Versa Sovereign SASE

Overview

"Sovereign SASE" has become a crowded label, with vendors marketing data residency as sovereignty when the two are not the same. This guide defines what sovereignty requires and shows how Versa Sovereign SASE is purpose-built to deliver it.

Sovereignty encompasses who controls access to data, services, inspection, and management, and under whose law the service operates. Meeting it takes more than keeping data in-region. Sovereignty spans four distinct planes: data, control, management, and jurisdiction. A gap in any one compromises sovereignty.

Versa treats sovereignty as an architecture, not a contractual assurance, and builds it directly into the VersaONE Universal SASE Platform through its Sovereign SASE solution across all four planes

Versa Sovereign SASE Key Benefits

- **In-region inspection.** Traffic inspection, threat prevention, and DLP run at in-country points of presence. No traffic is processed outside the region.
- **Local access decisions.** Identity validation, traffic forwarding engines, and the zero-trust policy engine run inside the sovereign environment. No dependency on external control infrastructure.
- **Exclusive management authority.** Configuration, logging, and telemetry stay under customer or authorized-sovereign-entity control. Vendor support is brokered through in-jurisdiction PAM.
- **Jurisdictional containment.** Locally domiciled contracting entity and operator keeps services under local law, reducing exposure to extraterritorial legal reach.

The Versa Sovereignty Model: Sovereignty Across Four Planes

Versa treats sovereignty as an architectural property that must hold across four distinct planes: data, control, management, and jurisdiction. Each is necessary, and none is sufficient on its own. Data residency addresses only where information sits. Genuine sovereignty goes further than data residency, considering where traffic is inspected, who decides access, who administers the platform, and under whose law the service operates.

Versa Sovereign SASE addresses all four on a single platform, the VersaONE Universal SASE Platform:

- **Data plane.** Performs traffic decryption/encryption; traffic inspection to provide threat prevention; content filtering; and data loss protection (DLP). Sovereignty requires these functions to execute at in-region points of presence, physically and legally within the jurisdiction, with no traffic hairpinned outside the boundary for processing.
- **Control plane.** Includes identity validation, traffic forwarding, policy evaluation, and access decisions, as well as the zero-trust policy engine that decides who can access what. Sovereignty requires these services to run inside the sovereign environment without dependency on external infrastructure, so no outside party can reach access policy through the control plane.
- **Management plane.** Includes configuration, logging, telemetry, and administrative control. Sovereignty requires these to stay under exclusive customer or authorized-sovereign-entity authority, with vendor support brokered through an in-jurisdiction privileged access management (PAM) system. Operators outside the jurisdiction should not be able to reach the tenant directly.
- **Jurisdiction plane.** Includes corporate ownership, operational control, and the legal basis under which the service runs. Sovereignty requires the service to be governed by and operated under local law through a contracting entity legally domiciled in-jurisdiction, restricting the reach of foreign legal regimes to the services, configuration, and operational data.

Plane	Sovereignty components
Data	Inspection and data protection execute in-jurisdiction; no out-of-region processing
Control	Identity, forwarding engine and policy engine run in-boundary; no external dependency
Management	Configuration, logs, and RBAC under exclusive local authority; support brokered in-jurisdiction
Jurisdiction	Contracting entity and operator domiciled locally; service under local law

Versa's model aligns with the plane-based view of Sovereign SASE that Gartner sets out in its 2026 Critical Capabilities for SASE Platforms and goes further by holding each plane to a specific sovereignty test.

The following sections discuss each plane as an architecture layer in more detail, with mappings to Versa components and roles.

Sovereign jurisdictional boundary: For Sovereign SASE the scope of the boundary pertains to where data is stored and processed by the SASE service. The boundary governs Versa's processing footprint, not where the connecting user happens to be sitting. So, for example a user in the US connecting to a Versa Sovereign SASE Gateway, hosted in a sovereign jurisdictional boundary within the EU, would be compliant provided their connection processing is handled according to Sovereign procedures across all functional planes.

Data Plane: Traffic Decryption, Inspection and Enforcement

The data-plane handles inspection and provides protection features at Versa Gateways, all within points-of-presence (PoP) physically and legally within the jurisdiction. Encrypted traffic is routed or steered to gateways through the control plane by customer-controlled policies and processing stays inside the boundary, even for security functions.

