Introduction

Setting the Stage; an Overview of Cybersecurity Struggles During COVID-19

The world was in a panic: workplaces worldwide were shut down, and workers feared that they may not be able to provide for their families. During this time, work emerged from home, which became a saving grace for workers and a nightmare for cybersecurity professionals across the country.

The work-from-home era was riddled with cybersecurity obstacles due to an increased quantity of cyberattacks and vulnerabilities. In the four months between January and April 2020, around 907,000 spam messages, 737 malware-related incidents, and 48,000 malicious URLs were detected directly tied to COVID-19 and the average ransomware payment rose by 60% [2]. Because "the change in work culture would also increase the chances of the cybersecurity attack," COVID-19 posed a cybersecurity challenge to organizations across the United States [1]. Since the average ransomware payment rose during the pandemic, companies were losing more money in cyberattacks. Furthermore, increased losses due to cyber-attacks during COVID-19 are reflective of the strife companies were facing not only in staying afloat but also in keeping themselves secure.

Overview of ZTNs

Zero Trust Architecture (ZTA) is a cybersecurity model that treats devices inside and outside the network with utmost scrutiny. It operates off of the assumption that devices on the network have been compromised, and treats each device with zero trust as the name suggests. In

a ZTA, all users must be continuously authenticated, authorized, and validated before accessing network applications and data [5].

Reshaping Network Infrastructure: The Impact of COVID-19 on Zero Trust Network Access

COVID-19 restructured the way companies thought about their networks through the shift to work from home, accelerating the adoption of Zero Trust Network Access motivated by profitability and security; ZTA's impact amid the time of strife underscores the architecture's effectiveness.

The Importance of Understanding ZTNs In Relation to Securely Working From Home

In the chaos that ensued during the COVID-19 pandemic, companies scrambled to stay afloat. Across the world, industry almost unanimously came to the same conclusion: they adopted work from home. However, with this switch from the physical world into cyberspace came new vulnerabilities and weaknesses that companies needed the infrastructure to deal with.

With shifting technology policies during the work-from-home era came newfound vulnerabilities and threats. Research into cloud-based zero trust control policy as an approach to support work-from-home found that "the fast-paced adoption of cloud resources increases network traffic and security issues related to hacking and spoofing" (). Since when "cloud resources are accessed from heterogeneous platforms using untrusted home networks, it leads to severe security breaches" organizations were struggling to keep pace with both managing new work-from-home technology and protecting their resources [1]. Research into Implementing Zero Trust Architecture indicates that "once employees leave the protected environment and use their devices to access company resources, the absence of robust cybersecurity measures makes

them vulnerable targets for hackers" [5]. Organizations were struggling to secure their resources because remote work redefined where the perimeters of a network should be.

ZTA arose during the COVID-19 pandemic as a solution to both securing and managing new work-from-home technology. At the time, "architectural access control policies" had to "be redesigned to support work-from-home-concept for accessing cloud resources seamlessly without human intervention." Research into ZTA in cloud computing proposed "a progressive access control policy based on zero trust" [1]. Specifically, ZTA's "core objective is comprehensive resource protection, requiring precise authentication and minimal authorization when users or assets attempt to access resources" [5]. Since network resources were at risk, and ZTA emphasized precise authentication, it grew in popularity as a solution to the resource management problems that work-from-home created. Furthermore, ZTA not only bolstered security but also "uses the IP trackback and port scanning techniques validation of the TCP packet, which reduces the computational overhead" [1]. Since work-from-home turned networks inside out, removing the defensive perimeters that have historically been heavily relied upon, it became imperative to both authenticate users and implement strict controls to manage devices on the network. ZTA also "strengthened" the ability of organizations to manage "internal systems and services' information security environment" because "if any internal services are compromised, this robust management framework can mitigate the extent of the breach's impact" [5]. Zero Trust "not only looks at the perimeter of a network but also looks at the components; systems, users, data, etc. as points to protect," thereby making it easier for organizations to exert precise control over the entirety of their network [3]. Therefore, ZTA emerged as a solution to both newfound security threats and increased overhead associated with working from home.

Background of Zero Trust Architecture

Definition and Principles of Zero Trust Architecture

Zero Trust Architecture (ZTA) is a framework that gained significant amounts of attention due to its ability to protect network resources from cybersecurity threats robustly. Zero Trust Architecture is a security concept based on the principle of "never trust, always verify." While traditional network security models focus on securing the network perimeter, zero-trust architecture treats devices inside and outside of the network the same way: all hosts are treated with zero trust [4]. ZTA requires continuous verification from all devices trying to access resources within or outside the network, regardless of their location [5]. The approach simultaneously creates a streamlined and secure method of accessing network resources. The core principle of ZTA is to trust no one—dubbed the zero trust principle—, continuously verifying everyone, regardless of whether or not they are inside the network perimeter.

