Why Zero Trust Framework Adoption Has Emerged During and After Covid-19 Pandemic

Abeer Z. Alalmaie[1], Priyadarsi Nanda[2], Xiangjian He[3], Mohrah Saad Alayan[4]
[1] School of Electrical and Data Engineering, University of Technology Sydney, Sydney, Australia
abeer.z.alalmaie@student.uts.edu.au
[2] School of Electrical and Data Engineering, University of Technology Sydney, Sydney, Australia
priyadarsi.nanda@uts.edu.au
[3] School of Computer Science University of Nottingham Ningbo, China
Sean.He@nottingham.edu.cn
[4] School of software, university of technology Sydney, Sydney, Australia
Mohrah.S.AlAlyan@student.uts.edu.au

Abstract. The rise of COVID-19 brought an unprecedented change in the way people lived. It left several people in a work-from-home situation. This Paper aims to investigate the recent works which applied Zero Trust and the reason that this framework adoption has emerged during and after the Pandemic. In this regard, a questionnaire was prepared, and its results are reported. According to its results, with ZTA gaining skyrocket popularity and trust, for around 60% corporates, ZT Access is planned for future, while for around 30% corporates, the project is in pipeline. None of the organizations surveyed have the ZTA in place. 14% of organizations are uninterested in adopting ZTA. Plus, in past 2 years, the percentage of north American organizations having a ZTA on the plans to establish one in the next 12-18 months has shot up.

1 Introduction

COVID-19 advanced at a very unprecedented time; leading a ceaseless work-from-home situation that organizations were prepared for. Businesses perpetually dealt with portable devises shortage, insufficient bandwidth, undersized infrastructure of Virtual Private Network (VPN) with IT department pushing the limits to maintain efficiency by enabling employee access to corporate resources/applications to work in full capacity. The pandemic caused profound re-modification and reorganization of human-to-human interaction [1]. Before the pandemic, interest in Zero Trust (ZT) was being driven by a need to modernize how the information security stack works. The traditional perimeter-centric security model is not compatible with the way businesses are working today. The pandemic forced the organizations looking at ZT because so many employees shifted to remote work that the organizations' networks were no longer a source of trust. Increased attack surface is a concern and increased mobility was already happening but accelerated in the pandemic. ZT offers encouraging solutions, but requires reasonable re-architecture, re-modification, and re-investment. That means work-from-home scenario is a continuous arrangement for job profiles who can fulfil professional obligations without commuting to and from their job site. These factors have seen the risk for cybercrime and cyberattacks increase. With older technologies like VPNs making headlines for security issues, a new approach to empowering distributed teams while ensuring optimal data security has emerged: ZT network architecture.

In this regard, a survey is conducted which its results can help designing future works for developing an Intrusion Detection System (IDS) using Zero Trust Architecture (ZTA). Most of our respondents were around 40+ CISO's from various IT companies, banks and government in India and Saudi. The specific survey's objectives include:

1) Why businesses experienced similar pain points to enable secure remote work?
2) How a ZTA could assist business continuity in pandemic outbreaks?
3) Why organizations are committed to adopting a ZT security architecture?
4) Which are the key initiatives to enable ZT security adoption in their organization?

The rest of the paper is organized as follow: In section 2 and 3 we review some related works and investigate the impact of COVID-19 on existing IT infrastructure, respectively. In section 4, we explain how a ZT network functions. In section 5 and 6 our survey objectives and results are mentioned, respectively. Eventually, in section 7 we prepared a short conclusion.

2 Background

In [2], over 200 executive board members of 80 companies from 2014 to 2016 were interviewed, asking "How do we secure increasingly dynamic architecture in an environment without a perimeter?". The answers revealed Bring Your Own Devices (BYOD) were valuable opportunities but posed onerous risks. Setting up a centralized and scalable Mobile Device Management system using access controls (LDAP/AD[1]) was reported to be the most important challenge. This suggests a more-risk based approach to cybersecurity is needed in today's dynamic technological environment.

According to [3], ZT treated all network traffic as untrusted, continuously confirming users and endpoints by securing cloud data. The benefit of ZT is a highly flexible infrastructure that can be integrated with the cloud to enhance organizational security. To ensure the networks safety amid new cybersecurity threats, cybersecurity professionals should embrace additional philosophies alongside a ZT mindset.

