Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Systematic Literature Review on Secure Access Service Edge (SASE) and Zero Trust Network Access (ZTNA) Implementation to Ensure Secure Access

Sivakameni Indran[1,3], Najwa Hayaati Mohd Alwi[1,2,*]

[1] Faculty of Science and Technology, Universiti Sains Islam Malaysia, 71800 Nilai, Negeri Sembilan, Malaysia
[2] Cybersecurity and Systems Research Unit, Faculty of Science and Technology, Universiti Sains Islam Malaysia, 71800 Nilai, Negeri Sembilan, Malaysia
[3] School of Information Technology, SEGi College Subang Jaya, USJ 1, 47500 Subang Jaya, Selangor, Malaysia

ABSTRACT

Secure Access Service Edge (SASE) and Zero Trust Network Access (ZTNA) are among the technologies used to secure access. This study aims to delve into the effectiveness of SASE and ZTNA in bolstering secure access for organizations, particularly considering the shortcomings of traditional security measures in the era of widespread cloud services and remote work. The study was conducted as a systematic literature review. Searches within the past five years (2018-2023) in Google Scholar, Scopus, Web of Knowledge, ACM Digital Library, and ScienceDirect identified 25 papers for the analysis. The keywords search used has included and excluded the necessary scope of the study. The result has revealed three core principles and components of SASE, as well as two distinct ZTNA architectures. Implementing SASE and ZTNA yields substantial security improvements, such as reduced data breaches, enhanced control over network traffic, improved user authentication, and mitigation of lateral network movement. Seven concrete benefits of SASE and ZTNA adoption were uncovered, emphasizing their critical role in modern cybersecurity. To maximize the advantages of these technologies, continuous evaluation and adaptation are recommended to counter evolving threats effectively. The review also spotlights four primary challenges tied to adopting and implementing SASE and ZTNA, emphasizing the need for meticulous planning and expertise. Five integration approaches of SASE and ZTNA were identified in the studies. Organizations choose a combination of these approaches to achieve their desired security and networking goals. Lastly, the review outlines four future directions for SASE and ZTNA, suggesting the adoption of customized frameworks tailored to each organization's unique security needs. In essence, this systematic review underscores the significance of SASE and ZTNA in contemporary cybersecurity. It stresses the importance of careful planning, assessment, and adaptation, acknowledges the complexities of integration, and advocates for customized solutions to strengthen organizational security in the face of evolving threats.

Keywords:

Zero trust network access; Secure access service edge; Integration approach; Secure access

[*] *Corresponding author.*
E-mail address: najwa@usim.edu.my

https://doi.org/10.37934/araset.56.2.182195

1. Introduction

Cybersecurity is super important for all organizations that handle sensitive information, whether they're businesses or government agencies. They all face the risk of losing important data that belongs to them or their customers. That's why many companies are focusing on setting up strong security systems for their computer networks to keep their data safe. In the past, companies used to build protective walls called firewalls around their computer networks. These walls helped employees work safely inside, keeping out any unauthorized people. But recently, this old way of doing things has become more difficult because of new rules that are making organizations switch to having employees work from home. The COVID-19 pandemic brought in rules to stop the virus from spreading. These rules made organizations change how they work and have more people working from home, which has made it harder to keep their computer systems secure.

As COVID-19 cases increased and people started working from home [1], it caused some issues with online services and more cyberattacks. Mandal & Khan [2] pointed out that when people work remotely, there's a big problem with the security of the networks because companies can't control how their employees connect to the internet. This means hackers might easily access company information on unprotected servers. Security is a big concern for all organizations. According to a survey by Verizon [3], there were 474 cases of data breaches worldwide. Most of these happened between March and June 2020, and they were mainly caused by hacking, stealing data, and brute force attacks. These numbers show that we need a better way to protect our online information. Ensuring the security of the entire infrastructure and staying one step ahead of cyber threats and malicious individuals should be a top priority for every IT leader when devising a strategic plan.

According to a survey conducted by cybersecurity company Palo Alto Networks, 68% of Malaysian organizations are accelerating their remote workforce, with increased investment in mobile applications, cloud adoption, and 5G [4]. According to Cisco [5], the study discovered that hybrid or remote work has proven to be highly implemented in organizations over the past two years. This shift towards digital technologies has brought on a new set of cybersecurity challenges for businesses that haven't been designed to keep up with the demands of a mobile workforce. In this regard, a managed Secure Access Service Edge (SASE) and Zero-Trust Network solution helps to keep an organization’s information safe with the use of its private network.

