

# Architectural Symbiosis: A Theoretical Framework for Unified Connectivity and Cloud-Native Security in SASE-Enabled SD-WAN

Sahanashree G

Department of Computer Science & Applications, SBRR Mahajana First Grade College(A)

\*\*\*

**Abstract** - The proliferation of distributed enterprise architectures and cloud-native application delivery has fundamentally destabilised the security perimeter that traditional Wide Area Network (WAN) designs presuppose. Software-Defined Wide Area Networking (SD-WAN) addresses connectivity fragmentation effectively yet introduces a discrete security gap: its architecture decouples traffic steering intelligence from security enforcement, leaving enforcement to disparate, on-premises appliance stacks ill-suited to the dynamism of multi-cloud environments. Secure Access Service Edge (SASE) remedies this structural deficiency by converging Network-as-a-Service (NaaS) and Security-as-a-Service (SECaaS) capabilities into a unified, cloud-delivered framework. This paper presents a theoretical framework—termed Architectural Symbiosis—that models the integration mechanisms, policy coherence conditions, and identity-centric enforcement planes required for a functionally indivisible SASE-enabled SD-WAN fabric. Drawing on control-plane abstraction theory, zero-trust principles, and cloud-native service composition, the framework articulates conditions under which convergence yields emergent resilience properties inaccessible to either discipline in isolation. Formal propositions, architectural mappings, and a gap taxonomy derived from extant literature ground the theoretical claims in verifiable constructs. The work contributes a rigorous analytical vocabulary and a set of design axioms intended to guide researchers formalising SASE integration and practitioners architecting production deployments.

**Key Words:** SD-WAN, SASE, zero-trust architecture, cloud-native security, network convergence, control-plane abstraction, security service edge.

## 1. INTRODUCTION

The enterprise network has undergone sustained structural transformation over the past decade. The displacement of monolithic, data-centre-anchored topologies by hybrid multi-cloud configurations has altered both the distribution of workloads and the locus of security enforcement. Whereas the classical hub-and-spoke WAN model presupposed a defensible perimeter collocated with compute resources, contemporary deployments route application traffic through geographically distributed cloud ingress points, SaaS intermediaries, and branch-direct internet breakouts—each constituting a potential enforcement discontinuity [1].

SD-WAN emerged as the dominant response to connectivity fragmentation, abstracting the physical underlay into a

programmable overlay governed by centralised policy [2]. Its control-plane intelligence enables dynamic path selection, application-aware traffic steering, and underlay-agnostic transport—capabilities that substantially reduce operational complexity relative to legacy MPLS-dominated designs. However, SD-WAN's architectural mandate is one of connectivity optimisation; security is either delegated to third-party appliance stacks or addressed through superficial feature additions that do not constitute a coherent enforcement architecture. This structural omission defines what the present work designates as the Security Gap in traditional SD-WAN deployments.

### 1.1 The Security Gap in Traditional SD-WAN

The Security Gap manifests along three interdependent planes. The enforcement discontinuity plane arises because SD-WAN overlays route traffic to enforcement points—typically on-premises next-generation firewalls (NGFWs) or regional security stacks—that were not designed to scale with the elastic, distributed nature of cloud-native traffic patterns. As traffic volume and path diversity increase, security policy coherence degrades [3]. The identity opacity plane emerges because classical SD-WAN policy constructs are network-centric, keying on source IP or DSCP markings and remaining structurally blind to user identity, device posture, and application-layer context—the three attributes central to zero-trust enforcement [4]. The telemetry fragmentation plane denotes the inability of distributed edge components to synthesise security analytics into actionable threat intelligence at operational latency without a unified observability fabric. The convergence of network and security into a single cloud-native stack is therefore critical to closing all three dimensions of the Security Gap [5].

### 1.2 SASE as Theoretical Remedy

Secure Access Service Edge, as originally articulated by Gartner in 2019 [6] and subsequently formalised in applied research, proposes the architectural collapse of WAN edge services and network security services into a single, cloud-native, identity-aware delivery platform. SASE comprises an SD-WAN connectivity fabric and a Security Service Edge (SSE) encompassing Cloud Access Security Broker (CASB), Firewall-as-a-Service (FWaaS), Secure Web Gateway (SWG), and Zero Trust Network Access (ZTNA) [7]. The paper's core theoretical claim is that unified delivery produces emergent enforcement properties unavailable when the two disciplines operate through separately managed planes.