According to [4], "Who we can trust with our data?" is one of the largest debates of our generation. It has never been more important to create security models that keep users safe. The author mentioned approximately 60% to 80% of network misuse comes from within the network. ZT therefore, offers a solution to both issues, with its ability to increase micro segmentation of a network offering more visibility of overall traffic through the inspection of users and devices which connect the network.

In [5], it was proved that working remotely, especially for employees with minimal cybersecurity resources, increased the risk for personal and organizational data to be compromised. In [6], authors elucidated the challenge pointing out the use of AI, and poorly secured technologies deployed in response to COVID-19 challenges increased risks for cybercrimes due to the high volume of data being generated and shared.

[1] Lightweight Directory Access Protocol / Active Directory

In [7], a two-stage ensemble classifier including hierarchical rotation forest and bagging classifiers, along with a hybrid evolutionary algorithm for feature selection was proposed for NID. In [8], a four-way ensemble classifier including Support Vector Machine, Linear Regression, Naïve Bayes, and Decision Tree was proposed which utilized a combination of feature selection methods.

Since ML methods require feature extraction and parameter tuning, DL methos have become a trend in AI problems like image, language, and speech processing and NID [9, 10]. A two-stage deep Neural Network (NN) was proposed for NIDS including a Deep Sparse AE as the feature extractor and a shallow NN classifier [11].

In [12], a Sparse Auto-Encoder was proposed for feature extraction, however, Support Vector Regression was used as the classifier instead of the shallow NN. The AE bottleneck features were shown to be effective in enhancing the NIDSs and giving the ability to feed any type of attributes to the NID model. Plus, bottleneck features were shown to be robust against noise.

In [13], a Recurrent Neural Network (RNN) was proposed for NID to consider the changes of the input in real-time applications. Also, deeper RNN models were used for NID which outperformed previous works. Since Long Short Term Memory (LSTM) cells hold the long term dependencies and prevent the vanishing gradient problem, in [14], extended the RNN models to LSTM and Bi-directional LSTM (BiLSTM) for NID.

In [15], a Convolutional Neural Network (CNN) classifier using a two-stage feature extraction including a PCA and a feature engineering method to select the most relevant have been proposed for NID. In [16], the CNN models have been used in combination of other classifier methods including RNN, LSTM, and Gated Recurrent Unit (GRU), which proved the power of CNN.

In [17], IGRF-RFE was introduced as a hybrid feature selection method for multi-class network anomalies using a Multi-Layer Perceptron network. It was a feature reduction model based on both the filter feature selection and the wrapper feature selection methods. The filter feature selection method was the combination of Information Gain (IG) and Random Forest (RF) importance, to reduce the feature subset search space. Recursive Feature Elimination (RFE) was a wrapper feature selection method to clear redundant features recursively on the reduced feature subsets.

In [18], a NID model was defined that fused a CNN and a gated recurrent unit. They tackled the low accuracy problems of existing ID models for multiple classification of intrusions and low accuracy of class imbalance data detection. They applied a hybrid sampling technique combining adaptive synthetic sampling and repeated edited nearest neighbors for sample processing to solve the positive and negative sample imbalance issue in the dataset. The feature selection was carried out by combining RF and Pearson correlation methods to address the feature redundancy problem.

In [19], an IDS was proposed to detect 5 categories in a network: Probe, Exploit, DOS, Generic and Normal. This system was based on misuse-based model, which acted as a firewall with some extra information added to it. Moreover, unlike most related works, they considered UNSW-NB15 as the offline dataset to design own integrated classification-based model for detecting malicious activities in the network.

3 Impact of COVID-19 on Existing IT Infrastructure

In [5], authors emphasized cybercrime is among the greatest threats for most organizations. The problem’s magnitude was further elucidated by the financial burden, which they report was $3 trillion in 2015 and was projected to be over $6 trillion every year by 2021. The damages cybercrime cause is profound touching on data destruction, reputation attacks, shattering company progress, loss of intellectual property, embezzlement, increasing mitigation cost, and cost of damage control in case such attacks happen. Therefore, having a secure cyber for organizations is necessary.

The average ransom payment demanded by cybercriminals carrying out ransomware attacks went up by 33% in the first quarter of the year to $111,605, compared to the previous quarter. Phishing attempts have also exploded, with Google’s Threat Analysis Group noting 18 million COVID-19-related phishing and malware Gmail messages each day in April.