Kaur [6] mentioned that Juan Huat Koo, Cisco Asian Cybersecurity Director strongly recommended a new security model known as Secure Access Service Edge (SASE) to be used for a hybrid workforce. Palo Alto Networks, a leading global cybersecurity company, is urging the industry to transition to Zero Trust Network Access 2.0 (ZTNA 2.0) as the foundation for a new era of secure access [7]. Furthermore, trust is one of five aspects of the human-centric model that strongly correlate with worker experience [8]. In conclusion, the rapid growth of remote work, driven by mobile apps, cloud, and 5G, poses cybersecurity challenges. Traditional security struggles to adapt. To protect data, organizations turn to Secure Access Service Edge (SASE) and Zero Trust Network Access (ZTNA), recommended by experts and industry leaders like Palo Alto Networks and Cisco.

The objectives of this SLR are:

i. to identify the benefits of SASE and ZTNA solutions that align with an organization's cybersecurity goals
ii. to identify the challenges faced by SASE and ZTNA implementation
iii. to determine the future path for the convergence of SASE and ZTNA solutions.

The structure of this paper is as follows: Section 2 describes the review methods. Section 3 discusses the outcome of many researchers and authors on the SASE and ZTNA security framework. Section 4 provide discusses the future adoption of integration between SASE and ZTNA and Section 5 presents the conclusion of this SLR.

2. Review Methods

This section outlines the review process, as depicted in Figure 1. The initial step entails the formulation of the research question. Following that, details the search process, encompassing the sources chosen and the keywords employed in the search. Subsequently, discuss the criteria for including or excluding articles, as well as the quality standards applied to primary articles. The data extraction phase involves gathering, organizing, and extracting pertinent information into a structured list. The outcomes of this process, i.e., summaries of the primary articles, are presented in Section 3 and can be found in Appendix A."

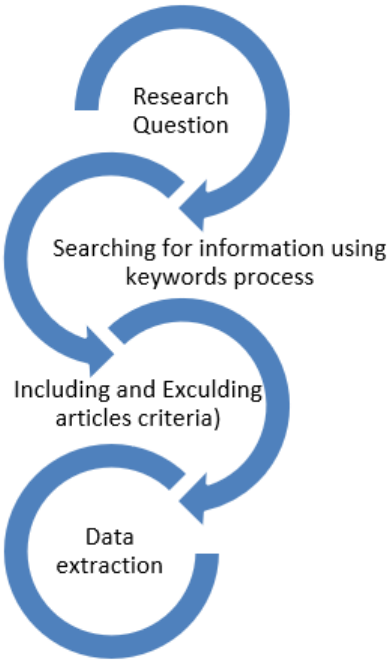

Fig. 1. The steps in SLR method

2.1 Formulating Research Questions

The objectives of the review are to answer the following research questions (RQ) in Table 1.

i. RO1: To identify the benefits of SASE and ZTNA solutions that align with an organization's cybersecurity goals.
ii. RO2: To identify the challenges faced by SASE and ZTNA implementation.
iii. RO3: To determine the future path for the convergence of SASE and ZTNA solutions.

Table 1
Research Questions in SLR

RQ#	Detail of Research Question
RQ1	How do SASE and ZTNA solutions align with and support an organization's specific cybersecurity goals ?
RQ2	What kind of challenges and obstacles do organizations encounter when implementing SASE and ZTNA solutions?
RQ3	How do organizations proactively prepare for the future convergence of SASE and ZTNA, staying ahead of evolving cyber threats?

2.2 Search Process

The search process plays a pivotal role in conducting a Systematic Literature Review (SLR). To find articles most relevant to the research area, conducted searches across diverse web sources such as: -

i. Web articles
ii. Web journals
iii. Web white paper
iv. Web thesis
v. Google Scholar

The search process is detailed in Figure 2. In Phase 1, various web sources were utilized to search for articles related to the implementation of Secure Access Service Edge (SASE) and Zero Trust Network Access (ZTNA) to ensure secure access. Initially, keyword searches were conducted in article titles and abstracts using primary keywords such as 'Zero Trust Network Access,' 'Secure Access Service Edge,' 'Integration Approach,' and 'Secure Access.' Phase 2 involved reviewing the titles and abstracts of the retrieved articles, followed by downloading relevant ones. Phase 3 played a critical role in refining the selection of primary articles for the study and analysis. Phase 4 involved searching for synonyms or related terms to broaden the search. In Phase 5, additional articles were selected based on the results of the synonym search conducted in Phase 4. Phase 6 involved establishing inclusion criteria, and specifying conditions for article inclusion, while exclusion criteria were applied to filter out articles that did not align with the research goals or quality standards. Finally, Phase 7 marked the decision-making process for including articles in the Systematic Literature Review (SLR)."

