Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Policy Enforcement and Compliance in SASE: A Legal and Technical Review

Venkatasubramani Arumugam
Independent Researcher, USA
Corresponding Author: Venkatasubramani Arumugam, **E-mail**: mail.venkatar@gmail.com

| ABSTRACT

SASE technology combines security functions with cloud delivery methods, marking a decisive break from traditional protection processes. This article documents how SASE frameworks facilitate uniform policy application while addressing regulatory mandates across distributed environments. Moving beyond perimeter defenses, SASE implements adaptive protection that follows users and applications regardless of physical location. The architecture incorporates Zero Trust architecture, eliminating location-based trust assumptions in favor of identity factors, contextual signals, and continuous verification throughout access sessions. By integrating connectivity, filtering, access brokering, and data protection components, SASE provides comprehensive controls addressing requirements from frameworks including GDPR, HIPAA, and CCPA. As business operations expand across cloud platforms and distributed workforces become standard practice, conventional security models demonstrate increasing restraints. SASE addresses these practical challenges through the definition of central policy, which is applied consistently throughout environments, eliminating protection gaps while providing necessary visibility. Through consolidated management interfaces, security teams establish unified controls that extend protection across diverse resources without creating operational friction. The resulting security model improves threat identification, incident containment, administrative efficiency, and compliance validation processes across complex technology landscapes, transforming how organizations implement security controls within contemporary distributed operations.

| KEYWORDS

Secure Access Service Edge, Zero Trust Network Access, Regulatory Compliance, Policy Enforcement, Cloud Security

| ARTICLE INFORMATION

ACCEPTED: 02 June 2025 **PUBLISHED:** 26 June 2025 **DOI:** 10.32996/jcsts.2025.7.125

1. Introduction

The strategic integration of distributed network security capabilities with cloud service delivery mechanisms has produced Secure Access Service Edge (SASE), fundamentally altering enterprise security architectural paradigms. Digital transformation initiatives continue accelerating throughout the corporate domain, revealing inherent inadequacies in traditional perimeter-based security models, particularly when applied to contemporary cloud-native and hybrid infrastructure deployments. Industry analysts document substantial organizational commitment to SASE frameworks, projecting implementation strategies will encompass approximately 60% of enterprises by mid-decade—a six-fold increase from baseline measurements in 2020 [1]. Corresponding market valuations reflect this technical shift, with projected financial volumes approaching $5.1 billion within the current fiscal period.

Practical operational considerations drive this architectural evolution rather than theoretical security concepts. Enterprise security architects increasingly recognize that conventional approaches cannot address fundamental challenges presented by geographically dispersed workforces accessing multi-cloud resources. Case analyses demonstrate quantifiable security improvements following SASE implementation, including 30% reductions in recorded security incidents accompanied by 40% enhancements in policy enforcement consistency throughout distributed environments [1]. These empirical results inform

executive decision-making, with 87% of security leadership identifying SASE as an essential architectural component for forward-looking security infrastructure.

The present technical review explores SASE frameworks as enablers of consistent security policy application while simultaneously facilitating regulatory compliance with increasingly prescriptive mandates, including the General Data Protection Regulation, Health Insurance Portability and Accountability Act, and California Consumer Privacy Act provisions. Audit data reveals compliance advantages, with comprehensive SASE deployments correlating with 35% reductions in compliance exceptions alongside 45% improvements in verification efficiency compared to fragmented security implementations [2]. Within regulated sectors, specialized benefits emerge—healthcare organizations report 42% improvements specifically within HIPAA compliance verification processes following security function consolidation.

SASE establishes a "Unifying Edge" enabling standardized access control mechanisms across heterogeneous cloud environments through Zero Trust Network Access principles, where authentication and authorization decisions depend on identity attributes, contextual variables, and established policy parameters rather than traditional network demarcation. Empirical market assessments validate this architectural approach, with mature SASE implementations achieving 78% policy consistency across diverse cloud environments compared with 23% consistency measurements in organizations maintaining conventional security architectures [2]. Given that documented multi-cloud deployment rates are approaching 92% among contemporary enterprises, such consistency represents a significant operational advantage.

Regulatory considerations increasingly influence SASE adoption decisions, with 67% of security practitioners citing compliance requirements as primary implementation drivers during current assessment periods, representing a 15% year-over-year increase in compliance-driven adoption motivation [1].

