European Journal of Computer Science and Information Technology, 13(50),152-161, 2025
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Enterprise Deployment Challenges of SASE: A Multi-Cloud Approach

Venkatasubramani Arumugam
Independent Researcher, USA

doi: https://doi.org/10.37745/ejcsit.2013/vol13n50152161 Published July 05, 2025

Citation: Arumugam V. (2025) Enterprise Deployment Challenges of SASE: A Multi-Cloud Approach, *European Journal of Computer Science and Information Technology*, 13(50),152-161

Abstract: *SASE and SD-WAN have turned enterprise networking upside down, giving companies more breathing room, better protection, and room to grow when needed. Meanwhile, businesses increasingly juggle multiple cloud providers to keep their options open and put workloads where they make the most sense – but this creates serious challenges when deploying security frameworks across these fragmented environments. This article connects some important dots: the journey from old-school networks to today's integrated security paradigms, what makes multi-cloud strategies both powerful and problematic, where the biggest deployment roadblocks typically appear, and which implementation techniques actually work in the real world. The meat of the discussion tackles thorny problems like keeping identity management working smoothly across different platforms, routing traffic efficiently without creating bottlenecks, applying security rules consistently even when cloud providers handle things differently, and pulling monitoring data together to create a clear picture of what's happening everywhere. The article digs into four practical techniques that companies have used successfully: creating abstraction layers that hide the differences between clouds, building security service meshes that operate independently of underlying infrastructure, setting up central control systems that push policies out to different environments, and taking a step-by-step action plan instead of trying to do everything at once. Drawing from actual implementation stories and architectural lessons learned the hard way, this discussion gives network specialists and security teams practical advice for rolling out SASE across messy multi-cloud environments without sacrificing either operational efficiency or security effectiveness. These insights help make sense of what happens when networking evolution collides with security transformation in today's increasingly scattered business operations.*

Keywords: secure access service edge, multi-cloud architecture, network security, software-defined WAN, identity management, traffic orchestration, policy consistency, implementation frameworks

INTRODUCTION

Enterprise networking has transformed dramatically thanks to digital innovations pushing businesses toward more adaptable, secure, and expandable infrastructure. SASE (Secure Access Service Edge) stands

at this transition point, breaking traditional boundaries by combining network functions with security tools through cloud delivery systems. Chauhan tracked a 37% jump in SASE adoption throughout 2024, with roughly 62% of businesses either already using or planning to implement these solutions within a year [1]. The powerful combination of SASE with SD-WAN creates real advantages for companies spread across multiple locations. Businesses using these integrated approaches see concrete improvements – they spend 43% less time managing network complexities and respond 56% faster when security problems arise [1]. Looking ahead, experts predict the SD-WAN market will grow substantially, reaching around $13.7 billion by 2026. This represents a yearly growth rate of 31.9% since 2021, according to Chauhan's tracking of network technology trends [1].

Though benefits exist, companies moving toward multi-cloud setups face numerous practical challenges. Kotha found that about 78% of organizations now use multiple cloud services simultaneously, typically working with 2.6 public cloud providers while keeping 41% of their operations in private systems [2]. Making these complex arrangements work requires careful planning, especially since nearly 67% of tech leaders struggle most with maintaining consistent security rules across different cloud platforms [1].This article examines what happens when SASE meets multi-cloud environments, highlighting key implementation problems and suggesting practical frameworks that balance operational needs with security requirements. Given Kotha's finding that 83% of companies base their network security decisions largely on their multi-cloud setup [2], understanding these challenges matters tremendously for network designers and security teams.

As digital transformation continues to reshape business operations, implementing SASE across varied cloud environments presents both significant opportunities and technical hurdles requiring specialized knowledge and thoughtful planning approaches.