Versa sovereignty checkpoints:

- Inline inspection and threat prevention terminate at in-region PoPs.
- Content filtering and DLP evaluate decrypted content without leaving sovereign boundaries.
- Encryption and decryption occur locally, with key custody held in-region.

Architecture

In the Versa data plane, traffic from remote users, branches, campuses, and data-center gateways is steered to an in-region PoP. There, Versa decrypts the traffic using certificates managed under sovereign processes. The Versa Operating System (VOS), the single-pass software engine that runs Versa's networking and security functions, then applies its full security stack: it inspects each packet with every enabled engine and re-encrypts it, without redirecting traffic to separate services or regions.

All security inspection engines part of Versa Security Service Edge follow this sovereign approach. This includes: NGFW and IPS for network threat prevention, SWG for web and content control, CASB for SaaS governance, DLP for sensitive-data control, Advanced Threat Protection (ATP) with dynamic sandboxing, and Remote Browser Isolation (RBI). These services run inline at the same enforcement point, so decrypted content, threat-analysis payloads, and DLP inspection are kept inside sovereign boundaries. Cleaned, policy-enforced traffic then egresses to the Internet, SaaS, or private applications from within the region, and the return path is re-inspected on the same pass.

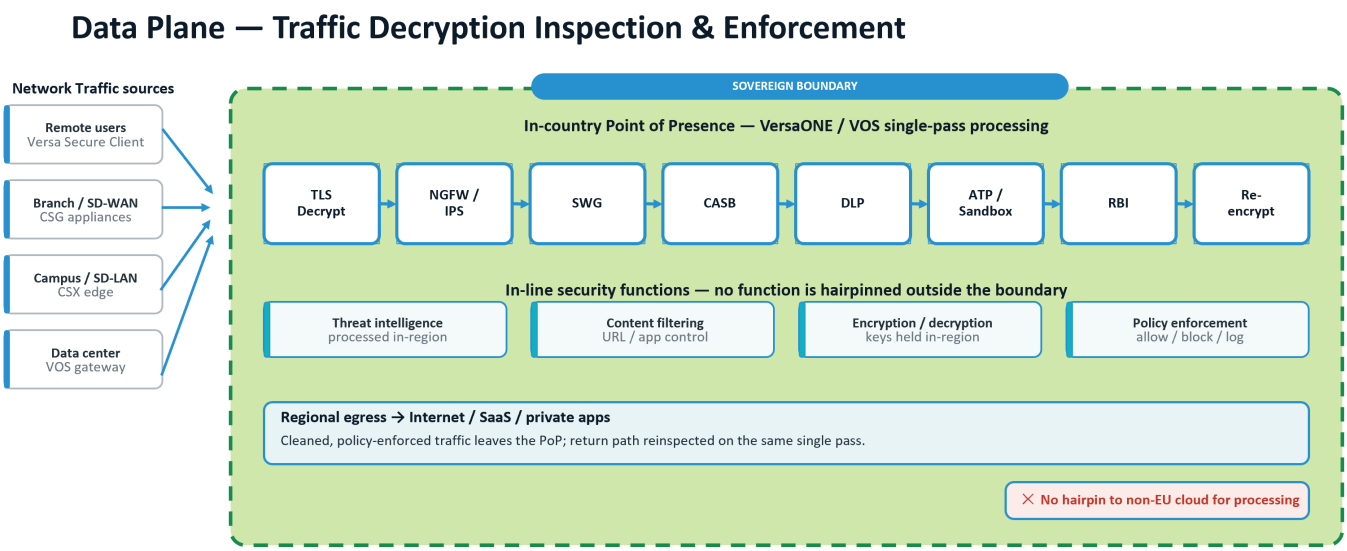

Figure 1. Data-plane architecture: single-pass VOS inspection at an in-country PoP; no out-of-region processing.

Architecture

Function	Versa components and roles
Traffic inspection	Inline decryption → inspection → re-encryption at in-region PoP
Threat prevention	NGFW, IPS, ATP and sandboxing, executed locally
Content filtering	SWG for URL, category, and application control; RBI for isolating risky browsing sessions
Data protection	DLP on decrypted content and CASB for cloud application control, all in-boundary

Sovereignty red flag: Sovereignty breaks when any inspection, service, or function is sent to an out-of-region cloud for processing, even when storage remains local.