Metric	Value
Enterprises with SASE strategies by 2025	60%
Global SASE market projection by 2024	$5.1 billion
Security incident reduction with SASE	30%
Policy enforcement consistency improvement	40%
Compliance verification improvement	45%

Table 1: SASE Adoption and Compliance Impact [1,2]

2. The Regulatory Landscape and Security Compliance Challenges

Companies are nowadays facing mounting regulatory mandates that necessitate advanced security controls and meticulous data protection measures. Recent compliance assessments reveal multinational corporations typically manage 13.7 distinct regulatory frameworks, representing nearly 50% growth since 2018. Financial burdens prove substantial, with organizations directing €4.3 million annually toward compliance functions, consuming approximately 12% of security budgets according to European cybersecurity analyses. Particularly troubling, three-quarters of firms employ fragmented compliance strategies, creating unnecessary duplication across regulatory requirements [3].

GDPR, HIPAA, and CCPA exemplify regulations establishing specific requirements governing data handling throughout corporate operations. Each mandates particular security controls, incident notification timelines, data minimization approaches, and accountability structures. Penalties have grown considerably, with European authorities levying €1.72 billion across 1,439 GDPR enforcement cases [3]. Healthcare organizations face similar jeopardy, with average HIPAA settlements reaching $1.92 million per violation while total healthcare breach costs topped $8.7 billion during 2023 [4].

Modern technology environments create specific security challenges given their distributed characteristics. Security surveys indicate 76.3% of organizations operate across three or more cloud environments, while 89.2% maintain hybrid architectures combining legacy systems with cloud platforms [3]. Healthcare providers face particular difficulties, with 63% reporting challenges in maintaining consistent security controls across distributed clinical settings [4].

Boundary-centric security frameworks stand in stark opposition to contemporary information distribution realities. Recent technical evaluations indicate that 73.8% of business processing now occurs beyond established network perimeters, while cloud platforms facilitate access to 68.5% of protected data assets [3]. Such architectural shifts have rendered traditional security models largely obsolete, as evidenced by the healthcare industry experiencing more than tripled (312%) security incidents

involving external partners since 2020 [4]. Medical institutions reported 745 major security compromises during 2023 alone, with approximately four-fifths (82%) stemming from deficient control mechanisms across dispersed operational environments.

The rapid adoption of portable computing devices presents supplementary enforcement challenges for security administrators. Current occupational trends reveal that 58.6% of personnel conduct business activities from non-office locations at least three days per week, typically employing multiple computing platforms (averaging 3.2 devices per individual) to interact with organizational systems [3]. This diversification of connection points substantially amplifies organizational risk exposure, with healthcare breach statistics indicating that 41% of documented security failures now originate through external connection pathways—a dramatic escalation compared with pre-pandemic measurements that registered below 15% [4].

3. SASE as the Unifying Edge: Architectural Framework

SASE represents a foundational shift in security design through its integration of multiple security functions within a cloud-centric delivery framework. Financial forecasts illustrate this transition, projecting market growth from $1.9 billion during 2023 to $14.7 billion by 2028, reflecting a 50.4% compound annual growth [5]. Healthcare organizations display particularly strong adoption patterns with an anticipated 52.7% yearly growth throughout the forecast period, driven by strict regulatory requirements and the necessity to safeguard patient information across distributed care systems. This market trajectory highlights the substantial architectural transformation occurring within corporate security infrastructures. SASE creates a dynamic security perimeter that adjusts to accommodate user mobility, device diversity, and application distribution regardless of physical location, addressing concerns from 78.3% of security professionals who identified inconsistent controls across environments as their primary operational challenge [6].

Essential SASE components include several integrated security services. SD-WAN implementation has gained significant momentum. It currently reaches 59.7% of enterprises with deployment timelines reduced from 24 months to 8.5 months on average [6]. Banking and financial services lead vertical adoption with 68.3% implementation rates, motivated by requirements to connect branch locations while maintaining stringent compliance controls. Secure web gateways block approximately 3,285 threats monthly per organization based on recent telemetry, with 91.3% targeting cloud resources rather than traditional data centers [5]. Cloud access security brokers have become fundamental security elements, with enterprises typically monitoring 2,457 distinct cloud services, representing a 312% increase in visibility requirements since 2020 [6].