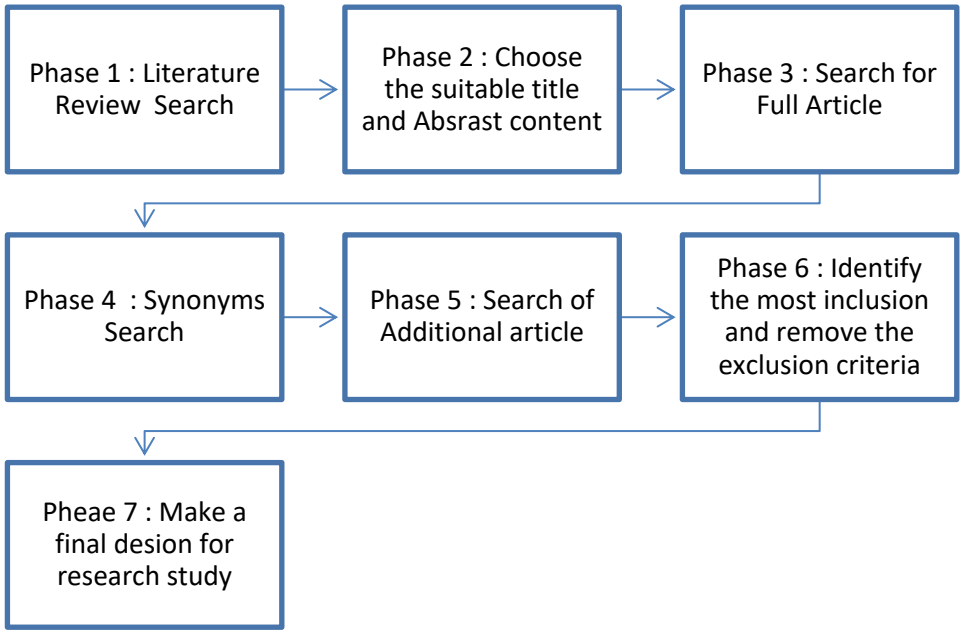

Fig. 2. Search process for Systematic Literature Review (SLR)

2.3 Inclusion-Exclusion Criteria

Articles were subjected to a screening process based on predefined inclusion and exclusion criteria before being classified as primary articles for the final review. The inclusion criteria used for the selection of primary articles are detailed in Table 2.

Table 2
Inclusion Criteria

Inclusion #	Inclusion criteria explanation
Inclusion 1	SASE, ZTNA, remote workers, integration approach, and secure access are the research topics for this paper.
Inclusion 2	Articles should report how these research topics help an organization.
Inclusion 3	Some articles focus on SASE components.
Inclusion 4	Some articles focus on ZTNA architecture.

Additionally, some articles that do not meet the criteria outlined in Table 3 were excluded.

Table 3
Exclusion Criteria

Exclusion #	Exclusion criteria explanation
Exclusion 1	Some articles do not provide information about SASE and ZTNA Integration.
Exclusion 2	Some articles do not mention about challenges faced during the adoption of SASE and ZTNA.

2.4 Data Extraction and Quality Assessment

Data extraction aims to consistently gather findings that address the review questions. To achieve this, a data extraction form is utilized to impartially and precisely document information from chosen articles. Table 4 illustrates four criteria used to assess the quality of these articles. A ratio scale is applied, where 'Yes' equals 1 point, 'No' equals 0 points, and 'Partially' equals 0.5 points.

Table 4
Quality Assessment Checklist

No	Criteria	Answer
1	Articles have undergone a formal evaluation process by experts or peers in the same field of study before it is accepted for publication in a scholarly journal.	Yes / No
2	Did the research include a well-defined statement of its objectives?	Yes/ No/ Partially
3	Was there a sufficient presentation of the research context, including a clear identification of the problems prompting the study and a comprehensive explanation of the research methodology employed?	Yes/ No/ Partially
4	Was the data collection well-executed, and did the evaluation of the proposed approach effectively address the research questions, with a thorough discussion of the results in the article?"	Yes/ No/ Partially

3. Results and Discussions

Before delving into the results, the selected studies are introduced in Section 3.1. Following that, Section 3.2 presents the results by addressing each of the research questions outlined in Table 1.

3.1 Selected Studies

Through keyword searches, initially gathered 50 articles from various sources, including journals, conference proceedings, technical reports, book chapters, web articles, and theses. Then narrowed this down to 25 relevant articles for a detailed review. Additionally, by searching for synonyms based on the introduction, 6 more relevant articles were found. After applying inclusion and exclusion criteria, finalized the selection with a total of 31 primary articles for this review.

3.1.1 SASE components

In 2019, Gartner introduced an important concept called SASE (Secure Access Service Edge) in cloud network security. While it's still in its early stages, SASE is expected to change and improve over time. Table 5 provides 3 relevant articles about SASE.