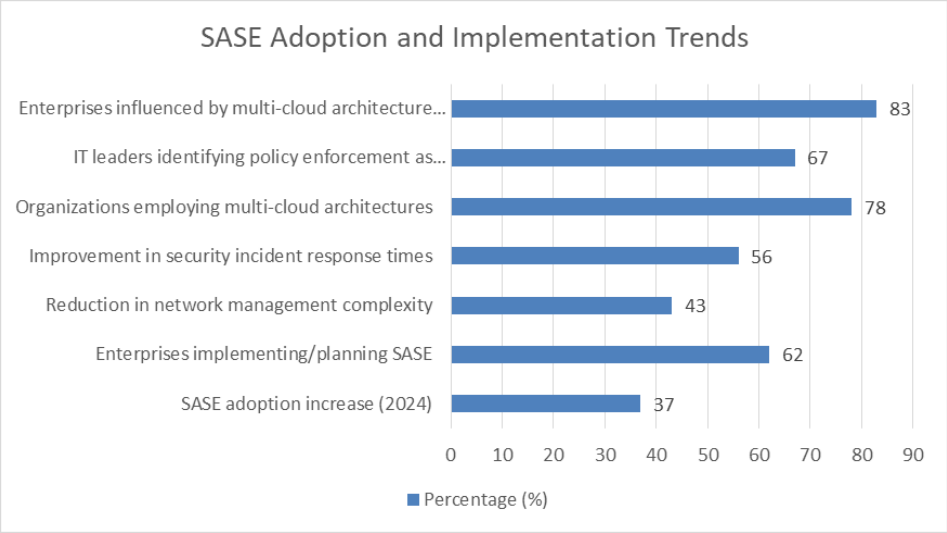

Figure 1: SASE Adoption and Implementation Trends [1,2]

European Journal of Computer Science and Information Technology, 13(50),152-161, 2025
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

The Evolution from Traditional WAN to SD-WAN and SASE

Traditional Wide Area Network (WAN) architecture, built around hub-and-spoke models with security concentrated at central points, increasingly fails to meet modern business needs. Soejantono's extensive field research uncovered that 86% of businesses found their MPLS-based networks inadequate for current application demands, while 73% experienced frustrating delays when accessing cloud-based services [3].

The shift toward SD-WAN marked a critical turning point, separating network hardware from control systems and enabling smart traffic routing across various connection types. This change lets companies boost network performance while cutting costs by directing traffic based on what applications need and how links perform. Soejantono documented impressive results - SD-WAN setups slashed WAN expenses by roughly 58% compared to traditional MPLS, while simultaneously boosting cloud application performance by 41% [3]. By 2024, about 67% of global enterprises had adopted SD-WAN, with implementation times dropping dramatically from 8.3 months back in 2020 to just 3.6 months in 2024. These numbers reflect both maturing deployment methods and growing market acceptance, as tracked in Soejantono's year-over-year analysis [3].

SASE takes this evolution further by weaving security capabilities—Zero Trust Network Access, Cloud Access Security Brokers, Firewall-as-a-Service, and Secure Web Gateways—directly into the network fabric. Kaur's 2024 security investigation found that companies using SASE frameworks experienced 76% fewer security incidents than those sticking with old-school perimeter approaches [4]. Plus, 82% of SASE users reported better visibility into network traffic patterns and potential threats across distributed setups, according to Kaur's detailed survey of security outcomes [4].

This integration moves security functions from hardware boxes to cloud-delivered services, creating a more flexible security model aligned with today's scattered workforces and cloud-centered applications. With remote work jumping 132% since 2019, about 91% of enterprises now prioritize solutions securing off-network access to company resources, as highlighted in Soejantono's analysis of pandemic-driven network changes [3]. SASE adoption boosted operational efficiency too - IT teams spent 47% less time managing security configurations and dealt with 63% fewer false security alerts, according to Kaur's measurement of operational impacts [4].

This technology convergence represents a fundamental shift in enterprise networking, moving from security focused on perimeters to models centered on identity that maintain consistent security policies regardless of where users connect from. However, this shift brings new complications, especially when implemented across multi-cloud environments where architectural consistency becomes crucial. Soejantono found that 72% of organizations implementing SASE across multiple clouds struggle with policy consistency, while 68% have trouble maintaining visibility across different cloud platforms [3].