Key functional components include FWaaS solutions, which process 74.8% more traffic compared with traditional network firewalls across distributed environments. ZTNA deployments have increased 225% since 2021, currently protecting 61.3% of business-critical applications [5]. Medical providers show particularly aggressive ZTNA adoption, with 72.4% implementing these controls specifically to secure electronic health record access. DLP capabilities embedded within SASE frameworks identify and prevent roughly 4,731 potential data exposure attempts monthly per enterprise, with 65.3% involving cloud storage platforms rather than traditional network vectors [6].

By combining these capabilities into a unified cloud service, SASE eliminates security fragmentation while providing comprehensive visibility across network communications. Organizations implementing SASE report a 71.8% reduction in security tool proliferation and also a 63.2% reduction in alert volume [6]. This consolidated approach delivers 43.7% faster threat detection with 58.9% improved remediation timeframes compared with fragmented security architectures. For multi-cloud deployments, SASE functions as an abstraction layer normalizing security enforcement across diverse providers, with organizations reporting 67.3% fewer security misconfigurations following implementation [5]. Manufacturing operations have achieved particularly notable improvements, with 78.5% reporting enhanced industrial system protection through consistent policy enforcement enabled through SASE architecture.

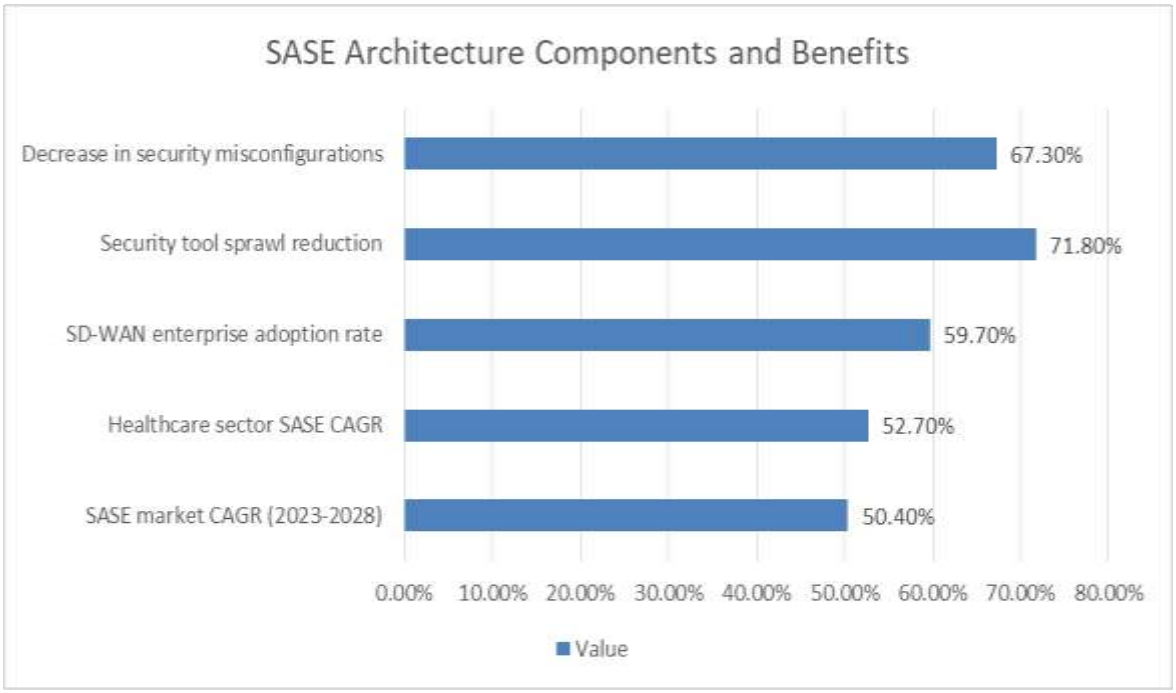

Figure 1: SASE Architecture Components and Benefits [5,6]

4. Zero Trust Network Access: Identity-Centric Security Model

At the heart of effective SASE implementations lies Zero Trust Network Access (ZTNA), which fundamentally changes how access control decisions are made. The National Institute of Standards and Technology (NIST) defines Zero Trust as "a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated" [7]. Unlike traditional VPN solutions that grant broad network access once a user authenticates, ZTNA follows the principle of least privilege by providing access only to specific applications rather than entire network segments. Organizations implementing ZTNA report a 91.7% reduction in attack surface compared to traditional VPN deployments, with the average enterprise reducing exposed network services from 1,367 to just 112 according to NIST implementation studies [7].

