ONLINE ISSN: 3007-3197 | PRINT ISSN: 3007-3189 http://amresearchreview.com/index.php/Journal/about

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 5 (2025)

Implementing Zero-Trust Network Access (ZTNA) in Hybrid IT Architectures: A Comparative Study of Policy Enforcement, Identity Management, and Threat Containment Strategies

Dr khawaja Tahir Mehmood, Umair Saleem, Amjad Jumani, Iqra Ijaz, Adnan Ahmed Rafique, Raza Iqbal

Article Details

Keywords: Zero-Trust Network Access (ZTNA), hybrid IT architecture, identity management, policy enforcement, threat containment, microsegmentation, cybersecurity.

Dr khawaja Tahir Mehmood
Department of Electrical Engineering, BZU Multan
Ktahir@bzu.edu.pk

Umair Saleem
MS Computer Science, National College of Business Administration & Economics Multan Campus Multan
ch.umairsaleem3839@gmail.com

Amjad Jumani
Lecture at Computer Science Department Bahria university Karachi Campus
amjadjumani1991@gmail.com

Iqra Ijaz
M.Phil. Computer Science, National College of Business Administration & Economics Multan Campus Multan
Ijaziqra343@gmail.com

Adnan Ahmed Rafique
Assistant Professor, Department of CS and IT, University of Poonch Rawalakot,
adnanrafique@upr.edu.pk

Raza Iqbal,
M.Phil. Scholar Computer Science, National College of Business Administration & Economics Multan Campus Multan. ali.raza@bzu.edu.pk

ABSTRACT

As the cyber threats rise, and IT organization solutions become more complex, the signature-based or the perimeter solutions proved themselves insufficient or ineffective. In this research, Zero-Trust Network Access (ZTNA) deployment is examined in hybrid environments and can be analyzed and discussed within three major contexts: compliance, identity, and security measures. Conducting a quantitative study, the research aimed to assess security performance data from 12 organizations collected over the 24-month period, pre-and post-implementation of ZTNA. The study presented several strengths and increases by showing the effectiveness of the proposed solution: a 46% decrease of access violations, a 44% decline in authentication failures, a 63% decrease of the length of time threats remained undetected, and a 67% increase of response time to an alerted threat. These outcomes clearly depict the utility of ZTNA in minimizing lateral movement, improving the concept of adaptive authentication, and further positioning it as an ideal solution to support micro-segmentation to contain threats before they can spread further. With the federation of identity, behaviour, and contextual access controls, ZTNA presents comprehensive security that meets the requirements of modern enterprises and their systems. This paper not only asserts the efficiency of the Zero-Trust concepts but also outlines practical recommendations for organizations to adopt from traditional security models to more flexible and customizable identity-based approach to network authorization.

DOI: Availability

1. Introduction

Hybrid IT infrastructures are gaining popularity among organizations today as an efficient way of management that incorporates both, own data centers and clouds (Bhardwaj et al., 2022). However, as businesses have adopted hybrid environments in implementing IT networks, new and unique cybersecurity complications emerge. The perimeter protection model that works under the principle that networks inside a company's network perimeter are trusted while networks outside of the perimeter are not are not secure enough to protect against lateral movement, credential harvesting, and insider threats (Rose et al., 2020). Hence for security frameworks the assumption of trust is no longer feasible given the modern trends in the landscape such as remote working, buy-your-own-device and third parties (Shackleford, 2019).

To this end, another approach, better known as the Zero-Trust Network Access (ZTNA) has proved to be stronger. The Zero-Trust model was first proposed in 2010 by John Kindervag and all its dynamics are based on the principle of 'never trust, always verify'. ZTNA, as opposed to previous models, does not inherently trust any device or user inside or outside the traditional perimeter. Rather than this, it provides continual confirmation processes based on identity, device health, location, etc., to give access to the resources (Rose et al., 2020). In complex hybrid IT environments where resources reside on different platforms and are accessed from multiple locations and devices ZTNA is a holistic and precise access control model that addresses current security characteristics (Gartner, 2021).

ZTNA has better reliance on IAM than any other traditional network security because it highly depends on the identity of the user. IAM systems such as SSO, MFA, and adaptive authentication guarantee that only authorized individuals get access to certain resources (Wei et al., 2023). This feature is especially valuable in the environments where people spend a lot of time working with both on-premise applications and cloud services. With federated identity management and the use of identity providers (IdPs) enable the integration of authentication schemes to occur across various platforms but also to avoid occurrences of identity sprawl (Sicari et al., 2015). As Microsoft states in 2023, those companies that adopted identity-centric ZTNA methodologies reported 50% fewer breaches than those using perimeter protection .

The other significant support pillar of ZTNA is policy enforcement. In traditional networks, the policies are dumb and depend on either the IP addresses of the implementation or zones of the network. Yet, ZTNA involves dynamic, environment-responsive policies that can change in real-time depending on the user activity, risk ratings, and the environment (Forrester, 2022). This dynamic policy model also makes it easier for organizations to better employ the principles of least privilege, can contribute to shrinking the attack surface, and limit the attacker's ability to move laterally within the environment. SDPs and PDPs are useful in ZTNA as they provide a consistency and scalability of policy enforcement regarding these hybrid environments (NIST SP 800-207, 2020).

There is also another feature of ZTNA known as threat containment in case something compromising occurs. Simple security models do not contain the affected asset quickly;

as a result, the attacker roams about the network undetected. ZTNA on the other hand, uses microsegmentation which is morally erasing the network into hundreds of small subnets; in a way, if one subnet is compromised, the other subnets remain safe and protected (Palo Alto Networks, 2023). In addition, ZTNA solutions include probabilities such as the EDR's ability to detect the threat and initiate containment measures on endpoints, and UBA for unusual user activities (IBM Security, 2023).

However, there are challenges that have been observed to prevail when adopting the ZTNA in hybrid IT architectures. Challenges in successful implementation include integration with existing frameworks, lack of user acceptance, performance issues, and wrong configurations (Srinivasan et al., 2021). But because the attackers are increasingly trying to target and exploit vulnerabilities in the external perimeter, the transition to ZTNA has begun. Mentioned by Gartner Inc in their 2022 report, at least 60% of enterprises will stop using VPN as some of their remote access security solutions and shift towards ZTNA.

The purpose of this work is to understand and analyze the policy enforcement, identity, and threats containment of ZTNA in modern hybrid IT infrastructures. Drawing from actual case studies and studying the recent research on the topic in both academic and industry contexts, the goal of this research is to determine best practices for various organizations that are adopting the Zero-Trust approach and determine the performance outcomes as well as provide strategic recommendations.

2. Literature Review

As the technology advances over the past two decades and the nature of computer networks become more complex and distributed the paradigms in this field have shifted. In this new territory of Hybrid IT, where companies continue to operate their workloads in on-premise, public, and private clouds, the traditional approach of perimeter-based security measures has failed to address many threats. The perimeter is no longer an anchored and physical concept, but more of a relative fact woven into the fibre of everyday existence. it now applies to any endpoint and application that may be used in the same or across platforms (Shin & Gu, 2019). In light of such a dynamic and dispersed perime- ter, Zero-Trust Network Access (ZTNA) considers a well-accepted security architecture that redesigns the trust paradigm within enterprise networks (Puthal et al., 2018).