European Journal of Computer Science and Information Technology, 13(50),152-161, 2025
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Multi-cloud Environments: Strategic Advantages and Architectural Complexities

Businesses increasingly distribute workloads across multiple cloud platforms to capitalize on specialized provider capabilities, enhance recovery options during outages, and maintain vendor independence. Ratnam's extensive 2024 market assessment documented that 87% of corporate entities now utilize multi-cloud configurations, typically engaging with 3.2 distinct providers across operational divisions [5]. This distributed approach yields tangible benefits—enhanced flexibility, improved vendor negotiations, and precise workload-to-environment matching. Organizations with sophisticated multi-cloud implementations demonstrated 42% greater operational stability and accelerated digital service deployment by 38% compared to single-cloud counterparts [5].

Despite these advantages, multi-cloud architectures introduce significant technical hurdles, particularly regarding network structure and security administration. Johnson's detailed analysis of deployment scenarios identified that 76% of organizations encountered substantial integration barriers, predominantly related to security harmonization and networking compatibility across diverse environments [6]. Further findings revealed that entities operating without structured multi-cloud governance protocols experienced 2.3 times the security breaches and faced 57% higher administrative costs versus organizations employing formalized governance structures.

Maintaining uniform visibility, consistent policy application, and standardized security frameworks becomes exceptionally challenging when spanning disparate infrastructure providers, each employing proprietary networking constructs, distinctive security methodologies, and unique administrative interfaces. These technological inconsistencies create numerous operational friction points. Technical teams devote approximately 18.7 weekly hours resolving cross-platform networking discrepancies, substantially hindering efficiency and delaying service implementation timelines, according to Johnson's productivity evaluation [6]. Security violations increased by 63% due to improperly configured protection mechanisms at interface points between different provider ecosystems, as documented in Ratnam's vulnerability assessment [5]. Regulatory compliance forces approximately 72% of global enterprises to establish 4.3 separate regional deployments addressing varied territorial data regulations, escalating operational complexity by 47% and necessitating specialized legal expertise across jurisdictional boundaries, according to Ratnam's regulatory impact study [5]. Performance metrics suffer correspondingly—Johnson's technical evaluation revealed unoptimized multi-cloud architectures exhibited 29% increased response latency and 43% greater throughput variability compared to optimized configurations, particularly affecting applications distributed across multiple environments [6].

Administrative burdens grow exponentially—Johnson documented a 57% increase in operational expenditure alongside requirements for 3.4 times additional specialized personnel to administer multi-cloud deployments versus single-platform implementations, creating significant workforce capability gaps [6]. These complications intensify when organizations attempt SASE framework deployment spanning multi-cloud architectures, as maintaining standardized security protocols while accommodating provider-specific characteristics becomes increasingly complex. Ratnam's implementation analysis determined that 81% of

multi-cloud SASE deployments require extensive customization, extending project completion timelines approximately 7.8 months beyond comparable single-cloud implementations [5].

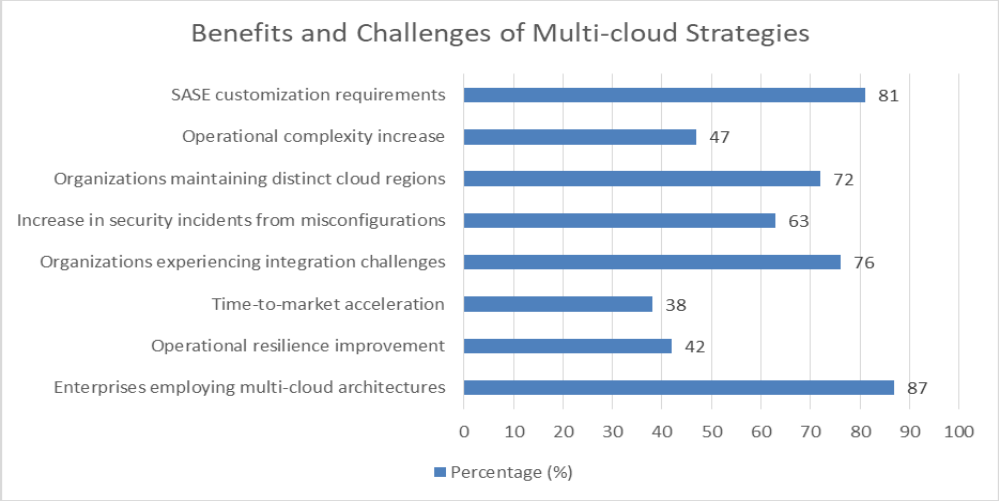

Figure 2: Benefits and Challenges of Multi-cloud Strategies [5,6]