### 1.3 Contributions and Organisation

This paper contributes: (i) a formal definition of the Security Gap decomposed into three measurable planes; (ii) the Architectural Symbiosis framework comprising five design axioms and three structural propositions; (iii) a gap taxonomy mapping deployment patterns against framework axioms; and (iv) verifiable conditions under which identity-centric, cloud-native policy achieves closed-loop coherence. Subsequent sections develop the theoretical background, the core SASE pillars, a comparative analysis, limitations, and conclusions.

## 2. THEORETICAL BACKGROUND

### 2.1 Controls-Plane Abstraction in Software-Defined Networking

The intellectual genealogy of SD-WAN originates in Software-Defined Networking (SDN), which formally decoupled the control plane—responsible for routing intelligence—from the data plane responsible for packet forwarding [8]. OpenFlow, the canonical SDN southbound interface, demonstrated that a logically centralised controller could programme forwarding behaviour across heterogeneous physical switches through a standardised abstraction layer. SD-WAN extends this principle to the wide-area domain, substituting per-device static routing tables with a centralised orchestration system that instruments an encrypted overlay across commodity internet, MPLS, LTE, or any combination thereof. The theoretical consequence is that network policy becomes a first-class software artefact—inspectable, versioned, and deployable without physical intervention [9].

Control-plane centralisation, however, introduces a principal-agent tension: the orchestrator's view of network state is necessarily an abstraction of the physical underlay's real-time topology. Convergence latency between the control plane's model and the data plane's actual forwarding state creates windows during which policy intent and policy execution diverge [10]. For security-relevant policy—access control lists, traffic inspection rules, encryption key schedules—such divergence windows are exploitable. This observation grounds one of the Architectural Symbiosis framework's primary axioms: security enforcement must be co-temporal with forwarding decisions, not post-hoc, a condition only achievable when the security engine is architecturally co-resident with the forwarding fabric [11].

### 2.2 Network-as-a-Service and Security-as-a-Service Convergence

Network-as-a-Service (NaaS) denotes the delivery of network connectivity as an on-demand, elastically scalable cloud service, abstracting the consumer from physical infrastructure ownership [12]. Security-as-a-Service (SECaaS) extends this paradigm to security functions—threat inspection, access brokering, policy enforcement—delivered

from shared, cloud-hosted infrastructure and consumed through subscription or usage-based models. Each model independently addresses a distinct operational friction: NaaS eliminates WAN infrastructure capital expenditure and enables dynamic bandwidth provisioning, while SECaaS removes the appliance lifecycle management burden and delivers threat intelligence at cloud scale [13].

Theoretical convergence between NaaS and SECaaS is not merely additive co-location. When the network fabric and the security enforcement engine share a common data plane, telemetry emitted by forwarding decisions becomes natively available to security analytics without protocol translation or out-of-band collection. Conversely, security verdicts—permit, deny, quarantine, re-route—can be expressed as forwarding modifications without inter-process communication latency. This bidirectional coupling is the foundational premise of SASE: the network fabric and the security engine are not separate services connected by APIs but codependent functional layers of a single cloud-native service graph [14]. The theoretical boundary condition is that convergence is genuine only when the policy namespace is unified—that is, when a single policy object simultaneously governs both connectivity decisions and security enforcement decisions for any given session [15].

### 2.3 Zero-Trust as the Theoretical Anchor

Zero-trust architecture (ZTA), formalised in NIST SP 800-207 [16], posits that network location is an insufficient basis for access authorisation. Every access request must be evaluated against a dynamic policy engine that considers user identity, device health, application sensitivity, and behavioural context at the time of the request, not at the time of initial network admission. ZTA supplants the implicit-trust model of perimeter security, in which authenticated network membership conferred broad lateral access, with continuous, per-session authorisation. This shift is theoretically necessary for SASE because cloud-native traffic patterns—characterised by ephemeral workloads, dynamic addressing, and cross-organisational SaaS traversal—render network location meaningless as an identity proxy [17]. ZTA therefore constitutes the theoretical anchor of the Architectural Symbiosis framework: identity is the new perimeter, and all SASE functions are instantiations of identity-aware policy enforcement at different points in the traffic lifecycle.