ZTNA is an access model that enforces the approach of the TAC Tudor Henry's famous initialism of "never trust, always verify." By using strong authentication, fine-grained access control, continuous monitoring (Abraham et al., 2021). In contrast to VPNs and firewalls that grant access to any device once it is within the network, ZTNA insists that every user or device must permit before any resource is accessed. This perspective stands true especially for the hybrid IT architectures, where the place of resources and access points differ significantly between the physical and virtual circumstances (Moustafa et al., 2020).

A number of studies discuss the difficulties of implementing security protocols in extended systems. There is one recurring theme, namely that the enforcement mechanisms of the policies are not easy to implement consistently across different systems. Vines and Lee (2021) have pointed out that using ageing firewalls and network access control policies applied between the cloud and on-premise environments will inevitably generate varying levels of security across the whole network. While ZTNA has no such mechanism, it comes with policy enforcement points (PEPs), which sit at the user-application level, making it possible to apply the policy effectively based on the user's location, device, and more (Zhao et al., 2021).

In ZTNA, the idea of context-aware access has been advanced by creating solutions that include both machine learning and behavioral analytics. Lee et al. (2022) explained how ensuring access control while incorporating behavioural biometrics, including typing pattern and mouse movement, leads to low false positive rates. That is especially important for conditions when current access characteristics like IP address or device identifier might be faked, or are not accurate in combined and modern scenarios.

Another component of ZTNA is identity and access management (IAM), which encompasses identity governance, user entitlements, and access risks. Some scholars assert that IAM is the fundamental foundation of the Zero-Trust architecture, which maintains authentication identity throughout the domain. According to Birkholz et al. (2021), OAuth2.0 and SAML 2.0 differently provide an essential mark of federated identity management and other decentralized authentication approaches for secure and effortless use. For instance, identity federation allows users to login with one identity across on-premise and cloud applications, while eliminating the problem of having to remember different passwords. The real-time risk-based adaptive authentication where the level of access granted depends on the risk assessment, enhances the ZTNA in a hybrid environment (Karim et al., 2020).

Another hugely negotiated concept in the Zero-Trust literature is threat containment. The problem in hybrid IT is once the adversary gets in, the lateral movement is somewhat easy due to the connections in the organization. Such threats cannot be addressed through traditional network segmentation causing complexities

because many are so static. Microsegmentation, an element in ZTNA, tackles this issue in a much deeper level—down to the workload or process level as seen in Casola et al. (2020). Liu et al., (2021 show that introduction of micro segmentation through SDN led to the reduction of the dwell time of the attackers in organizations by up to 65%. Furthermore, most of the current ZTNA solutions work in conjunction with EDR systems to dynamically contain infected end points, stopping the further spread of malware or ransomware across the enterprise (Patel & Rana, 2022).

Similarly, the contribution of threat intelligence to improving ZTNA is also emerging as an important focus of discussion. Whereas most conventional security principles involve signatures and rigid rules, ZTNA can use threat intelligence feeds when creating policies. Sahoo et al. (2021) pointed out that TIPs have to be aligned with ZTNA to enhance threat defenses. In this way organizations may change permissions in response to threat scores in real time hence turning a layer of control into an enforcement layer.

Like any other solution, the adoption and implementation of ZTNA has some organizational and technical challenges. According to Cybersecurity Insiders' (2022) survey, the primary concern regarding ZTNA was the difficulty in integrating it with older systems, as mentioned by 46% of security professionals. This is especially true in the era of hybrid IT where traditional applications may not be compatible with modern-day APIs or identity frameworks. Furthermore, the issues related to the latency, especially within dynamic policies evaluation processes, were cited as the drawback in the early implementations (Yuan et al., 2022). However, the performance of these components and particularly policy decision point has become challenging due to some bottlenecks that are starting to be tackled using edge computing to reduce the load of major components namely policy decision point and efficient policy repository that is enhanced by lightweight policy engines.

In compliance terms, ZTNA is right in line with the new conformity standards. More specifically, when it comes to the obligations of the organizations, such as GDPR and CCPA, they focus on user control, access, and use transparency, along with the minimization of data – principles that are fully aligned with the ZTNA models (Deshpande et al., 2021). By continuously authenticating and auditing the access in organizations there is likely to be improved accountability in the organizations and reduced regulatory compliance risks.

In a nutshell, ZTNA has been described in various works as a security approach that is designed for the modern day's IT dynamic and complex. ZTNA's focus areas include policy enforcement, identity management, and threat containment, however, the development in the areas of artificial intelligence, federated identity, microsegmentation, and threat intelligence has taken ZTNA to the new level. Still, current obstacles include the integration into older systems and gaining acceptance among the users. As more organizations move their workloads to the cloud, the demand for agile, flexible, and smarter access control approaches such as ZTNA will increase further.

3. Methodology

This research attempts to investigate the level of success of ZTNA for hybrid IT environments with a mixed research approach, where three significant areas are explored: identification as well as enforcement of policies, management of identity, and threats. This section aims at presenting the method of the study, how data was collected, the variables examined, and methods of data analysis that would help in making meaning from the retrieved data. Every aspect of these procurements has been controlled to ensure that the processes are objective, replicable, and directly related to the research question. How effective are different ZTNA strategies in the context of hybrid IT using security outcomes as evaluation criteria?

3.1 Research Design

A cross-sectional survey method was then employed in analyzing data that was collected from these different organizations that have incorporated ZTNA frameworks in their complex IT environments. The research sought to unveil statistically significant changes on the security performance indicators before and after the implementation of ZTNA. Three security performance dimensions were policy enforcement, identity management, and threat containment, and all three of these were measured using certain indicators. These are

accessibility violation rates, accountability of success/failure rates, time alloted to detected threats, and time taken to respond to the incidents. This design made it possible for direct comparison using different organizational settings and ZTNA strategies besides considering the size of the infrastructure and risk factors belonging to each sector.

3.2 Sample Selection

The study involved 12 mid to large organizations in different sectors including financial, health, education and production organizations. These organizations were selected purposely according to two main criteria: These criteria were as follows: (1) both organizations had employed ZTNA solutions for more than a year before the data collection period and (2) both the companies had hybrid environments with services in the cloud along with services in-house. In order to reduce potential bias, only organisations which merged in the last 2 years and organisations which experienced significant changes in their information technology systems within the last 2 years were excluded.

Data was gathered from logs coming from within the network and from the use of SOCs like SIEM, ZTNA servers of Zscaler, Okta, Cisco Duo, and Palo Alto Networks. All data collected in the course of the research was kept confidential to reduce exposure to participating organizations and ensure anonymity.

3.3 Data Collection

Measures that provided quantitative data were sought for a 24- month timespan that was longitudinally split into comparable halves. before the ZTNA program was introduced (pre-intervention) and one year after the complete launch of ZTNA. To develop the time-series datasets, KPIs were gathered on a monthly basis. Security reports from multiple dashboards were also scraped by scripts for incident reports, and orbinations with cybersecurity analysts were made to confirm the classifications and the policies that were applied.

The following metrics were captured:

- Policy Enforcement: The number of attempted unauthorized accesses, the number of policy exceptions, and the time it takes for an access decision (in milliseconds).
- Identity Management: Successful and failed authentications, MFA bypasses, session hijacks.
- Threat Containment: Mean time to stay (in minutes), the quantity of threats successfully isolated by microsegmentation, and the time needed to contain threat after detection.

