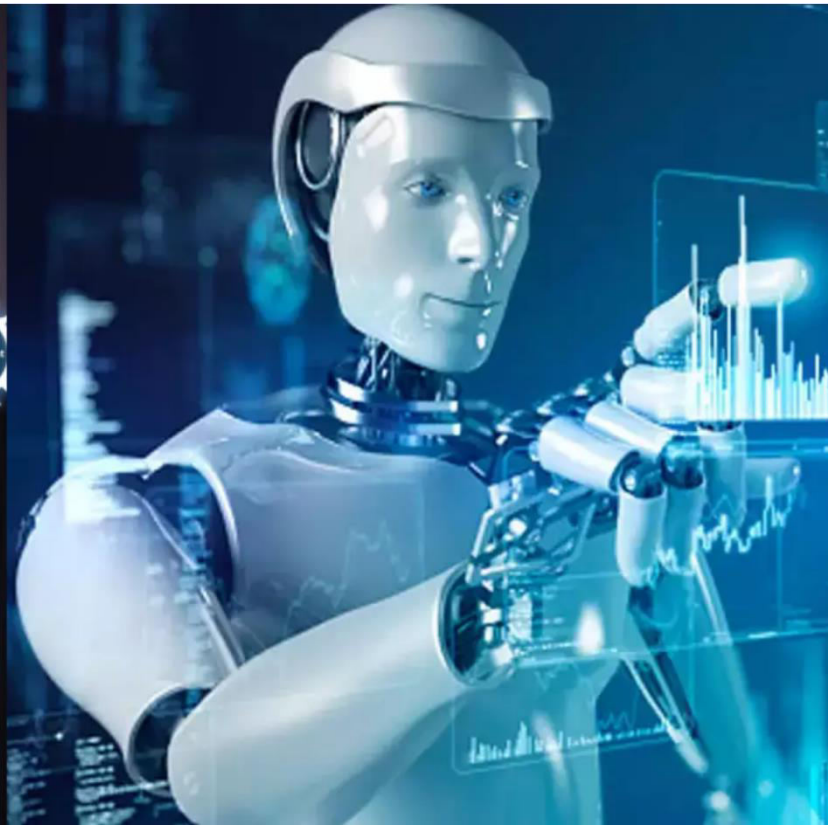
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Issue 3, March 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503231|

Secure Access Service Edge (SASE): A Comprehensive Review of Architecture, Security Capabilities, and Enterprise Adoption

Tirth Chande, Dr. Himanshu Maniar

Student, Bhagwan Mahavir College of Computer Application, Bhagwan Mahavir University, Surat, India

Guide, Assistant Professor, Bhagwan Mahavir College of Computer Application, Bhagwan Mahavir University, Surat, India

ABSTRACT: Secure Access Service Edge (SASE) is an emerging cybersecurity architecture that integrates networking and security capabilities into a unified cloud-delivered service. The rapid adoption of cloud computing, SaaS applications, mobile users, and remote workforces has significantly expanded the traditional network perimeter, making conventional security models inadequate. SASE addresses these challenges by combining technologies such as Software-Defined Wide Area Networking (SD-WAN), Secure Web Gateways (SWG), Cloud Access Security Brokers (CASB), Firewall-as-a-Service (FWaaS), and Zero Trust Network Access (ZTNA) into a single cloud-native framework. This review paper analyzes the SASE architecture, its key components, operational model, benefits, limitations, and industry adoption trends. The study is based on a comprehensive review of thirty research articles, industry whitepapers, and cybersecurity publications. The findings indicate that SASE provides improved scalability, centralized policy enforcement, and secure connectivity for distributed enterprises while reducing infrastructure complexity. However, organizations must carefully consider implementation strategies, vendor selection, and integration challenges when adopting SASE solutions.

KEYWORDS: SASE, SWG, CASB, DLP, SDWAN, ZTNA, FWaaS

I. INTRODUCTION

Modern enterprises are undergoing rapid digital transformation driven by cloud computing, mobile workforces, and the widespread adoption of Software-as-a-Service (SaaS) applications. Traditional network security architectures were designed based on the concept of a secure perimeter, where users and applications resided within a controlled corporate network. However, this model has become ineffective due to the shift toward distributed environments.

