EasyChair Preprint

№ 10878

The Challenges and Processes of Achieving Optimal Implementation of Zero Trust Architecture in Workplace

Chinazunwa Uwaoma

September 10, 2023

The Challenges and Processes of Achieving Optimal Implementation of Zero Trust Architecture in Workplace

Chinazunwa Uwaoma

Center for Information Systems & Technology, Claremont Graduate University, chinazunwa.uwaoma@cgu.edu

Zero Trust Architecture (ZTA) is one of the newest approaches in tackling cyber threats in organizations. While the goal is to reduce the impact of cyber threats by assuming no implicit trust, as well as constant monitoring, and restricted access to critical enterprise resources, the adoption and implementation in many organizations has not reached the maturity level and faces myriads of challenges given the heterogeneity of the various components including Internet of Things (IoT) and mobile devices that constitute the architecture. This paper examines the state-of-the-art approaches in the implementation of ZTA in workplaces, and its extension to mobile and IoT devices used to access organizational resources remotely. Although there has been existing work that have proposed effective ways of implementing ZTA across spectrum of organization's resources and applications, the challenges of the implementation in mobile and IoT solutions in workplaces have not been fully addressed. Based on a holistic exploration of the ZTA concepts as presented in recent research publications, this work identifies the key challenges impeding realization of ZTA in resource-constrained devices and discusses strategic schemes that could help in achieving ZTA in both enterprises' vertical and horizontal business processes, as advanced by the National Institute of Standards and Technology (NIST) standards and framework.

CCS CONCEPTS • Security and privacy~Network security • Applied computing~Enterprise computing~IT architectures • Human-centered computing~Ubiquitous and mobile computing

Additional Keywords and Phrases: Zero Trust Architecture, Workplace, Business process, Internet of Things

1 INTRODUCTION

Zero Trust Architecture is fast replacing the legacy perimeter-based network security. This is because given the increasing complexity of a typical enterprise in its operational services including internal networks, remote offices, local infrastructure, cloud services, and mobile individuals, there is no single identifiable perimeter that is sufficient to protect the entire infrastructure. Further, when an attacker succeeds in breaking the perimeter, it opens door to lateral movement of such attacks. A ZTA based on Zero Trust (ZT) principles is designed to prevent data breaches and limit internal lateral movements. The primary focus of the approach is on data and service protection; however, it has been expanded to include enterprise assets – devices, infrastructure, virtual and cloud components, as well as subjects (end users and applications) that request information from enterprise resources. The ZT models apparently assume that an attack is present in the environment, and that both enterprise-owned and non-enterprise-owned environments cannot be trusted [1].

There have been on-going research efforts on the adoption and implementation of ZT as a new paradigm for securing enterprise resources. The initiative is designed to be implemented across government agencies, industries, and educational institutions, as well as mid-size and small businesses [1]. The study in [2] presents an elaborate analysis of the ZT paradigm with detailed description of the fundamental tenets. The article provides a wide range of viable options for successfully implementing the ZTA model in its true sense. The authors describe the role of authentication and access controls as the key principles of ZTA, and present thorough discussions on the cutting-edge techniques for authentication and access control. They further discuss on conventional methods of security automation, micro-segmentation, and encryption as additional tenets for deploying ZTA.

ZT comprises of a collection of guiding principles for operations, system design, and workflow that are used to enhance an organization's security posture, and as such, cannot be viewed as a single architecture [1]. Transitioning from legacy perimeter-based security to ZTA is a journey or movement that allows an organization to assess the risks associated with its mission; and this cannot be done by simply replacing all of the current technology [1]. Hence, the ZT principles are implemented incrementally by organizations to safeguard their assets and operational processes as appropriate.

ZTA has evolved over the years and have been implemented under different names and acronyms most which are government agencies' initiatives. Black Core, the 2004 Jericho Forum, the Federal Information Security Modernization Act (FISMA), the Risk Management Framework (RMF), the Federal Identity, Credential, and Access Management (FICAM), Trusted Internet Connections (TIC), and the Continuous Diagnostics and Mitigation (CDM) programs are a few examples [1]. However, it is not only government agencies that have witnessed the transformation of ZT security strategy. Both the private sector and higher education system have also undergone this evolution from perimeter-based security to a security approach based on ZT tenets [1].