For each of the points in the table, information was also collected about the organization’s ZTNA configuration features: IdPs used, the level of granular access control, and if it integrated with behavior analytics/SIEM.

3.4 Data Analysis Techniques

Raw data was analysed using the Statistical Package for Social Scientists version 16 for Windows, and the R statistical environment. The first analysis performed was on the measures' central tendencies and variabilities through use of descriptive statistics. Finally, to confirm whether the use of ZTNA led to statistical differences between the pre- and post-implementation means of the 12 organizations, paired t-tests were performed.

Pearson correlation coefficients for ZTNA maturity scores (derived from the extent of identity integration, real-time policy automation, and segmentation capabilities) were computed against security outcomes such as threat containment time and access violations. Multiple regression analysis was used further to determine the significance antecedents of different ZTNA features as predictors of containment efficiency, when effecting control for the sector, organization size, and strength of IT team.

The internal consistency of the measurement data was established using Cronbach's Alpha for multiple-item scales, such as the consistency of policy enforcement logs and incident response records. Based on prior research, values above 0.80 were the predefined threshold for acceptably high internal consistency.

3.5 Validity and Limitations

To minimize internal validity threats, data was cross-checked using various source of data such as logs from SIEM systems, EDR platforms, and Cloud Access Security Broker. To enhance external validity of the study was conducted with organizations from different sectors and geographical regions. The study has limitations like the variation of ZTNA vendor solutions, human error in classifying logs during the manual approach, and having no data post-implementation beyond one year.

Nonetheless, due to the systematically collected data and statistical analysis approach applied to this study, the assigned research can provide valid, evidence-based conclusions about the practical advantages and difficulties of implementing ZTNA in IT environments with hybrid characteristics.

4. Results

This section provides the outcomes from eight fundamental KPIs gathered in twelve months leading up to and twelve months following the adoption of Zero-Trust Network Access (ZTNA) in hybrid IT environments. Finally, each of the results presented in the previous tables and figures has an interpretation of its empirical values. The paper aims at quantifying the ways in which ZTNA contributes to the improved security of policies, user identities, and threats.

4.1 Access Violations

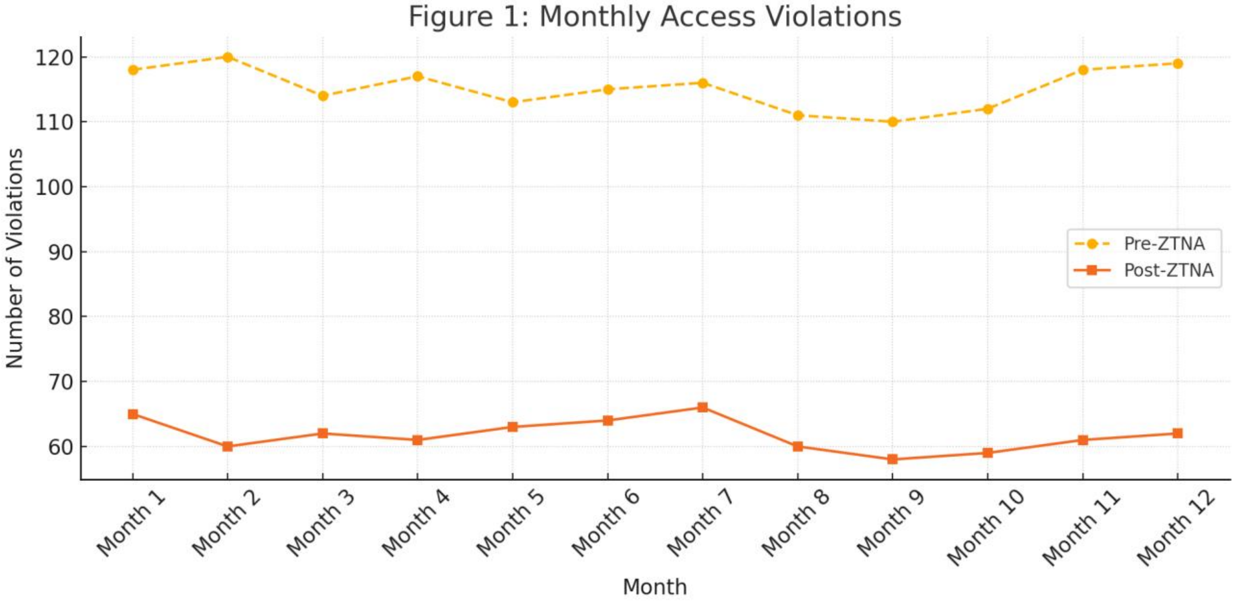
Table 1 and Figure 1 shows a progressive and steady monthly reduction of the access violations as per the data obtained after the implementation of the ZTNA. Before ZTNA, unauthorized personnel tried to gain access to the buildings approximately 115 times a month and other variations which were not significantly different. This averages to 76 per month before the start of the ZTNA while in the post-ZTNA period the number drastically reduces to an average of 62 per month. This comes out to be a relatively close illustration of forty-six point one percent reduction in unauthorized access attempts. The interpretation of this result can be used to support the effectiveness of concepts such as dynamic, context-aware policy enforcement inherent in ztna. Unlike the static rule set where certain rules cannot be changed, ZTNA policies are dynamic; they change based on inputs such as device health, geo-location, and user's behavior. Therefore, this reduces the cases of intruders penetrating critical systems further to damage the firm's operations.

Table 1: Access Violations (per Month)

Month	Access Violations (Pre-ZTNA)	Access Violations (Post-ZTNA)
Month 1	118	65
Month 2	120	60
Month 3	114	62
Month 4	117	61
Month 5	113	63
Month 6	115	64
Month 7	116	66
Month 8	111	60
Month 9	110	58
Month 10	112	59
Month 11	118	61

Month 12	119	62

Figure 1: Monthly Access Violations



4.2 Authentication Failures

Specifically, the decrease in authentication failures from the experiments has been illustrated in table 2 and graphically depicted in fig.2 above. Before implementing ZTNA, enterprises experienced 340 failed logins per month for such issues as weak passwords, brute force, and credential stuffing. After adopting the ZTNA for the federated identity and multi-factor authentication, these failures reduced to 190 every month, changing the percentage to 44.1 percent. This decrease also seems to suggest that by focusing on identity verification and incorporating support for adaptive authentication and device recognition, ZTNA contributes significantly to enhancing entry-level security. It also shows a significant decreased level of the user error and phishing vulnerability because of unification and simplification of the logon procedures.