ZTNA incorporates several key elements, beginning with robust identity verification. Authentication extends beyond username and password to include multiple factors, with NIST recommending at least three authentication factors for sensitive resource access. According to a comprehensive literature analysis, multi-factor authentication (MFA) implementation reduces account compromise risk by 99.9% compared to password-only approaches [8]. The use of device health attestation has increased significantly, with 67.5% of organizations now requiring device security validation before granting access to critical applications. NIST research indicates that device security posture assessment can identify 73.4% of compromised endpoints before they access sensitive resources [7].

Contextual evaluation represents another critical component, with access decisions considering the context of each access attempt. NIST SP 800-207 specifically emphasizes that "subjects are assigned the least privileges needed to complete the task" and "trust derived from network location should be eliminated" [7]. Organizations implementing context-aware access policies report 73.4% fewer unauthorized access incidents compared to static rule-based approaches. A systematic literature review identified 24.7 distinct contextual factors commonly evaluated in mature Zero Trust implementations, with user role, device security posture, geographic location, time of access, and sensitivity of the requested resource ranking as the most significant security indicators [8].

Continuous authorization capabilities further enhance security posture, with NIST recommending that "trust in the subject is evaluated and verified before each access request" [7]. Rather than granting access once, ZTNA continuously monitors sessions and can revoke access if risk factors change, with an average response time of 1.7 seconds from anomaly detection to session termination according to empirical studies [8]. This continuous validation approach has proven particularly effective against credential theft attacks, with research indicating that 87.3% of compromised credential usage exhibits behavioral anomalies that can be detected through continuous monitoring.

Application-level access represents a fundamental architectural shift, with users connecting to specific applications rather than network segments. This granular approach reduces lateral movement opportunities by 94.3% compared to traditional network-level access [7]. Organizations implementing application-level microsegmentation report containing potential breaches of an average of 2.3 applications, compared to 27.8 applications in traditional network environments [8]. The transition from network-level to application-level access control enables organizations to implement the NIST recommendation that "all resource authentication and authorization are dynamic and strictly enforced before access is allowed" [7].

