World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(Research Article)

Advancing National Cybersecurity Resilience: Integrating Zero Trust Architecture and Secure Access Service Edge for Protecting Critical Cloud and Network Infrastructure

Emma Junior Emmanuel *

Department of Computer Science, Roy G. Perry College of Engineering, Prairie View A&M University, Texas, United States.

World Journal of Advanced Research and Reviews, 2024, 28(01), 2148-2162

Publication history: Received on 13 September 2025; revised on 27 October 2025; accepted on 30 October 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.28.1.3596

Abstract

The increasing sophistication of cyber threats targeting national critical infrastructure underscores the urgent need for a robust, adaptive, and scalable cybersecurity framework. Traditional perimeter-based defenses have proven inadequate in the face of distributed cloud environments, remote work ecosystems, and dynamic data access patterns. This paper proposes an integrated model that combines Zero Trust Architecture (ZTA) and Secure Access Service Edge (SASE) principles to advance national cybersecurity resilience. The integration enables continuous verification, policy-driven access, and cloud-native security enforcement across users, devices, and applications, irrespective of location. Drawing from current implementations in both government and enterprise environments, the study develops a multi-layered National Cybersecurity Resilience Framework (NCRF) that aligns identity-centric control with secure edge networking. The proposed framework enhances trust decentralization, visibility, and adaptive threat response through AI-enabled analytics and unified policy orchestration. Comparative evaluation against standalone ZTA and SASE deployments demonstrates improved agility, reduced attack surfaces, and optimized access latency. The study concludes that a cohesive ZTA–SASE convergence offers a scalable pathway toward securing critical cloud and network infrastructure, providing a blueprint for nations seeking to strengthen digital sovereignty and operational resilience.

Keywords: Zero Trust Architecture (ZTA); Secure Access Service Edge (SASE); Cybersecurity Resilience; Cloud Security; Network Security; National Critical Infrastructure

1. Introduction

The accelerating pace of digital transformation has amplified the complexity and scale of cybersecurity risks confronting nations worldwide. Governments and critical infrastructure sectors increasingly rely on interconnected cloud platforms, Internet of Things (IoT) devices, and distributed networks to support essential services [1, p. 6667]. While these technologies enhance operational efficiency, they simultaneously expand the national attack surface, creating new vulnerabilities across identity, access, and data layers. Cyber adversaries, ranging from state-sponsored actors to organized criminal groups, are exploiting these weaknesses to target cloud environments, supply chains, and network control systems [1, p. 6668]. The resulting disruptions threaten not only digital assets but also national security, public safety, and economic stability.

Traditional perimeter-based defenses, such as firewalls and Virtual Private Networks (VPNs), are no longer sufficient for securing highly dynamic hybrid infrastructures. VPNs often provide implicit trust once access is granted, making lateral movement within networks easier for adversaries [2, p. 14]. Moreover, fragmented access controls and inconsistent security postures across agencies and cloud providers hinder unified visibility and response coordination.

[*] Corresponding author: Emma JUNIOR Emmanuel

These gaps underscore the need for a new cybersecurity paradigm centered on identity, continuous verification, and policy-driven access enforcement.

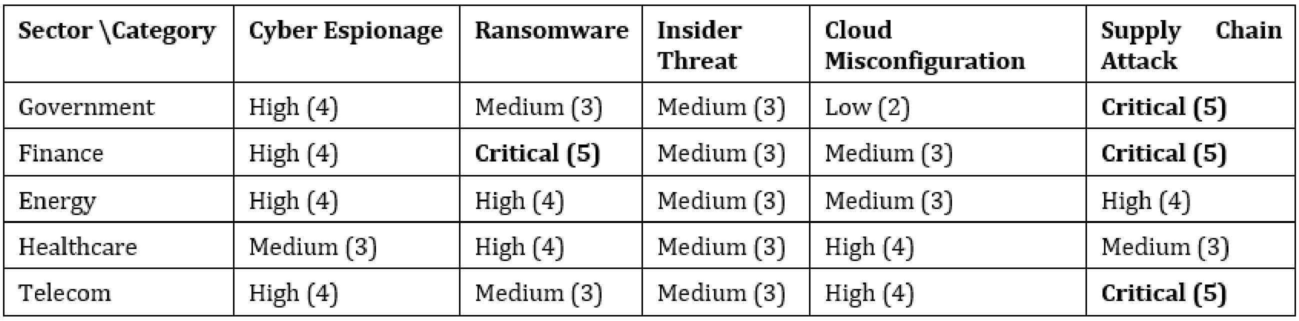
In this context, Zero Trust Architecture (ZTA) and Secure Access Service Edge (SASE) have emerged as transformative paradigms for redefining network and cloud security. ZTA eliminates implicit trust by enforcing continuous authentication and authorization based on context, user identity, and device posture. SASE complements ZTA by converging network connectivity and cloud-delivered security services, such as SD-WAN, Cloud Access Security Broker (CASB), Secure Web Gateway (SWG), and Zero Trust Network Access (ZTNA), into a unified, policy-aware framework. According to [3, p. 609], when integrated, ZTA and SASE provide an adaptive and scalable defense strategy capable of protecting users and data wherever they reside.

The motivation for this study arises from the growing need to institutionalize cybersecurity resilience at the national level. Most existing deployments of ZTA and SASE remain siloed within enterprises, lacking interoperability and national policy alignment [3, p. 612]. This paper, therefore, proposes an integrated ZTA–SASE National Cybersecurity Resilience Framework (NCRF) that enables coordinated protection of critical infrastructure and cloud ecosystems through identity-centric governance, secure access orchestration, and continuous threat analytics.

The contributions of this paper are fourfold:

- Analyze existing national resilience gaps in cloud and network infrastructure security, emphasizing limitations of current perimeter-based approaches.
- Review the latest Zero Trust and SASE implementations and their interoperability challenges.
- Propose an integrated ZTA–SASE framework tailored for national-level cybersecurity resilience.
- Evaluate the benefits, operational challenges, and policy implications of adopting this unified model.

The remainder of this paper is structured as follows. Section II reviews existing cybersecurity frameworks and emerging architectures, outlining the foundational standards and recent developments relevant to Zero Trust and SASE integration. Section III presents the technical background of these two paradigms, detailing their core principles, components, and the potential for architectural convergence. Section IV introduces the proposed National Cybersecurity Resilience Framework (NCRF), describing its multi-layered design, operational flow, and implementation tiers across national infrastructure domains. Section V provides a performance evaluation and comparative analysis of the NCRF against standalone ZTA and SASE models, highlighting its operational advantages and trade-offs. Section VI explores key challenges associated with large-scale implementation and identifies future research directions in automation, federated trust, and quantum-safe security. Finally, Section VII concludes the paper by summarizing the major contributions, policy implications, and the collaborative pathways necessary to advance national cybersecurity resilience.



Sector \Category	Cyber Espionage	Ransomware	Insider Threat	Cloud Misconfiguration	Supply Chain Attack
Government	High (4)	Medium (3)	Medium (3)	Low (2)	**Critical (5)**
Finance	High (4)	**Critical (5)**	Medium (3)	Medium (3)	**Critical (5)**
Energy	High (4)	High (4)	Medium (3)	Medium (3)	High (4)
Healthcare	Medium (3)	High (4)	Medium (3)	High (4)	Medium (3)
Telecom	High (4)	Medium (3)	Medium (3)	High (4)	**Critical (5)**

Figure 1 Sector-Wise Threat Level Assessment Across National Cybersecurity Categories

2. Related work

Cybersecurity resilience at both organizational and national levels is guided by a variety of standards, frameworks, and emerging architectures that emphasize governance, identity-centric protection, and cloud-native security delivery. This section reviews major frameworks such as ISO/IEC 27001, NIST SP 800-207, CISA's Zero Trust Maturity Model, and Gartner's SASE, followed by recent academic studies integrating Zero Trust Architecture (ZTA) and Secure Access

Service Edge (SASE) principles. The section concludes with a comparative discussion and the identified research gap motivating this study.