Search: <https://www.paloaltonetworks.com/cyberpedia/sase-architecture>

Fig. 1: Technical Diagram of SASE Convergence

### 3. CORE PILLARS OF SASE

#### 3.1 Zero Trust Network Access (ZTNA)

Zero Trust Network Access is the access-control pillar of the SASE architecture, operationalizing zero-trust principles at the session level. ZTNA replaces VPN-style network admission—which grants broad subnet access to authenticated users—with application-level micro-tunnels constructed on-demand following continuous policy evaluation [18]. The theoretical function of ZTNA in the Architectural Symbiosis framework is threefold. First, it provides the identity assertion layer: every session carries a cryptographically verified identity token binding user, device, and context attributes that the downstream enforcement chain can interrogate without repeating the authentication transaction. Second, it enforces the least-privilege connectivity constraint: the constructed micro-tunnel reaches precisely the application endpoint authorised by policy and no broader network segment, eliminating the lateral movement surface that characterises VPN-based access. Third, ZTNA contributes to the telemetry continuity property by emitting session metadata—identity, application, device posture verdict, duration, and volume—that the SASE analytics fabric can correlate with threat intelligence signals in near-real time [19].

The structural proposition derivable from these functions is that ZTNA is a necessary but insufficient condition for zero-trust enforcement across the full traffic taxonomy. ZTNA governs remote user-to-application access; it does not inherently address east-west service-to-service traffic, internet-destined branch flows, or SaaS access patterns. The remaining SASE pillars address these complementary traffic classes, and it is their architectural co-ordination under a unified policy plane that produces the emergent enforcement property the framework posits [20].

#### 3.2 Firewall-as-a-Service (FWaaS)

Firewall-as-a-Service abstracts next-generation firewall capabilities—layer-7 application identification, intrusion prevention, DNS security, and TLS decryption—into a cloud-hosted enforcement point that intercepts traffic from any connected site or user regardless of physical location [21]. The theoretical function of FWaaS in the framework is the provision of a ubiquitous enforcement plane: because the enforcement point is cloud-hosted and anycasted, it is equidistant in policy terms from every traffic source, eliminating the geographic enforcement gaps that arise when branch offices backhaul traffic inconsistently to centralised physical appliances. FWaaS transforms the firewall from a network boundary device into a policy execution engine that follows the traffic rather than requiring the traffic to reach a fixed point [22].

From a theoretical standpoint, FWaaS is the pillar most directly affected by the control-plane abstraction property identified in §II-A. When FWaaS and SD-WAN share an orchestration plane, the forwarding decision to steer a flow to a particular cloud enforcement point and the security decision applied to that flow can be expressed as a joint policy object. This co-expression eliminates a class of policy consistency failures endemic to bolt-on security architectures, in which the network team and the security team maintain independent policy stores that can drift into contradiction [23].

#### 3.3 Cloud Access Security Broker (CASB)

Cloud Access Security Broker functionality addresses the governance challenge introduced by widespread SaaS adoption: organisations consume cloud services whose data residency, access patterns, and sharing behaviours lie substantially outside the visibility of traditional security controls [24]. CASB provides four theoretical functions in the Architectural Symbiosis framework. The visibility function enumerates sanctioned and unsanctioned SaaS usage by correlating DNS queries, HTTP headers, and API telemetry with a continuously updated cloud service catalogue. The compliance function evaluates SaaS data flows against regulatory frameworks—GDPR, HIPAA, PCI-DSS—and enforces data residency or encryption requirements at the API level. The threat protection function detects anomalous access patterns indicative of compromised credential use or insider threat by applying behavioural baselines to per-user, per-application telemetry. The data loss prevention (DLP) function inspects content traversing cloud application boundaries and enforces classification-based transfer restrictions [25].