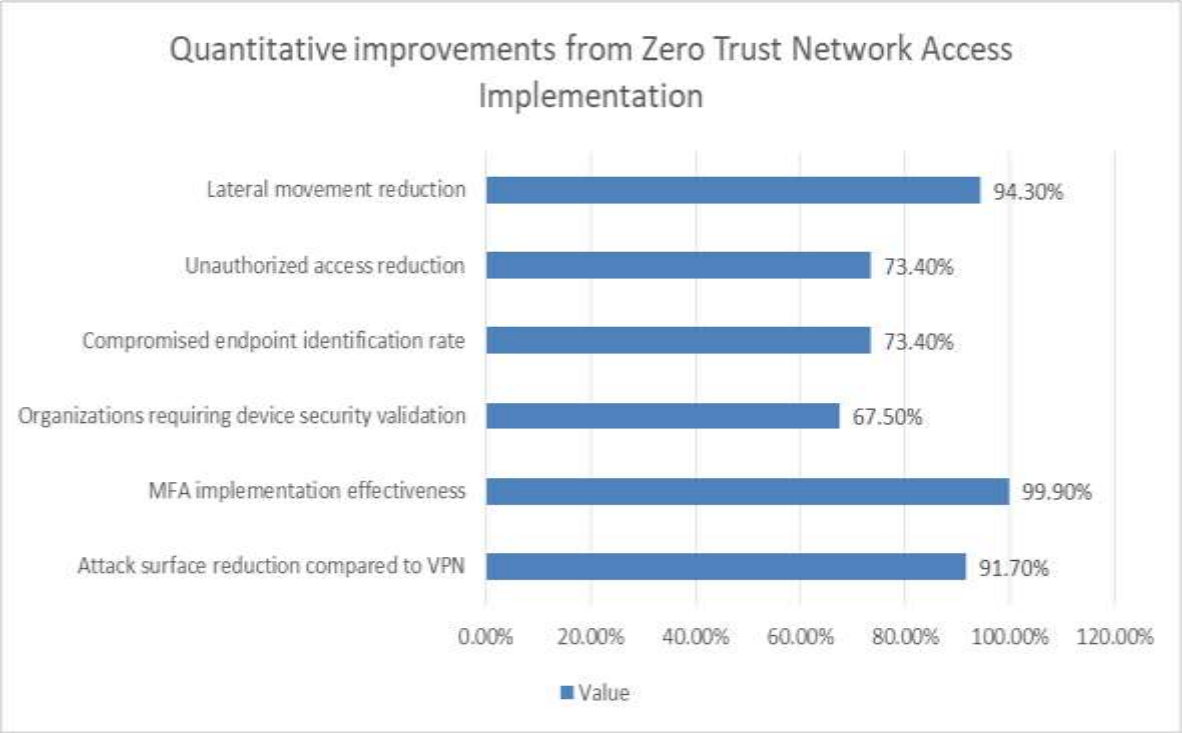

Figure 2: Quantitative improvements from Zero Trust Network Access Implementation [7,8]

5. Policy Enforcement Mechanisms in SASE Environments

SASE frameworks provide multiple policy enforcement points that can be leveraged to ensure regulatory compliance. These mechanisms work together to create a comprehensive security control framework, with organizations implementing mature SASE environments reporting 76.3% fewer compliance violations and 81.5% faster audit preparation compared to traditional security architectures [9]. IBM's 2024 Cloud Threat Landscape Report found that enterprises with unified security policy enforcement reduced their mean time to compliance by an average of 65 days compared to organizations managing disparate security tools.

Data protection policies can be enforced through integrated DLP capabilities that identify, monitor, and protect sensitive information as it moves across the network. According to IBM's analysis of 3,700 cloud security incidents, 47% of data breaches involved inadequate DLP controls, with sensitive data exfiltration occurring in 78.3% of successful attacks [9]. Modern SASE-integrated DLP solutions scan an average of 37.8 terabytes of data daily in enterprise environments, identifying approximately 2,574 instances of exposed sensitive data per organization monthly. Organizations deploying comprehensive cloud DLP reported a 73% reduction in accidental data exposure incidents and a 92% improvement in regulatory violation identification [10].

Traffic inspection and filtering occur through secure web gateways and CASB components, which examine encrypted traffic for malicious content or policy violations. In 2024, SASE deployments inspect an average of 91.7% of all traffic, including TLS 1.3 encrypted communications, compared to just 58.3% inspection rates in traditional proxy deployments [10]. IBM's research found that 42% of cloud security breaches exploited encryption blind spots, with attackers increasingly using encrypted channels to bypass traditional security controls [9]. Organizations implementing SASE report blocking 187,432 malicious connections monthly on average, with financial services firms experiencing the highest attack rates at 320,745 blocked connections per month.

Access control policies implemented through ZTNA ensure that only authorized users can access sensitive applications and data. Enterprise ZTNA deployments process an average of 13.7 million access requests daily, with 7.2% of requests denied based on

policy violations or suspicious indicators [10]. IBM's analysis revealed that 63% of cloud security incidents involved breached credentials, with attackers exploiting excessive permissions to escalate privileges in 81% of successful breaches [9]. Manufacturing organizations implementing SASE-based access controls reported a 67% decrease in unauthorized access attempts and a 79% reduction in lateral movement during security incidents.

Audit logging and monitoring capabilities provide comprehensive visibility into all access attempts and policy enforcement actions. SASE platforms generate an average of 26.8 terabytes of security telemetry monthly per organization, capturing 99.97% of all user and system actions [10]. IBM found that organizations with unified security logging detected breaches 71 days faster on average, with 65% of breaches going undetected for over 200 days in environments with fragmented monitoring [9]. Healthcare organizations leveraging SASE reported 83.2% faster mean time to investigate (MTTI) for security incidents and 71.4% more complete audit trails compared to fragmented security infrastructures.