Table 5
3 articles of SASE

Title	Authors
Research Gaps and Opportunities for Secure Access Service Edge	Walt & Hein [9]
MEF SASE Services Framework	Lev [10]
Secure Access Service Edge (SASE)	Cloudflare [11]

Walt *et al.,* [9] mentioned that Gartner proposed SASE as a network security framework. SASE is a new approach that combines different tools for Wide Area Networking (WAN) with various security functions like Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Firewall as a Service (FWaaS), and Zero Trust Network Access (ZTNA) described by Gartner [12]. It's designed to help modern digital companies securely and dynamically access their networks:

i. FWaaS (Firewall as a Service), or cloud firewalls, do the same job as regular firewalls by managing where network traffic comes from.
ii. CASB (Cloud Access Security Broker) acts as a security middleman between users of cloud services and the cloud service providers. It decides which apps can or can't be used.
iii. Cloud SWG (Secure Web Gateway) provides web security from the cloud to protect devices while surfing the web. It also ensures that everyone follows company security rules.
iv. ZTNA (Zero Trust Network Access) only lets trusted devices access specific apps and always checks if the device and user are who they claim to be. It doesn't rely on IP addresses for this.
v. SD-WAN (Software-defined Wide Area Network) is a new way to manage wide area networks. It separates the network hardware from its control, making it easier to manage and control network traffic.

However, there is a valuable resource in the MEF White Paper of 2020, where the MEF SASE Services Framework is defined [10]. This framework serves as a foundation for implementing SASE and provides a valuable tool for both enterprises and service providers to assess and compare the approaches of different vendors when it comes to SASE adoption.

Figure 3 explains SASE integrates software-defined wide area networking (SD-WAN) features with multiple network security functions, all delivered through a unified cloud platform. This approach allows employees to securely authenticate and connect to internal resources from any location while granting organizations enhanced control over inbound and outbound network traffic and data. SASE includes four core security components Secure web gateways (SWG), Cloud access security broker (CASB), Zero Trust Network Access (ZTNA), and Firewall-as-a-service (FWaaS).

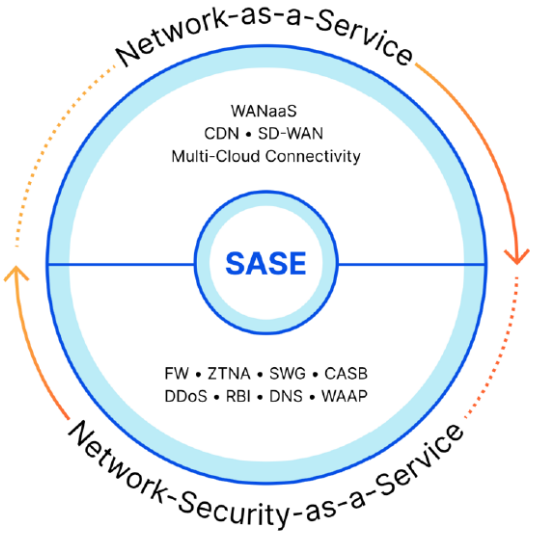

Fig. 3. SASE framework [11]

3.1.2 ZTNA architecture

Wang *et al.,* [13] explore Zero Trust Network Access (ZTNA) architecture and its benefits in modern enterprise networks. Pointed out that ZTNA replaces the traditional castle-and-moat approach, also known as Perimeter Security. ZTNA's core principle is to grant minimal resource access, reducing the risk of unauthorized entry and data breaches. In essence, ZTNA is presented as

a superior and more efficient approach to securing network environments in contemporary enterprises. Table 6 provides 2 relevant articles of ZTNA.

Table 6
2 articles of ZTNA

Title	Authors
Zero Trust - Zero Trust Reference Architecture	Wang *et al*., [13]
Zero Trust Security	Versa Network (14)

Figure 4 explains the Zero Trust architecture is built on five pillars, each requiring trust verification to determine access permission. Building trust across these pillars enhances visibility, enabling comprehensive end-to-end analytics. These aspects of visibility and analytics are pivotal in the Zero Trust framework, extending its influence across all five pillars.

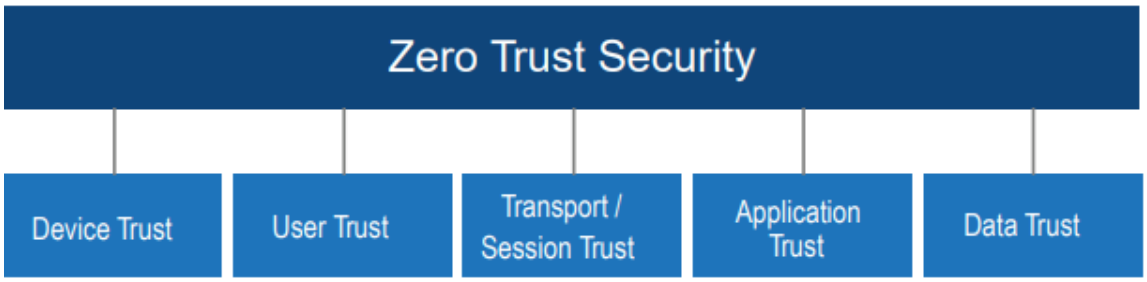

Fig. 4. Zero Trust architecture

Versa Network [14] described the key features of ZTNA architecture as:

i. Establishing a logical access boundary for applications based on identity and context.
ii. Concealing applications from discovery and regulating access through a trusted broker for specified entities.
iii. Confirming the identity, context, and adherence to policies of participants before granting access and preventing lateral network movement.
iv. Operating on the assumption that all network traffic is inherently untrusted, necessitating control over resource access through identity, context, and policy enforcement.
v. Applying the principles of zero trust to IP addresses, devices, connections, and applications.
vi. Granting user access dynamically, aligning it with specific requirements, and verifying identity and context.
vii. Giving precedence to identity-based trust over network location as the primary determinant of trust.