While the zero-trust principle is incredibly effective, ZTA locks down resource access even more through its heavy reliance upon the principle of least privilege. The principle of least privilege means that users and devices are granted the minimum level of access that they need to perform their tasks [4]. Zero Trust assumes that devices on the network have already been compromised [3]. The principle of least privilege reduces the risk of unauthorized access in case of a compromised device. By combining continuous verification with the principle of least privilege, ZTA can ensure proper authentication and proper allocation of resources within the network, ultimately strengthening a company's overall cybersecurity posture.

Zero trust architecture even takes security a step further by implementing micro-segmentation to divide the network into smaller segments, each with its own set of security controls. Research conducted on the security of zero trust networks in cloud computing suggests that "The addition of micro-segmentation and Zero Trust does not have an enormous impact on performance of the network" [4]. However, research conducted on the Strategy for Implementing Zero Trust Architecture makes it clear that while micro-segmentation may not enhance the performance of a network, it strengthens security by inhibiting lateral movement of threats within the network and reduces the impact of a potential breach [5]. Since micro-segmentation locks down the network and avoids potential security threats that can result from a contaminated device, zero trust architecture assumes that every device on the network is a threat and contains each device to only the part of the network that it needs.

While zero trust architecture is comprised of a robust system of controls, it bolsters cybersecurity operations not only with control capabilities but also continuous monitoring and analytics. ZTA emphasizes continuous monitoring of user behavior to detect anomalies and potential threats in real-time. This process may involve the use of an "artificial neural network (ANN)-based detection method", which utilizes AI technology "to detect, and distinguish network behavior from noisy and incomplete data sources" [1].

Benefits of ZTNs

Zero Trust Architecture has emerged as an efficient and secure framework for tackling cybersecurity and challenges traditional security models by assuming zero trust. ZTA can enhance cybersecurity and make remote work more manageable.

Zero trust architecture can improve a company's security posture. Research into taking a zero-trust approach in healthcare has shown that organizations can significantly mitigate the risk of data breaches and unauthorized access by adopting ZTA [3]. By assuming that every device within a network has already been compromised, ZTA minimizes the impact that a threat actor could have within a network.

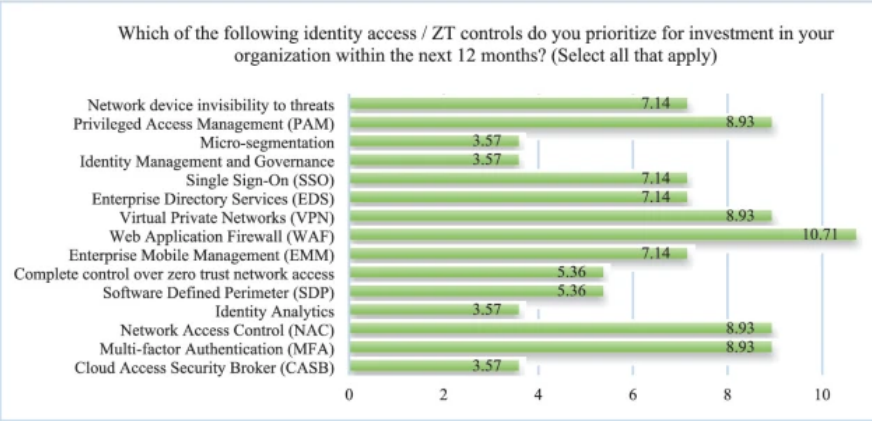
ZTA also offers increased visibility and control to organizations that adopt the framework. By implementing micro-segmentation, organizations can manage access to resources more effectively and exert precise control over everything on the network. Adopting zero trust "enables network administrators to tackle critical issues such as how to inhibit internal and external cyber threats, enhance the visibility of the network, automate the calculation of trust for network entities, and orchestrate security for users" [4]. In healthcare, Enhanced visibility allows organizations to respond to security threats expediently, thereby reducing the likelihood of a successful attack [3]. Increased visibility also makes it easier for companies to conduct analytic operations on their network.