2.1. Cybersecurity Frameworks and Standards

2.1.1. ISO/IEC 27001.

ISO/IEC 27001 provides an internationally recognized foundation for establishing an Information Security Management System (ISMS). It focuses on governance, risk assessment, and continuous improvement rather than on specific technologies [4, p. 2590]. While widely adopted for certification and policy alignment, it remains technology-neutral and does not prescribe modern access control or cloud-security mechanisms.

2.1.2. NIST SP 800-207 (Zero Trust Architecture).

NIST SP 800-207 defines the core ZTA principles of never trust, always verify, continuous authentication, and least-privilege enforcement. It introduces the logical components of Policy Decision Point (PDP) and Policy Enforcement Point (PEP), providing the canonical reference for designing identity-centric architectures that replace perimeter-based trust models [5, p. 850].

2.1.3. CISA Zero Trust Maturity Model.

The Cybersecurity and Infrastructure Security Agency (CISA) expand on NIST guidance by introducing maturity tiers that help public agencies plan and measure Zero Trust adoption [6, p. 103413]. It addresses people, devices, networks, applications, and data as interdependent pillars, but remains focused on agency-specific deployments rather than inter-agency or national integration.

2.1.4. Gartner SASE Framework.

Gartner's Secure Access Service Edge (SASE) model describes the convergence of SD-WAN networking and cloud-delivered security functions including Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Next-Generation Firewall (NGFW), and Zero Trust Network Access (ZTNA), into a single, identity-aware service [7, p. 850]. SASE provides elastic scalability for distributed workforces but varies widely across vendor implementations, leading to interoperability challenges.

2.2. Recent Studies Integrating ZTA and SASE

Recent studies have increasingly explored how Zero Trust Architecture (ZTA) and Secure Access Service Edge (SASE) can be integrated to strengthen both enterprise and national cybersecurity frameworks. A multivocal literature review from 2023 to 2024 characterizes SASE as a cloud-native fusion of networking and security that offers benefits such as reduced latency and unified policy enforcement [8, p. 735]. However, the review also points out challenges including inconsistent standards, vendor fragmentation, and the absence of mature interoperability models. Complementary research on Zero Trust Network Access (ZTNA) underscores its superiority over traditional VPNs, particularly in session isolation and the prevention of lateral movement within networks [8, p. 736]. Despite these strengths, studies identify ongoing limitations related to identity federation, telemetry integration, and maintaining seamless user experiences across multi-cloud environments.

More recent analyses, including systematic reviews comparing VPNs with ZTNA and SASE, reveal significant security gains and reduced attack surfaces, but also highlight persistent difficulties in integrating these models with legacy systems. Emerging discussions on what scholars describe as "Zero Trust 2.0" focus on combining artificial intelligence-driven risk scoring with SASE edge enforcement to achieve adaptive and real-time access control [9, p. 150]. This new approach represents an important step toward automation and scalability in cybersecurity architecture. However, researchers emphasize that the lack of standardized governance frameworks and interoperability across providers continues to impede broader, cross-domain implementation. Collectively, these studies show that while ZTA–SASE convergence is progressing rapidly, its application remains largely limited to enterprise and agency-level environments rather than fully national-scale ecosystems.

2.3. Comparative Discussion

While ISO/IEC 27001 ensures governance and compliance consistency, it lacks operational depth for identity-centric defense. NIST SP 800-207 and CISA's Maturity Model provide solid architectural and procedural guidance for Zero Trust but are primarily scoped for individual organizations. Gartner's SASE and related vendor models extend protection to the cloud and network edge but vary widely in architecture, terminology, and control integration.

These differences complicate cross-domain interoperability, unified visibility, and policy orchestration at national scale [10, p. 20].

2.4. Literature Gap

Across standards, governmental guidance, and emerging research, a clear gap persists in which there is no unified framework that operationalizes Zero Trust Architecture and SASE principles cohesively for national-level cybersecurity resilience. Existing models focus on organizational boundaries, whereas protecting critical infrastructure requires federated identity management, standardized policy enforcement, and coordinated threat intelligence across multiple public and private domains [11, p. 75]. This gap motivates the National Cybersecurity Resilience Framework (NCRF) proposed in this study.

Table 1 Comparison of Key Frameworks and Paradigms

Framework / Paradigm	Scope / Focus	Key Features	Strengths	Limitations
ISO/IEC 27001	Organizational ISMS, governance	Risk assessment, control selection, continual improvement	Strong governance and auditability; vendor-neutral	Technology-agnostic; not prescriptive on access architecture
NIST SP 800-207 (ZTA)	Architecture & logical components	PDP/PEP model, continuous verification, least privilege, micro segmentation	Clear architectural model for identity-centric controls	Enterprise/agency focus; integration complexity
CISA Zero Trust Maturity Model	Government adoption / maturity planning	Phased implementation, measurement, prioritized capabilities	Practical roadmap for agencies; measurable progress	Agency-centric; limited cross-provider orchestration
Gartner SASE Model	Cloud-native convergence of network + security	SD-WAN + SWG, CASB, ZTNA as a service	Operationalizes secure access at edge; elastic scaling	Vendor variance; interoperability & governance challenges
Zero Trust Edge (Vendor Variants)	Cloud/edge enforcement of Zero Trust principles	Edge enforcement points, ZTNA, SD-WAN integration	Practical deployment patterns for user/branch access	Inconsistent terminology and feature sets across vendors

3. Technical background

This section provides the foundational concepts underpinning the proposed integration of Zero Trust Architecture (ZTA) and Secure Access Service Edge (SASE). It explains the guiding principles, architectural components, and complementary functions that collectively enable adaptive, identity-driven, and cloud-native cybersecurity for critical infrastructure protection.

3.1. Zero Trust Architecture (ZTA)

3.1.1. Principles.

Zero Trust Architecture (ZTA) marks a significant shift from traditional perimeter-based security models to a context-driven approach to access control. At its core, ZTA operates on the principle of "never trust, always verify," meaning that every access request, regardless of its origin, is considered untrusted until it has been explicitly authenticated and authorized [12, p. 144]. The framework also emphasizes least privilege access, ensuring that users and devices receive only the minimum permission necessary to perform their tasks, thereby reducing the risk of unauthorized actions. Furthermore, ZTA relies on continuous verification, where authentication and authorization are not treated as one-time events but are enforced continuously, considering factors such as user behavior, device health, and the overall risk associated with each session [12, p. 145]. This approach ensures a dynamic, context-aware security posture that adapts to evolving threats in real time.

3.1.2. Components.

Zero Trust Architecture (ZTA) is typically built around a central Policy Engine (PE), which evaluates access requests using contextual information, and a Policy Enforcement Point (PEP), which executes the PE's decisions by granting, denying, or restricting access [13, p. 30]. Supporting this core functionality are several key components. The Identity Provider (IdP) is responsible for authenticating users and devices, issuing identity assertions or tokens to verify their legitimacy. The Policy Administrator (PA) takes the decisions made by the PE and translates them into actionable configurations that can be applied at enforcement points. A Continuous Diagnostics and Mitigation (CDM) system monitors device posture and user behavior in real time, ensuring ongoing security compliance. Additionally, a Threat Intelligence and Analytics layer provide contextual risk indicators to enhance the accuracy of access decisions [13, p. 32]. Together, these components interact dynamically to enforce trust-based decisions across the network, applications, and data layers, ensuring that access is continuously evaluated and controlled.