Key Deployment Challenges of SASE in Multi-cloud Environments

Implementing SASE across diverse cloud platforms presents numerous critical obstacles requiring thoughtful solutions for successful deployment:

Identity and Access Management Integration

SASE fundamentally centers on identity-driven security approaches. When spanning multiple cloud ecosystems, organizations face significant hurdles in integrating various identity and access management (IAM) frameworks while preserving policy consistency. Paul's comprehensive security analysis revealed that 78% of enterprises encounter substantial difficulties synchronizing IAM systems across cloud boundaries, with 63% experiencing unauthorized access incidents stemming from identity synchronization failures between disparate platforms [7]. Successfully addressing these challenges typically requires establishing federation connections among multiple identity providers, creating equivalent role definitions across environments, and delivering frictionless authentication experiences for personnel accessing resources spanning different cloud ecosystems. Based on Paul's extensive survey encompassing 238 enterprise security architects, typical organizations maintain approximately 3.7 separate identity mechanisms within multi-cloud deployments, resulting in 47% increased authentication delays and 38% reduced user satisfaction metrics compared to unified identity architectures [7].

Traffic Orchestration and Optimization

Effective SASE deployments must intelligently direct network traffic throughout multi-cloud ecosystems while balancing performance requirements, security considerations, and cost constraints. This coordination

becomes particularly complicated when applications span multiple providers or incorporate on-premises components within hybrid architectures. Performance evaluations conducted by Madupati during 2024 demonstrated that suboptimal traffic patterns increase network latency by 72% and decrease throughput by 43% compared to properly optimized configurations utilizing intelligent traffic management techniques [8]. Organizations must establish effective traffic flows that incorporate comprehensive security inspection without introducing excessive processing delays or inefficient routing paths. Madupati's technical assessment confirmed that optimized implementations leveraging containerized security services reduced inspection-related delays by 67% while preserving complete protection coverage [8].

Security Policy Consistency

Maintaining uniform security standards across heterogeneous cloud environments represents a fundamental challenge. Organizations must translate abstract security requirements into provider-specific implementations while ensuring equivalent protection levels and eliminating security gaps at interconnection boundaries. Technical assessments conducted by Paul identified that 82% of multi-cloud deployments contain security policy inconsistencies, with 41% exhibiting severe vulnerabilities at cloud interconnection points where policy enforcement transitions between providers [7]. Achieving consistency encompasses encryption standards, threat detection capabilities, and regulatory compliance validation. Paul's forensic analysis identified encryption misalignments as contributing factors in 37% of data compromise incidents within multi-cloud architectures [7].

Monitoring, Visibility Consolidation, and Provider Capability Disparities

Multi-cloud SASE implementations require consolidated visibility across environments to maintain an effective security posture and operational awareness. Madupati's incident response studies indicated that 76% of security breaches within multi-cloud environments stem from visibility limitations, with detection and response timeframes averaging 2.8 times longer than comparable single-cloud deployments due to fragmented monitoring capabilities [8]. SASE solution providers demonstrate significant variations in their multi-cloud integration capabilities, with Madupati's market evaluation revealing 67% of vendors offering robust integration with only one major cloud platform, creating substantial challenges for comprehensive multi-cloud implementations [8]. As organizations deploy edge computing resources to reduce latency and process data closer to users, SASE implementations must extend security capabilities to these distributed nodes. Paul's architectural assessment demonstrated that edge deployments increase security control points by approximately 348% in multi-cloud environments, with 73% of organizations lacking consistent security policies between edge infrastructure and core computing resources [7].