With employees accessing enterprise resources from various locations and devices, organizations face challenges such as increased attack surface, lack of visibility, and performance bottlenecks. Traditional Virtual Private Networks (VPNs) introduce latency and are not designed to handle modern cloud-based workloads efficiently.

Secure Access Service Edge (SASE) was introduced as a revolutionary framework that converges networking and security into a unified cloud-delivered architecture. Unlike legacy approaches, SASE leverages globally distributed Points of Presence (PoPs) to deliver security services closer to users, reducing latency and improving performance.

II. METHODOLOGY

This research is based on a **Systematic Literature Review (SLR)** methodology to analyze the concept, architecture, and implementation of Secure Access Service Edge (SASE). The SLR approach ensures a structured, unbiased, and comprehensive evaluation of existing research studies and industry publications.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503231|

2.1 Research Design

The study follows a qualitative research design based on secondary data collected from academic journals, conference papers, whitepapers, and industry reports related to SASE architecture. The objective is to analyze the evolution, components, and impact of SASE in modern enterprise networks.

2.2 Data Collection

Data was collected from multiple reliable sources such as:

- IEEE Xplore Digital Library
- ACM Digital Library
- ResearchGate
- Google Scholar
- Industry whitepapers (Palo Alto Networks, Cisco, Netskope, Zscaler)

A total of **25 research papers and technical documents** were selected based on their relevance to SASE architecture, cloud security, and enterprise networking.

2.3 Paper Selection Criteria

The selection of research papers was based on the following criteria:

Inclusion Criteria:

- Papers related to SASE architecture
- Studies discussing SD-WAN, CASB, ZTNA, SWG, and FWaaS
- Research published between 2019 and 2024
- Peer-reviewed journals and credible industry reports

Exclusion Criteria:

- Papers unrelated to cloud or network security
- Duplicate studies
- Non-technical or opinion-based articles

2.4 Data Extraction

From each selected research paper, the following information was extracted:

- Author and publication year
- Research objectives
- Methodology used in the study
- Key findings
- Technologies involved in SASE implementation

The extracted data was organized systematically to enable structured comparison.

2.5 Data Analysis

The collected data was analyzed using a comparative and analytical approach. The analysis focused on:

- Evolution of SASE architecture
- Integration of networking and security components
- Performance improvements over traditional security models
- Role of Zero Trust in SASE

2.6 Comparative Evaluation

A comparative analysis was conducted between traditional network security architectures and SASE-based architectures based on:

- Security model (Perimeter vs Zero Trust)
- Deployment model (On-premise vs Cloud)
- Scalability
- Network performance
- Management complexity

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503231|

2.7 Research Gap Identification

Based on the analysis of selected literature, several research gaps were identified:

- Limited real-world enterprise deployment studies
- Lack of comparative analysis between different SASE vendors
- Insufficient performance benchmarking data
- Limited research in developing regions

2.8 Limitations of the Study

The study is limited to secondary data sources and does not include primary data collection or real-time enterprise deployment analysis. Additionally, some industry reports may introduce vendor bias.

III. SASE OVERVIEW

The concept of SASE emerged as enterprises began migrating their infrastructure to cloud environments. Traditional wide area network (WAN) architectures relied on backhauling traffic through centralized data centers for security inspection. While this approach worked for legacy networks, it introduced latency and performance issues in modern cloud-based environments.

To address these challenges, Software-Defined Wide Area Network (SD-WAN) technology was introduced to provide dynamic and intelligent routing across distributed networks. At the same time, cloud-delivered security services such as Secure Web Gateways and Cloud Access Security Brokers began gaining popularity.

