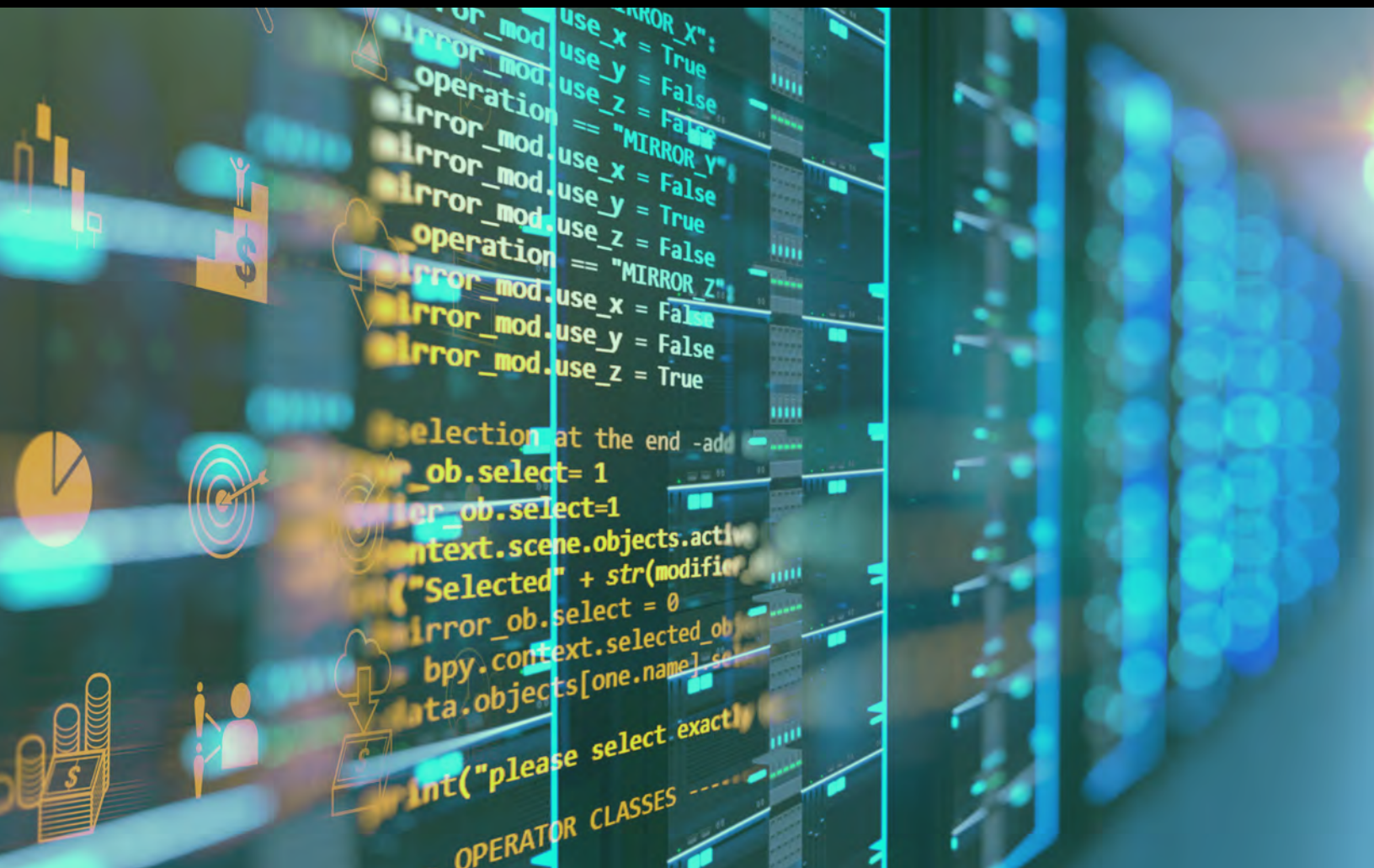
GTT + HPE

WHITEPAPER

BEYOND JUST SASE: A PRAGMATIC BLUEPRINT FOR SECURE, EFFICIENT CONNECTIVITY TO PROTECT ALL USERS AT THE EDGE



GTT + HPE

EXECUTIVE SUMMARY

SASE is thrown around quite a bit when it comes to discussing networking and security. However, most enterprises are still operating with a separate SD-WAN overlay, multiple appliances for security protection, siloed policy management and limited visibility across their edge and cloud.