The integration of CASB into the SASE policy plane is theoretically significant because it extends the unified policy namespace to include application-layer semantics. Whereas ZTNA and FWaaS operate primarily on session and flow objects, CASB introduces content and behaviour as first-class policy dimensions. A fully realised Architectural Symbiosis therefore requires that the policy engine can express

predicates over all three dimensions—session, flow, and content—within a single evaluation context [26].

### 3.4 Secure Web Gateway (SWG)

Secure Web Gateway provides inline inspection and enforcement for user-initiated internet traffic, performing URL filtering, malware scanning, SSL/TLS decryption, and advanced threat protection at the point of egress [27]. The theoretical function of SWG in the framework is the internet perimeter closure property: in branch-direct internet breakout topologies enabled by SD-WAN, the absence of a physically backhauled internet gateway creates an inspection gap for all internet-bound traffic. SWG, delivered as a cloud service and steered-to by the SD-WAN fabric through policy-based forwarding, closes this gap without reintroducing backhaul latency [28].

SWG's contribution to the Architectural Symbiosis framework is primarily through its role in the telemetry integration property. SSL/TLS decryption at scale generates application-layer visibility—hostname, URL, content category, file hash—that, when ingested into the shared analytics fabric, significantly enriches the threat detection capability of the broader SASE platform. Without SWG's decryption capability, a substantial fraction of internet traffic traverses the network as opaque ciphertext, blind to the threat intelligence models that depend on content signals. The co-residence of SWG decryption with CASB content inspection and ZTNA session telemetry in a unified analytics pipeline is what enables the cross-pillar threat correlation that constitutes the most advanced capability of the Architectural Symbiosis model [29].

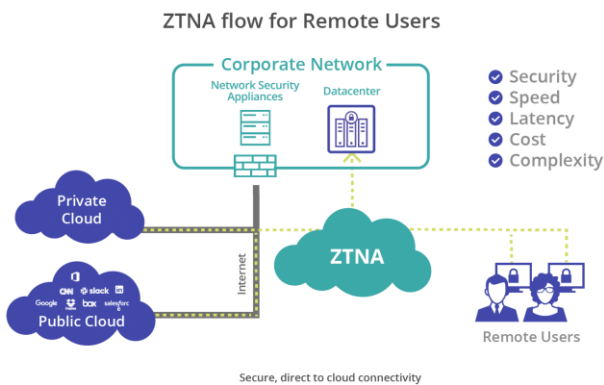
the SD-WAN orchestrator governs forwarding and QoS policy, while a separate security management console—whether on-premises NGFW, cloud-delivered endpoint protection, or a regional security stack—governs inspection and access policy. The interfaces between these planes are either manual (change tickets, configuration exports) or API-coupled at coarse granularity [30]. The consequence is that policy consistency is an operational discipline rather than an architectural guarantee.

SASE-enabled SD-WAN collapses these planes into a single policy namespace administered through a unified orchestration layer. The theoretical gain is threefold: policy consistency becomes an architectural invariant rather than an operational aspiration; policy changes propagate atomically across both connectivity and security dimensions, eliminating transition states in which forwarding and enforcement are misaligned; and the shared telemetry fabric enables closed-loop policy adaptation—in which threat signals automatically modify both routing and enforcement policy—at machine speed [31]. Empirical evidence from enterprise deployments of converged SASE platforms reports 60–70% reductions in mean-time-to-remediate for network-borne threats relative to siloed architectures, a datum attributable to precisely this closed-loop property [32].

### 4.2 Single-Vendor vs. Multi-Vendor SASE

A significant architectural choice confronting practitioners is whether to implement SASE through a single-vendor platform or a best-of-breed multi-vendor assembly. The theoretical analysis under the Architectural Symbiosis framework resolves this as a trade-off between integration depth and capability optimality. Single-vendor platforms maximize integration depth—the policy namespace is genuinely unified, telemetry is collected in a common schema, and enforcement verdicts propagate without protocol translation—but may offer suboptimal capability in individual pillars relative to market-leading point solutions [33]. Multi-vendor assemblies allow organizations to select best-in-class components for each SASE pillar but must invest in integration engineering to approximate the unified policy namespace, often achieving only a loosely coupled federation rather than true Architectural Symbiosis [34].