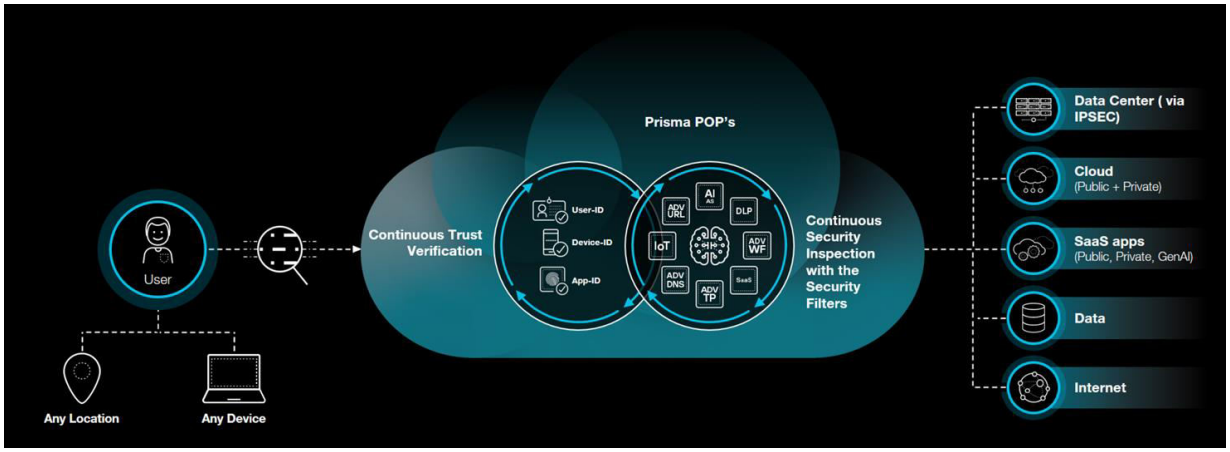
SASE represents the convergence of these technologies. Instead of deploying multiple standalone appliances for networking and security, organizations can use a single cloud platform that provides integrated capabilities. The SASE architecture is designed to deliver security inspection and network optimization at the edge of the network through globally distributed points of presence (PoPs).

3.1 SASE Architecture

The architecture of SASE is based on a cloud-native model that delivers networking and security services through distributed edge locations. Users connect to the nearest point of presence where their traffic is inspected and routed to the appropriate destination.

Key characteristics of SASE architecture include identity-based access control, cloud-native infrastructure, and global scalability. Unlike traditional security architectures that rely on IP-based policies, SASE uses user identity and device posture as the primary factors for access control.

Another important aspect of SASE architecture is the use of distributed cloud nodes. These nodes perform security inspection, traffic optimization, and access enforcement close to the user. This approach reduces latency and improves application performance while maintaining strong security controls.



International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503231|

3.2 Core Components of SASE

The SASE framework integrates multiple networking and security technologies into a unified platform.Software-Defined Wide Area Network (SD-WAN) enables organizations to intelligently route traffic across multiple network paths. It improves network performance and reliability by dynamically selecting the best available path.

Secure Web Gateway (SWG) provides protection against malicious web traffic by filtering URLs, scanning content, and enforcing acceptable use policies.

Cloud Access Security Broker (CASB) acts as an intermediary between users and cloud applications. It provides visibility into cloud usage, enforces security policies, and protects sensitive data.

Firewall-as-a-Service (FWaaS) delivers firewall capabilities through the cloud. It performs deep packet inspection, threat detection, and access control without requiring on-premise hardware appliances.

Zero Trust Network Access (ZTNA) ensures that users are granted access only to the specific resources they are authorized to use. Instead of trusting users inside the network perimeter, ZTNA continuously verifies identity and device posture before granting access.

3.3 Advantages of SASE

One of the major advantages of SASE is its ability to provide consistent security policies across distributed environments. Because the security services are delivered through the cloud, organizations can enforce the same policies for remote users, branch offices, and headquarters.

Another advantage is improved network performance. Traditional architectures often require traffic to be routed through centralized data centers for inspection, which increases latency. In contrast, SASE performs inspection at distributed edge locations, reducing the distance traffic must travel.

SASE also simplifies network management by consolidating multiple security tools into a single platform. This reduces operational complexity and lowers infrastructure costs.