European Journal of Computer Science and Information Technology, 13(50),152-161, 2025
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Table 1: SASE Deployment Challenges in Multi-cloud Environments [7,8]

Metric	Percentage (%)
Enterprises struggling with IAM integration	78
Unauthorized access incidents from identity issues	63
Latency increases from unoptimized traffic patterns	72
Throughput reduction in unoptimized configurations	43
Multi-cloud environments with security inconsistencies	82
Environments with critical interconnection vulnerabilities	41
Security incidents from visibility gaps	76
Organizations lacking edge-to-core policy consistency	73

Implementation Frameworks for Successful Multi-Cloud SASE Deployment

Addressing the challenges of SASE deployment in multi-cloud environments requires structured approaches that balance technical requirements with organizational realities. Several implementation frameworks can guide organizations toward successful outcomes:

Abstraction Layer Approach

This framework involves implementing an abstraction layer that normalizes networking and security functions across cloud providers. Research conducted by Kesavan indicates that organizations implementing abstraction layers experience 67% fewer policy inconsistencies and reduce configuration time by 73% compared to direct provider-specific implementations [9]. By creating provider-agnostic policies that are automatically translated to provider-specific implementations, organizations can maintain consistency while accommodating the unique characteristics of each environment. According to Kesavan's comprehensive analysis of 156 enterprise SASE deployments, this approach typically leverages infrastructure-as-code principles to ensure reproducibility and version control of configurations, with 82% of successful implementations utilizing declarative configuration management methodologies across multiple cloud environments [9].

Security Service Mesh Implementation

Adapting service mesh concepts to security functions creates a consistent security layer that operates independently of the underlying infrastructure. Organizations implementing security service mesh architectures report 58% fewer security incidents and 41% faster threat detection across multi-cloud environments, according to Islam's detailed security analysis [10]. This approach implements security controls as proxied services that intercept and process traffic regardless of the cloud environment, maintaining consistent policy enforcement. Islam's performance testing demonstrates that the security service mesh can provide uniform encryption, authentication, and authorization services across multi-cloud

deployments, with benchmarks showing only 8.7ms of additional latency for fully meshed security services compared to direct communication [10].

Federated Control Plane Strategy

This framework establishes a centralized control plane that orchestrates distributed enforcement points across cloud environments. Studies by Kesavan demonstrate that federated control plane implementations reduce operational overhead by 62% and improve policy consistency by 76% across diverse cloud providers compared to decentralized management approaches [9]. The federated approach allows for consistent policy definition while accommodating provider-specific implementation details. This strategy typically involves a central management console that pushes configurations to cloud-specific connectors or agents that adapt policies to local environments, with Kesavan's research showing that 93% of successful implementations utilize automated synchronization mechanisms to maintain configuration consistency [9].

Progressive Implementation Methodology and Hybrid Orchestration Model

Rather than attempting full SASE implementation across all cloud environments simultaneously, the progressive approach advocates for methodical deployment beginning with critical applications or specific security functions. Organizations following progressive implementation methodologies report 43% higher success rates and 57% lower budget overruns compared to "big bang" approaches, according to Islam's implementation case studies [10]. The hybrid orchestration model recognizes that complete standardization across cloud providers may be impractical. Islam's economic analysis demonstrates that organizations utilizing hybrid orchestration models reduce integration costs by 47% while maintaining 92% of the security benefits of fully standardized approaches, creating an optimal balance between security consistency and implementation efficiency [10].

Table 2: SASE Framework Effectiveness Comparison [9,10]

Metric	Percentage (%)
Policy inconsistency reduction with abstraction layers	67
Configuration time reduction	73
Security incident reduction with service mesh	58
Threat detection improvement	41
Operational overhead reduction (federated control plane)	62
Policy consistency improvement	76
Success rate improvement with progressive methodology	43
Integration cost reduction with hybrid orchestration	47