The perimeter security model has historically been founded on the idea of inherent trust, where everything inside the network is taken for granted as being reliable. ZT model on the other hand is designed to drastically reduce risks inside the network, thereby enabling network operators and providers to live up to their security responsibilities and commitments. ZT is built on an identity-centric approach that combines traditional defense-in-depth security principles with runtime policy-based authorization [3].

Report in [4] notes that organizations that depend on perimeter-based security models do not have the visibility, solution integration, and agility to deliver timely end-to-end security protection. It thus, suggests that such organizations need a security model like ZTA that does not only adapt to the complexity of modern environment, but also accommodates the mobile workforce, protect people, devices, applications and data, irrespective of their location. The ZT security approach in its journey to maturity is envisioned "as an integrated security philosophy and end-to-end strategy" that should apply to the entire digital estate [4]. Table 1 highlights the key differences between perimeter-based and zero trust security models.

Table 1: Zero Trust Model Vs. Perimeter-based Security Model

Perimeter-based Model	Zero Trust Model
Operates on the basis that anyone or any device inside the corporate network is trusted.	Built on the principle that no user or device should be inherently trusted.
Involves layered security where IT teams put perimeters of security around individual assets.	Access is based on identity verification irrespective of location, network, or device.
More effective when the network is entirely on-premises.	Accommodates mobile and remote workforce.
Lacks visibility, solution integration, and delivery of end-to-end security protection.	Ability to protect people, devices, applications and data irrespective of their location.
Cumbersome, expensive, and vulnerable to maintain.	Adapts to complexity of modern environment.

It has been predicted that the next-generation IoT will enable much of the world's economic activities and thus, controls the critical infrastructure (smart power grid, smart healthcare, smart manufacturing) in the digital transformation era [5, 6]. However, most IoT devices are still vulnerable to Distributed Denial-of-Service (DDoS) attack which is the most common cyberattack against critical infrastructure in recent times with catastrophic consequences. The study in [7] proposes a "Quantum-safe Deterministic IoT" that will drastically reduce DDoS attacks, and also provide Quantum-safe encryption that can withstand attacks by Quantum computers. The proposed paradigm in the article is envisaged to improve cybersecurity in IoT and to significantly reduce enterprise's operational costs.

While these research efforts show numerous approaches and benefits of implementing ZTA to effectively reduce the attack surface of enterprise resources by threat actors, not so much attention has been focused on the impact on the workforce who are the main and regular users of the IoT and mobile devices used to communicate and access organization's information and assets. The objective of this study is to examine the implementation of ZT model, to identify the key challenges facing the adoption of ZTA as a new security paradigm, as well as the processes organizations need to follow to secure their critical assets and workforce wherever they are located. The contributions of this study include:

- Identifying and examining the critical challenges of implementing ZTA that covers resource constraint devices used in workplace.
- Recommendation of strategic schemes for all-inclusive realization of ZTA in organizations.
- A simplified process model for transitioning from perimeter-based security model to ZTA.

The rest of the paper is structured as follows: Section 2 examines the state-of-the-art and the challenges of ZTA implementation in workplaces. Processes and strategic schemes for achieving optimal ZTA are discussed in section 3. Section 4 provides the conclusion and future direction of the study.

2 IMPLEMENTATION AND ASSESSMENT OF ZERO TRUST ARCHITECTURE IN WORKPLACES

The adoption of IoT, edge computing, and other emerging and disruptive technologies in workplaces has thrown up a new challenge in the ability of an enterprise to effectively secure its assets and critical infrastructure using the traditional perimeter-based security architecture [2]. Digital transformation in workplaces creates a new work environment that allows both employees and partners to collaborate and access corporate resources remotely or virtually on any device without it hindering or affecting their productivity. As organizations drive their digital efforts, the security perimeter is no longer built around on-premise network, but it extends to other infrastructural components including cloud applications as well as mobile and IoT devices installed through the corporate network and clients' locations.

The conventional perimeter-oriented security firewall - implemented as a Virtual Private Network (VPN) security model, was never built to protect or support today's digital estate that consists of services and endpoint devices managed by public cloud providers. The legacy model is considered to be cumbersome, expensive, and vulnerable to maintain. There is no "threat-free" environment and thus, every company that engages in digital transformation process will also need to transform the security model – one which assumes breach at all times and therefore requires explicit verification of activities, automatically enforces security controls, and employs the Principle of Least Privilege (PoLP) access as envisioned in ZTA [4].