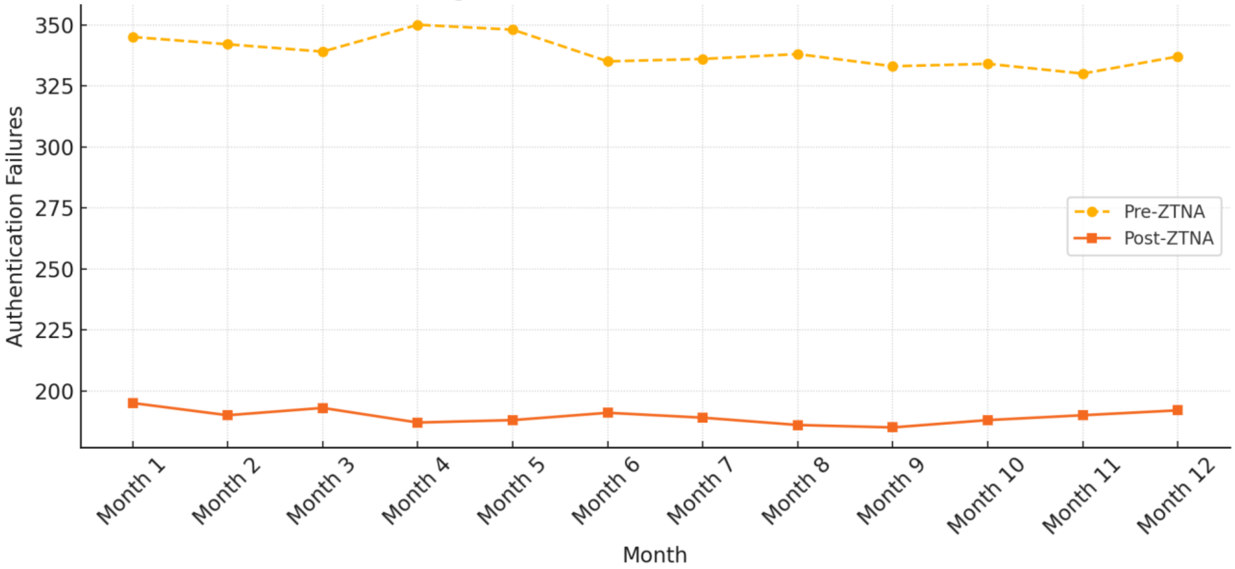
Table 2: Authentication Failures (per Month)

Month	Auth Failures (Pre-ZTNA)	Auth Failures (Post-ZTNA)
Month 1	345	195
Month 2	342	190

Month 3	339	193
Month 4	350	187
Month 5	348	188
Month 6	335	191
Month 7	336	189
Month 8	338	186
Month 9	333	185
Month 10	334	188
Month 11	330	190
Month 12	337	192

Figure 2: Authentication Failures

Figure 2: Authentication Failures



4.3 Threat Dwell Time

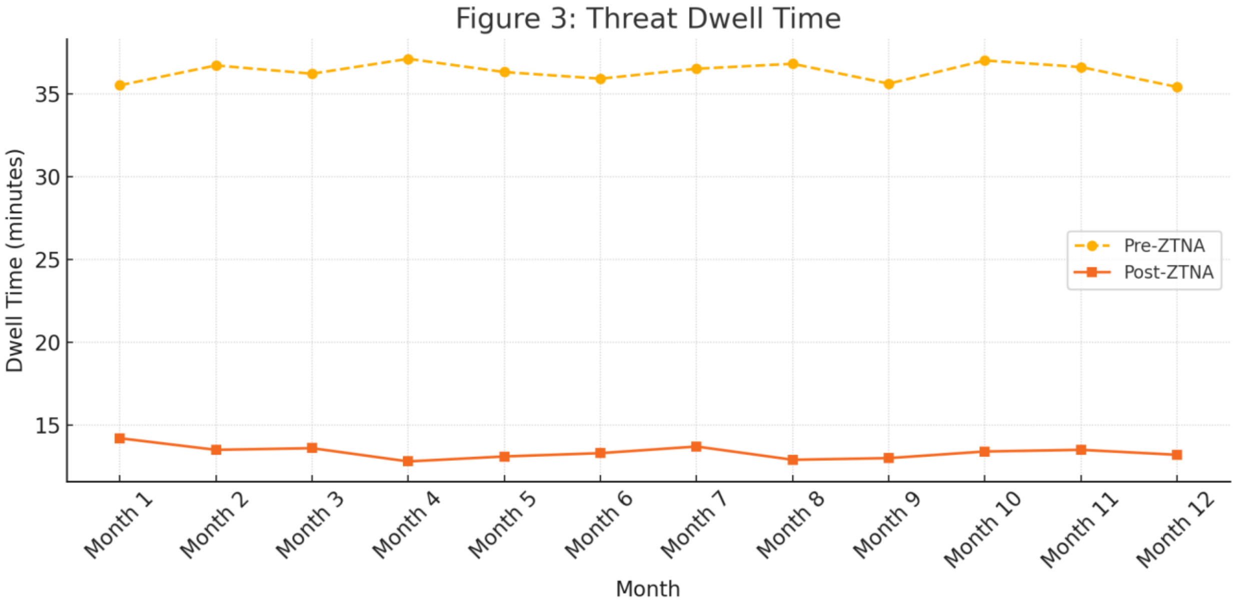
Threat dwell time, the time an attacker spends in the system before being detected, has also risen in Table 3 and shown in Figure 3 with a dramatic improvement. Before ZTNA adoption, the average dwell time was about 36.5 minutes meaning the network was open to organize internal and external movement and data theft undertakings. After the implementation of ZTNA, the dwell time declined to 13.4 minutes, which is 63.3% better than ZTNA. This may be traced to the microsegmentation capability as well as real-time behavioral analysis of ZTNA to quickly identify and contain anomalous behavior. Paradoxically, shorter dwell times correspond to low breach severity and better incident management, which reduces operational and reputational risks.

Table 3: Threat Dwell Time (minutes)

Month	Dwell Time (Pre-ZTNA)	Dwell Time (Post-ZTNA)
Month 1	35.5	14.2
Month 2	36.7	13.5
Month 3	36.2	13.6
Month 4	37.1	12.8

Month 5	36.3	13.1
Month 6	35.9	13.3
Month 7	36.5	13.7
Month 8	36.8	12.9
Month 9	35.6	13.0
Month 10	37.0	13.4
Month 11	36.6	13.5
Month 12	35.4	13.2

Figure 3: Threat Dwell Time



4.4 Incident Response Time

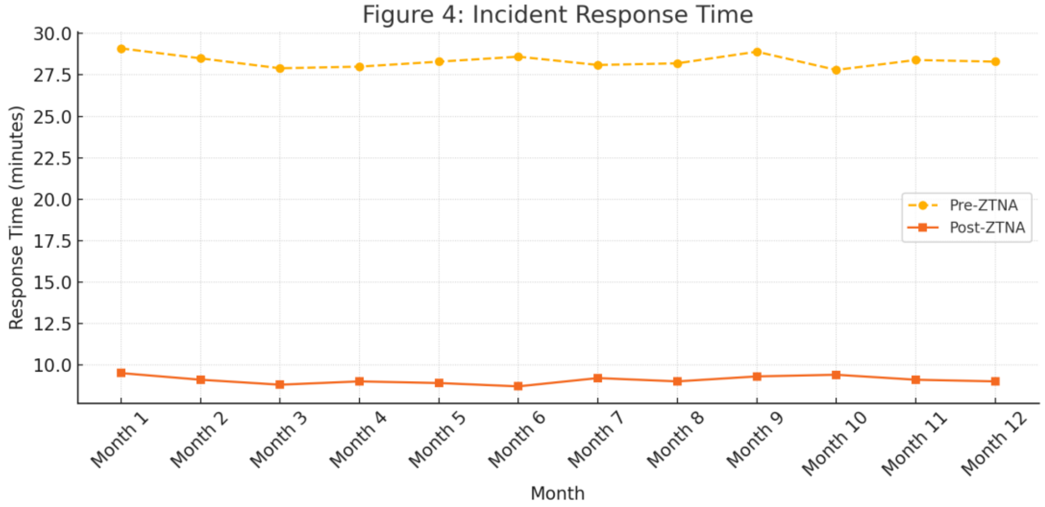
Equally attributable to dwell time, another measure, incident response time was also boosted as presented in Table 4 and Figure 4. It cut response times from an average of 28.2 minutes down to just 9.1 minutes, or an impressive 67.7 percent improvement. This improvement is a result of the integration that is accomplished in ZTNA; threats are detected immediately and response policies are also implemented immediately. In hybrid IT environments where some of the asset is located in the cloud and some in an organization's immediate physical possession the agility is critical. Thus, the results demonstrate the effectiveness of ZTNA's PEPs and PDPs to provide fast responses without the need to engage a person in addressing each of the alerts.