Control Plane: Access and Policy Decisions

Sovereignty requirement

The control plane encompasses identity validation, routing and steering, policy evaluation, and access decisions. This also includes the zero trust policy engine that decides who can access what. If any component of the orchestration layer, policy store, or identity-verification system sits outside the sovereign boundary, access decisions are effectively made by or through infrastructure in another jurisdiction. A US court order compelling a US-operated orchestration service to alter or expose access policy could then reach the sovereign environment through the control plane, even if data never leaves the region.

Versa sovereignty checkpoints:

- Identity validation and the policy engine execute inside the boundary.
- Routing and steering engine operates inside the boundary
- The policy store and session/token issuance reside in-region.
- No external control dependency is required for the service to make access decisions.

Architecture

Versa's control plane centers on its zero trust access model. Versa Zero Trust Network Access (ZTNA) brokers per-session access based on identity, device posture, application, and risk context. In the sovereign reference design, identity validation federates to the customer's own identity provider, but the assertions are consumed in-region and the access decision itself is not delegated to any out-of-jurisdiction service.

Versa's control plane also may include SD-WAN controllers which provide distributed routing via secure tunnels to Versa Operating System (VOS) appliances hosted in data centers or customer sites. They operate primarily as multi-tenant MP-BGP route reflectors, authenticating sites, distributing routes, and topology information. VOS sites consume this information to dynamically construct encrypted site-to-site data tunnels, with a variety of path performance enhancements including real-time SLA measurement, application identification, and traffic steering.

Policy evaluation runs against an in-region policy store, and the sovereign orchestration control that distributes policy, Versa's unified management console, is deployed inside the boundary rather than as a shared external service. Therefore every function of the control plane remains within sovereign boundaries

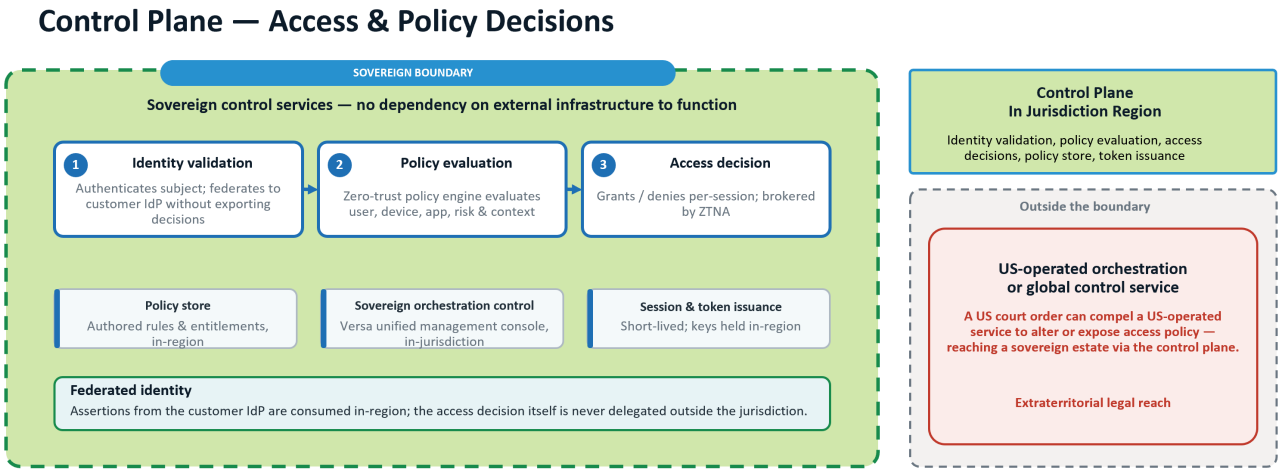

Figure 2. Control-plane architecture: identity, policy eval, and access decisions contained in-boundary; extraterritorial reach has no dependency to exploit.