Study in [2] identifies key requirements for the implementation of ZTA which include: authentication, access control, encryption, micro-segmentation, and security automation. The authors present a simplified ZT logical model adapted from the core logical components architecture developed by NIST. The article highlights the functionalities of three components, namely: Policy Engine (PE), Policy Administrator (PA), and Policy Enforcement Point (PEP). Whereas PE is responsible for making access decision based on enterprise policies, (and thus, functions as the 'brain' of ZTA), PA works closely with PE to ascertain whether to allow or deny access as per PE's decision. PEP on the other hand, enables, monitors, and also terminates connection between subjects and enterprise resources. According to the report in [4], there are six foundational elements for implementing ZTA controls and technologies, which are: identity, devices, applications, data, infrastructure, and networks. Figure 1 presents the logical components of ZT model adapted from [1, 2, 4]. In the picture, the subject elements (identities and device) are categorized as 'untrusted', while the object element or subscribed resources (data, apps, infrastructure, and network) are categorized as 'trusted'. Both the subjects and the objects are located on the data plane of the network infrastructure. The control plane houses the PE and PA components while the PEP component is situated on the data plane alongside the elements to provide access control on enterprise's critical resources based on the security policies. The figure also illustrates the capability of the model to provide visibility and analytics as well as automation requirements of the architecture, this capability apparently increases towards the trusted zone and decreases towards the untrusted zone.

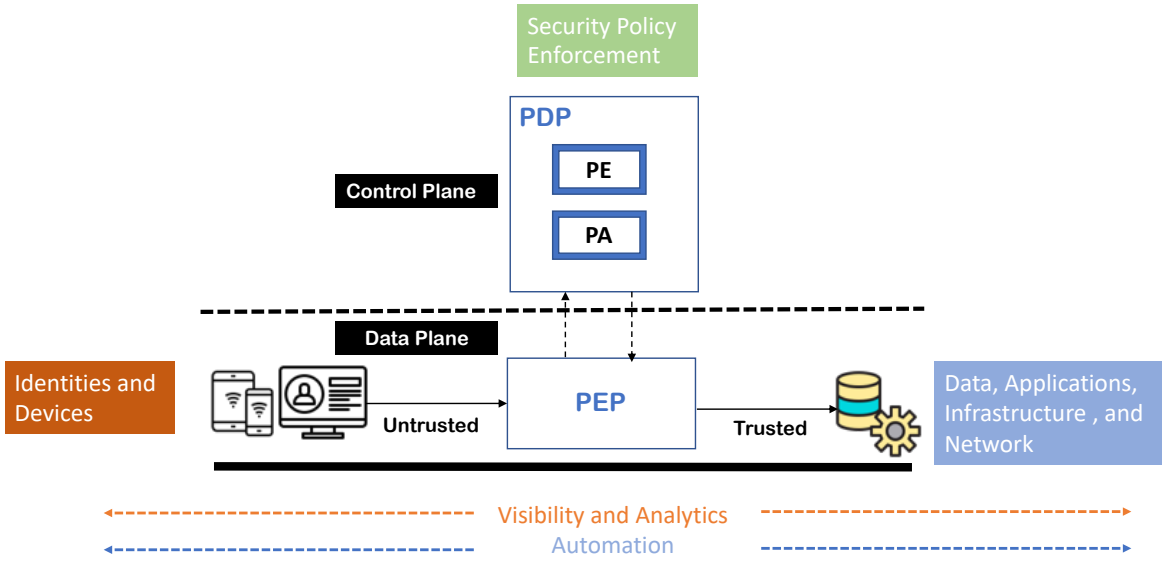

Figure 1: Logical Components of Zero Trust Model

2.1 Deployment Scenarios and Use Cases of ZTA

Many organizations are embracing ZTA tenets and have implemented some of the elements in their enterprises' security architecture. Originally, ZTA is envisioned for organizations that are spatially dispersed and or have highly mobile or remote workforce [1]. Table 2 shows the mapping of ZTA requirements and organization's security policies to ZT elements.

A deployment could be a hybrid implementation of both perimeter-based and ZTA infrastructure which can run concurrently in an enterprise's operations. The publication in [1] identifies the following deployment scenarios and use cases: (a) Enterprise with satellite facilities (b) Multi-cloud/Cloud-to-cloud Enterprises (c) Enterprise with contracted services (d) Collaboration across Enterprise boundaries (e) Enterprise with public or customer-facing services.