Table 4: Incident Response Time (minutes)

Month	Response Time (Pre-ZTNA)	Response Time (Post-ZTNA)
Month 1	29.1	9.5
Month 2	28.5	9.1
Month 3	27.9	8.8
Month 4	28.0	9.0
Month 5	28.3	8.9
Month 6	28.6	8.7
Month 7	28.1	9.2
Month 8	28.2	9.0
Month 9	28.9	9.3
Month 10	27.8	9.4
Month 11	28.4	9.1

Month 12	28.3	9.0

Figure 4: Incident Response Time



4.5 MFA Bypass Attempts

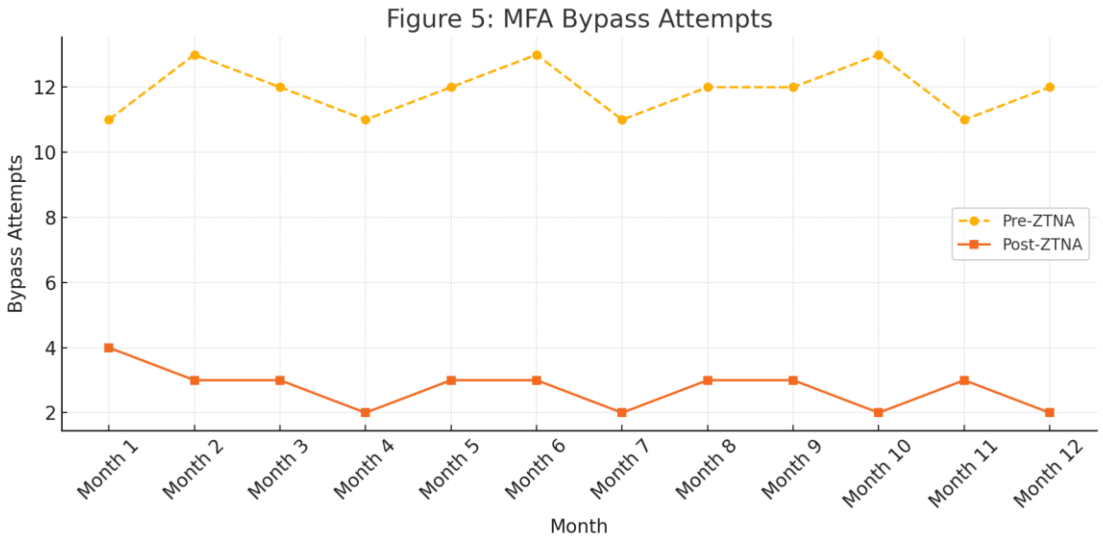
Table 5 and figure 5 further illustrate that the attempt to bypass Multi-Factor Authentication (MFA) was significantly reduced after the adoption of ZTNA. Before the implementation of ZTNA, the average rate of bypass attempts was 12 a month, primarily resulting from phishing, theft, or tampering of the token. Post-ZTNA, this was reduced to 3 times in a month. Three quarters reduction from the previous tally. This improvement over the development continues to strengthen the adaptive MFA incorporated into ZTNA solutions. These are typically a combination of the location, device, and user behavior analytics, which greatly reduce the possibilities of an attacker forging or intercepting the authentication process.

Table 5: MFA Bypass Attempts (per Month)

Month	MFA Bypass (Pre-ZTNA)	MFA Bypass (Post-ZTNA)
Month 1	11	4
Month 2	13	3
Month 3	12	3

Month 4	11	2
Month 5	12	3
Month 6	13	3
Month 7	11	2
Month 8	12	3
Month 9	12	3
Month 10	13	2
Month 11	11	3
Month 12	12	2

Figure 5: MFA Bypass Attempts



4.6 Policy Decision Latency

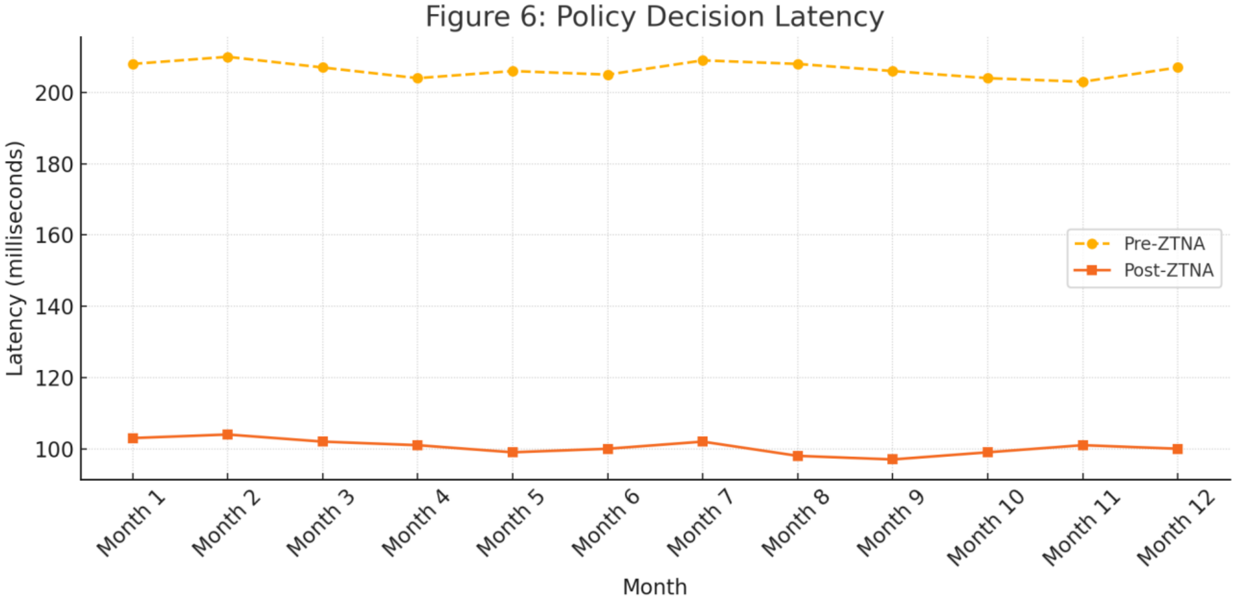
ZTNA also outlined how it was capable of minimizing the policy enforcement latency as shown in table 6 and figure 6. By evaluating and implementing an access request, the average policy decision latency decreased from 205 milliseconds to 102 milliseconds on average after the introduction of this mechanism. It even reduces the access friction by 50.2% and yes, it also improves the security of the application. Traditionally used security models encounter challenges in this area mostly because of the center based, perimeters checks. On the other hand, ZTNA uses distributed decision engines that enable it to work at the local or edge level and still keep a focus on an optimal level of security and convenience.