Most companies with remote teams must address new cybersecurity concerns and points of vulnerability. They are working diligently to fortify their network perimeter, implementing the latest in hardened routers, next generation firewalls, and IDSs. However, a lot of IT departments weaken their own security by standing up websites, home banking systems, ERP/ERM systems that provide access to other networks and computers behind firewall; this enables the attackers to penetrate in the system. The major reason behind such diluted security is lack of acceptance and trial of different methods other than this traditional one.

Nowadays, as some users work from home and the network structures of all the organizations are changing, the traditional way of working is orienting towards the cloud and there is rise in the use of Software as a Service (SaaS). Meanwhile, many organizations are embracing flexible working, with staff connecting from multiple devices in various locations. Leading to declining traditional network cycle/perimeter which is causing decline in security. Additionally, hackers attempting to find unaddressed vulnerabilities in newly deployed remote work infrastructure. Hence, the businesses have felt a compelling need for advanced and dependable security solution.

Organizations are being driven by the stress the pandemic was putting on their infrastructure, particularly on VPNs. Before the pandemic, VPNs were good-enough to satisfy most companies' work-at-home demands, which were occasional. Though, it is difficult to cross VPN overnight, but factors like return on investment of traditional systems in present times and unanticipated cost of VPNs make businesses to find a suitable way. The legacy system model works on the principle of trust, where it considers the elements inside a particular network as harmless. Today, employees are working from home, which poses a huge threat to the security of network. With employees now connecting a lot, they are effectively creating a hacker's playground, with new, vulnerable endpoints and access points being exposed. However, all is not lost since the ever-advancing technology space has realized the ZTA importance, which can enhance cybersecurity and safety through its principles.

4 How a Zero Trust Network Functions

In prevailing times, with legacy model of security like VPNs witnessing non-success in security, ZTA is gaining popularity for its optimal data security and empowering redistributed teams. The idea behind ZT networks is hardly new. ZTA is operated through the basic philosophy that no technology user should be trusted [20]. It is self-explanatory, which means trust no network. ZTA is a security tenet that asks organizations not to automatically allow access from inside/outside into the network structure, but instead to verify each request trying to connect.

ZTA offers cybersecurity paradigms that are more focused on users, assets, and resources as opposed to traditional paradigms that were more static and network-based oriented. By evoking ZT principle in the restructuring workstation cyber-system security, ZTA seals the major loopholes exploited by hackers and malicious intruders. As in [21] authors noted the tactic to more the firewall from outside to inside the system architecture, ZTA makes it harder to target the system internally, which is the most used approach in cybercrimes. The checking and recording of traffic within a network allow for effective system monitoring, further securing the system. They cite the four main methods that help achieve a feasible and effective ZT strategy. The 4 steps emphasize the effectiveness of scalable security infrastructure:

1) Identity authentication, which validates credibility to be allowed in a network.
2) Access control regulates the layering degree an authenticated user can access.
3) Continuous encryption-based diagnosis to offer monitoring and feedback services that help trace a threat with ease to an origin point and potential damage.
4) Mitigation, which is critical in reducing the occurrence of damages through threat identification and preventions strategies.

ZTA goal is to prevent unauthorized access to data along with creating enforcement notions for control. To achieve this vision, several technical elements are necessary, and it is important to note a single commercial tool or technology will not be able to deliver all capabilities. As Per National Institute of Standards and Technology (NIST), the logical elements of ZT include policy engine, policy administrator, and policy enforcement point. Several data sources are necessary to provide input to these policy-based mechanisms which will feed the trust algorithm that ultimately determines whether to grant/deny access to information resources based on the level of evaluated trust of the endpoint/user combination. ZT models, according to the NIST, assumes an attacker is present on the network and an enterprise-owned network infrastructure is no different than any non-enterprise owned network. NIST categorizes the types of input as: access request; user identification, attributes, and privileges; asset database and observable status; resource access requirements; and threat intelligence (Fig. 1).