Table 2: Mapping ZTA Requirements and Security Policies to the Elements

ZT Elements	ZT Requirements	Applicable Security Policies
Identities (people and services)	Authentication & Adaptive Access Control	Verify Identity Provider, MFA, and User/session risks
Devices (Corporate and unmanaged)	Adaptive Access Control & Authentication	Check device risk and compliance state Verify device identity
Data (emails & documents, Structured data)	Encryption	Ensure data classification, labelling, and encryption
Applications (Cloud Apps, On-premises Apps)	Adaptive Access Control & Micro-segmentation	Provision adaptive access to resources and assets
Infrastructure (Cloud services, JIT and version control)	Access Control, Threat intelligence, Security automation and orchestration	Provide access and runtime control, and ensure threat protection
Network (Network delivery & Internal micro-segmentation	Micro-segmentation & Software-Defined Network (SDN)	Provide access and runtime control, and ensure threat protection

2.2 Migrating to a ZTA

How an enterprise transitions to a ZTA strategy depends on its current cybersecurity architecture, posture, and operations. According to the publication in [1], ZTA implementation should be an incremental process, rather than a wholesale replacement of the existing infrastructure. This however, requires a baseline competence which include: identifying and cataloging assets, subjects, business processes, traffic flows, and dependency mapping. The different flavors of ZTA migration are briefly described in the subsections below.

2.2.1 Pure Zero Architecture.

This migration approach also known as 'greenfield' approach, is where ZTA is built from ground-up, and may require organizational changes. However, it is not considered a viable option for Federal agencies or organizations with established networks.

2.2.2 Hybrid ZTA and Perimeter-based Architecture.

This approach creates room for flexibility, and enables ZTA workflows to co-exist with non-ZTA workflows in an enterprise. Steps to introducing ZTA to a perimeter-based network are as follows: (1) Identify Actors on the Enterprise. (2) Identify Assets Owned by the Enterprise. (3) Identify Key Processes and Evaluate Risks Associated with Executing Process. (4) Formulating Policies for the ZTA Candidate. (5) Identifying Candidate Solutions. (6) Initial Deployment and Monitoring [8].

2.3 Threats and Risks Associated with ZTA

Implementation of a ZTA does not provide absolute cover against cybersecurity risks in an enterprise. However, a careful implementation and maintenance of ZTA in addition to other security measures, could help mitigate the overall risk and protect against common known threats. When implementing a ZTA, there are some threats with unique features which need to be considered. ZTA, when not properly implemented or maintained can suffer the following attacks or threats.

1. Subversion of ZTA Decisions Processes: As the PE and PA are the key components of the architecture, an improper configuration or monitoring could compromise these components and thus, creates open doors for attacks.
2. Denial-of-Service or Network Disruption: Enterprises implementing ZTA can mitigate this threat by applying redundancy approach, i.e. storing the policy enforcement in a properly secured cloud environment or replicating it across many sites in accordance with cyber resilience recommendations [9].
3. Stolen Credentials and Insider Threats: The ZT principle of no implicit trust based on network context or location implies that for an attacker to obtain access to an enterprise, they would need to compromise an existing account, system, or device.
4. Visibility on the Network: Some network traffic may be opaque to layer 3 network analysis tools. An enterprise that cannot perform deep packet inspection (probably due to apps/services that are resistant to passive monitoring) must use other methods to assess a possible attacker on the network.
5. Storage of System or Network Information: Stored data resulting from network traffic monitoring and analysis could be a target for attackers, and thus, should be protected against reconnaissance attack. Management tools could also be another source of attack or attack vectors for stored information.
6. Reliance on Proprietary Solutions (Vendor-Lock-in): The tendency of not having common or open standards for assets used to store and process information can lead to interoperability issues with possible risks of disrupting core business functions of an enterprise and decreased network performance and stability.
7. Use of non-person entities (NPE) in ZTA administration: Automated technologies such as AI agents used for configuration and policy enforcement are prone to 'false positive' and false negative' detection of attacks which may impact the security robustness of the ZTA. The risk here is that "an attacker will be able to induce or coerce an NPE to perform some task that the attacker is not privileged to perform" [1].

2.4 Extending the ZTA to Mobile Devices and IoT solutions used in Workplaces

With a significant increase in the adoption of mobile and IoT devices as key enablers of remote and hybrid work model, many organizations are dealing with new security concerns and an expanded attack surface that they are not fully equipped to handle. Securing IoT and mobile devices requires an end-to-end implementation, however, this comes with additional layer of complexity given the heterogeneity in the design of the various components which increases the challenges of integrating them into existing security tools in the enterprise network. Another challenge in securing IoT and mobile devices is their limited capability and connectivity coupled with their ubiquitous deployment in remote work stations which exposes their high-value target to attackers.

