Q3 2021 | VMware SASE*. [online] Available at: https://sase.vmware.com/resources/the-forrester-new-wave-zero-trust-network-access_TY [Accessed 15 Dec. 2022].

17. Wang, X., Mansour, S. and El-Said, M. (2022). Introducing Zero Trust in a Cybersecurity Course. *The 23rd Annual Conference on Information Technology Education*. doi:10.1145/3537674.3555779.

18. www.archonsecure.com. (n.d.). *The Future of VPN: Transitioning from Traditional VPNs to Zero Trust*. [online] Available at: https://www.archonsecure.com/blog/the-future-of-vpn-transitioning-from-traditional-vpns-to-zero-trust [Accessed 15 Dec. 2022].

19. Zscaler. (2022). *ZTNA's most reliable application segmentation powered by AI*. [online] Available at: https://www.zscaler.com/blogs/product-insights/how-ai-powering-ztna-be-most-reliable-way-segment-applications [Accessed 15 Dec. 2022].

20. Buck, C., Olenberger, C., Schweizer, A., Völter, F. and Eymann, T. (2021). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. Computers & Security, 110, p.102436. doi:10.1016/j.cose.2021.102436.

21. Alevizos, L., Ta, V.T. and Hashem Eiza, M. (2021). Augmenting zero trust architecture to endpoints using blockchain: A state-of-the-art review. Security and Privacy. doi:10.1002/spy2.191.

22. He, Y., Huang, D., Chen, L., Ni, Y. and Ma, X. (2022). A Survey on Zero Trust Architecture: Challenges and Future Trends. Wireless Communications and Mobile Computing, 2022, pp.1–13. doi:10.1155/2022/6476274.

23. Syed, N.F., Shah, S.W., Shaghaghi, A., Anwar, A., Baig, Z. and Doss, R. (2022). Zero Trust Architecture (ZTA): A Comprehensive Survey. IEEE Access, 10, pp.57143–57179. doi:10.1109/access.2022.3174679.

24. Towards a Model for Zero Trust Data. (2022). American Journal of Science & Engineering, 3(1). doi:10.15864/ajse.3103.