3.1.3 SASE and ZTNA adoption benefits

RQ1: How do SASE and ZTNA solutions align with and support an organization's specific cybersecurity goals.

Table 7 provides 7 relevant articles of SASE and ZTNA adoption benefits. Deshpande [15] strongly pointed out that ZTNA provides a more secure approach to network security by allowing companies to know who is accessing what, and where, anywhere in the network, which is very beneficial for remote working and even in a situation where employees need to work from one central location.

Also pointed out, the adoption of ZTNA has been critical for improved data security for the affected firms, especially in scenarios such as mergers and acquisitions, cloud migration, and third-party access. Cerqueira *et al.,* [16] also discuss the merits of adopting a Secure Access Service Edge (SASE) framework during business digital transformations. It covers SASE's core components—infrastructure, network, security, and orchestration layers—and emphasizes its benefits, including enhanced security, scalability, and cost-efficiency. This article also offers insights into the adoption journey and key success factors. Another article by Sarkar *et al.,* [17] mentioned that Zero Trust eliminates trust zones, emphasizing continual verification over blocking. It prioritizes data-centric security, optimizing cloud networks for efficiency and cost-effectiveness. Implementing Zero Trust enhances data protection, mitigates insider threats, and bolsters overall security, making it a vital strategy in safeguarding cloud environments. He *et al.,* [18] in their article mentioned that the ZTNA model offers several advantages, including enhanced security through mandatory authentication and authorization for all access requests, irrespective of user location or device. It also minimizes the risk of data breaches by limiting access to sensitive resources and provides improved visibility into network traffic and user activity, aiding in threat detection and prevention.

Table 7
7 articles of SASE and ZTNA benefits

Title	Authors
Relevance of Zero Trust Network Architecture amidst and its rapid adoption amidst Work from Home enforced by COVID-19	Deshpande. A [15]
Embrace digital transformation with scalable and secure cloud-based network services Secure Access Service Edge (SASE) Point of view	Cerqueira *et al.,* [16]
Security of Zero Trust Networks in Cloud Computing: A Comparative Review	Sarkar *et al.,* [17]
A Survey on Zero Trust Architecture: Challenges and Future Trends	He *et al.,* [18]
The convergence of network and security is here: It's called SASE.	Accenture [19]
Understanding Secure Access Service Edge (SASE) Architectures	Citrix [20]
SASE: the digital business enabler for your workforce	Orange Cyberdefense [21]

Accenture ([19] highlights how Secure Access Service Edge (SASE) benefits enterprises by combining network and security solutions for cost-efficiency, improved security, unified functionality, and alignment with zero trust principles." Citrix [20] in the article underscores the advantages of implementing a SASE architecture, such as enhanced user experience, universal security, and streamlined IT operations. It stresses the importance of selecting the right technology partner. Citrix is recommended as a trusted provider for comprehensive SASE services, aiding enterprise networking and security transformation. Orange Cyberdefense [21] in the article mentioned SASE solves the challenges posed by remote work and cloud services, offering a global network for secure, accessible services. It combines network and security management into a single, programmable system, directing cloud traffic efficiently.

3.1.4 SASE and ZTNA adoption challenges

RQ2: What kind of challenges and obstacles do organizations encounter when implementing SASE and ZTNA solutions?

Table 8 provides 4 relevant articles of SASE and ZTNA challenges. Citrix [20] in the article mentioned implementing a Zero Trust model offers advantages but also comes with potential downsides. These downsides encompass heightened complexity, necessitating substantial IT infrastructure alterations. Furthermore, it can result in increased expenses, demanding additional hardware, software, and personnel. Users might also face a less straightforward experience, requiring multiple authentications for resource access. Miller [22] pointed out that organizations may encounter various obstacles while implementing SASE, including administrative overhead, expenses, intricacy, and deficiencies in security readiness. As per the 2022 Global SASE report by Frost & Sullivan [23], organizations encounter challenges in completely adopting the new SASE architecture due to their legacy technology setups. A significant number still opt for a modular approach, integrating components such as SD-WAN, FWaaS, SWG, and ZTNA. Concerns about vendor limitations drive them to select the most fitting solutions to ensure a positive user experience and avoid discontent. Information Security branch [24] in the article mentioned that Zero Trust, a new network security approach, poses challenges due to inexperience in implementation. This results in poorly designed setups, user privacy concerns, and frustration over access justifications. Users sometimes turn to insecure personal devices, elevating security risks. Success requires enterprise-wide support, leadership commitment, expert administrators, and user compliance with governance policies.