2.4.1 Mobile Security.

The increasing acceptance and implementation of digital transformation in workplaces adds to the challenge of protecting enterprise resources using the traditional perimeter-based network security. This is because digital transformation creates a new work environment that allows both employees and partners to work together and access organizational resources either virtually or remotely on any device without limiting their efficiency. One of the benefits of using mobile devices in workplaces is that it allows organization's users to access information resources anytime and anywhere. This however, presents both opportunities and challenges. While constant internet access and availability through cellular and Wi-Fi connections makes business practices more efficient and effective, there is also the challenge to guarantee the availability, confidentiality and integrity of the information accessed, processed, and stored by these mobile devices.

There is no doubt that mobile security vulnerabilities can scale along with their deployment in organization's business processes. Some factors that contribute to this threat include: "Failure to document security issues; Lack of resources to respond to reported threats; Incorrect device usage, leading to data leaks; and Inability to train an influx of users on security" [10]. Scaling security along with mobile deployment does not only require some significant amount of time but also some level of expertise which means network administrators must be able to respond to every security issue as it arises; and this can be difficult or impossible as more devices are introduced into the network. To keep up with this mobile security challenge, a tool known as "EMM software" has been developed that provides remote control of every device in the field. This helps administrators to solve security problems from any location.

A ZTA solution to mobile security issues as proposed by NIST in [11] include:

1. Configuring 'trust' (trustworthiness) in mobile device that are used to access organization's resources.
2. Containerization (Micro-segmentation) – i.e. separating organization's data from employee's data
3. De-provisioning of mobile devices when they are no longer in use (either stolen or employee leaves the company)
4. Enabling identity federation
5. Enhancing visibility for systems administrators into mobility security events (quickly providing notifications and alerts about a device and data compromise).
6. Implementing industry standards for mobile security controls, thereby reducing (long-term) costs and the risk of vendor lock-in.

*2.4.2 IoT Security***.**

The use and deployment of IoT devices have become ubiquitous in many business operations. This development is largely helpful, as these devices provide numerous measurable advantages like improved efficiency and real-time data insights. When setting up these networks, it is necessary to consider the vulnerabilities, including having unsecure IoT devices. IoT devices are increasingly being used in offices, and many of them unintentionally give cybercriminals access to a wider

range of opportunities. It is possible to use these systems safely, but doing so requires certain steps that many companies and users fail to take. [12].

One of the IoT device vulnerabilities is the lateral movement attack as the connected IoT devices have the tendency to expand the attack surface of an organization's security infrastructure. A network's potential entry points increase with the number of items on it. Due to the quick adoption of IoT by modern businesses, cybercriminals now have more ways than ever to compromise these systems [4]. Another vulnerability is the limited built-in protection in IoT device which compounds the threat of lateral movement in organization's network. While the security of regular computers and other electronics used in workplaces are supported by anti-malware software, automatic updates, and encrypted traffic, that is not the case with IoT devices as they lack sufficient built-in security. Some solutions have been proposed to address the vulnerability issues in IoT devices. This include: network segmentation, changing default settings on devices, enabling automatic updates in devices' firmware, and employing stricter device policies in organizations [12].

3 PROCESSES OF ACHIEVING OPTIMAL ZTA IN WORKPLACE

As mentioned earlier, a successful ZTA implementation is not a wholesale replacement of the traditional perimeter-based architecture, rather, it is an incremental journey that involve certain processes to achieve the optimal security outcome intended in the design of the ZT model. The planning and execution of a Zero Trust security model differs depending on a variety of factors, including organizational needs, existing technology implementations, and security stages. This section discusses the processes and schemes that can help organizations maximize ZTA benefits in securing their workplace and assets.

3.1 ZTA Maturity Model

It is encouraging to note that some communication service providers like Ericsson [3] and cloud service providers like Microsoft [4] and Google [13] have started to implement the ZTA; still, very few of the organizations have reached the optimal ZT maturity level as advocated in [8]. This goes to show that there are certain barriers that need to be overcome by the various organizations to attain the optimal ZTA maturity level. Figure 2 shows different levels of ZTA Maturity Model as proposed in [8].