Implementing ZTA can also simplify security operations, especially as it pertains to remote work. By adopting a zero-trust model, organizations can reduce the complexity of their security infrastructure by removing the headache associated with securing using a VPN to access network resources remotely [3]. Some research underscores "the potential" of ZTNs "as an alternative to VPNs for internal enterprise networks" [4]. Furthermore, because zero trust architecture could limit the overhead involved with setting up secure VPN infrastructure, it can simplify security operations when dealing with remote work.

The Feasibility of ZTNs

Competing Survey Hypothesis: Can ZTNs Replace Existing Approaches

While some research on the security of zero trust in cloud computing raises doubts regarding the feasibility and utility of zero trust architecture, this information is in tension with existing information on companies that have already implemented ZTNs. Sarkar and his associates' comparative review of Zero Trust Architecture in cloud computing found that "Of the papers surveyed, many authors also state that ZTNs have not been able to replace existing approaches to network security" [4], which may cause some to question the feasibility and utility of zero trust architecture. Because for new technology to be useful, it has to be capable of, in some way, replacing the old ways of doing things, the purported incapability of Zero Trust Infrastructure to replace existing approaches would threaten both the utility and the feasibility of ZT in practice. Since one could conclude that zero trust infrastructure is unfeasible and unuseful, there would presumptively be no appeal for companies to adopt the architecture; however, research titled "Why Zero Trust Framework Adoption has Emerged During and After Covid-19 Pandemic," surveyed companies who have adopted ZT infrastructure, establishing that ZT is both feasible and useful for network purposes, given that 7.14% of those surveyed reported that they prioritize Zero Trust Network Device Invisibility to threats, 8.93% reported that they prioritize zero trust Network Access Controls when it comes to their



organization's investments, 10.71% prioritized web application firewalls, and 8.93% prioritized Virtual private networks [6]. There is a pronounced difference between surveyed research and observations concerning organizations that are actually implementing Zero Trust Technology. Because more than a quarter of those who adopt zero trust architecture prioritize network-related matters, it is clear that ZTA is useful for network-related purposes, otherwise, organizations would not have implemented the technology.

Surveys Versus Case Studies of What Happened During COVID-19

The feasibility of ZTA is proven not only by surveys of organizations but also through case studies of what occurred during the COVID-19 pandemic. As organizations were forced to provide network access to millions of employees working remotely, they also began to adopt Zero Trust Architecture [6]. Furthermore, there has also been research by individuals like Vukotich into the benefits of implementing Zero Trust Architecture into healthcare systems [3]. Because there has been an observable increase in the use of Zero zero-trust architecture in organizations, and there is even research on its implementation into its benefits in healthcare systems, the technology is feasible.

Impact of COVID-19 on Cybersecurity

COVID-19's Effects on Attack Quantity

Amidst the COVID-19 pandemic, the frequency of cyber attacks jumped drastically, pushing security analysts to refine their methods of operation. Cyber attacks increased by 50.1% and an associated 30,000 cyber-attacks which were specifically COVID-19 related during the

pandemic (). Furthermore, “CGI reported a 30,000% increase in the number of cyber threats, specifically due to COVID-19” (). The “sudden transformation” to working from home during the COVID-19 pandemic “also introduced many new cybersecurity dilemmas. Many enterprises struggled to promptly adapt to these changes, resulting in a drastic surge in cybersecurity threats [5]. Statistically, during the COVID-19 pandemic, not only the health of Americans was at risk, but also the security of organizations across the country.

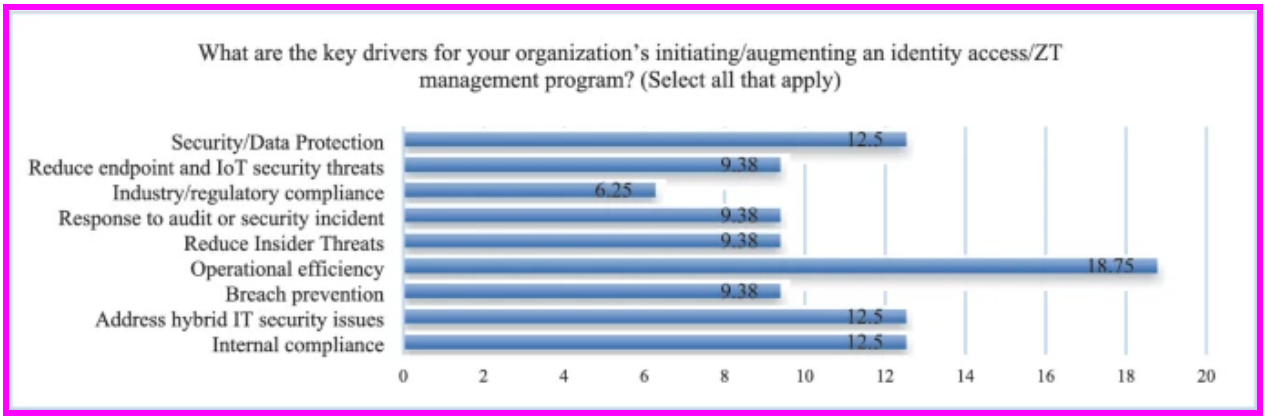
Adopting ZTNs to Deal With Increased Attacks