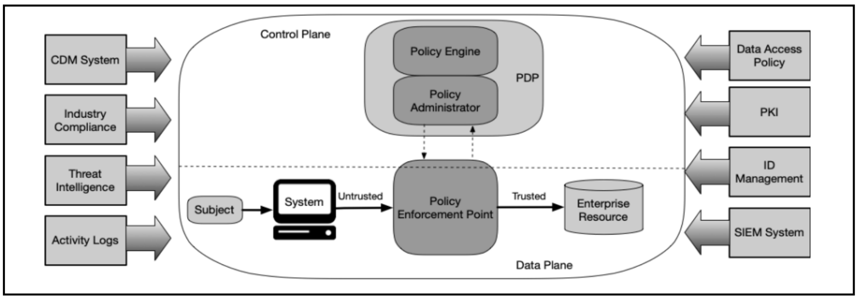

Fig. 1. NIST, 800-207, ZTA 2nd Draft

Authors in [22] noted that the scalable approach is thwarted threats to cybersecurity in a multistage strategy, hence more reliable than traditional network architecture.

Innate trust is removed from the network under ZTA principles which means one does not necessarily access to everything on network even though they are connected to that network. Inherent trust is removed and defied, so the devices and users are denied the access until they are verified on basis of pre-defined parameters. The pre-requisite for gaining access is authorization and crossing security set level. This works best in avoiding breachers who witness an attacker and move laterally into the network in cases where everything is trusted in the network. Treating the network as hostile has many advantages. By leveraging micro-segmentation and granular perimeter enforcement based on end-user characteristics like location, role, and permissions, a ZTA only gives people access to the specific resources they need. Therefore, the strategy secure layers with fine-grained segmentation, stringent system access controls, strict data retrieval management, and sophisticated data protection strategy [21]. All users access a system through gadgets must be authenticated while the information degree accessed is highly controlled and restricted to need-to-know bases [22]. The encryption ZTA strategy protects the information from internal and external intrusion and maintains a continuous monitoring and adjustment process that maintain proprietary interfaces in check. Thus, this study evaluates the effectiveness of adopting ZTA in the COVID-19 era to reduce the cyber threats risk and incidence.

5 Survey Objectives - Adoption of ZTA

We conducted a survey across multiple mediums (email, SMS, and web surveys). It incorporates qualitative and quantitative data to offer a qualifying and justifiable argument about the ZTA role in reducing cyber threats amid coronavirus pandemics.

5.1 Sampling and Sample Size

The survey involved 10-14 companies sampled through purposeful sampling method and then grouped into 2 categories. The 1st category of 5-7 companies, those using VPNs, is the primary architecture in cybersecurity. Number of them is based on accessible companies in the locality that can offer insights into the issue.

5.2 Data Collection and Analysis

The survey's data collection process entails asking the relevant question from selected individuals in the identified companies aimed to determine the degree of cybersecurity and safety offered by ZT networks compared to VPNs strategies. The data collection was done by sending the survey tool to the information technologists or persons responsible for maintaining cybersecurity in those organizations. Once they completed the questionnaire, they resent them via email for data extraction and analysis. The data was analyzed thematically for qualitative data while quantitative data was analyzed using SPSS version 22 to yield descriptive and appropriate inferential statistics.

6 Survey Results

With work-from-home, safeguarding company's network perimeter is more complex than logging in from a single location. Fig. 2 and 3 show results of the survey's 1st and 2nd question. In Fig. 2, at risk devices means unknown, unsanctioned or non-compliance endpoints, and the top challenge of companies in terms of securing the access to application and resources is the complex manual process. So, the ability to react quickly is an important feature for practical industry systems. In Fig. 3, application-specific access is based on a user's identity, device posture, and group membership, and most in most companies it was the chosen method.

