VERSA

SOLUTION BRIEF

Sovereign SASE Explained

Complete SASE. Sovereign by Design.

The Challenge

Enterprises are increasingly required to demonstrate sovereignty — not just protection of data, but control over how users connect, how traffic is inspected, and how security and networking platforms are operated.

Some organizations have begun moving workloads into regional or sovereign cloud environments. However, networking and security services often remain globally operated. Even when infrastructure appears local, access decisions, security processing, or platform management may still depend on systems outside the intended operating environment.

This creates a gap between sovereignty expectations and how security is delivered. Sovereignty is no longer only about where data resides; it also depends on who controls access, inspection, and management.

What Is Sovereign SASE?

Sovereign SASE extends Secure Access Service Edge (SASE) by incorporating sovereignty controls into the networking and security architecture.

It delivers SASE capabilities while ensuring that the systems responsible for connectivity, enforcement, and operations align with defined operating boundaries.

A Sovereign SASE architecture ensures that access decisions, traffic inspection, and platform management function together across the control, data, and management planes in the same operating environment. Sovereignty depends on all three layers working together consistently.

Why Traditional Shared SASE Isn't Enough

Traditional shared SASE platforms were designed for global scale and centralized service delivery. These architectures rely on shared infrastructure and globally operated control and management systems.

Users may connect through nearby Points of Presence (PoPs), but the presence of an in-region PoP does not mean all security processing occurs locally. In many shared SASE environments, functions such as threat protection, analytics, or portions of inspection workflows are handled in centralized locations elsewhere.

When traffic leaves the local environment for inspection or analysis, enforcement is no longer locally governed and sovereignty expectations are not fully met. This model can also introduce traffic hairpinning, where traffic is redirected to centralized processing systems, increasing latency and affecting performance.

Shared SASE architectures were built around centralized processing models rather than localized operational control.

Why Many Sovereign SASE Approaches Still Fall Short

In response to sovereignty requirements, some providers have introduced regional or sovereign variations of SASE by deploying local PoPs or isolating portions of infrastructure.

These approaches improve traffic locality but often address only where traffic enters the network. Security processing, policy evaluation, or operational workflows may still rely on globally shared platforms.

If threat protection, analytics, or policy enforcement occur outside the intended environment, sovereignty objectives remain incomplete. These architectures may also continue to depend on traffic redirection for certain functions, resulting in the same hairpinning and performance impacts seen in shared SASE models.

Sovereign SASE requires alignment across the control plane, data plane, and management plane. Localizing only parts of the architecture does not fully establish control over access decisions and platform operations.

Key Requirements for Sovereign SASE

SASE deployments can be evaluated against requirements that address the control, data, and management planes together.

Localized Access Control (Control Plane)

Access decisions should occur within the sovereign environment. Identity validation, policy evaluation, and connection decisions should not rely on globally shared control systems outside the intended operating boundary.

Localized Traffic Inspection (Data Plane)

Traffic inspection and protection functions — including threat prevention and traffic analysis — should occur at sovereign Points of Presence without redirecting traffic to external processing environments.

Localized Platform Management (Management Plane)

Administration, monitoring, logging, configuration, and operational access should remain locally governed so platform oversight stays aligned with sovereignty expectations. This includes both customer administration and vendor operational access, avoiding dependence on centralized global management systems.

Service Delivery and Legal Operating Model

Technical architecture alone does not determine whether a deployment meets sovereignty expectations. Organizations may also evaluate how the service is legally provided and operated, including which regional legal entity delivers the service and how operational responsibility is structured. Alignment between deployment architecture and the service operating model helps ensure governance and service delivery remain consistent with sovereignty objectives.

Full SASE Capability (Across All Planes)

A Sovereign SASE solution includes core SASE capabilities such as SD-WAN connectivity, Zero Trust Network Access, Firewall as a Service, Secure Web Gateway, and unified policy and visibility operating across the control, data, and management planes.

Versa Sovereign SASE

Versa Sovereign SASE delivers full SASE capabilities with sovereignty incorporated into the platform architecture.

Access decisions, traffic inspection, and security processing remain localized, while platform management and operations align with the intended operating model.

By addressing the data, control, and management planes together — and avoiding reliance on external inspection or management environments — Versa Sovereign SASE removes the gaps created when only portions of a SASE architecture are localized.

Versa Networks, Inc, 2550 Great America Way, Suite 350, Santa Clara, CA 95054
Tel: +1 408.385.7660 | Email: info@versa-networks.com | Website: www.versa-networks.com