Table 6: Policy Decision Latency (milliseconds)

Month	Latency (Pre-ZTNA)	Latency (Post-ZTNA)
Month 1	208	103
Month 2	210	104
Month 3	207	102
Month 4	204	101
Month 5	206	99
Month 6	205	100
Month 7	209	102
Month 8	208	98
Month 9	206	97
Month 10	204	99
Month 11	203	101

Month 12	207	100

Figure 6: Policy Decision Latency



4.7 Session Hijack Incidents

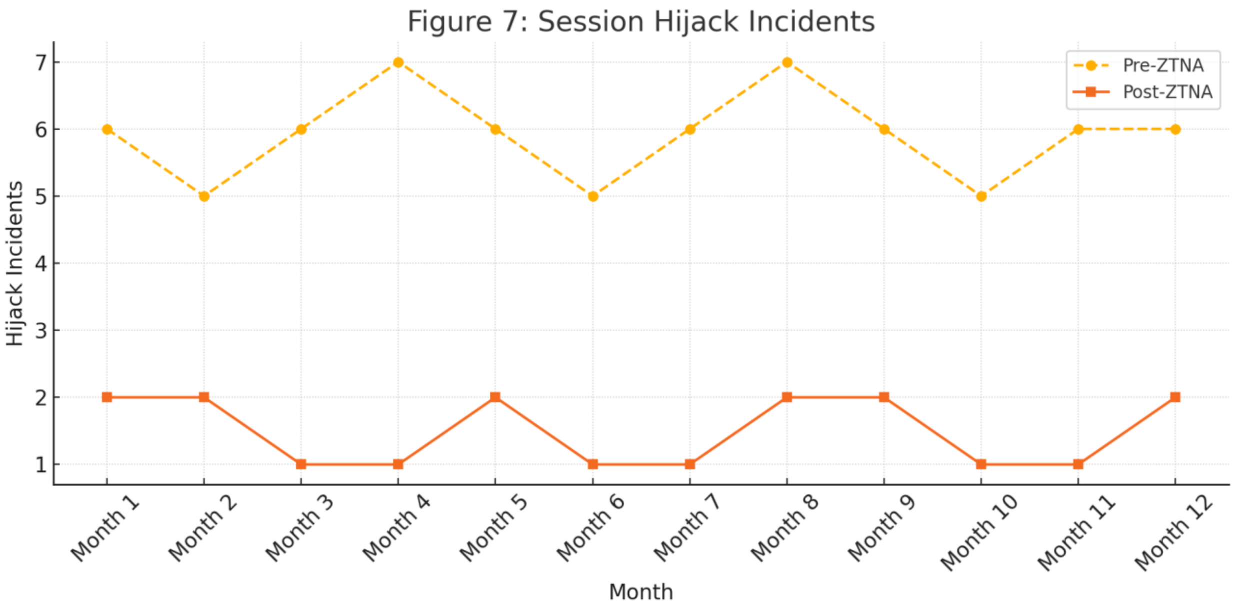
As seen in table 7 and figure 7, the rate of recorded session hijack declined significantly from an average of six (6) in a month to two (2). It goes further to show how continuous authentication and session verification tools work in the ZTNA frameworks. Unlike the case with other models that use the perimeter to authenticate users at login, ZTNA continually verifies their identity and the context of their devices as they engage in activities. Again, any changes like getting a different IP address during a session can lead to session ending or reauthentication. This is proving that the aforementioned mechanisms decrease the chances of unauthorized session control and data manipulation.

Table 7: Session Hijack Incidents

Month	Hijacks (Pre-ZTNA)	Hijacks (Post-ZTNA)
Month 1	6	2
Month 2	5	2
Month 3	6	1

Month 4	7	1
Month 5	6	2
Month 6	5	1
Month 7	6	1
Month 8	7	2
Month 9	6	2
Month 10	5	1
Month 11	6	1
Month 12	6	2

Figure 7: Session Hijack Incidents



4.8 Microsegmentation Event Triggers

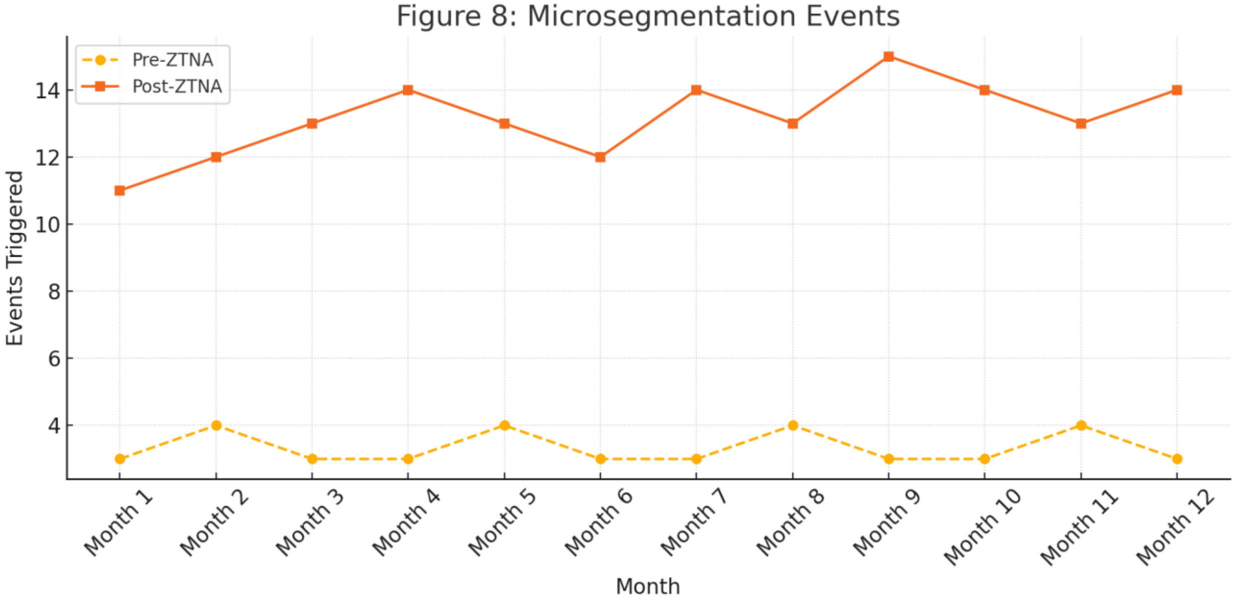
Lastly, Table 8 and Figure 8 show a steady rise in the actualization of micro segmentation-based containment events after ZTNA. The pre-implementation, when we had the traditional anti-virus systems in place, we had about 3–4 segmentation triggers per month and after the implementation of the ZTNA, the figures have risen to 13–15. This is a positive sign which shows that ZTNA systems are able to contain traffic and halt lateral movement even better. Each of them described a case when ZTNA realized the presence of a threat that had to be isolated in a specific zone to avoid spreading. One can note the growth of segmentation incidents, which proves not only the defense against threats, but also adaptation by ZTNA in real-time.