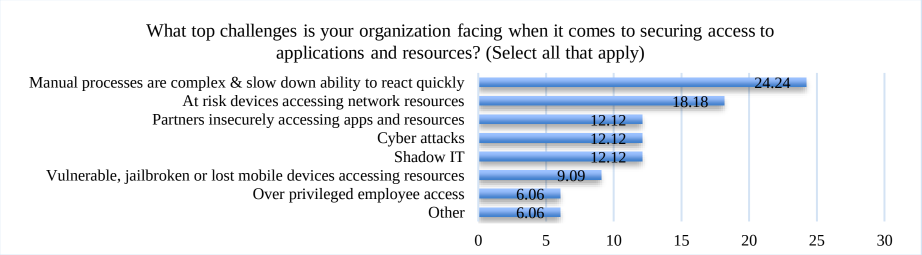

Fig. 2. Result for the first question in the survey

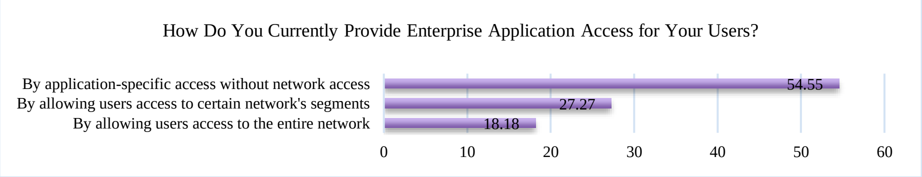

Fig. 3. Result for the second question in the survey

Recently, security was equal to the perimeter security model. It is built on its strength of outer defense. To make the network safe, the perimeter needs to be deemed impenetrable. Hence, there are ways incorporated like VPN, network segmentation and firewalls. Though, the model does not ensure security. Some attackers have demonstrated the complexity for large firms to avoid breach. The opportunity cost for security in perimeter-based security is operational agility. Plus, the network is kept secure via forming outer boundaries, what takes effort and efficiency is managing in the world micro-services and cloud computing where service communication requirements are changing frequently. Fig. 4 illustrates the result of the 3rd question.

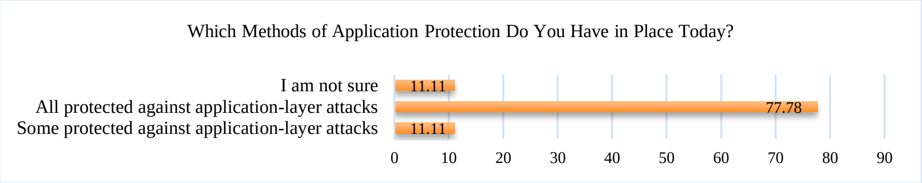

Fig. 4. Result for the third question in the survey

In Fig. 4, no one chose “None of our corporate applications are protected against application-layer attacks.” option, and the majority mentioned their corporate applications are protected against application-layer attacks with a Web Application Firewall (WAF). Thus, WAF is the most-used current method for protection against application-layer attacks. In Fig. 5, the result for 4th question is shown, in which entity verification obviously means user, device, infrastructure, etc.

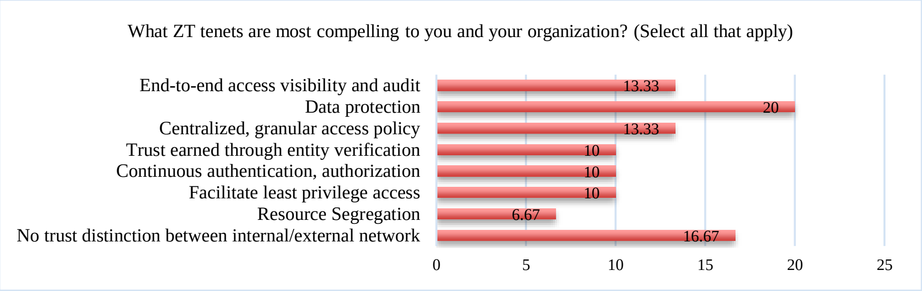

Fig. 5. Result for the fourth question in the survey

The idea is, when ZTA is detaching trust from the network, it simply amplifies the trust in the users, devices, and services. It is possible via undeterred authorization, authentication, and encryption. Its efficiency arises from its principle of authenticating each user connecting to the server regardless of where the access request is generated from. For effective use, the authentication and authorization levels and access policies should be well-defined, partaking all circumstances. The trust degree depends on the data value magnitude and impact of the performed action. Implementing ZTA on traditional systems is difficult. It needs to be installed in phases with iterations. Once the new approach foundation is laid over the legacy system, the establishment will be easier to further build on. Establishing a strong identity for users and devices or deploying modern authentication across the organization can be time-consuming.

According to the survey, 66% were neutral about adopting ZTA while 33% fall under the Satisfied to Extremely Satisfied spectrum. Around 60% plans to implement ZTA capabilities on-premises and SaaS. Fig. 6 presents the 5th question's result.