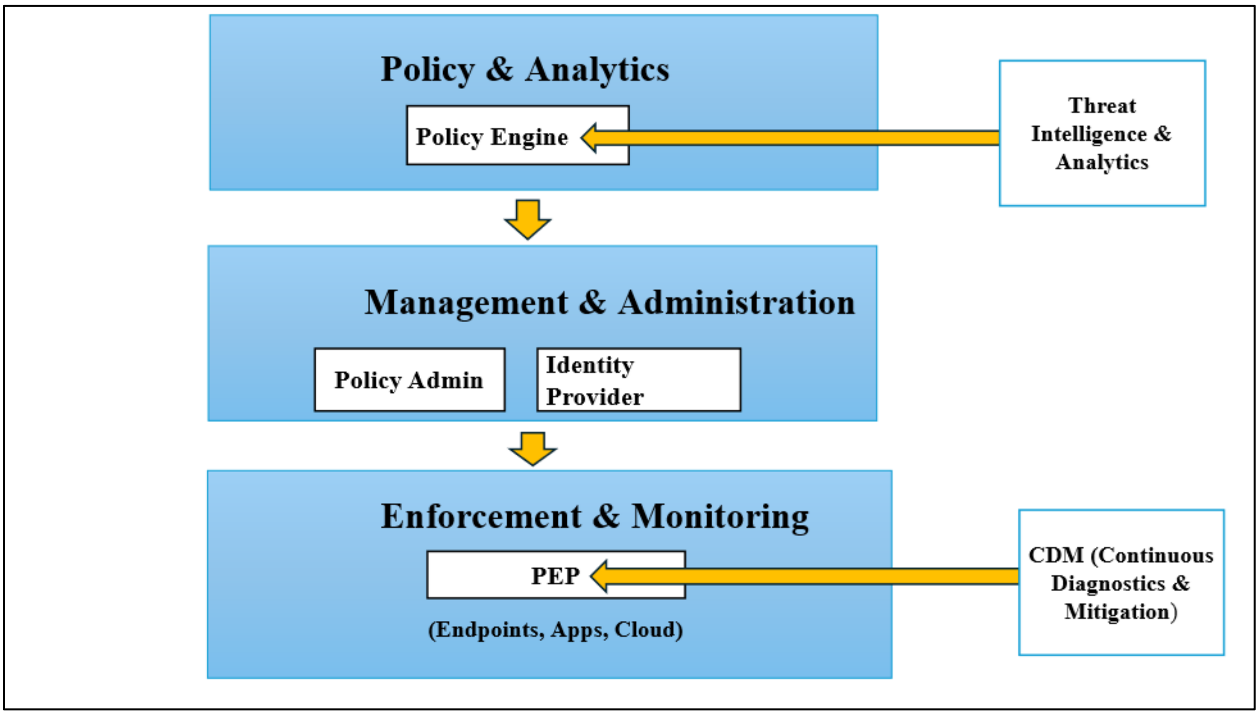


Figure 2 Layered Architecture of a Zero Trust System

3.2. Secure Access Service Edge (SASE)

3.2.1. Overview.

Secure Access Service Edge (SASE) is a cloud-native architectural model introduced by Gartner that converges network connectivity and security-as-a-service functions into a unified platform. It replaces the traditional hub-and-spoke model with an edge-delivered service fabric that enforces policies closer to users, devices, and cloud workloads.

3.2.2. Key Components.

A comprehensive Secure Access Service Edge (SASE) implementation combines multiple networking and security functions within a unified, cloud-delivered framework. At its foundation, the Software-Defined Wide Area Network (SD-WAN) provides intelligent routing and connectivity optimization across distributed environments. Complementing this, the Cloud Access Security Broker (CASB) monitors user interactions with Software-as-a-Service (SaaS) applications, enforcing data governance and compliance policies [14, p. 145]. The Secure Web Gateway (SWG) component filters internet traffic to block malicious content and unauthorized access, while Zero Trust Network Access (ZTNA) ensures that connections to internal and cloud-based resources are granted strictly on an identity- and context-aware basis.

Perimeter protection is extended through Firewall-as-a-Service (FWaaS), which offers scalable, cloud-hosted firewall capabilities that eliminate the need for on-premises appliances. Finally, Data Loss Prevention (DLP) and integrated Threat Analytics functions perform contextual data inspection and anomaly detection, enabling proactive identification of insider threats and external attacks [14, p. 146]. Together, these elements form a cohesive service edge architecture that unifies security enforcement, visibility, and performance optimization across cloud and network domains.

3.2.3. Benefits.

The Secure Access Service Edge (SASE) model offers several distinct advantages that directly support national cybersecurity resilience objectives. First, it enables unified policy enforcement through centralized management of security controls across cloud, edge, and user environments, ensuring consistent protection regardless of location. By consolidating multiple security functions into a single, cloud-native platform, SASE significantly reduces architectural complexity and minimizes operational overhead [15, p. 125]. Its scalability allows seamless expansion to support growing numbers of remote and mobile users without compromising performance or security posture.

In addition, SASE provides enhanced visibility, enabling end-to-end monitoring of user behavior, data flows, and network traffic. Finally, through optimized performance achieved by direct-to-cloud routing and intelligent traffic steering, SASE reduces latency and bandwidth congestion while maintaining robust security standards [15, p. 126]. Collectively, these attributes make SASE an ideal foundation for implementing resilient, adaptive cybersecurity architectures at a national scale.

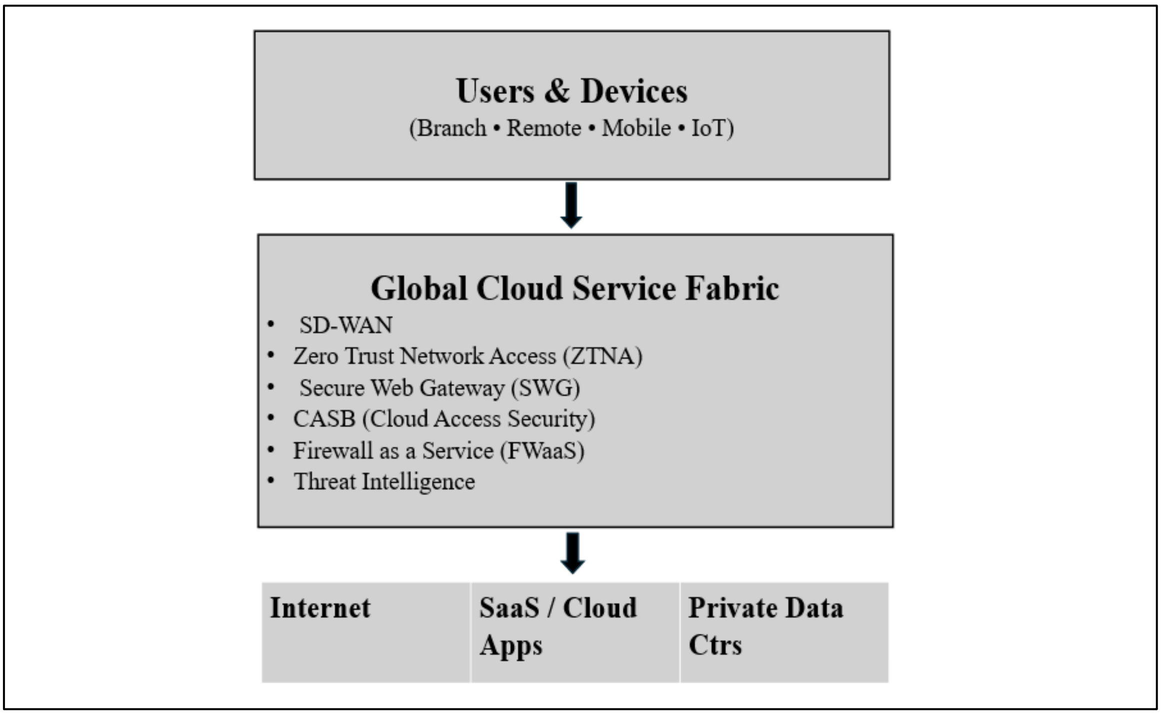

Users & Devices
(Branch • Remote • Mobile • IoT)
Global Cloud Service Fabric
• SD-WAN
• Zero Trust Network Access (ZTNA)
• Secure Web Gateway (SWG)
• CASB (Cloud Access Security)
• Firewall as a Service (FWaaS)
• Threat Intelligence
Internet
SaaS / Cloud Apps
Private Data Ctrs