Because Cyber attacks quantitatively increased massively during the pandemic and ZTA is a solution for making remote network access more secure, ZTNs became more broadly adapted to deal with new types of cybersecurity threats. Since “the most significant issue stemmed from the relocation of previously trusted areas to those beyond protective boundaries,” trust laid at the core of the new prominence of cyber-attacks [5]. Because ZT avoids trusting any area, it became an effective means of dealing with the newfound threats associated with trusting devices solely because they are within the network perimeter [6]. Zero Trust Network Architecture also revolutionized cloud technology since “several emerging technologies have restructured our approach to the security of cloud networks; one such approach is the zero-trust network architecture (ZTNA), where no entity is implicitly trusted in the network, regardless of its origin or scope of access” [4]. Furthermore, since COVID-19 created new opportunities for remote work—fundamentally changing the way that networks worked by redefining who should and should not be trusted, and expanding access to network resources to millions of homes at once—, it created an opportunity for organizations to completely restructure their networks with security in mind for the first time since the internet itself was created. Consequently, since ZT

and remote work restructured the way that trust is defined within networks, “The concept of the zero-trust mechanism has made a substantial leap for restructuring policies and ensuring security against cybersecurity attacks in the COVID-19 pandemic” [1].

A Movement Toward Security or Profitability?

While ZTA greatly increases security within organizations, there is tension between scholarly research as to whether the shift toward ZTNs was motivated by security or profitability. While it is clear that zero trust is “shown how its applicability to healthcare” and other areas “can make a difference in protecting organizations,” security may not be the impetus for the movement toward zero trust [3]. Statistically, when surveyed, 18.75% of organizations labeled the key driver for initiating/augmenting a ZT management program as “operational efficiency.” While by combining various answers that are security-related, security purposes outranked this



answer, operational efficiency was still the most common survey response [6]. The fact that “operational efficiency” was most commonly the key driver for organizations to shift toward Zero Trust underscores both the feasibility and profitability of Zero Trust Architecture. An increase in operational efficiency ultimately leads to an increase in profitability, therefore ZT can make a company both more secure and profitable. Often, when new security mechanisms are

implemented, the unfortunate tradeoff for integrity, availability, and confidentiality is increased overhead—much like the difference between TCP and UDP. However, for zero trust, organizations can simultaneously become more efficient and secure. Security is not the sole driver for Zero Trust Architecture's adoption, which in the time of restructuring that COVID-19 brought about, may have given organizations an even more compelling reason to switch to ZTNA [5].

Effectiveness of Zero Trust Architecture Implementation

Prevalence Versus Effectiveness

Since the data indicates the most prevalent type of cyber-attack during the COVID-19 pandemic, it's easy to assume that Zero Trust Network Architecture was an ineffective solution to the cybersecurity issues of the pandemic; however, cybersecurity effectiveness does not necessitate prevalence. During the COVID-19 pandemic, 86% of the biggest cyberattacks involved phishing or smishing [2]. Because network security seemingly does not have much bearing on whether or not a social engineering attack is successful, it's easy to assume that Zero Trust Network Architecture fails to effectively deal with phishing attacks; however, research into "Strategy for Implementing of Zero Trust Architecture" indicates that "For attackers using tactics like spear-phishing... to entice or designate victims to download custom-made malicious tools for account theft and lateral expansion, this approach can utilize enhanced and continuous verification and authorization methods to validate the abnormal behavior" [5]. Therefore, ZTA has the tools to effectively handle phishing attacks. However, while ZTA is capable of mitigating

the impact of a wide array of different attacks, data does not exist on whether there was a statistical decrease in cybercrime because of ZTA.

Questions that Still Remain

Was there a statistical decrease in cybercrime because of ZTA?

While ZTA had the tools to effectively deal with the increased quantity of cybercrime during the COVID-19 pandemic, sufficient data does not exist to determine its statistical effects on organizations in which they have been implemented. This makes it difficult to determine exactly how statistically effective Zero Trust Networks were during the pandemic. Literature on zero trust architecture primarily exists on what should happen when the principle is applied, rather than an observatory analysis of organizations that have implemented ZT and how much they have benefited from it.