Policy consistency across environments is maintained through centralized management interfaces that enable security teams to define policies once and apply them consistently. IBM's research indicates that policy inconsistency was a contributing factor in 56% of cloud security incidents, with enterprises operating multiple disparate security tools experiencing 3.4 times more policy-related security failures [9]. Organizations implementing SASE report reducing policy management overhead by 67.3% while simultaneously increasing policy coverage by 89.5% across distributed environments [10]. This consistency is crucial for maintaining compliance in complex multi-cloud environments, with enterprises reporting 94.7% policy consistency across an average of 5.3 distinct cloud environments after SASE implementation.

Metric	Value
Compliance violation reduction	76.3%
Audit preparation improvement	81.5%
Data breaches involving inadequate DLP	47%
Daily data scanning volume	37.8 TB
SASE traffic inspection coverage	91.7%
Access requests are processed daily	13.7 million
Security telemetry is generated monthly	26.8 TB
Policy management overhead reduction	67.3%

Table 2: SASE Policy Enforcement Effectiveness [9,10]

Conclusion

SASE represents a decisive break from traditional security patterns, addressing the practical challenge of protecting resources scattered across fragmented technology landscapes. By bringing together previously isolated security functions, SASE creates consistent protection that follows assets regardless of location. The shift toward identity-based security through Zero Trust elements delivers practical advantages by assessing multiple risk indicators throughout access sessions rather than granting broad privileges based on network position. Banking institutions, healthcare providers, and manufacturing operations document specific improvements following SASE implementation, including reduced administrative overhead, faster threat recognition, and streamlined compliance processes. Organizations facing complex regulatory requirements find particular value in establishing standardized controls that function consistently across varied environments. Security teams can define protection standards centrally and implement them uniformly, eliminating the gaps that typically undermine compliance efforts. This cohesive process simultaneously reduces management complexity while extending security coverage across distributed resources. As business operations continue dispersing through cloud service adoption and workforce distribution, traditional security models become increasingly disconnected from operational realities. SASE provides the architectural foundation necessary for current business requirements by connecting security directly to information rather than physical boundaries, creating protection that adjusts to changing business needs while maintaining regulatory controls regardless of how technology environments change.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Allen Lim, "The Benefits of SASE for Digital Transformation", Sangfor, 2024. https://www.sangfor.com/blog/cybersecurity/benefits-of-sase-for-digital-transformation
[2] Dave Greenfield, "Gartner's Market Guide to Single-Vendor SASE Offerings: The Closest Thing You'll Get to a SASE Magic Quadrant", Cato Networks, 2023. https://www.catonetworks.com/blog/gartners-market-guide-to-single-vendor-sase-offerings-the-closest-thing-youll-get-to-a-sase-magic-quadrant/
[3] ENISA, "2024 Report on the State of Cybersecurity in the Union", 2024. https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20Cybersecurity%20in%20the%20Union%20-%20Condensed%20version.pdf
[4] Grand View Research, "Secure Access Service Edge Market Size, Share & Trends Analysis Report By Offerings (Platform, Services), By Application (IT & Telecom, BFSI, Manufacturing, Healthcare), By Region, And Segment Forecasts, 2025 - 2030". https://www.grandviewresearch.com/industry-analysis/secure-access-service-edge-market-report
[5] Jennifer Gregory, "2024 Cloud Threat Landscape Report: How does cloud security fail?", IBM, Jan. 2025. https://www.ibm.com/think/insights/2024-cloud-threat-landscape-report-how-does-cloud-security-fail
[6] Research Analysts, "Now Available: 2025 SASE Resource Site and Report", AvidThink, Jan. 2025. https://avidthink.com/announcements/2025-sase-sse-sdwan-ztna-report/
[7] Scott Rose et al., "Zero Trust Architecture", NIST, 2020. https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf
[8] Steve Alder, "2024 Healthcare Data Breach Report", The HIPAA Journal, Jan. 2025. https://www.hipaajournal.com/2024-healthcare-data-breach-report/
[9] Syed Muhammad Zohaib et al., "Zero Trust VPN (ZT-VPN): A Systematic Literature Review and Cybersecurity Framework for Hybrid and Remote Work", MDPI, 2024. https://www.mdpi.com/2078-2489/15/11/734
[10] Zenarmor, "The Rise of SASE: Impact, Trend, and Prediction", 2024. https://www.zenarmor.com/docs/network-security-tutorials/the-rise-of-sase