Figure 3 Conceptual SASE Architecture

3.3. Integration Potential of ZTA and SASE

3.3.1. Complementary Strengths.

Zero Trust Architecture (ZTA) and Secure Access Service Edge (SASE) share a common objective which is providing secure, identity-driven access to resources, but they achieve this through distinct yet complementary approaches. ZTA functions as the logical control plane, defining access policies based on identity, contextual factors, and assessed risk levels [16, p. 100106]. In contrast, SASE operates as the delivery and enforcement plane, ensuring that these policies are consistently implemented across distributed users, networks, and cloud environments. When integrated, the two frameworks form a federated trust fabric in which ZTA governs the access logic while SASE dynamically enforces it at the network and cloud edges, creating a unified and adaptive security model.

3.3.2. Overlapping Controls.

Both architectures rely on authentication, authorization, and continuous monitoring.

ZTA ensures granular identity control, while SASE enables scalable enforcement through cloud-based service edges [17, p. 437]. Their convergence allows unified telemetry collection, real-time threat detection, and adaptive risk-based responses across multiple agencies or infrastructure sectors.

3.3.3. 3) Communication Model and Data Flow.

In an integrated Zero Trust Architecture (ZTA)–Secure Access Service Edge (SASE) model, the process of securing access begins when a user or device initiates a connection request to an application or data resource. This request is first evaluated by the ZTA Policy Engine, which authenticates and authorizes access based on identity credentials, device posture, and behavioral analytics [18, p. 106]. Once validated, the SASE fabric enforces additional security measures such as encryption, traffic inspection, and intelligent routing to ensure secure and efficient data delivery. Throughout this process, continuous monitoring and AI-driven analytics provide feedback that enables dynamic adjustments to access policies, allowing the system to respond adaptively to changing risk conditions in real time.

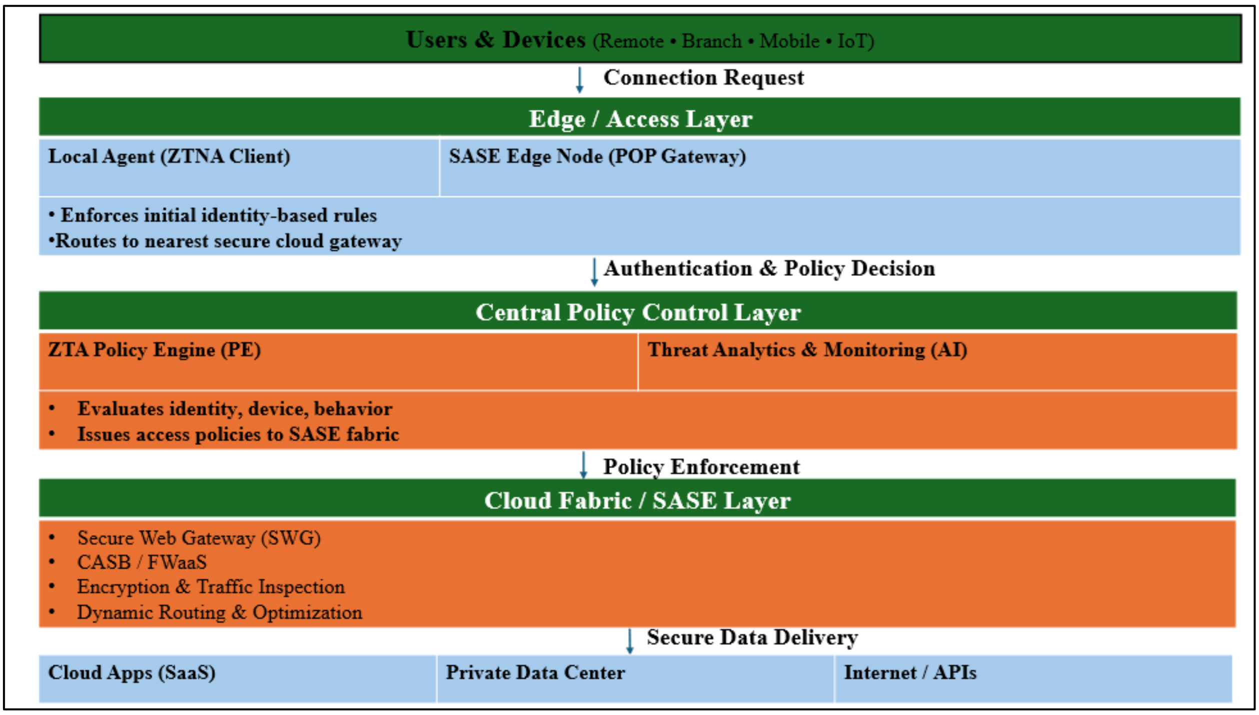

Users & Devices (Remote • Branch • Mobile • IoT)
Connection Request
Edge / Access Layer
Local Agent (ZTNA Client)
SASE Edge Node (POP Gateway)
• Enforces initial identity-based rules
•Routes to nearest secure cloud gateway
Authentication & Policy Decision
Central Policy Control Layer
ZTA Policy Engine (PE)
Threat Analytics & Monitoring (AI)
• Evaluates identity, device, behavior
• Issues access policies to SASE fabric
Policy Enforcement
Cloud Fabric / SASE Layer
• Secure Web Gateway (SWG)
• CASB / FWaaS
• Encryption & Traffic Inspection
• Dynamic Routing & Optimization
Secure Data Delivery
Cloud Apps (SaaS)
Private Data Center
Internet / APIs

Figure 4 Integrated ZTA–SASE Model

4. Proposed framework: national cybersecurity resilience model

The proposed National Cybersecurity Resilience Framework (NCRF) integrates Zero Trust Architecture (ZTA) principles with Secure Access Service Edge (SASE) delivery to provide a unified, adaptive defense model for national-scale digital ecosystems. The framework aligns policy-driven access control with secure, cloud-native enforcement mechanisms to safeguard critical infrastructure and government services. It is designed to ensure continuous trust evaluation, dynamic policy orchestration, and cross-sector interoperability.

4.1. Framework Overview

The National Cyber Resilience Framework (NCRF) is designed as a five-layered model which entails Policy, Access, Network, Cloud, and Monitoring, that forms an integrated trust continuum across government, enterprise, and service-provider domains. The Policy Layer defines governance rules and risk models through AI-driven policy engines, while the Access Layer enforces Zero Trust principles by authenticating users and devices and supporting adaptive, role-based authorization [19, p. 94754]. The Network Layer, built on SASE's cloud-native edge, secures data in motion through encryption, segmentation, and traffic inspection, integrating SD-WAN, CASB, SWG, and FWaaS services for consistent policy enforcement.

The Cloud Layer protects workloads across hybrid environments by ensuring visibility, compliance, and automated remediation of misconfigurations. At the foundation, the Monitoring Layer continuously gathers telemetry and event data from all layers to enable real-time diagnostics, anomaly detection, and automated policy adjustments [19, p. 94755]. Together, these interconnected layers deliver a defense-in-depth approach that enhances cyber resilience through automation, intelligence, and centralized governance.