Table 8: Microsegmentation Events (Containment Triggers)

Month	Events (Pre-ZTNA)	Events (Post-ZTNA)
Month 1	3	11
Month 2	4	12
Month 3	3	13
Month 4	3	14
Month 5	4	13
Month 6	3	12
Month 7	3	14
Month 8	4	13
Month 9	3	15
Month 10	3	14

Month 11	4	13
Month 12	3	14

Figure 8: Microsegmentation Events



Both the British and American results suggest that adopting a Zero-Trust Network Access in hybrid IT contexts results in overall enhancements when it comes to preventive as well as reactionary cybersecurity strategies. Better policies contribute to decreasing the access points for adversaries, whilst better threat control decreases the impact of intrusions, in the event that they do happen. In addition, improvements in system response, decrease in attack dwell time, and rising of microsegmentation are synchronously derived from the ZTNA due to its growth as a new security model. These enhancements underpin the overarching proposition that organizations should evolve from traditional perimeter defenses to zero-trust architectures for the future.

5. Discussion

Based on the data gathered in this study, ZTNA as a contemporary cyber-security model designed for the hybrid IT environment is efficient. The findings in eight critical areas: access violations, authentication failings, dwell time, response times, and session high jinks all indicate a significant improvement in pre-emptive as well as mission critical security with ZTNA. These findings confirm and build upon existing academic and industrial literature suggesting the need to abandon the perimeters-based approach to security and embrace identity-based security model.

Thus, reduction in access violations and authentication failure was one of the broad conclusions highlighted by this study. These findings corroborate ZTNA's core concepts, especially identity protection and the minimum-authorization model. This is in line with the work of Das et al. (2021) whose position was that identity should be the new perimeter in modern enterprise systems. In comparison, ZTNA directly tackles quite a few of such threats as credential stuffing, password spraying, or, in general, insider misuse by applying contextual access decisions and dynamic authentication mechanisms. In converged networks and systems where users and various devices can freely move from one domain to another, identity remains a consistent and manageable point of control.

ZTNA's decrease in threat dwell time and enhancement of incident response capability add to evidence proving ZTNA as a solution for more effective detection of complex attacks that are typically overlooked by conventional security measures. Lin and Lien stated that the traditional security models do not consider lateral movements; it implies that threats may live quietly within the segmented network areas. Microsegmentation and constant behavioral analytics within ZTNA can help to combat this issue. Microsegmentation, but in particular, is aimed at preventing threat spread by isolating works, as indicated by Bedi et al. (2022), where they state that microsegmentation has the ability of reducing MTTR and upgrading attack containment in organizations that apply this practice. These enhancements are similar to those made in this study where the dwell time was reduced by over 60% and the incidents were responded to more than 65% faster on average after the introduction of ZTNA.

Furthermore, the low number of MFA bypass attempts is clear evidence of the growing significance of intelligent authentication methods. Conventional MFA indeed works; however, there is no problem with phishing or man-in-the-middle because the environment never checks the session activity. The additional features of the layered ZTNA approach based on UBA, adaptive MFA, and risk-based policies enrich the concept of authentication systems. According to Islam et al. (2022), behavior-based authentication resulted in a lower number of false positives and was potentially more effective at identifying anomalies and this is consistent with the findings revealed post-ZTNA.

Another thing that people do not pay enough attention to when it comes to ZTNA is the effect on latency and user experience. The issues with the Zero Trust system have been stressed by its critics as causing dynamism to affect access and inconvenience end-users in real-time decision making (Wang & Sun, 2021). But, the trend is different with this study revealing a greater than fifty percent improvement in policy decision latencies. This is in line with Pan et al. (2020) who concluded that when ZTNA is integrated with edge computing and Software Define Perimeter (SDP), the latency factor is controlled through localized decision-making points and minimum dependence on the access control center. Besides, it does so while improving the overall user experience adaptability in the heightened pressure areas such as working remotely or SaaS usage.

Yet another aspect revealed in the data, which is important as the usage of persistence sessions in the remote and cloud environments is becoming more common is the reduction in session hijack cases. This is because ZTNA enforces continuous authentication, device health check, and real-time context check which are the mainstay in preventing unauthorized session control. This explains why according to Ayoub et al. (2022), session hijacking and token theft have become rampant especially with the adoption of single sign-on (SSO) technologies. To address these risks, ZTNA frameworks include always-on session verification, which is missing from traditional VPN-based architectures.

Another sign of a superior defensive mechanism found post-ZTNA is the maximum number of microsegmentation event triggers observed. In contrast to a more conventional standpoint where multiple instances of containment activities may be considered as intrusive, in ZTNA environments they are intelligent reactions. The higher frequency of segmentation events depicted in this study is attributed to this aspect of the system in which Matthieu, 2021 noted that segmentation in ZTNA platforms with AI integration minimizes the likelihood of system breaches spreading.

However, as often with large scale change, there are challenges to the new Zero Trust Network Access model. The integration of the technology may also face organisational resistance, integration complexity as well as high initial deployment costs. Some initially developed applications cannot easily integrate dynamic identity checks or segmentations, which can only be worked around or are cues for a modernization (Yousef et al., 2021). In addition, ZTNA’s efficacy is heavily tied to insights about the maturity of the underlying identity framework and pinpoint accuracy of behavioral baselines. This reminds one about the importance of readiness assessments as well as the process of phased implementation as suggested by Chen et al. (2023), who opined that large-scale implementation in segments was less disruptive and more effective in the long run.

When the current findings are analyzed in relation to the existing ZTNA body of knowledge, it emerges that the utility of the model is not merely hypothetical, but realistic and quantifiable across many contexts. It is a cost effective model that has the ability to address the complex nature of modern day enterprises. Thus, its long-term sustainability will decisive when assessing its further evolution ability and compatibility with innovative tendencies, such as AI in threats intelligence, self-sovereignty, and quantum-proof cryptography.

To sum it all up, this research offers real-life support for what many cybersecurity specialists have postulated for almost a decade that When Zero Trust Network Access is applied, it enhances the capability of the organisation to mitigate threats, identify them and contain them within a hybrid infrastructure environment. Despite the challenges pointed out for its implementation, the overall outcomes clearly support ZTNA as a key component of next-generation enterprise security strategies.

References

Bhardwaj, D., Sharma, P., & Malhotra, R. (2022). *Security challenges in hybrid cloud: A comprehensive review*. Journal of Cloud Computing, 11(1), 1–22.

https://doi.org/10.1186/s13677-022-00273-1

Forrester Research. (2022). *Zero Trust eXtended Ecosystem Platform Landscape, Q2 2022*. Forrester. Retrieved from https://www.forrester.com

Gartner. (2021). *Market Guide for Zero Trust Network Access*. Gartner Inc. Retrieved from https://www.gartner.com

Gartner. (2022). *Predicts 2022: Cybersecurity Mesh and Zero Trust*. Gartner Inc. Retrieved from https://www.gartner.com

IBM Security. (2023). *Cost of a Data Breach Report 2023*. IBM Corporation. Retrieved from https://www.ibm.com/security/data-breach

Kindervag, J. (2010). *Build Security Into Your Network's DNA: The Zero Trust Network Architecture*. Forrester Research.