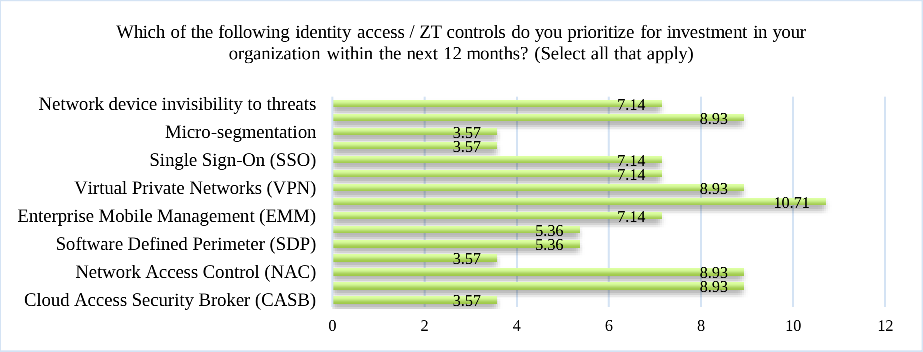

Fig. 6. Result for the fifth question in the survey

Many organizations that have implemented VPNs, with enterprise VPN usage may face data breaches in the absence of regular patching, updates, and the implementation of MFA for remote access accounts. For dealing with the challenges, IT teams attempted to make the access secured. Around 50% companies provided application access by allowing user access to only a certain network segment, however, other enacted by 38% organizations is by allowing application specific access, without network access post authorization scrutiny. Fig. 7 shows the 6th question's result.

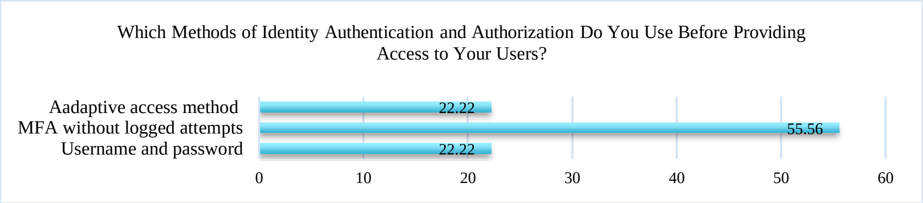

Fig. 7. Result for the sixth question in the survey

While transitioning to a new architecture, it is not suitable to start decommissioning traditional security controls before you have implemented and tested ZT controls. Due to the ZTA nature, it may leave systems exposed at considerable risk if they are not properly configured. Thus, it is vital not to dismantle the VPN establishment until the ZTA starts to perform satisfactorily. VPN can manage the potential threats if needed. Systems may be hosted using a traditional architecture or might not support the features of ZTA. So, some environments may need to manage both a traditional perimeter and a ZTA. This could involve using a split VPN tunnel to the legacy application or an authentication proxy. Figs. 8-11 present the results for 7th-10th questions.