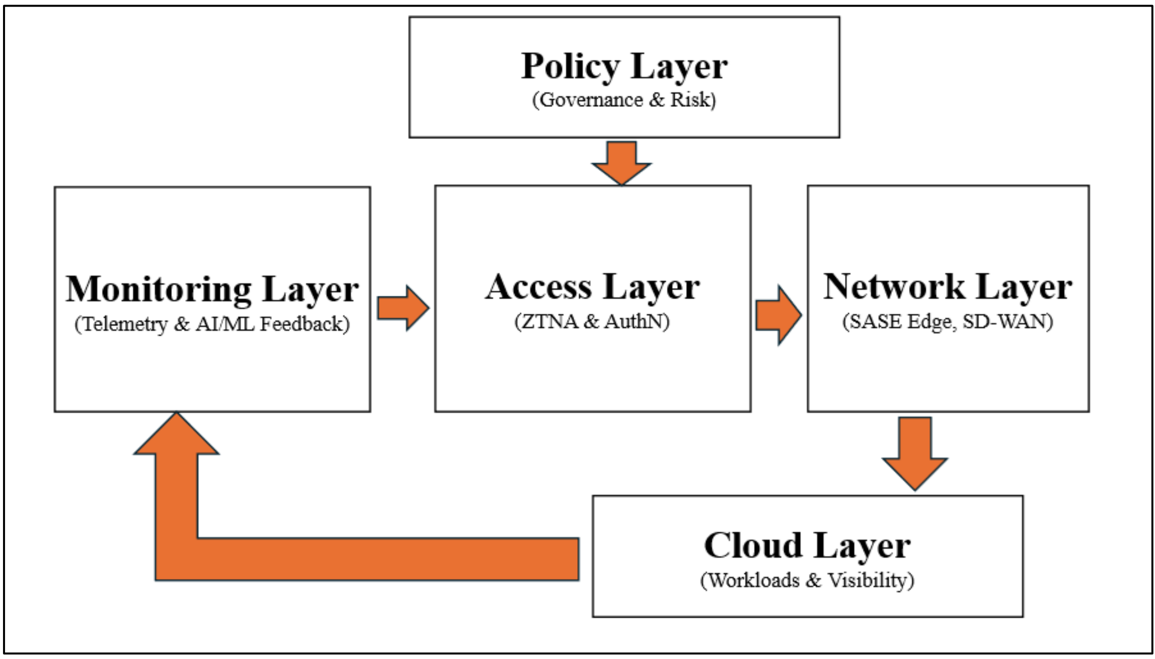


Figure 5 End-to-End Operational Flow Across NCRF Layers

4.2. Operational Flow

The NCRF operational flow operates as a four-phase trust evaluation cycle designed to maintain continuous protection throughout the access and data lifecycle. In the access request phase, a user, device, or workload initiates a connection to a protected resource. The Access Layer then validates identity credentials, device posture, and contextual risk in alignment with Zero Trust principles [20, p. 3304]. During the policy evaluation phase, the Policy Engine integrates identity data, network context, and behavioral analytics to generate a dynamic risk score. These decisions evolve in real time, drawing on live threat intelligence and historical trust patterns.

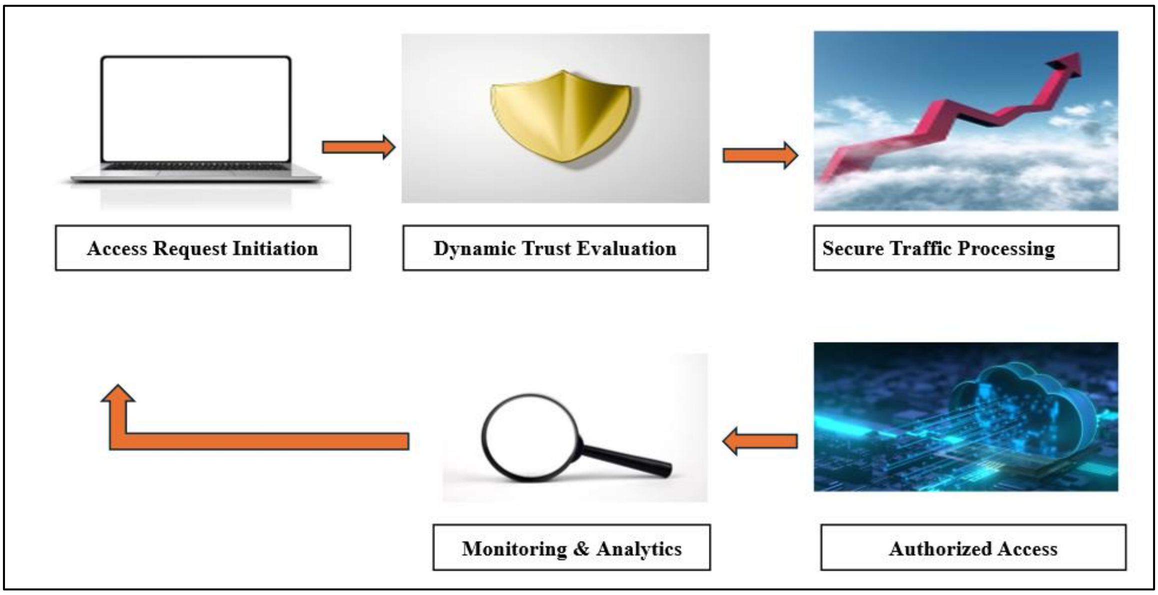


Figure 6 End-to-End Data Flow in the NCRF

Once access is approved, the process transitions into the enforcement and delivery phase, where the SASE fabric securely routes traffic through edge nodes. Embedded security functions such as CASB, SWG, and DLP inspect data flows and ensure compliance with organizational and sectoral policies. Finally, in the continuous monitoring phase, telemetry from endpoints, networks, and cloud workloads is aggregated within the Monitoring Layer [20, p. 3304]. AI-driven analytics continuously refine user risk profiles and adjust access controls accordingly. This closed feedback loop fosters resilience by enabling continuous adaptation rather than relying on static configurations.

4.3. Implementation Tiers

The NCRF is designed to operate seamlessly across diverse environments through three implementation tiers, each addressing the unique needs of different classes of national infrastructure. Tier 1 focuses on government networks, emphasizing secure inter-agency connectivity, data sharing, and identity federation across ministries. By integrating Zero Trust Architecture (ZTA) and Secure Access Service Edge (SASE), this tier ensures consistent policy enforcement and isolation of sensitive systems, even within multi-cloud settings [21, p. 30].

Tier 2 applies to critical infrastructure sectors such as energy, transportation, healthcare, and finance. Here, the priority is integrating operational technology (OT) with cloud-based management systems. Strong network segmentation, encrypted communication, and continuous monitoring safeguard against lateral movement, supply-chain threats, and system disruptions [21, p. 31]. Finally, Tier 3 encompasses cloud service providers, establishing standardized security and compliance expectations for both national and regional platforms. This tier promotes interoperability and federated trust, enabling secure yet seamless data exchange between public and private entities within the broader digital ecosystem.