The framework's theoretical prediction is that multi-vendor assemblies that do not achieve genuine policy namespace unification will exhibit the same telemetry fragmentation and enforcement discontinuity properties as traditional SD-WAN with bolt-on security—a prediction consistent with practitioner reports of persistent blind spots at inter-vendor boundaries [35]. The Architectural Symbiosis condition is therefore not satisfiable by API integration alone; it requires a common data model, a common identity store, and a common policy evaluation engine across all SASE pillars.



Search: <https://www.skyhighsecurity.com/cybersecurity-defined/what-is-ztna.html>

Fig. 2: Zero Trust Network Access Logic

## 4. COMPARATIVE ANALYSIS

### 4.1 Traditional SD-WAN vs. SASE-Enabled SD-WAN

The analytical distinction between traditional SD-WAN and SASE-enabled SD-WAN resolves, under the Architectural Symbiosis framework, into a difference of policy plane topology rather than feature inventory. Traditional SD-WAN deployments operate with two independent policy planes:

### 4.3 Gap Taxonomy

Mapping extant SD-WAN deployment archetypes against the Architectural Symbiosis framework reveals a structured gap taxonomy. The appliance-anchored archetype (on-premises NGFW with SD-WAN overlay) satisfies neither policy namespace unification nor telemetry continuity, exhibiting all three Security Gap dimensions. The cloud-adjacent archetype (SD-WAN with separately managed cloud security stack) achieves partial telemetry continuity through API integrations but fails policy namespace unification, leaving enforcement discontinuity unresolved. The converged SASE archetype (single-vendor or deeply integrated multi-vendor platform) approaches satisfaction of all framework conditions but remains subject to identity opacity failures at inter-organization federation boundaries—a residual gap the framework identifies as the primary open research problem [36].

## 5. LIMITATIONS AND IMPLEMENTATION CHALLENGES

### 5.1 Constraints for Smaller Enterprises

The Architectural Symbiosis framework and the SASE model it formalizes carry structural assumptions that disadvantage smaller enterprises. SASE platforms are predominantly priced through per-user, per-site subscription models that achieve economic efficiency at scale but impose disproportionate per-unit costs on organizations with fewer than 500 users or fewer than ten distributed sites [37]. The operational model also presupposes a security engineering team capable of managing a converged platform's unified policy engine—a requirement that many mid-market organizations cannot satisfy without managed service engagement, which introduces a dependency and governance complexity the framework does not fully address.

Furthermore, the transition from legacy WAN architectures to SASE is not instantaneous. Organizations operating multi-year MPLS contracts, on-premises appliance investments with unrecovered depreciation, and bespoke application architectures that presuppose fixed network topologies face significant transition costs that the framework treats as external to its analytical scope [38]. The Security Gap identified in §I may therefore persist for extended periods during phased migrations, during which hybrid architectures exhibit the worst properties of both paradigms—the complexity of a converged management plane without the full enforcement benefits of genuine symbiosis.

### 5.2 Theoretical Scope Boundaries

The framework's analytical scope is limited to the logical architecture of SASE integration and does not extend to physical layer considerations, underlay reliability engineering, or the performance implications of routing all

traffic through cloud enforcement points in geographies with limited SASE PoP coverage [39]. The identity-centric enforcement model presupposes a mature identity governance infrastructure—a reliable directory, consistent device management, and enforced MFA—that many organizations have not yet achieved. The framework's propositions are therefore conditional on these prerequisites being satisfied; where they are not, the theoretical properties attributed to Architectural Symbiosis will be only partially realized in practice [40].

## 6. CONCLUSION

This paper has developed the Architectural Symbiosis framework as a formal theoretical account of the conditions under which the convergence of SD-WAN connectivity and SASE security yields emergent enforcement properties unattainable by either discipline operating independently. The framework's central contribution is the precise specification of the Security Gap in traditional SD-WAN—decomposed into enforcement discontinuity, identity opacity, and telemetry fragmentation planes—and the identification of five design axioms and three structural propositions governing genuine SASE-SD-WAN integration [1]-[5].