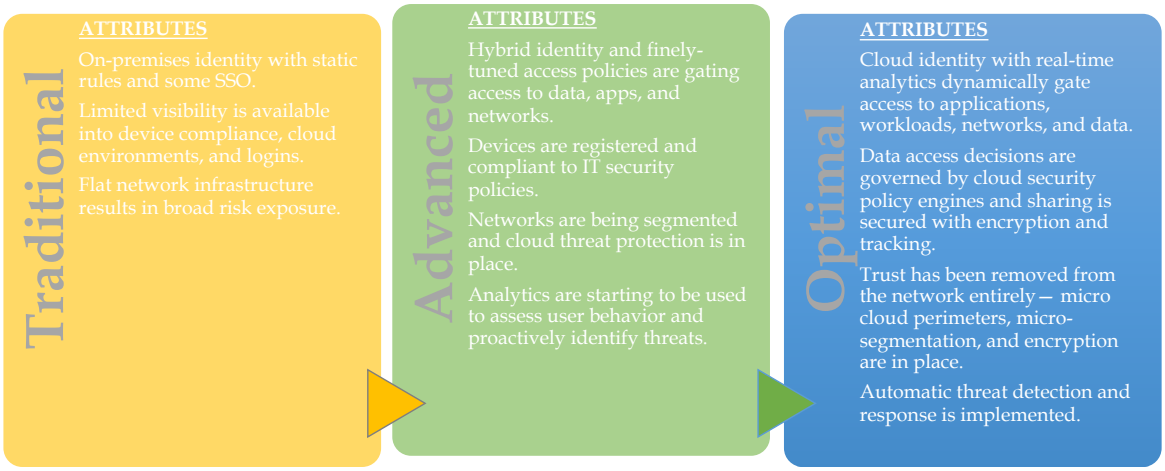

Figure 2: Levels of ZTA Maturity Model [4, 8]

Organizations transitioning to ZTA will by default, start at the traditional level where they need to take a thorough inventory and evaluation of the resources across on-premises and cloud environments, prioritizing security measures according to their level of significance to the enterprise [4]. Here, an organization considers reducing password risks using methods like MFA and SSO access to cloud apps. It also put in place, mechanisms that can provide visibility into device compliance, cloud environments, and logins to detect any form of abnormality. At this stage, an organization deploys networks segmentation to limit lateral movement inside the firewall perimeter. The advanced level shows a significant progress in the ZTA implementation where an organization uses real-time risk analytics to assess user behavior and device health to make smarter decisions. The organization also engages proactively in identifying and fixing flaws due to configuration errors and missing patches to reduce threat vectors [4]. The optimal level is the mature stage of ZTA implementation where an organization is "able to dynamically enforce policies after access has been granted to protect against violations" [4]. At this stage, the organization devises mechanisms to analyze productivity and security signals that will help drive user experience optimization through self-healing and actionable insights [4].

The maturity model described above needs not to be followed rigidly. Transitioning to ZTA can be an overwhelming task for many organizations particularly, small and mid-size businesses and such organizations may not want to go into full scale adoption of ZTA. Also, some organizations may decide based on their security policies, not to adopt cloud services to reach the optimal maturity level. Figure 3 illustrates a simplified process model that can help organizations transition to ZTA according to their security needs.

The first step is to discover all the organization's physical and virtual assets including network components, core business applications, network traffic, subjects, and service accounts. The second step is the assessment which involves detailed inventory of the assets and performing a threat-modelling exercise using the criteria defined in the organization's PE and enforcement policies. This is followed by the initial deployment of the architecture and requires the implementation of the logical components and modification of the components to reflect new security rules and policies. The next step is to continuously monitor the system's operations to identify any anomaly and to understand communication patterns. The information gathered can be used to established a baseline to help further refine the enforcement policies. After enough confidence has been attained in the initial deployment, the organization can expand its ZTA coverage to accommodate other business processes while persistently monitoring the network infrastructure. This process can be adapted based on the organizational security posture and risk tolerance.