Table 8
4 articles of SASE and ZTNA challenges

Title	Authors
Understanding Secure Access Service Edge (SASE) Architectures	Citrix [20]
SASE for dummies	Miller. L [22]
Global Secure Access Service Edge Industry	Frost and Sullivan [23]
Information Security Thought Paper – Zero Trust	Information Security Branch [24]

3.1.5 SASE and ZTNA integration approach

Table 9 provides 5 relevant articles of SASE and ZTNA integration approach. Zero-trust network access (ZTNA) 2.0, and Secure Access Service Edge (SASE), are two approaches that are gaining steam as organizations seek to better secure their increasingly dispersed remote workforces against cyber-attacks. Chapple [25] mentioned that today's cybersecurity professionals believe that both zero trust and SASE are trends to watch closely and integrate into forward-looking architectural decisions. Honnachari *et al.,* [26] strongly believe that SASE and ZTNA jointly offer a highly adaptable and context-driven networking and security solution, perfectly suited to meet the ever-changing requirements of modern businesses. Menlo Security [27] points out the positive outcomes of using ZTNA and SASE together in a hybrid working environment. The combination of moving security to the cloud using SASE and instituting a zero-trust approach to cybersecurity can fix the security problem and ultimately change outcomes. SASE brings security closer to apps, users, and data in the cloud, but relying on detect-and-remediate cybersecurity is flawed. Bad actors can adapt and evade detection, leaving corporate resources vulnerable. To overcome this, a Zero Trust approach treats all content as suspect and subject to enterprise security controls. By combining SASE and Zero Trust, cybersecurity teams can effectively protect against evolving threats and achieve better outcomes. IBM [28] emphasizes the significance of implementing a zero-trust architecture as a critical measure for organizations adopting SASE. This approach ensures the effective security of new distributed working models and safeguards mission-critical services that have transitioned to the cloud. By

embracing this approach, customers can confidently accelerate their secure digital transformation, supporting essential initiatives such as enabling secure employee productivity from any location and facilitating faster M&A transactions. Lumen [29] highlighted that the integration of SASE (Secure Access Service Edge) and ZTNA (Zero Trust Network Access) offers a robust solution for precise access control to applications and data. Combining SASE and ZTNA enables IT teams to implement a seamless and comprehensive security approach, reducing risks, ensuring compliance, and simplifying management.

Table 9
5 articles of SASE and ZTNA integration approach

Title	Authors
Why it's SASE and zero trust, not SASE vs. zero trust	Chapple.M. [25]
SASE & ZTNA	Honnachari *et al.,* [26]
What's the relationship between SASE and Zero Trust?	Menlo Security) [27]
IBM Expands Zero Trust Strategy Capabilities with New SASE Services to Modernize Network Security	IBM [28]
SASE And ZTNA Empower and Protect Hybrid Workforces	Lumen [29]

3.1.6 Future direction of SASE and ZTNA

RQ3: How do organizations proactively prepare for the future convergence of SASE and ZTNA, staying ahead of evolving cyber threats?

ZTEdge [30] strongly pointed out that SASE platforms combine various technologies to provide secure access from anywhere, aligning with Zero Trust principles. These cloud-edge systems integrate SDWAN, firewalls, antivirus, and newer tools like CASB, SWG, and ZTNA. Traditional cybersecurity methods are inadequate against evolving threats like ransomware. Zero Trust assumes all entities are risky, emphasizing user verification, precise policies, and network segmentation in response to the changing digital landscape. Palo Alto Network [31] also mentioned that Zero Trust Architecture and SASE offer proactive, location-independent cybersecurity. SASE combines cloud-based networking and security, while Zero Trust eliminates implicit trust, continually verifying digital interactions, collectively enhancing security for organizations. Table 10 provides 4 relevant articles of SASE and ZTNA future directions.

Table 10
4 articles of SASE and ZTNA future directions

Title	Authors
What's the Zero Trust - SASE Connection?	ZTEdge [30]
The Federal Government must adopt security best practices [and] advance towards ZeroTrust Architecture"	Palo Alto Network [31]
Factors to consider when implementing Zero Trust and SASE (Secure Access Service Edge) architecture	Carney. M [32]
How Zero Trust and SASE Can Work Together	Palo Alto Network [33]

CISCO and Palo Alto Networks are prominent vendors in the field of network security, specializing in delivering secure network solutions. They each offer unique approaches and solutions for implementing SASE (Secure Access Service Edge) and ZTNA (Zero Trust Network Access), two essential components of secure network implementation.