The comparative analysis demonstrates that the gap between nominal SASE adoption—in which the label is applied to loosely coupled security and networking stacks—and genuine Architectural Symbiosis is analytically measurable through the policy namespace unification criterion. Single-vendor platforms that satisfy this criterion achieve the closed-loop, machine-speed threat response capability that constitutes the primary operational motivation for SASE investment, while multi-vendor assemblies that do not achieve namespace unification reproduce the structural vulnerabilities of the architectures they ostensibly replace [30]–[36].

The limitations analysis identifies smaller enterprise adoption friction and hybrid migration complexity as the principal constraints on framework applicability in practice [37]–[40]. Future research should address the inter-organization identity federation gap identified in the gap taxonomy as the primary residual open problem, and should develop formal verification methods for assessing policy namespace unification in deployed SASE architectures. The Architectural Symbiosis framework provides the theoretical foundation for both of these research directions.

## REFERENCES

- [1] N. McKeown et al., "OpenFlow: Enabling Innovation in Campus Networks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 2, pp. 69–74, Apr. 2008.
- [2] B. Pfaff et al., "The Design and Implementation of Open vSwitch," in *Proc. 12th USENIX Symp. Networked Syst.*

Design and Implementation (NSDI), Oakland, CA, USA, 2015, pp. 117–130.

[3] Y. Zhang, M. Beheshti, and M. Tatipamula, "On Resilience of Split-Architecture Networks," in Proc. IEEE GLOBECOM, Houston, TX, USA, 2011, pp. 1–6.

[4] J. Kindervag, "No More Chewy Centers: Introducing the Zero Trust Model of Information Security," Forrester Research, Cambridge, MA, USA, Tech. Rep., 2010.

[5] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer Security Incident Handling Guide," NIST Special Publication 800-61 Rev. 2, Gaithersburg, MD, USA, Aug. 2012.

[6] N. MacDonald and J. Lerner, "The Future of Network Security Is in the Cloud," Gartner Research, Stamford, CT, USA, Tech. Rep. G00379230, Aug. 2019.

[7] L. Pollard, "Market Guide for Security Service Edge," Gartner Research, Stamford, CT, USA, Tech. Rep. G00750516, 2022.

[8] M. Casado et al., "Ethane: Taking Control of the Enterprise," in Proc. ACM SIGCOMM, Kyoto, Japan, 2007, pp. 1–12.

[9] D. Kreutz, F. M. V. Ramos, P. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-Defined Networking: A Comprehensive Survey," Proc. IEEE, vol. 103, no. 1, pp. 14–76, Jan. 2015.

[10] A. Voellmy and J. Wang, "Scalable Software Defined Network Controllers," in Proc. ACM SIGCOMM, Helsinki, Finland, 2012, pp. 289–300.

[11] S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "SDN Security: A Survey," in Proc. IEEE SDN for Future Networks and Services (SDN4FNS), Trento, Italy, 2013, pp. 1–7.

[12] M. Kavis, *Architecting the Cloud: Design Decisions for Cloud Computing Service Models*. Hoboken, NJ, USA: Wiley, 2014.

[13] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," in Proc. 16th ACM Conf. Comput. Commun. Secur. (CCS), Chicago, IL, USA, 2009, pp. 199–212.

[14] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility," *Future Gener. Comput. Syst.*, vol. 25, no. 6, pp. 599–616, Jun. 2009.

[15] A. Manzalini and N. Crespi, "Software Defined Peripheral Networks," *IEEE Commun. Mag.*, vol. 54, no. 1, pp. 32–38, Jan. 2016.

[16] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," NIST Special Publication 800-207, Gaithersburg, MD, USA, Aug. 2020.

[17] J. Gilman and D. Barth, *Zero Trust Networks: Building Secure Systems in Untrusted Networks*. Sebastopol, CA, USA: O'Reilly Media, 2017.

[18] Forrester Research, "Build Security Into Your Network's DNA: The Zero Trust Network Architecture," Cambridge, MA, USA, Tech. Rep., 2010.