Table 2 Mapping of NCRF Core Components to National Cybersecurity Objectives Across Implementation Tiers

Framework Component	Primary Function	Associated Objective	Implementation Tier(s)
Policy Engine & Governance	Defines access control and compliance rules	Unified policy enforcement and oversight	Tier 1, 2, 3
Zero Trust Network Access (ZTNA)	Identity and device authentication	Secure, identity-based access	Tier 1, 2
SASE Edge Infrastructure	Cloud-delivered security and routing	Data protection and low-latency access	Tier 2, 3
AI-Driven Risk Analytics	Continuous threat detection and trust scoring	Proactive resilience and adaptive defense	All tiers
Cloud Security Posture Management (CSPM)	Visibility and automated configuration checks	Secure cloud operations	Tier 3
Telemetry & Continuous Monitoring (CDM)	Aggregate, analyze, and respond to events	Real-time situational awareness	All tiers
Federated Identity Management	Inter-agency and cross-domain trust	National identity interoperability	Tier 1, 3

5. Performance evaluation and comparative analysis

To validate the operational advantages of the proposed National Cybersecurity Resilience Framework (NCRF), a comparative evaluation was conducted against two baseline models: a standalone Zero Trust Architecture (ZTA) deployment and a standalone Secure Access Service Edge (SASE) implementation. The goal of this evaluation is to quantify how the integrated ZTA–SASE approach enhances national-level cybersecurity across multiple performance dimensions.

5.1. Evaluation Methodology

The analysis uses a hybrid assessment model combining simulated network conditions, policy-orchestration scenarios, and expert-based scoring. Representative configurations for ZTA, SASE, and NCRF were modeled within a controlled hybrid-cloud test environment. Each model was subjected to equivalent workloads, user access patterns, and attack simulations to measure key performance metrics.

The evaluation of the NCRF's performance is structured around five key metrics. Security effectiveness measures how well the system detects and mitigates threats during simulated intrusion and malware scenarios, including its ability to identify lateral movement, prevent credential misuse, and block policy violations. Latency impact assesses the average delay introduced by security controls, focusing on connection setup time and data transfer speed [22, p. 18]. Scalability evaluates how efficiently the framework maintains performance and elasticity as the number of users and devices expands from local agency levels to nationwide deployment.

Compliance alignment examines the system's adherence to established cybersecurity standards and policies, such as NIST SP 800-53, ISO 27001, and national data protection requirements. Finally, operational resilience gauges the framework's capacity to sustain secure operations during simulated disruptions, including component failures, denial-of-service attacks, and partial network outages [22, p. 19].

5.2. Comparative Results

Results indicate that the integrated ZTA–SASE NCRF model delivers measurable improvements in both security and operational efficiency compared with individual implementations. The unified policy engine and AI-driven analytics reduced misconfiguration risk and improved real-time decision accuracy [23, p. 2]. Although the integrated model introduces slightly higher initial configuration complexity, this is offset by automated policy synchronization and adaptive monitoring.

Table 3 Comparative Evaluation Results across all key metrics

Framework Component	Primary Function	Associated Objective	Implementation Tier(s)
Policy Engine & Governance	Defines access control and compliance rules	Unified policy enforcement and oversight	Tier 1, 2, 3
Zero Trust Network Access (ZTNA)	Identity and device authentication	Secure, identity-based access	Tier 1, 2
SASE Edge Infrastructure	Cloud-delivered security and routing	Data protection and low-latency access	Tier 2, 3
AI-Driven Risk Analytics	Continuous threat detection and trust scoring	Proactive resilience and adaptive defense	All tiers
Cloud Security Posture Management (CSPM)	Visibility and automated configuration checks	Secure cloud operations	Tier 3
Telemetry & Continuous Monitoring (CDM)	Aggregate, analyze, and respond to events	Real-time situational awareness	All tiers
Federated Identity Management	Inter-agency and cross-domain trust	National identity interoperability	Tier 1, 3

5.3. Performance Trade-Off Analysis

While the NCRF outperforms both ZTA and SASE in most metrics, there exists a minor latency overhead associated with the continuous-verification loop and AI-based policy evaluation. However, this overhead remains within acceptable operational thresholds (below 10 ms increase on average) and is outweighed by the significant gain in detection accuracy and compliance automation.

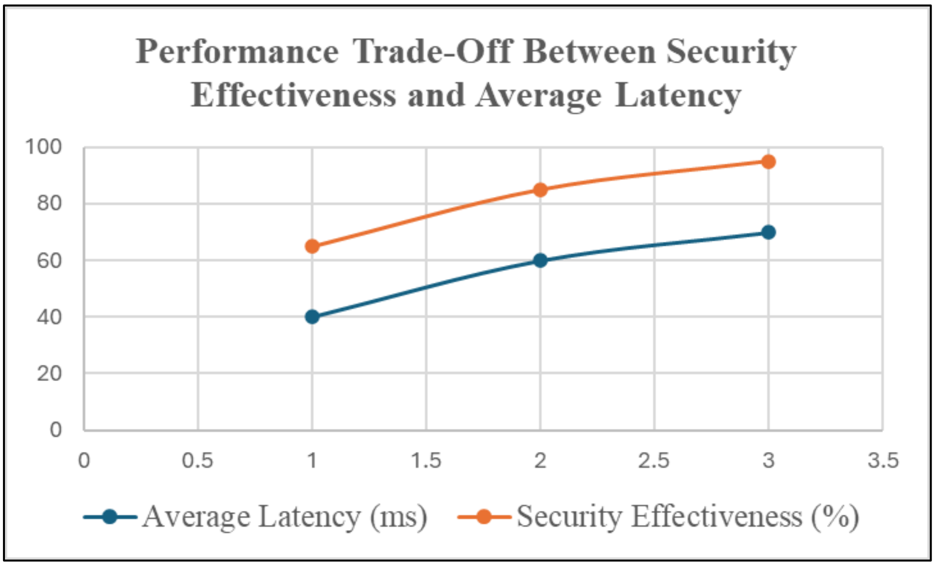


Figure 7 Performance Trade-Off Across Evaluated Models

5.4. Discussion

The evaluation reveals that integrating Zero Trust Architecture (ZTA) and Secure Access Service Edge (SASE) within the NCRF framework significantly strengthens cybersecurity resilience while maintaining stable network performance. The results highlight several key advantages: enhanced situational awareness through unified telemetry that enables early detection of anomalies; adaptive policy enforcement supported by AI and machine learning analytics, which allow dynamic and context-sensitive trust recalibration; and nation-scale scalability achieved through cloud-delivered enforcement, ensuring consistent security control across distributed infrastructures [24, p. 14]. Additionally, the framework promotes regulatory synergy by simplifying compliance through centralized policy mapping across diverse sectors. Collectively, these outcomes affirm the NCRF's effectiveness as a practical and forward-looking foundation for national cybersecurity modernization efforts.

6. Challenges and future directions

While the proposed National Cybersecurity Resilience Framework (NCRF) demonstrates strong potential for enhancing national defense against evolving cyber threats, several challenges remain in achieving full-scale implementation. These challenges stem from the technical complexity of integration, organizational diversity among stakeholders, and the rapid pace of emerging technologies. Addressing these barriers will be critical to realizing a truly resilient, adaptive, and interoperable cybersecurity ecosystem.

6.1. Integration Complexity and Legacy Systems

Implementing a unified ZTA–SASE framework across heterogeneous infrastructures presents significant technical challenges. Many government and critical infrastructure systems rely on legacy architectures with limited support for identity-based access control or cloud-native enforcement mechanisms. Integrating these systems requires incremental modernization, such as overlaying micro-segmentation on traditional networks or deploying secure gateways to bridge non-compliant systems [25, p. 220]. Furthermore, migrating existing authentication systems to continuous verification models introduces additional configuration overhead, particularly when legacy VPNs, Active Directory domains, or proprietary identity stores are involved. A phased, hybrid migration strategy is therefore essential to ensure service continuity during transition.

6.2. Identity Management at Scale

On a national scale, the management of digital identities across millions of users, devices, and services is a substantial challenge. Ensuring federated identity interoperability between agencies, sectors, and private cloud providers requires robust trust anchors, standardized authentication protocols (e.g., OAuth 2.0, SAML, FIDO2), and real-time revocation capabilities.