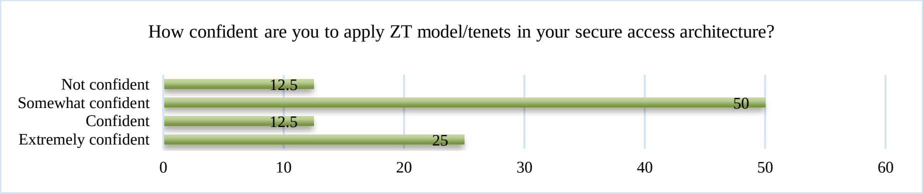

Fig. 8. Result for the eighth question in the survey

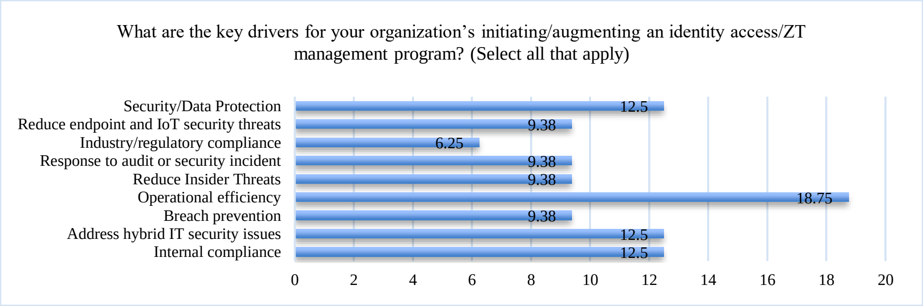

Fig. 9. Result for the seventh question in the survey

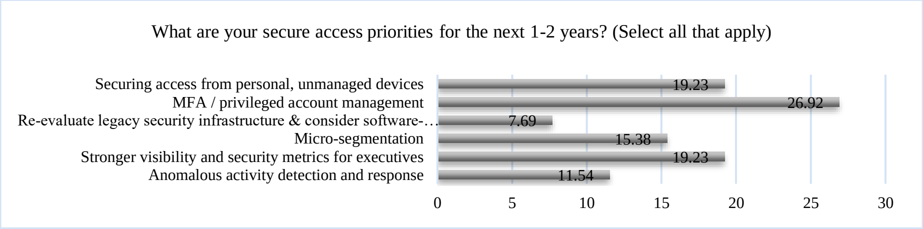

Fig. 10. Result for the ninth question in the survey

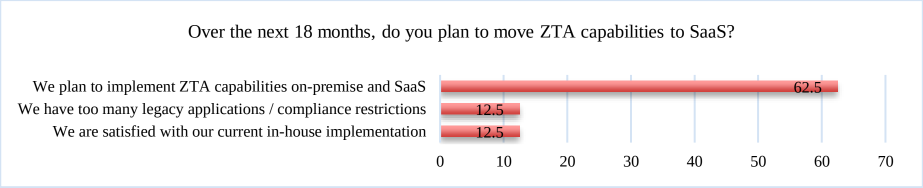

Fig. 11. Result for the tenth question in the survey

Fig. 8 shows that more than 85% of the surveyed people have confidence to an extent about applying ZT model, which proves the problem of traditional approaches and the potential benefits of using this model. In Fig. 9, regulatory compliance could be HIPAA, GDRP, PCI DSS, etc. Plus, it shows that the most important management key driver for companies is operational efficiency. According to Fig. 10, the least appropriate secure access priority for companies is re-evaluating legacy security infrastructure and considering software-defined access. Furthermore, in Fig. 11, no one choose “Significant – we plan to solely use SaaS-based ZT access capabilities” option.

7 Conclusion

Employees are increasingly working from home. There is always potential risk while accessing corporate network or data even with strong arrangements. COVID-19, has taught businesses, resilience and preparation for uncertainty. Hence reliability on ZTA in terms of cybersecurity will enhance the future alertness and adaptability. To summaries, the followings are a few disadvantages of perimeter-based security model:

1) Perimeter security largely ignores the insider threat.
2) The impenetrable fortress model fails in practice.
3) Network segmentation is time-consuming and difficult.
4) Defining network perimeter is difficult in a remote-work, BYOD multi-cloud world.
5) VPNs are often misused and exacerbate the further issues.

ZT attempts to mitigate these shortcomings by the following principles:

1) Trust flows from identity, device-state, and context; not network location.
2) Treat both internal and external networks as untrusted.
3) Act like you are already breached because you probably are.
4) Each device, user, and application must be authenticated, authorized, and encrypted.
5) Access policy should be dynamic and built from multiple sources.

The literature is replete with evidence supporting the superiority of ZTA over traditional VPNs in providing maximum possible cybersecurity and safety. However, ZTAs are not without challenges that can complicate their adoption and usage in securing personal and organization data against intrusions. At a time where cyberspace has attracted masses secondary to the pandemic complications, it is prudent to explore ZTAs feasibility in preventing and protecting cyber interactions and transactions from malicious attacks. Ultimately, implementing ZTA is the best choice for businesses which want to give remote access to users while maintaining the security posture.

References

1. Lallie, Harjinder Singh; A. Shepherd, Lynsay; Nurse, Jason R.C.; Erola, Arnau; Epiphaniou, Gregory; Maple, Carsten; Bellekens, Xavier, "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Computers & Security,* vol. 105, 2021.
2. Griffy-Brown, Charla; Lazarikos, Demetrios; Chun, Mark, "How Do You Secure an Environment Without a Perimeter? Using Emerging Technology Processes to Support Information Security Efforts in an Agile Data Center," *Journal of Applied Business and Economics,* vol. 18, no. 1, pp. 90-102, 2016.
3. Puthal, Deepak; Mohanty, Saraju P.; Nanda, Priyadarsi; Choppali, Uma, "Building Security Perimeters to Protect Network Systems Against Cyber Threats [Future Directions]," *IEEE Consumer Electronics Magazine,* vol. 6, no. 4, 2017.
4. P. Assunção, "A Zero Trust Approach to Network Security," in *Proceedings of the Digital Privacy and Security Conference*, 2019.