CONCLUSION

Mixing SASE frameworks with multi-cloud setups creates both exciting possibilities and massive headaches for companies pushing through digital transformation. When networking and security features blend, remote workers and distributed applications get unprecedented flexibility and protection, but making everything work smoothly across different cloud platforms isn't simple. Companies juggling AWS, Azure, Google Cloud, and maybe some private infrastructure face real challenges getting identity systems to talk to each other, routing traffic efficiently without security gaps, enforcing consistent policies across platforms that handle things differently, and pulling monitoring data together to spot problems quickly. The frameworks covered earlier – abstraction layers, security service meshes, central control planes, and step-by-step implementation – offer practical paths forward, though none are perfect. Smart companies pick and choose elements that match their specific needs, sometimes using native tools where they make sense, while insisting on consistency for critical security functions. What's becoming crystal clear is that the old ways of handling networks and security separately just don't cut it anymore. As applications scatter across multiple clouds and users connect from anywhere, the future belongs to companies that successfully blend SD-WAN and SASE technologies. Those who figure out this complex puzzle gain tremendous advantages – more agility to adapt quickly, stronger protection against increasingly sophisticated threats, and the ability to scale up or down without rethinking their entire security paradigm. The real challenge isn't technical specs or product features, but rather finding the right balance between standardization and flexibility across increasingly distributed and complex digital environments. Companies that get this right position themselves to handle whatever comes next in the rapidly evolving digital landscape.

REFERENCES

[1] Jaskirat Singh Chauhan, "SD-WAN: Transforming Cloud Infrastructure For The Modern Enterprise", IJRCAIT, Mar.-Apr. 2025. [Online]. Available: https://iaeme.com/MasterAdmin/Journal_uploads/IJRCAIT/VOLUME_8_ISSUE_2/IJRCAIT_08_02_006.pdf

[2] Rajesh Kotha, "Multi-Cloud Strategies for Enhanced Resilience and Flexibility", ResearchGate, 2023. [Online]. Available: https://www.researchgate.net/publication/383617187_Multi-Cloud_Strategies_for_Enhanced_Resilience_and_Flexibility

[3] Gemilang Kurniawan Soejantono et al., "Performance Evaluation of SD-WAN Deployment for XYZ Enterprise Company in Indonesia", ResearchGate, 2021. [Online]. Available: https://www.researchgate.net/publication/356825996_Performance_Evaluation_of_SD-WAN_Deployment_for_XYZ_Enterprise_Company_in_Indonesia

[4] Tanvir Kaur, "Secure Access Service Edge (SASE): Extending Network Security to Client", ResearchGate, 2024. [Online]. Available: https://www.researchgate.net/publication/382458683_Secure_Access_Service_Edge_SASE_Extending_Network_Security_to_Client

[5] Karthik Venkatesh Ratnam, "An Analysis of Multi-Cloud Implementation Strategies and their Impact on Enterprise Computing: Current Practices and Future Trends", IJCET, Jan.-Feb. 2025. [Online]. Available: https://iaeme.com/MasterAdmin/Journal_uploads/IJCET/VOLUME_16_ISSUE_1/IJCET_16_01_192.pdf

[6] Omoniyi Babatunde Johnson et al., "Designing multi-cloud architecture models for enterprise scalability and cost reduction", Open Access Research Journal of Engineering and Technology, 2024. [Online]. Available: https://oarjpublication.com/journals/oarjet//sites/default/files/OARJET-2024-0061.pdf

[7] Anthony Lawrence Paul, "Security Challenges and Solutions in Multi-Cloud Environments", ResearchGate, 2024. [Online]. Available: https://www.researchgate.net/publication/381074289_Security_Challenges_and_Solutions_in_Multi-Cloud_Environments

[8] Bhanuprakash Madupati, "Kubernetes for Multi-Cloud and Hybrid Cloud: Orchestration, Scaling, and Security Challenges", Journal of Scientific and Engineering Research, 2023. [Online]. Available: https://jsaer.com/download/vol-10-iss-6-2023/JSAER2023-10-6-290-297.pdf

[9] Namboodiri Arun Mullamangalath Kesavan, "SASE Compliance Framework: A Comprehensive Guide To Regulatory Requirements And Implementation Strategies In Distributed Networks", IJRCAIT, 2024. [Online]. Available: https://iaeme.com/MasterAdmin/Journal_uploads/IJRCAIT/VOLUME_7_ISSUE_2/IJRCAIT_07_02_106.pdf

[10] Md. Rashed Islam, "Secure Multi-Cloud Architectures: Best Practices for Data Protection", ResearchGate, 2024. [Online]. Available: https://www.researchgate.net/publication/387077033_Secure_Multi-Cloud_Architectures_Best_Practices_for_Data_Protection