The results aren't surprising: security tool sprawl and alert fatigue, non-homogeneous regulatory requirements, communication breakdowns and exorbitant costs. The mean time to respond (MTTR) to attacks on the infrastructure increases, which in turn fuels strain between vendors, NetOps the Network Operations Center and the Security Operations Center.

Let's move beyond vendor labels and establish a practical blueprint to integrate software-defined WAN (SD-WAN), Secure Service Edge (SSE), zero trust access and policy-based controls to protect all users, devices and applications the edge.

The goal is simple. Secure connectivity without adding complexity.

THE EDGE IS NOW EVERYWHERE

Your edge is no longer a branch office. It includes:

- Remote and hybrid workers
- IoT and OT devices
- Cloud-native applications
- Multi-cloud environments
- Partner ecosystems
- Regional data centers

The context is constantly shifting with different applications, locations, users, devices and networks. Applications are based in SaaS, public cloud, and are accessed remotely from multiple unmanaged networks by mobile users. Endpoint devices are no longer kept in traditional perimeters.

Traditional security controls are not keeping pace with evolving demands from centralized data centers. Backhauling traffic results in higher costs, latency and increased network congestion. Blind spots are created by stacked appliances, and both site- and vendor-specific policies vary widely.

At the same time, boards expect resilience, compliance and measurable risk reduction.

This is the challenge facing CIOs and CISOs today.

WHY "SASE" ALONE IS NOT ENOUGH

SASE is a framework for secure access as a cloud-based service. It unites SD-WAN and SSE into a single architecture. In practice, many deployments look different:

- SD-WAN from one vendor
- Cloud access security from another
- Different management consoles
- Manual policy coordination

The outcome is partial convergence. Security telemetry is all over the place and identity policies aren't consolidated or consistent. Performance needs to be tuned in sync across all tools to mitigate bottlenecks. Incident response is almost always a cross-functional effort that involves many teams.

The challenge is not the SASE framework itself but the fragmented way it is often implemented.

Research from the Ponemon Institute's 2025 Global Study on Closing the IT Security Gap found that 56% of organizations say managing multiple security vendors weakens their security posture, often resulting in redundant tools, inconsistent policies and operational inefficiencies. Additionally, 47% of organizations report difficulty achieving collaboration between network and security teams, reinforcing how fragmented tooling can create operational silos.

When networking and security operate across disconnected platforms, telemetry becomes fragmented, identity policies remain inconsistent and performance tuning becomes complex across multiple tools.

Moving beyond SASE means moving beyond packaging alone. It requires operational integration, shared policy logic and architectural clarity. This ensures networking and security services function as a unified system rather than a collection of separate technologies.

A PRAGMATIC BLUEPRINT FOR SECURE EDGE CONNECTIVITY

A secure edge architecture should meet five core design principles:

5 CORE DESIGN PRINCIPLES
1. Identity-first access control
2. Converged networking and security fabric
3. Policy-driven orchestration
4. Continuous visibility and telemetry
5. Operational simplicity with measurable outcomes

Let's break each one down.

Principle 1: Identity-First Access Control

Trust should never be tied to a specific location. Every connection attempt must be validated based on:

- User identity
- Device posture
- Application context
- Risk signals

Zero Trust Network Access (ZTNA) replaces traditional perimeter-based security models by verifying user identity, device posture and contextual signals before granting application access. Rather than granting broad network access, Zero Trust policies enforce least-privilege access to specific applications and services.

Identity-based access is becoming foundational to modern security architectures. According to the Ponemon Institute, 48% of organizations have already deployed universal Zero Trust Network Access (ZTNA) to enable secure application access regardless of user location.

This approach allows enterprises to securely support hybrid work, cloud-based applications and third-party collaboration without exposing the underlying network infrastructure.

As we move further into a cloud and mobile-first world, CIOs and CISOs are recognizing controlled access takes precedence over perimeter defense. Auditability and compliance alignment are priorities.