CISCO offers its own SASE solution known as Cisco Secure Access Service Edge (Cisco SASE). This comprehensive solution combines multiple security and networking functionalities within a cloud-native architecture. According to Carney [32], Cisco SASE integrates crucial elements such as cloud security, secure web gateways, firewalls, secure web access, zero-trust network access, and more. Its primary objective is to ensure secure and flexible access to applications and data, regardless of the user's geographical location. Palo Alto Networks [33] offers its own SASE implementation by leveraging a combination of its existing security products and services. According to Palo Alto Network, they integrate their Prisma Access cloud-delivered security and Global Protect VPN solutions to ensure secure access to applications and data. Their approach involves incorporating next-generation firewalls, secure web gateways, CASB (Cloud Access Security Broker), SD-WAN (Software-Defined Wide Area Networking), and Zero Trust principles into a unified SASE architecture.

Zero Trust Network Access (ZTNA) is an approach to network security that emphasizes the verification and authorization of access based on user identity, device posture, and additional contextual factors. Both Cisco and Palo Alto Networks have developed their solutions for ZTNA. Cisco offers Cisco Zero Trust Network Access as its ZTNA solution. This solution enables secure access to applications and resources by adhering to the principles of Zero Trust. It achieves this by employing a combination of user and device identity verification, policy-based access control, and segmentation, ensuring secure access to applications. Palo Alto Networks implements ZTNA through its Prisma Access solution. Prisma Access embraces the principles of Zero Trust by verifying user identity, device posture, and other contextual factors before granting access to applications. It leverages technologies such as Multi-Factor Authentication (MFA), device profiling, and network segmentation to establish secure access.

4. Conclusion

In the contemporary work landscape, characterized by remote and hybrid work setups, organizations grapple with substantial cybersecurity challenges. Traditional security methods like firewalls prove inadequate in safeguarding sensitive data as employees increasingly operate from diverse locations. To address these concerns, experts endorse two primary solutions: Secure Access Service Edge (SASE) and Zero Trust Network Access (ZTNA).

SASE and ZTNA are in alignment with organizations' cybersecurity objectives, emphasizing heightened security via a zero-trust model, adaptability to changing digital landscapes, improved user experiences, and potential long-term cost savings. Nevertheless, their implementation poses challenges, including intricate deployment, change management, vendor selection, and ongoing maintenance.

In summary, SASE and ZTNA solutions offer a compelling path forward for organizations seeking robust cybersecurity in the age of remote work and digital transformation. Despite implementation challenges, their benefits make them a strategic choice for IT leaders. As the cybersecurity landscape evolves, the convergence of these solutions is likely to play a pivotal role in shaping the future of secure remote access.

Acknowledgement
This research was not funded by any grant.