5. T. Ahmad, "Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity," *SSRN Electronic Journal,* 2020.
6. Al Hajj, Aayad; Rony, M., "Cyber Security in the Age of COVID-19: An Analysis of Cyber-Crime and Attacks," *International Journal for Research in Applied Science & Engineering Technology (IJRASET),* vol. 8, no. VIII, pp. 1476-1480, 2020.
7. Tama, Bayu Adhi; Comuzzi, Marco; Rhee, Kyung-Hyune, "TSE-IDS: A Two-Stage Classifier Ensemble for Intelligent Anomaly-Based Intrusion Detection System," *IEEE Access,* vol. 7, pp. 94497 - 94507, 2019.
8. Krishnaveni, Sivamohan; Sivamohan, Sivanandam; Sridhar, Subramanian; Prabhakaran, Subramani, "Network intrusion detection based on ensemble classification and feature selection method for cloud computing," *Concurrency Computat Pract Exper,* vol. 34, no. 11, 2022.
9. Tohidi, Nasim; Rustamov, Rustam B., "A review of the machine learning in gis for megacities application," in *Geographic Information Systems in Geospatial Intelligence*, London, IntechOpen, 2020, pp. 29-53.
10. Abolghasemi, Majid; Dadkhah, Chitra; Tohidi, Nasim, "HTS-DL: Hybrid Text Summarization System using Deep Learning," in *The 27th International Computer Conference, the Computer Society of Iran*, Tehran, Online, 2022.
11. Jiang, Kaiyuan; Wang, Wenya; Wang, Aili; Wu, Haibin, "Network Intrusion Detection Combined Hybrid Sampling With Deep Hierarchical Network," *IEEE Access,* vol. 8, pp. 32464 - 32476, 2020.
12. Preethi, Devan; Khare, Neelu, "Sparse auto encoder driven support vector regression based deep learning model for predicting network intrusions," *Peer-to-Peer Networking and Applications,* vol. 14, p. 2419–2429, 2021.
13. Almiani, Muder; AbuGhazleh, Alia; Al-Rahayfeh, Amer; Atiewi, Saleh; Razaque, Abdul, "Deep recurrent neural network for IoT intrusion detection system," *Simulation Modelling Practice and Theory,* vol. 101, 2020.
14. Lee, Inwoong; Kim, Doyoung; Lee, Sanghoon, "3-D Human Behavior Understanding Using Generalized TS-LSTM Networks," *IEEE Transactions on Multimedia,* vol. 23, pp. 415-428, 2020.
15. Al-Turaiki, Isra; Altwaijry, Najwa, "A Convolutional Neural Network for Improved Anomaly-Based Network Intrusion Detection," *Big Data,* vol. 9, no. 3, p. 233–252, 2021.
16. Vinayakumar, R.; Soman, K.P.; Poornachandran, Prabaharan, "Applying convolutional neural network for network intrusion detection," in *International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Udupi, India, 2017.
17. Yin, Yuhua; Jang-Jaccard, Julian; Xu, Wen; Singh, Amardeep; Zhu, Jinting; Sabrina, Fariza; Kwak, Jin, "IGRF-RFE: A Hybrid Feature Selection Method for MLP-based Network Intrusion Detection on UNSW-NB15 Dataset," *arXiv:2203.16365,* 2022.
18. Cao, Bo; Li, Chenghai; Song, Yafei; Qin, Yueyi; Chen, Chen, "Network Intrusion Detection Model Based on CNN and GRU," *Applied Sciences,* vol. 12, no. 9, 2022.
19. Kumar, V.; Sinha, D.; Das, A. K.; Pandey, S. C.; Goswami, R. T., "An integrated rule based intrusion detection system: analysis on UNSW-NB15 data set and the real time online dataset," *Cluster Computing,* vol. 23, p. 1397–1418, 2020.
20. Rose, Scott; Borchert, Oliver; Mitchell, Stu; Connelly, Sean, "Zero Trust Architecture," National Institute of Standards and Technology (NIST), 2020.
21. Yan, Xiangshuai; Wang, Huijuan, "Survey on Zero-Trust Network Security," in *International Conference on Artificial Intelligence and Security*, Singapore, 2020.
22. K. Uttecht, "Zero Trust (ZT) Concepts for Federal Government Architectures," Lincoln Laboratory, Massachusetts Institute of Technology, Lexington, Massachusets, 2020.