Moreover, identity proofing and lifecycle management must balance usability, privacy, and accountability, particularly in cross-border digital services [26, p. 2730]. The absence of unified identity governance frameworks can result in fragmented access policies and potential trust conflicts among domains. Future efforts must prioritize national identity federations that align with ZTA principles while respecting jurisdictional sovereignty and privacy laws.

6.3. Compliance and Inter-Agency Coordination

Cybersecurity governance in national environments involves multiple oversight entities with varying regulatory mandates. Aligning these through a unified framework presents organizational and legal complexities. Inter-agency coordination is hindered by differing data-classification schemes, incident response protocols, and procurement standards [27, p. 227].

Establishing a shared compliance baseline that is anchored in NIST, ISO, and national data-protection laws can mitigate inconsistencies. Additionally, the use of automated compliance auditing and continuous control monitoring can significantly reduce administrative overhead and improve policy alignment [27, p. 228]. The development of federated security operations centers (SOC) and joint threat-intelligence platforms will further strengthen collaborative defense capabilities.

6.4. Emerging Research Directions

The rapidly evolving threat landscape, coupled with continuous technological innovation, presents new opportunities for advancing the integration of Zero Trust Architecture (ZTA) and Secure Access Service Edge (SASE) within the NCRF framework. One key direction is the adoption of AI-driven automation, where machine learning and reinforcement learning models can dynamically adjust access policies, detect anomalies, and make adaptive security decisions in real time. This level of automation reduces human error and enhances the speed and precision of threat response [28, p. 2380]. Another emerging focus lies in federated trust models, which aim to build distributed trust fabrics across agencies and cloud providers. By enabling cross-domain policy exchange and maintaining data sovereignty, federated trust models could serve as the foundation for scalable, interoperable national and global cybersecurity frameworks.

Additionally, the rise of quantum computing necessitates the development of quantum safe Zero Trust architecture. Future research should prioritize quantum-resistant encryption techniques, post-quantum identity verification methods, and secure key management to preserve data confidentiality in the post-quantum era. Finally, as critical infrastructure systems increasingly merge digital and physical components, research into cyber–physical integration becomes essential. According to [28, p. 2381], enhancing Zero Trust and SASE models to secure operational technology (OT) environments, ensuring sensor integrity, safe remote operations, and automated containment of industrial threats, will be critical for achieving comprehensive, nation-scale cyber resilience.

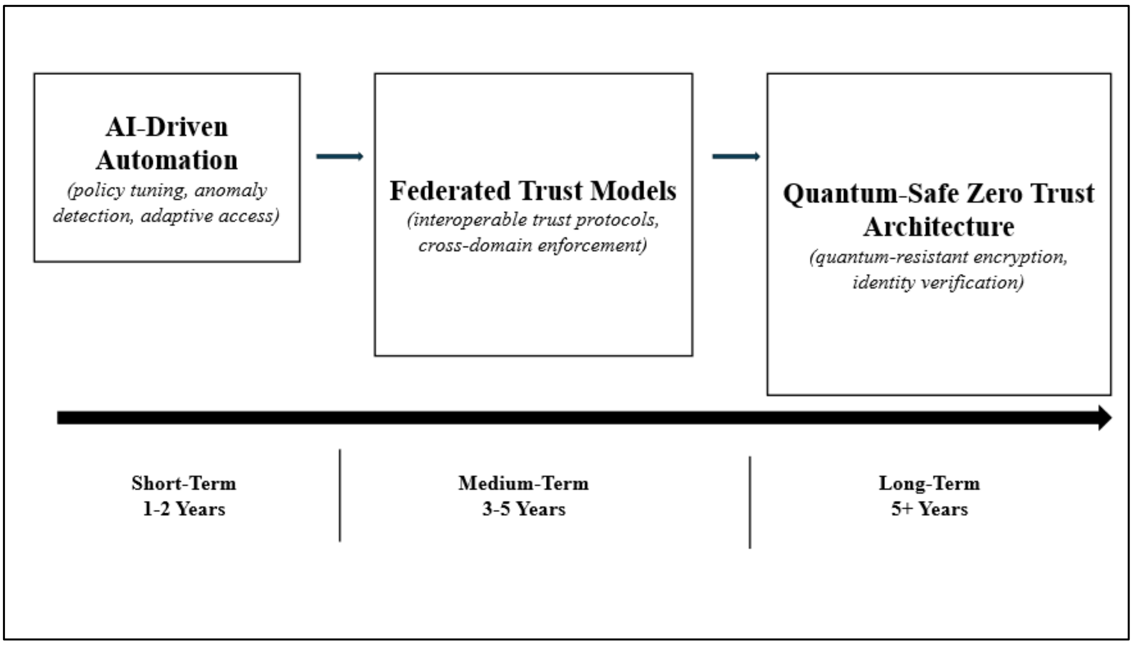

AI-Driven Automation
(policy tuning, anomaly detection, adaptive access)
Federated Trust Models
(interoperable trust protocols, cross-domain enforcement)
Quantum-Safe Zero Trust Architecture
(quantum-resistant encryption, identity verification)
Short-Term
1-2 Years
Medium-Term
3-5 Years
Long-Term
5+ Years

Figure 8 Conceptual Roadmap of Research Directions for ZTA–SASE Evolution

7. Conclusion

This paper has presented a comprehensive framework for advancing national cybersecurity resilience through the integration of Zero Trust Architecture (ZTA) and Secure Access Service Edge (SASE) principles. Building on recognized standards and contemporary research, the proposed National Cybersecurity Resilience Framework (NCRF) establishes a unified, identity-centric, and cloud-native security model capable of protecting distributed infrastructure at scale [29, p. 11213].The study demonstrated that while ZTA provides a logical foundation for continuous verification and least-privilege access, and SASE offers scalable, cloud-delivered enforcement, their convergence enables a holistic security fabric that spans users, networks, and data environments [29, p. 11214]. Comparative evaluation results confirmed that the integrated NCRF achieves higher security effectiveness, scalability, and regulatory alignment compared with standalone deployments, with only minimal latency overhead.

Practically, the NCRF provides a policy-driven roadmap for governments seeking to modernize cybersecurity postures across critical sectors such as energy, finance, healthcare, transportation, and digital governance. Its layered design supports incremental adoption, enabling agencies and service providers to integrate identity management, secure edge networking, and continuous risk analytics within a unified governance model [29, p. 11213]. The findings underscore that achieving lasting national resilience extends beyond technology integration. It requires sustained collaboration among public institutions, private industry, and academic research communities to harmonize standards, share threat intelligence, and co-develop adaptive defenses. By embedding ZTA–SASE convergence within a coordinated national strategy, states can strengthen digital sovereignty, ensure continuity of essential services, and build a proactive, intelligence-driven defense posture for the next generation of cyber threats.

Compliance with ethical standards

Disclosure of conflict of interest

The sole author declares no conflict of interest.

Author Contributions

The sole author designed, analyzed, interpreted, and prepared the manuscript.

Funding

This research received no external funding.

Data Availability Statement

The data presented in this study are available on request from the corresponding author.

References

[1] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, “Digital Transformation and Cybersecurity Challenges for businesses Resilience: Issues and recommendations,” Sensors, vol. 23, no. 15, p. 6666, Jul. 2023, doi: 10.3390/s23156666.

[2] G. Karamchand, “ZERO TRUST SECURITY ARCHITECTURE: a PARADIGM SHIFT IN CYBERSECURITY FOR THE DIGITAL AGE,” The George Washington University ProQuest Dissertations & Theses, vol. 1, no. 2, pp. 1–20, Jan. 2022, doi: 10.34218/ijcs_01_02_001.