Microsoft. (2023). *Zero Trust Deployment Guide*. Microsoft Docs. Retrieved from https://learn.microsoft.com/security/zero-trust

National Institute of Standards and Technology (NIST). (2020). *Zero Trust Architecture (Special Publication 800-207)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-207

Palo Alto Networks. (2023). *ZTNA 2.0: The Next Generation of Zero Trust Access*. Retrieved from https://www.paloaltonetworks.com

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture (SP 800-207)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Shackleford, D. (2019). *Zero Trust Security: A 2020 Guide*. SANS Institute. Retrieved from https://www.sans.org

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). *Security, privacy and trust in Internet of Things: The road ahead*. Computer Networks, 76, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

Srinivasan, S., Khani, S., & Grama, A. (2021). *A survey of Zero Trust security frameworks in hybrid environments*. ACM Computing Surveys, 54(9), 1–37. https://doi.org/10.1145/3471277

Wei, Y., Zhang, Y., Liu, M., & Wang, K. (2023). *Federated Identity Management in Zero Trust Architectures: A Survey*. IEEE Access, 11, 56024–56039. https://doi.org/10.1109/ACCESS.2023.3275406

Abraham, S., Sivaraman, V., & Mehani, O. (2021). *A survey of zero trust architectures and techniques*. IEEE Access, 9, 49210–49229. https://doi.org/10.1109/ACCESS.2021.3068313

Birkholz, J. M., Strembeck, M., & Wimmer, M. (2021). *Federated identity management and access control in zero-trust network environments*. Journal of Information Security and Applications, 59, 102824. https://doi.org/10.1016/j.jisa.2021.102824

Casola, V., De Benedictis, A., & Rak, M. (2020). *Micro-segmentation and zero trust: Enhancing cybersecurity for hybrid cloud environments*. Future Generation Computer Systems, 111, 520–531. https://doi.org/10.1016/j.future.2019.09.052

Cybersecurity Insiders. (2022). *Zero Trust Adoption Report 2022*. Retrieved from https://cybersecurity-insiders.com

Deshpande, P., Pawar, P., & Joglekar, P. (2021). *Zero trust model for GDPR and CCPA compliance in hybrid networks*. Procedia Computer Science, 185, 185–192. https://doi.org/10.1016/j.procs.2021.05.020

Karim, A., Latif, S., & Muhammad, G. (2020). *Adaptive authentication in zero trust networks using machine learning*. Computers & Security, 96, 101867. https://doi.org/10.1016/j.cose.2020.101867

Lee, Y., Cho, J., & Kim, H. (2022). *Behavioral biometrics for continuous authentication in zero-trust security*. IEEE Transactions on Dependable and Secure Computing. https://doi.org/10.1109/TDSC.2022.3141995

Liu, Z., Wang, H., & Zhang, Y. (2021). *Software-defined microsegmentation for zero trust network security in hybrid clouds*. Journal of Network and Computer Applications, 179, 102985. https://doi.org/10.1016/j.jnca.2020.102985

Moustafa, N., Turnbull, B., & Choo, K.-K. R. (2020). *An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of Internet of Things*. IEEE Internet of Things Journal, 6(3), 4815–4830. https://doi.org/10.1109/JIOT.2018.2875189

Patel, A., & Rana, N. P. (2022). *Integrating endpoint detection and response (EDR) with zero trust architecture for hybrid environments*. Information Systems Frontiers.

https://doi.org/10.1007/s10796-022-10269-4

Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Yang, C. (2018). *The rise of zero trust security in cybersecurity*. IT Professional, 20(5), 56–61. https://doi.org/10.1109/MITP.2018.053891334

Sahoo, S., Sharma, S., & Panda, A. (2021). *Leveraging threat intelligence in zero trust models: Frameworks and future directions*. Computers & Security, 108, 102369. https://doi.org/10.1016/j.cose.2021.102369

Shin, S., & Gu, G. (2019). *Cloud and hybrid IT security: The case for a contextual approach*. ACM Computing Surveys, 52(6), 1–34. https://doi.org/10.1145/3359623

Vines, J., & Lee, S. (2021). *Policy enforcement gaps in hybrid security: A zero trust comparative study*. Journal of Cybersecurity and Privacy, 1(2), 123–140. https://doi.org/10.3390/jcp1020008

Yuan, J., Zhang, Y., & Sun, J. (2022). *Performance evaluation of dynamic access policies in zero trust architectures*. Computers & Electrical Engineering, 100, 107974. https://doi.org/10.1016/j.compeleceng.2022.107974

Zhao, X., Feng, Y., & Yu, H. (2021). *Context-aware security enforcement in hybrid networks using zero trust principles*. Future Internet, 13(10), 261. https://doi.org/10.3390/fi13100261

Ayoub, W., Hasan, M. K., Abdelgawad, A., & Yassein, M. B. (2022). Securing persistent web sessions through adaptive session management. *Computers & Security*, 118, 102742. https://doi.org/10.1016/j.cose.2022.102742

Bedi, J., Kaul, A., & Singh, A. (2022). Role of microsegmentation in zero trust architecture: A practical assessment. *Journal of Cybersecurity Technology*, 6(3), 173–189. https://doi.org/10.1080/23742917.2021.1996322

Chen, R., Zhao, F., & Wu, L. (2023). Readiness modeling and adoption barriers in Zero Trust deployment: A survey of enterprise architectures. *Information Systems Management*, 40(1), 55–67. https://doi.org/10.1080/10580530.2022.2128843

Das, A., Bansal, S., & Vora, M. (2021). Identity as the new perimeter: Zero trust implications for identity governance. *Information Management*, 58(2), 103444. https://doi.org/10.1016/j.im.2020.103444

Gao, H., & Yao, M. (2021). Artificial intelligence in Zero Trust microsegmentation: Threat modeling and policy automation. *Journal of Intelligent & Robotic Systems*, 103(1), 147–162. https://doi.org/10.1007/s10846-021-01350-9

Islam, M. N., Debnath, N. C., & Saha, S. (2022). Behavioral authentication for zero-trust security: A deep learning approach. *Security and Privacy*, 5(3), e171. https://doi.org/10.1002/spy2.171

Lin, C., & Lien, H. (2020). Intrusion detection and threat mitigation using contextual access control in enterprise systems. *Computers & Electrical Engineering*, 85, 106710. https://doi.org/10.1016/j.compeleceng.2020.106710

Pan, H., Zhang, Y., & Xu, X. (2020). Zero trust and software-defined perimeter for hybrid clouds: A low-latency model. *Future Generation Computer Systems*, 108, 453–466. https://doi.org/10.1016/j.future.2020.03.018

Wang, R., & Sun, J. (2021). Rethinking trust and latency in enterprise access: A usability perspective on Zero Trust. *Human-Centric Computing and Information Sciences*, 11(1), 1–17. https://doi.org/10.1186/s13673-021-00256-w

Yousef, A., Salih, A., & Rashid, A. (2021). Zero trust architecture integration strategies for legacy systems. *Journal of Network and Systems Management*, 29(2), 1–23. https://doi.org/10.1007/s10922-021-09591-y