Additionally, SASE supports modern workforce requirements by enabling secure remote access to enterprise applications. As remote and hybrid work models continue to grow, SASE provides a scalable solution for secure connectivity.

3.4 Challenges and Limitations

Despite its benefits, implementing SASE presents several challenges for organizations. One of the primary challenges is integration with existing legacy infrastructure. Many enterprises have already invested heavily in traditional networking and security appliances.

Another challenge is vendor dependency. Because SASE platforms integrate multiple services into a single solution, organizations may become heavily dependent on a specific vendor.

Performance monitoring can also be complex in SASE environments. Since traffic flows through distributed cloud nodes, organizations must rely on advanced monitoring tools to maintain visibility into network performance and security events.

Finally, adopting SASE requires skilled cybersecurity professionals who understand both networking and cloud security architectures.

3.5 SASE Use Cases

SASE is particularly beneficial for organizations with distributed workforces. Employees working remotely can securely access enterprise applications through SASE platforms without requiring traditional VPN connections.Another

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503231|

common use case is branch office connectivity. Instead of deploying multiple security appliances at each branch location, organizations can route branch traffic through SASE edge nodes for inspection.

SASE is also useful for securing cloud application access. With the increasing adoption of SaaS platforms, organizations need visibility and control over cloud usage. CASB and SWG components within SASE provide these capabilities.

3.6 Future Trends in SASE

The adoption of SASE is expected to increase significantly in the coming years as organizations continue migrating to cloud-based infrastructures. Advances in artificial intelligence and machine learning are likely to enhance threat detection capabilities within SASE platforms.

Another emerging trend is the integration of SASE with edge computing and 5G networks. As more devices connect to enterprise networks, SASE will play a critical role in securing edge environments.In addition, the zero-trust security model will continue to influence the development of SASE solutions. Identity-driven security policies and continuous authentication will become standard features in future SASE platforms.

3.7 Conclusion

Secure Access Service Edge represents a fundamental shift in the design of enterprise networking and cybersecurity architectures. By converging networking and security services into a unified cloud platform, SASE enables organizations to securely connect users and applications regardless of their location.

As digital transformation continues to reshape enterprise environments, SASE is expected to become a core component of modern cybersecurity strategies.

IV. RELATED WORK

Secure Access Service Edge (SASE) has gained significant attention in recent years due to the increasing adoption of cloud computing and remote work environments. Various researchers and industry experts have studied its architecture, components, and impact on enterprise security.

4.1 SASE Concept and Framework

MacDonald et al. (2019) introduced the concept of SASE and emphasized the convergence of networking and security into a cloud-delivered model. The study highlighted the limitations of traditional perimeter-based architectures.

Shackleford (2020) analyzed the SASE framework and identified key components such as SD-WAN, CASB, and Zero Trust Network Access (ZTNA). The research emphasized the importance of identity-based security.

4.2 Cloud Security and Zero Trust

Zscaler (2022) explored Zero Trust Network Access and demonstrated its advantages over traditional VPN-based security models. Similarly, Google Cloud (2021) introduced the BeyondCorp model, which focuses on identity-based access control.

Netskope (2023) highlighted the role of CASB in providing visibility and control over cloud **applications.**

4.3 Performance and Network Optimization

Cisco (2021) studied enterprise networking and showed that SD-WAN improves network performance through intelligent traffic routing. VMware (2023) further analyzed SD-WAN integration within SASE and its impact on bandwidth optimization.

4.4 Edge Security and Distributed Architecture

Cloudflare (2023) examined edge-based security models and emphasized the role of distributed Points of Presence (PoPs) in reducing latency and improving performance.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503231|

IEEE (2021) also highlighted the importance of edge computing in enhancing security and scalability.

4.5 Implementation and Challenges

Fortinet (2022) discussed unified security frameworks and emphasized simplified management through SASE. TechTarget (2022) analyzed real-world deployment challenges such as migration complexity and vendor dependency.