Principle 2: Converged Networking and Security Fabric

Traditional architectures treat networking and security as separate domains. However, modern distributed enterprises require these capabilities to operate as a unified fabric.

Secure Service Edge (SSE) platforms combine multiple security services—including Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Zero Trust Network Access (ZTNA), and digital experience monitoring—into a cloud-delivered security layer that protects users and applications wherever they reside. Modern platforms increasingly integrate these capabilities directly with SD-WAN infrastructure to simplify operations and improve policy consistency.

For example, HPE Networking Unified SASE integrates secure SD-WAN with cloud-native SSE services and AI-powered device intelligence into a single architecture. By replacing loosely connected solutions with a unified platform, organizations can apply consistent policies across users, devices, applications and data from the branch to the cloud.

This convergence reduces operational complexity while strengthening both network performance and security posture.

Principle 3: Policy-Driven Orchestration

Manual rule creation does not scale. Policy must be abstracted from devices and defined in business terms:

- User role
- Application category
- Geographic region
- Compliance requirement

Once defined, orchestration engines enforce policies across edges, cloud security gateways, and endpoint agents. This reduces configuration drift. It ensures global consistency and shortens change windows.

This is critical for enterprise architects as it changes security from device-centric oversight to intent-driven governance.

Principle 4: Continuous Visibility and Telemetry

Simply put, you cannot protect what you cannot see. Edge security requires real-time telemetry from:

- Network flows
- User behavior
- Endpoint posture
- Cloud workloads
- Threat intelligence feeds

Visibility is critical because most organizations still struggle to detect and respond to threats quickly across distributed environments.

Ponemon research shows that only 35% of organizations report they can recover from a cyber incident within four hours, highlighting the need for improved telemetry, faster detection capabilities, and automated response workflows.

Principle 5: Operational Simplicity with Measurable Outcomes

Security architecture must support business agility. With this in mind, key operational outcomes include:

- Faster branch deployment
- Reduced vendor count
- Lower mean time to detect and respond
- Clear executive reporting
- Improved user experience

Executives need to be able to view risk posture, SLA compliance and service adoption through real-time, enterprise-wide visualizations (that don't require manual data roll-up).

REFERENCE ARCHITECTURE: BRINGING IT TOGETHER

A practical edge security reference architecture includes:

Global Backbone Connectivity

A high capacity, low latency IP core delivers network consistency and reliability in line with cloud-first traffic patterns. No longer are you at the mercy of your local ISP with direct peering and a truly global footprint.

SD-WAN Edge

Application-aware routing for broadband, DIA, wireless and satellite links integrates with other security applications to inspect encrypted communications without degrading network speeds.

Secure Service Edge Layer

A cloud-delivered security stack enforces:

- Secure web filtering
- SaaS access controls
- Data loss prevention
- Zero trust access
- Firewall inspection

Identity and Device Integration

Integration with corporate identity providers, End Point Providers (EPPs) and endpoint security tools enables conditional policy enforcement based on the user and endpoint risk posture.

Centralized Orchestration and Digital Experience

All information is accessible through a single interface, providing immediate visibility on current network performance, security incidents and current configuration status. Policy changes are propagated to all points on the network.

Automated Threat Intelligence and Remediation

Threat feeds and vulnerability data provide an incredible amount of valuable information for security teams to leverage.

GTT + HPE

PROTECTING EVERY USER AT THE EDGE

A pragmatic blueprint must address three user categories:

HYBRID WORKFORCE	Applications are accessed from home, the office and on the move. Secure connectivity should not be tied to VPN concentrators. Zero trust and cloud inspection ensure consistent policy is enforced without having to send all traffic back to the hub.
THIRD PARTY ACCESS	Partners and third-party contractors may only need access to a small group of applications. Identity-based segmentation restricts exposure.
MACHINE AND IOT USERS	Edge compute and IoT technologies have introduced a new attack surface. Segmentation, monitoring and strong policy controls are all required to prevent laterals and mitigate risk.