What is the future of ZTA Post-Pandemic?

While ZTA grew substantially in popularity during the pandemic, it's uncertain whether or not the architecture will continue to gain traction. During the COVID-19 pandemic, there was an unprecedented opportunity for restructuring the way that networks operate within organizations because of work from home. There are still questions about whether or not work from home will stick around, or fade away. Organizations that do continue to have remote positions may opt for zero-trust networking approaches in the future, as they have been shown to increase operational efficiency and security [6].

Do users like ZTA?

While the companies that implement ZTA seem to enjoy bolstered operational efficiency, questions remain as to how much users like it. Often, when new security features are implemented they impede upon the user experience and cost convenience—like two-factor authentication. There is a gap in research as to whether users or employees enjoy or dislike using ZTA within their organizations.

Conclusion

Summary of Key Findings Regarding the Popularity of ZTA During the COVID-19 Pandemic

In summary, during the COVID-19 pandemic, Zero Trust Architecture (ZTA) grew in popularity due to an abrupt transition to remote work. Organizations increasingly adopted ZTA as both a means of bolstering operational efficiency and security in a time of heightened cybersecurity risks associated with remote work. Despite the tension within the scholarly literature on the feasibility of ZTA, survey data and case studies indicate that ZTA was both feasible and useful during the COVID-19 pandemic. ZTA aided organizations in enhancing their security posture and managing the complexities of remote work by implementing strict verification measures and assuming zero trust. ZTA proved effective in mitigating the increased cyber threats, providing organizations with a robust defense against cyber attacks.

Implications for Network Security Practices Moving Forward

Looking ahead, the future of ZTA post-pandemic remains uncertain. While it gained significant traction during the COVID-19 pandemic, its long-term popularity will likely depend upon factors such as the continuation of remote work and the perceived benefits of ZTA in

information security and operational efficiency. The pandemic underscored the utility of ZTA in combatting cybersecurity risks in remote work environments and highlighted ZTA's potential for improving overall security practices.

[1] S. Mandal, D. A. Khan, and S. Jain, “Cloud-Based Zero Trust Access Control Policy: An Approach to Support Work-From-Home Driven by COVID-19 Pandemic,” New Gener Comput, vol. 39, no. 3–4, pp. 599–622, 2021, doi: 10.1007/s00354-021-00130-6.

[2] H. S. Lallie et al., “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, p. 102248, Jun. 2021, doi: 10.1016/j.cose.2021.102248.

[3] G. Vukotich, “Healthcare and Cybersecurity: Taking a Zero Trust Approach,” Health Serv Insights, vol. 16, p. 11786329231187826, Jul. 2023, doi: 10.1177/11786329231187826.

[4] S. Sarkar, G. Choudhary, S. K. Shandilya, A. Hussain, and H. Kim, “Security of Zero Trust Networks in Cloud Computing: A Comparative Review,” Sustainability, vol. 14, no. 18, Art. no. 18, Jan. 2022, doi: 10.3390/su141811213.

[5] M. Tsai, S. Lee, and S. W. Shieh, “Strategy for Implementing of Zero Trust Architecture,” IEEE Trans. Rel., vol. 73, no. 1, pp. 93–100, Mar. 2024, doi: 10.1109/TR.2023.3345665.

[6] A. Z. Alalmaie, P. Nanda, X. He, and M. S. Alayan, “Why Zero Trust Framework Adoption has Emerged During and After Covid-19 Pandemic,” in Advanced Information Networking and Applications, L. Barolli, Ed., Cham: Springer International Publishing, 2023, pp. 181–192. doi: 10.1007/978-3-031-28694-0_17.

Color Key (For own planning)

- ☑ ~~**https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8239485/**~~

/////

- ☑ ~~**https://www.mdpi.com/2071-1050/14/18/11213**~~

/////

- ☑ ~~**Healthcare and Cybersecurity: Taking a Zero Trust Approach - PMC**~~

//////

- ☑ ~~**https://www.sciencedirect.com/science/article/pii/S0167404821000729**~~

///

- ☑ ~~**https://ieeexplore-ieee-org.ezaccess.libraries.psu.edu/stamp/stamp.jsp?tp=&arnumber=10381860**~~

/////////

- ☑ ~~**https://link.springer.com/chapter/10.1007/978-3-031-28694-0_17**~~

//////