References

[1] Jie, C. Y., and N. Mat Ali. "COVID-19: What are the challenges of online learning? A literature review." *International Journal of Advanced Research in Future Ready Learning and Education* 23, no. 1 (2021): 23-29.
[2] Mandal, Sudakshina, and Danish Ali Khan. "A Study of security threats in cloud: Passive impact of COVID-19 pandemic." In *2020 International Conference on Smart Electronics and Communication (ICOSEC)*, pp. 837-842. IEEE, 2020. https://doi.org/10.1109/ICOSEC49089.2020.9215374
[3] Verizon. "Analyzing the Covid-19 data breach landscape." (2020). https://www.verizon.com/business/en-sg/resources/articles/analyzing-covid-19-data-breach-landscape
[4] Jaafar, F. "More Malaysian companies encourage remote working on increased cloud adoption." (2022).
[5] Cisco. "Employees are ready for hybrid work, are you?" *Cisco Global Hybrid Work Study*, (2022).
[6] Kaur, D. "For a secure hybrid workforce." (2022). https://doi.org/10.1155/2022/7540891
[7] Palo Alto Network. "Palo Alto Networks Calls on Cybersecurity Industry to Adopt ZTNA 2.0 -- Zero Trust with Zero Exceptions." (2022).
[8] Suhaimin, Khairul Nizam, Wan Hasrulnizzam Wan Mahmood, Zuhriah Ebrahim, Halimaton Hakimi, and Syafiq Aziz. "Human Centric Approach in Smart Remanufacturing for End-Life-Vehicle (ELV)'s Stabilizer Bar." *Malaysian Journal on Composites Science and Manufacturing* 12, no. 1 (2023): 1-12. https://doi.org/10.37934/mjcsm.12.1.112
[9] van der Walt, Stephanus, and Hein Venter. "Research gaps and opportunities for secure access service edge." In *International Conference on Cyber Warfare and Security*, vol. 17, no. 1, pp. 609-619. 2022. https://doi.org/10.34190/iccws.17.1.75
[10] Lev. D.B. "MEF SASE Services Framework." (2022). https://www.mef.net/wp-content/uploads/2020/07/MEF-white-paper-MEF-SASE-Services-Framework.pdf
[11] Cloudflare. "Secure Access Service Edge (SASE) Accelerating network transformation and security modernization." (2023).
[12] Gartner. "Security and Performance Testing for SASE-ZT." (2021). https://assets.ctfassets.net/wcxs9ap8i19s/4qYeR69PoPzfFLkntE5PzR/fce0b8b285788ad9316fea0ecd6d58a5/WP_Security_Performance_Testing_SASE-ZT_RevA.pdf
[13] Wang. X, Zhu. H, Ni. H. "Zero Trust - Zero Trust Reference Architecture." (2023). https://networkbuilders.intel.com/docs/networkbuilders/zero-trust-zero-trust-reference-architecture-technology-guide-1668697587.pdf
[14] Versa Network. "Zero Trust Security." (2023). https://versa-networks.com/documents/white-papers/zero-trust-security.pdf
[15] Deshpande, Aniket. "Relevance of Zero Trust Network Architecture amidts and it's rapid adoption amidts Work From Home enforced by COVID-19." *Psychology and Education* 58, no. 1 (2021): 5672-5677. https://doi.org/10.17762/pae.v58i1.2190
[16] Cerqueira.B., Alves.B., Pires.C. "Embrace digital transformation with scalable and secure cloud-based network Services Secure Access Service Edge (SASE) Point of view." (2022). https://www2.deloitte.com/content/dam/Deloitte/pt/Documents/technology/Global-Telecom-Engineering-Excellence-(gTEE)-Secure-Access-Service-Edge-(SASE)-Point-of-view.pdf
[17] Sarkar, Sirshak, Gaurav Choudhary, Shishir Kumar Shandilya, Azath Hussain, and Hwankuk Kim. "Security of zero trust networks in cloud computing: A comparative review." *Sustainability* 14, no. 18 (2022): 11213. https://doi.org/10.3390/su141811213
[18] He, Yuanhang, Daochao Huang, Lei Chen, Yi Ni, and Xiangjie Ma. "A survey on zero trust architecture: Challenges and future trends." *Wireless Communications and Mobile Computing* 2022 (2022). https://doi.org/10.1155/2022/6476274
[19] Accenture. "The convergence of network and security is here: It's called SASE." (2023). https://www.accenture.com/content/dam/accenture/final/accenture-com/document/Accenture-SASE-Sales-Enablement.pdf
[20] Citrix. "Understanding Secure Access Service Edge (SASE) Architectures." (2023). https://www.citrix.com/content/dam/citrix/en_us/documents/white-paper/understanding-secure-access-service-edge-sase-architectures.pdf
[21] Orange Cyberdefense. "SASE: The Digital Business Enabler For Your Workforce." (2023). https://www.orange-business.com/sites/default/files/sase-the-digital-business-enabler-for-your-workforce_ebook.pdf
[22] Miller. L. "SASE for dummies." (2020). https://www.exclusive-networks.com/be/wp-content/uploads/sites/14/2020/12/sase-for-dummies.pdf
[23] Frost and Sullivan. "Global Secure Access Service Edge Industry." (2022). https://www.frost.com/wp-content/uploads/2022/07/2022-Award-Write-Up-Palo-Alto-Networks-SASE-Award.pdf

[24] Information Security Branch. "Information Security Thought Paper – Zero Trust." *British Columbia.* (2023).
[25] Chapple, M. "Why it's SASE and zero trust, not SASE vs. zero trust." (2020). https://www.techtarget.com/searchsecurity/tip/Why-its-SASE-and-zero-trust-not-SASE-vs-zero-trust
[26] Honnachari.R., Doyle.H., Townsend.K., Kerravala.Z., Connors.C., Monclus.P. "ZTNA and SASE for dummies." (2021). https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/secure-access-service-edge-sase/vmw-sdwan-sase-ztna-dummies-eb.pdf
[27] Menlo Security. "What's the relationship between SASE and Zero Trust?" (2021).
[28] IBM. "IBM Expands Zero Trust Strategy Capabilities with New SASE Services to Modernize Network Security." (2021).
[29] Lumen. "SASE And ZTNA Empower and Protect Hybrid Workforces." (2023).
[30] ZTEdge. "What's the Zero Trust - SASE Connection?" (2023). https://www.ericom.com/wp-content/uploads/2021/08/Whats-the-Zero-Trust-SASE-connection-8-2021.pdf
[31] Palo Alto Network. "A Zero Trust Approach is More Critical Than Ever." (2022). https://events.esd.org/wp-content/uploads/2022/11/Valarezo-Carlos-Palo-Alto-Networks-MI-Cyber-Summit-SASE-ZTNA-2.0.pdf
[32] Carney. M. "Factors to consider when implementing Zero Trust and SASE (Secure Access Service Edge) architecture." (2022).
[33] Palo Alto Network. "How Zero Trust and SASE Can Work Together." (2023).