Aligning NetOps and SecOps

One of the largest barriers to edge modernization is organizational. Network teams care about performance and uptime while security engineers focus on reducing risk and maintaining compliance. Separate tools just reinforce siloed efforts on all fronts. But a unified architecture reduces friction by:

- Sharing telemetry
- Aligning policy frameworks
- Centralizing reporting
- Reducing duplicate workflows

This supports collaboration rather than conflict.

Measuring Success

Modernization should produce measurable improvements across four dimensions:

Security Posture	Operational Efficiency	Performance	Financial Impact
• Reduction in exposed vulnerabilities • Reduced attack surface • Improved compliance audit readiness	• Lower vendor count • Fewer manual configuration tasks • Faster change deployment	• Improved latency to SaaS applications • Reduced packet loss • Higher SLA consistency	• Lower total cost of ownership • Reduced incident recovery cost • Optimized bandwidth utilization

Proper reporting should translate technical improvements into actionable business metrics.

MIGRATION STRATEGY: FROM FRAGMENTATION TO CONVERGENCE

Transformation should be phased.

Phase 1: Assessment

- Inventory vendors, contracts, edge devices and policy inconsistencies.
- Identify high-risk exposure points.
- Engage a trusted and knowledgeable partner.

Phase 2: Policy Alignment

- Define identity-first policies.
- Align access models across users and applications.

Phase 3: Converged Deployment

- Integrate a SASE framework (such as HPE Networking Unified SASE) with SD-WAN and an SSE stack. [DG4.1]
- Reduce appliance footprint at branch.

Phase 4: Telemetry Integration

- Unify logging and analytics.
- Establish executive reporting dashboards.

Phase 5: Continuous Optimization

- Refine policies based on user behavior, threat patterns and performance metrics.

This phased approach is optimal for reducing disruption while supporting measurable milestones to track progress.

THE ROLE OF STRATEGIC PARTNERSHIPS

Nobody wants to manage global backbone, edge devices, cloud security stack or be responsible for performing all their own vulnerability remediation.

GTT's clients enjoy a single source for networking, cloud, security and managed services. GTT operates one of the world's largest Tier 1 IP networks and covers more than 140,000 customer locations in over 170 countries. This proven scale supports consistent enforcement across distributed enterprises.

Building on the HPE Networking SSE features, enterprises will have identity-driven access control and cloud-based network security that matches the application-level performance of their SD-WAN.

CONCLUSION: MOVING BEYOND MARKET JARGON

Security at the edge is not about adopting the latest acronym; it is building an architecture that:

- Protects every user and device
- Unifies policy and enforcement
- Improves visibility
- Simplifies operations
- Supports business growth

Moving beyond just SASE involves a disciplined approach, requiring convergence at architectural, operational and governance levels. CIOs and CISOs who put integration over branding when it comes to their IT/InfoSec purchases will find themselves better equipped to manage risk, drive performance and deliver measurable value.

There's a clear path forward here: Unify -> Orchestrate -> Monitor -> Protect

For organizations planning their next phase of edge modernization, this blueprint offers a practical starting point for aligning SD-WAN, SSE through a SASE framework, a zero trust architecture and policy-driven control into one cohesive strategy.

ABOUT GTT

GTT is a leading networking and security as a service provider for multinational organizations, connecting people and machines to data and applications — anywhere in the world. We serve thousands of organizations, bringing together the right people, partners and technology to reduce the burden on IT teams and solve the most pressing networking and security challenges.

Built on our top-ranked global Tier 1 network, the GTT Envision platform provides visibility, insights, orchestration and control, enabling customers with consumable solutions to achieve business missions and meet ongoing demand when, where and how needed. Our portfolio includes SASE, SD-WAN, security, internet, voice and other connectivity options, complemented by a suite of professional services and exceptional sales and support teams in local markets around the globe. We partner with our customers to deliver Greater Technology Together.

HPE Networking delivers secure, AI-powered edge-to-cloud networking solutions, now tightly integrated into HPE's GreenLake edge-to-cloud platform. With the acquisition of Axis Security in 2023, HPE Networking launched Unified SASE, combining SD-Branch, SSE, and ZTNA under a single architecture, aiming to simplify secure connectivity across hybrid workforces and distributed enterprises

For more information, visit **gtt.net**

GTT + HPE

SASE/SecCon_WtPaper_GGMCM-3480_v3_06082026