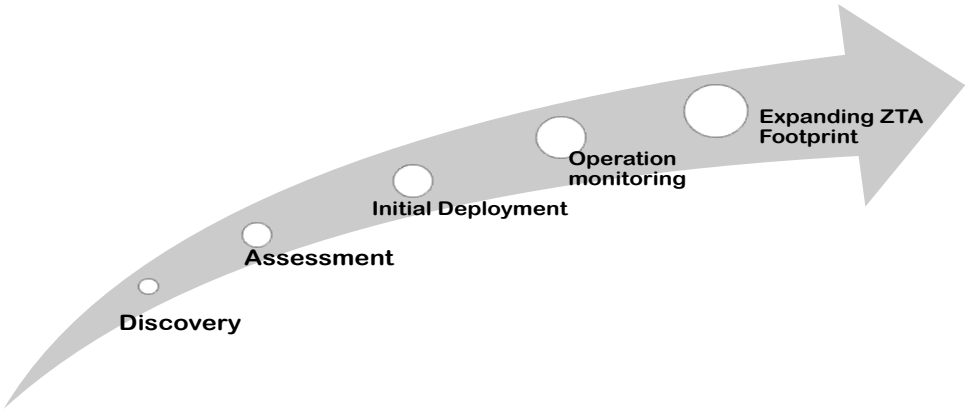

Figure 3: A Simplified Process Model for Transitioning to ZTA

3.2 Integrating Blockchain and 5G Technologies in Zero Trust Security Model

Proponents of ZTA have made strong cases for the inclusion of emerging technologies like smart blockchain [14], post-quantum cryptography [7], and 5G technology [3] in the adoption of ZTA to provide more robust security of enterprise resources and assets. The proposed ZT maturity model in [8] requires incorporating these new technologies to achieve or reach the optimal level of the ZTA maturity model. Each of these technologies have specific features that can be adapted to reinforce ZTA tenets on the various architectural components. For example, blockchain and 5G technologies can be used to provide a 'passwordless' authentication and real-time adaptive access for identities and devices elements of ZTA. The prospects of this integration have been touted in the financial industry [15].

This subsection provides a brief discussion on each of these technologies and how they can be leveraged to augment ZTA tenets onto the logical components, particularly the ones located in the 'untrusted' zone. Table 3 highlights the key enabling security features of the technologies that can enhance a successful launch of ZTA in organizations.

Table 3: Blockchain and 5G Enabling Security Features for ZTA Implementation

	Blockchain	5G Technology
Enabling Security Features	Immutable system of explicit trust	Secure digital identities for both subjects and objects (resources) of enterprise network.
	Distributed verification vs. Traditional client-server approach	Secure transport that enables secure data exchange between the user equipment and radio base stations using cryptographic algorithms.
	Threat Detection and Prevention	Enables enforcement of policy frameworks on micro-perimeter (or SDP) with granular and adaptive access control mechanisms.
	Provides early break of attack chain (i.e. lateral movement attack)	Monitoring of the security posture of network assets and adherence to security policies, which aids in threat detection.

3.2.1 Blockchain.

While ZTA assumes endpoint devices as well as users and subscribing services to be untrusted until they have been verified and authenticated, attackers can still gain foothold in an authenticated authorized session via the endpoints using Advance Persistent Threats (APT). The work in [14] proposes a Blockchain-enabled Intrusion Detection and Prevention System (BIDPS) that supplements ZTA capabilities of securing endpoints. According to the findings reported in the study, BIDPS does not only mitigate lateral movement attack but also creates an immutable system of explicit trust.

3.2.2 5G Technology.

Corporate networks and mobile devices that operate on 5G network and technology stand to gain more from ZTA implementation [3]. The 5G network access security features can provide users of mobile or connected IoT devices with secure access to services and protect against attacks between device and the radio node. The network domain security features on the other hand, enables nodes to have a secure communication between signaling data and user data. Another 5G security feature is the service-based architecture (SBA) domain security which supports web technology and protocols by enabling scalable deployments using virtualization and container technologies as well cloud-based processing platforms. This of course, complements the SDN and micro-segmentation requirement of the ZTA implementation [2].

4 CONCLUSION

The traditional mindset of securing a network perimeter can no longer sustain new organizational policies and working models such as Bring Your Own Device (BYOD) and remote workforce. A hybrid workforce comes with a number of security risks and challenges. Organizations are exposed to a new threat landscape as a result of these new working practices. In order to transition from the conventional perimeter-based security model to a borderless-based defense, a paradigm shift is therefore required. The transition towards Zero Trust model by organizations represents a major step change in the cybersecurity conventional operations. However, this migration requires thoughtful plans and processes that can help organization maximize the benefits, and reduce the risks associated with ZTA implementation in workplace.