V. MARKET ANALYSIS

Secure Access Service Edge (SASE) Market Size was valued at USD 15.73 Bn in 2025 and is predicted to reach USD 133.79 Bn by 2035 at a 24.0% CAGR during the forecast period for 2026 to 2035.

Secure Access Service Edge (SASE) Market Key Takeaways:

- Secure Access Service Edge (SASE) Market Size was valued at USD 15.73 Bn in 2025 and is predicted to reach USD 133.79 Bn by 2035
- Secure Access Service Edge (SASE) Market is expected to grow at a 24.0% CAGR during the forecast period for 2026 to 2035.
- Secure access service edge (SASE) market is segmented based on offering, organization size, and end-user.
- North America region is leading the Secure Access Service Edge (SASE) Market

VI. CONCLUSION

Secure Access Service Edge (SASE) represents a significant evolution in enterprise networking and cybersecurity by integrating networking and security services into a unified cloud-delivered architecture. With the rapid adoption of cloud computing, remote work environments, and SaaS applications, traditional perimeter-based security models are no longer sufficient to address modern security challenges.

This study, based on a systematic literature review, highlights that SASE effectively combines technologies such as SD-WAN, Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Firewall-as-a-Service (FWaaS), and Zero Trust Network Access (ZTNA) to provide secure and optimized connectivity. The analysis of various research studies demonstrates that SASE improves scalability, enhances network performance, and enables centralized policy enforcement across distributed enterprise environments.

Furthermore, SASE adopts a Zero Trust security model, ensuring identity-based access control and reducing the risk of unauthorized access. The comparative analysis indicates that SASE outperforms traditional security architectures in terms of flexibility, efficiency, and security posture.

However, despite its advantages, SASE implementation presents several challenges, including vendor lock-in, migration complexity, integration with legacy systems, and limited real-world deployment studies. These challenges highlight the need for further research in performance benchmarking, vendor comparison, and practical implementation strategies.

In conclusion, SASE is a future-ready architecture that aligns with modern enterprise requirements and digital transformation goals. Organizations adopting SASE can achieve improved security, better user experience, and simplified network management. Future work should focus on evaluating real-world deployments and optimizing SASE frameworks to enhance their effectiveness across diverse enterprise environments.

REFERENCES

1. MacDonald, N., Orans, L., & Skorupa, J. (2019). The Future of Network Security Is in the Cloud. Gartner Research.
2. Shackleford, D. (2020). Secure Access Service Edge Architecture Overview. SANS Institute.
3. Cisco Systems. (2021). Secure Access Service Edge Architecture Whitepaper.
4. Palo Alto Networks. (2022). Prisma SASE Architecture and Security Model.
5. Fortinet. (2022). Unified Networking Security Model.
6. Netskope. (2023). Understanding the SSE and SASE
7. Cloudflare. (2023). Secure Access Service Edge

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503231|

8. Zscaler. (2022). Introducing Zero Trust SASE
9. Google Cloud. (2021). BeyondCorp and Zero Trust Security Model.
10. NIST. (2020). Zero Trust Architecture Special Publication 800-207.
11. IBM Security. (2022). Cloud-based Network Security and SASE.
12. VMware. (2023). SASE Networking Architecture for Modern Enterprises.
13. Akamai Technologies. (2022). Enterprise Security with SASE Platforms.
14. IDC Research. (2023). Global Market Trends for Secure Access Service Edge.
15. IEEE Communications Magazine. (2021). Secure Edge Networking for Cloud Environments.
16. ACM Digital Library. (2020). Edge Security Architectures in Distributed Networks.
17. Microsoft Security. (2022). Cloud Security Frameworks for Modern Enterprises.
18. Cloud Security Alliance. (2021). Security Guidance for SASE Adoption.
19. TechTarget. (2022). SASE Implementation Strategies for Enterprises.
20. Gartner Analysis (2024) Market Opportunity Map: SASE, Worldwide
21. International Journal of Computer Networks. (2022). SD-WAN and Secure Access Integration.
22. SASE Market Research Report – Insight Ace Analytics (2026)
23. SASE Market – Dimension Market Research

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details