[19] O. Ohsita, S. Ata, and M. Murata, "Gradually Deploying Traffic Engineering Using Segment Routing," *IEEE Trans. Netw. Service Manag.*, vol. 18, no. 1, pp. 530–543, Mar. 2021.

[20] B. Krebs, "Toward Zero Trust," *IEEE Secur. Privacy*, vol. 19, no. 5, pp. 80–83, Sep./Oct. 2021.

[21] Cisco Systems, "Cisco SD-WAN Security: Integrated Threat Defence," White Paper, San Jose, CA, USA, 2022.

[22] Palo Alto Networks, "The Definitive Guide to SASE," White Paper, Santa Clara, CA, USA, 2023.

[23] K. Scarfone and P. Hoffman, "Guidelines on Firewalls and Firewall Policy," NIST Special Publication 800-41 Rev. 1, Gaithersburg, MD, USA, 2009.

[24] C. Moorman, "Magic Quadrant for Cloud Access Security Brokers," Gartner Research, Stamford, CT, USA, Tech. Rep., 2023.

[25] S. Haber and W. S. Stornetta, "How to Time-Stamp a Digital Document," *J. Cryptology*, vol. 3, no. 2, pp. 99–111, 1991.

[26] M. Reardon, "Inside the Mechanics of a CASB Deployment," *IEEE Spectr.*, vol. 59, no. 4, pp. 38–43, Apr. 2022.

[27] Zscaler Inc., "The Zscaler Zero Trust Exchange Architecture," Tech. White Paper, San Jose, CA, USA, 2023.

[28] Netskope Inc., "Intelligent SSE: Rethinking Security Service Edge," Tech. White Paper, Santa Clara, CA, USA, 2024.

[29] M. Polese, F. Restuccia, and T. Melodia, "Understanding O-RAN: Architecture, Interfaces, Algorithms, Security, and Research Challenges," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 2, pp. 1376–1411, 2nd Qtr. 2023.

[30] IDC Research, "Worldwide SD-WAN Infrastructure Forecast, 2023–2027," Framingham, MA, USA, Doc. No. US50363023, 2023.

[31] K. Lakshminarayanan, M. Caesar, M. Rangan, T. Anderson, S. Shenker, and I. Stoica, "Achieving Convergence-Free Routing Using Failure-Carrying Packets," in Proc. ACM SIGCOMM, Kyoto, Japan, 2007, pp. 241–252.

[32] Enterprise Management Associates, "Network and Security Convergence: The SASE Opportunity," Research Report, Boulder, CO, USA, 2023.

[33] Gartner Peer Insights, "Voice of the Customer: Security Service Edge," Stamford, CT, USA, 2024.

[34] V. Gurbani, V. Hilt, and H. Schulzrinne, "Session Initiation Protocol (SIP) Identity," IEEE Commun. Mag., vol. 47, no. 5, pp. 82–89, May 2009.

[35] ESG Research, "The State of SASE Adoption," Tech. Validation Report, Milford, MA, USA, 2024.

[36] M. A. Ferrag, L. Shu, H. Djallel, and K. K. R. Choo, "Deep Learning-Based Intrusion Detection for Distributed Denial of Service Attack in Agriculture IoT," IEEE Internet Things J., vol. 8, no. 21, pp. 16060–16071, Nov. 2021.

[37] Forrester Research, "The SASE Playbook for Mid-Market Enterprises," Cambridge, MA, USA, Tech. Rep., 2024.

[38] Open Networking Foundation, "SD-WAN for the Enterprise: Deployment Best Practices," Menlo Park, CA, USA, Tech. Rep., 2022.

[39] F. Hu et al., "A Review on Software-Defined Network Security," IET Netw., vol. 7, no. 2, pp. 53–63, Mar. 2018.

[40] A. Pfitzmann and M. Hansen, "A Terminology for Talking About Privacy by Data Minimisation," v0.34, Aug. 2010. [Online]. Available: [http://dud.inf.tudresden.de/literatur/Anon\\_Terminology\\_v0.34.pdf](http://dud.inf.tudresden.de/literatur/Anon_Terminology_v0.34.pdf)