In this paper, we examined different implementation approaches of ZTA in workplaces and identified critical challenges that impede its adoption by organizations. Given that migrating to ZTA as a new security paradigm is an incremental journey, we also discussed processes and strategic schemes that organizations can follow to realize full implementation of the ZTA in workplaces. While previous studies have focused on the ideal standards and approaches of implementing ZTA, this paper advanced the need to pay more attention to IoT and Mobile devices used in workplace as they are considered the 'weakest' point in the cyberattack chain. It also recommends a more simplified process model for transitioning to ZTA. This is an ongoing study, future work will focus on developing a ZT framework that integrates the emerging technologies discussed here and how the technologies can complement each other to help organizations realize full and optimal ZTA implementation.

REFERENCES

[1] Scott Rose, Oliver Borchert, Stu Mitchell, and Sean Connelly. 2020. *Zero Trust Architecture*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

[2] Naeem F. Syed, Syed W. Shah, Arash Shaghaghi, Adnan Anwar, Zubair Baig, and Robin Doss. 2022. Zero Trust Architecture (ZTA): A Comprehensive Survey. *IEEE Access* 10, (2022), 57143–57179. https://doi.org/10.1109/ACCESS.2022.3174679

[3] Jonathan Olsson, Andrey Shorov, Loay Abdelrazek, and Jorden Whitefield. 2021. 5G zero trust – A Zero-Trust Architecture for Telecom. *Ericsson Technology Review* 2021, 5 (May 2021), 2–11. https://doi.org/10.23919/ETR.2021.9904691

[4] Alex Weinert. 2021. Evolving Zero Trust—Lessons learned and emerging trends. *Microsoft Security Blog*. Retrieved February 28, 2023 from https://www.microsoft.com/en-us/security/blog/2021/11/03/evolving-zero-trust-lessons-learned-and-emerging-trends/

[5] WEFUSA_IndustrialInternet_Report2015.pdf. Retrieved February 28, 2023 from https://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf

[6] Industrial-internet-insights-report-for-2015 | GE News. Retrieved February 28, 2023 from https://www.ge.com/news/taxonomy/term/4386

[7] Ted H. Szymanski. 2022. The "Cyber Security via Determinism" Paradigm for a Quantum Safe Zero Trust Deterministic Internet of Things (IoT). *IEEE Access* 10, (2022), 45893–45930. https://doi.org/10.1109/ACCESS.2022.3169137

[8] 2021. CISA Zero Trust Maturity Model. (2021).

[9] Ron Ross, Victoria Pillitteri, Richard Graubart, Deborah Bodeau, and Rosalie McQuaid. 2021. *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*. National Institute of Standards and Technology, Gaithersburg, MD. https://doi.org/10.6028/NIST.SP.800-160v2r1

[10] SOTI. 2023. 3 Overlooked Problems in Enterprise Mobility—And How to Solve Them. *IoT For All*. Retrieved February 28, 2023 from https://www.iotforall.com/3-overlooked-problems-in-enterprise-mobility-and-how-to-solve-them

[11] Joshua Franklin, Kevin Bowler, Christopher Brown, Spike E Dog, Sallie Edwards, Neil McNab, and Matthew Steele. 2019. *Mobile device security: cloud and hybrid builds*. National Institute of Standards and Technology, Gaithersburg, MD. https://doi.org/10.6028/NIST.SP.1800-4

[12] Emily Newton. 2023. Unsecured IoT Devices Give Hackers a Backdoor into Your Network - Get Protected Now. *IoT For All*. Retrieved February 28, 2023 from https://www.iotforall.com/unsecured-iot-devices-give-hackers-a-backdoor-into-your-network

[13] BeyondCorp Zero Trust Enterprise Security. *Google Cloud*. Retrieved February 28, 2023 from https://cloud.google.com/beyondcorp

[14] Lampis Alevizos, Max Hashem Eiza, Vinh Thong Ta, Qi Shi, and Janet Read. 2022. Blockchain-Enabled Intrusion Detection and Prevention System of APTs Within Zero Trust Architecture. *IEEE Access* 10, (2022), 89270–89288. https://doi.org/10.1109/ACCESS.2022.3200165

[15] BBVA. 2020. Quantum computing, 5G and blockchain: technologies that will mark the next decade in banking. *NEWS BBVA*. Retrieved February 28, 2023 from https://www.bbva.com/en/quantum-computing-5g-and-blockchain-technologies-that-will-mark-the-next-decade-in-banking/