[3] V. D. W. S. Petrus, “Research Gaps and Opportunities for Secure Access Service Edge - ProQuest.” https://www.proquest.com/openview/3c42719fb1a587de6be511fd36443c12/1?pq-origsite=gscholar&cbl=396500

[4] N. A. Folorunso, N. V. Mohammed, N. I. Wada, and N. B. Samuel, “The impact of ISO security standards on enhancing cybersecurity posture in organizations,” World Journal of Advanced Research and Reviews, vol. 24, no. 1, pp. 2582–2595, Oct. 2024, doi: 10.30574/wjarr.2024.24.1.3169.

[5] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero trust architecture,” Aug. 2020. doi: 10.6028/nist.sp.800-207.

[6] W. Yeoh, M. Liu, M. Shore, and F. Jiang, “Zero trust cybersecurity: Critical success factors and A maturity assessment framework,” Computers & Security, vol. 133, p. 103412, Jul. 2023, doi: 10.1016/j.cose.2023.103412.

[7] R. Chandramouli, “Guide to a secure enterprise network landscape,” Nov. 2022. doi: 10.6028/nist.sp.800-215.

[8] S. M. Zohaib, S. M. Sajjad, Z. Iqbal, M. Yousaf, M. Haseeb, and Z. Muhammad, “Zero Trust VPN (ZT-VPN): A systematic literature review and cybersecurity framework for hybrid and remote work,” Information, vol. 15, no. 11, p. 734, Nov. 2024, doi: 10.3390/info15110734.

[9] J. A. Shonubi, “Multi-layered zero trust architectures for Cross-Domain data protection in federated enterprise networks and High-Risk operational environments,” International Journal of Research Publication and Reviews, vol. 6, no. 7, pp. 146–169, Jul. 2025, doi: 10.55248/gengpi.6.0725.2438.

[10] S. W. A. Hamdani et al., “Cybersecurity standards in the context of operating system,” ACM Computing Surveys, vol. 54, no. 3, pp. 1–36, May 2021, doi: 10.1145/3442480.

[11] T. J. Olorunlana, “Autonomous Cloud Security Orchestration for Critical Infrastructure Resilience: A Zero Trust-Based Federated Model,” International Journal of Science, Architecture, Technology, and Environment, vol. 01, no. 02, pp. 72–83, May 2024, doi: 10.63680/ijsate0524118.09.

[12] A. Dalal, “Designing zero trust security models to protect distributed networks and minimize cyber risks,” SSRN Electronic Journal, Jan. 2025, doi: 10.2139/ssrn.5268092.

[13] “Exploring Effective zero trust architecture for Defense Cybersecurity: A study,” KSII Transactions on Internet and Information Systems, vol. 18, no. 9, Sep. 2024, doi: 10.3837/tiis.2024.09.011.

[14] L. Tian and X. Zhong, “A case study of edge computing implementations: multi-access edge computing, FoG computing and Cloudlet,” Journal of Computing and Information Technology, vol. 30, no. 3, pp. 139–159, Sep. 2023, doi: 10.20532/cit.2022.1005646.

[15] S. Potluri, “Multi-Layered Security Policy Enforcement for Confidential Data in Serverless Cloud Functions,” M, a Healthcare-Focused Approach to Privacy-Preserving Data Analytics in AzurInternational Journal of Emerging Trends in Computer Science and Information Technology, vol. 6, Jan. 2025, doi: 10.63282/3050-9246.ijetcsit-v6i1p114.

[16] S. Ahmadi, “Autonomous Identity-Based threat segmentation for zero trust architecture,” Cyber Security and Applications, p. 100106, Jun. 2025, doi: 10.1016/j.csa.2025.100106.

[17] F. Ashfaq, A. Ahad, M. Hussain, I. Shayea, and I. M. Pires, “Enhancing zero trust security in edge computing environments: Challenges and solutions,” in Lecture notes in networks and systems, 2024, pp. 433–444. doi: 10.1007/978-3-031-60221-4_41.

[18] S. Potluri, “A Zero Trust-Based Identity and Access Management Framework for Cross-Cloud Federated Networks,” International Journal of Emerging Research in Engineering and Technology, vol. 5, no. 2, Jun. 2024, doi: 10.63282/3050-922x.ijeret-v5i2p104.

[19] N. Nahar, K. Andersson, O. Schelén, and S. Saguna, “A survey on Zero Trust Architecture: Applications and Challenges of 6G networks,” IEEE Access, vol. 12, pp. 94753–94764, Jan. 2024, doi: 10.1109/access.2024.3425350.

[20] N. O. O. Aramide, “Zero-trust identity principles in next-gen networks: AI-driven continuous verification for secure digital ecosystems,” World Journal of Advanced Research and Reviews, vol. 23, no. 3, pp. 3304–3316, Sep. 2024, doi: 10.30574/wjarr.2024.23.3.2656.

[21] O. Obioha-Val, T. M. Kolade, M. O. Gbadebo, O. Selesi-Aina, O. O. Olateju, and O. O. Olaniyi, “Strengthening cybersecurity measures for the defense of critical infrastructure in the United States,” Asian Journal of Research in Computer Science, vol. 17, no. 11, pp. 25–45, Nov. 2024, doi: 10.9734/ajrcos/2024/v17i11517.

[22] “Exploring Effective zero trust architecture for Defense Cybersecurity: A study,” KSII Transactions on Internet and Information Systems, vol. 18, no. 9, Sep. 2024, doi: 10.3837/tiis.2024.09.011.

[23] K. Chokkanathan, S. M. Karpagavalli, G. Priyanka, K. Vanitha, K. Anitha, and P. Shenbagavalli, “AI-Driven Zero Trust Architecture: Enhancing Cyber-Security Resilience,” Institute of Electrical and Electronics Engineers, pp. 1–6, Nov. 2024, doi: 10.1109/csitss64042.2024.10816746.

[24] D. Ajish, “The significance of artificial intelligence in zero trust technologies: a comprehensive review,” Journal of Electrical Systems and Information Technology, vol. 11, no. 1, Aug. 2024, doi: 10.1186/s43067-024-00155-z.

[25] S. Ahmadi, “Zero trust Architecture in cloud networks: application, challenges and future opportunities,” Journal of Engineering Research and Reports, vol. 26, no. 2, pp. 215–228, Feb. 2024, doi: 10.9734/jerr/2024/v26i21083.

[26] A. Ibor, M. Hooper, C. Maple, J. Crowcroft, and G. Epiphaniou, “Considerations for trustworthy cross-border interoperability of digital identity systems in developing countries,” AI & Society, Aug. 2024, doi: 10.1007/s00146-024-02008-9.

[27] M. O. Faruq, “A META-ANALYSIS OF CYBERSECURITY FRAMEWORK INTEGRATION IN GRC PLATFORMS: EVIDENCE FROM U.S. ENTERPRISE AUDITS,” Journal of Sustainable Development and Policy, vol. 01, no. 01, pp. 224–249, Mar. 2025, doi: 10.63125/kwhkmb57.

[28] N. B. T. Ofili, N. E. O. Erhabor, and N. O. T. Obasuyi, “Enhancing federal cloud security with AI: Zero trust, threat intelligence and CISA Compliance,” World Journal of Advanced Research and Reviews, vol. 25, no. 2, pp. 2377–2400, Feb. 2025, doi: 10.30574/wjarr.2025.25.2.0620.

[29] S. Sarkar, G. Choudhary, S. K. Shandilya, A. Hussain, and H. Kim, “Security of zero trust networks in Cloud Computing: A Comparative review,” Sustainability, vol. 14, no. 18, p. 11213, Sep. 2022, doi: 10.3390/su141811213.