Control Plane - Versa capabilities

Function	Versa components and roles
Identity validation	Consumes IdP assertions in-region; access decisions stays local
Routing and traffic steering	Encrypted user flows are directed to gateways for decryption, inspection and policy enforcement through Versa SD-WAN and ZTNA forwarding engines
Endpoint posture evaluation	Versa collects endpoint information and reports posture to the gateway for evaluation against EIP policies
Policy evaluation	A single ZTNA policy engine scores user, device, application, and risk against an in-region policy store
Access decisions	Per-session grant or deny for private applications, internet, or SaaS destinations enforced in-boundary
Policy distribution	Versa's unified management console distributes policy to in-region enforcement points, keeping decisions in-boundary

Sovereignty red flag: Sovereignty breaks if the routing, traffic steering, forwarding engines, policy store, orchestration, or identity verification runs outside the boundary, as access decisions can be reached or altered through that external infrastructure.

Management Plane: Configuration and Administration

Sovereignty requirement

The management plane does logging, configuration, telemetry, and role-based access control (RBAC) that remain under exclusive customer or authorized-sovereign-entity authority. Tenant configuration, security policies, user access rules, and network topology should reside within the boundary and be accessible only to explicitly authorized parties. Vendor support access must be brokered through in-jurisdiction enforcement points, because if a vendor's operations team can reach the management plane from outside the jurisdiction, even temporarily, the management plane is not completely sovereign.

Versa sovereignty checkpoints:

- Configuration, logging, telemetry, and RBAC stay under local authority.
- Encryption-key life cycle and log storage remain in-region.
- Vendor support is brokered via in-jurisdiction PAM, MFA, time-bound windows, session recording, credential vaulting.

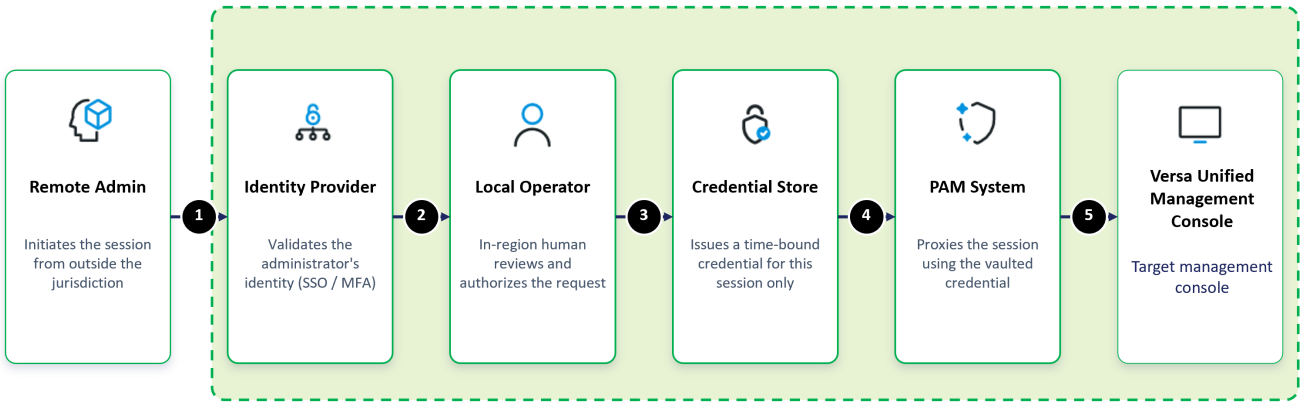

Figure 3. Vendor support access flow: remote admin session authorized in-region and proxied through the PAM broker; no direct access.

Architecture

Versa's management plane is delivered by Versa's unified management console, which provides orchestration, policy configuration, and life cycle management, along with logging, telemetry, and reporting. In the sovereign reference design, these run inside the boundary, so configuration and logs are stored in-region and RBAC is administered against an in-region identity source. Encryption-key generation, rotation, and custody are handled locally.

A key piece of management plane sovereignty is how support access is handled. Here, Versa takes a deliberately different approach. Rather than granting vendor operators direct administrative access, Versa brokers all privileged access through an in-jurisdiction privileged access management (PAM) system, with mandatory MFA, time-bound access windows, and session recording stored in-region. Credential vaulting ensures out-of-region operators never hold plaintext credentials. The intent is that even legitimate vendor support cannot reach the management plane from outside the jurisdiction except through this in-boundary broker.

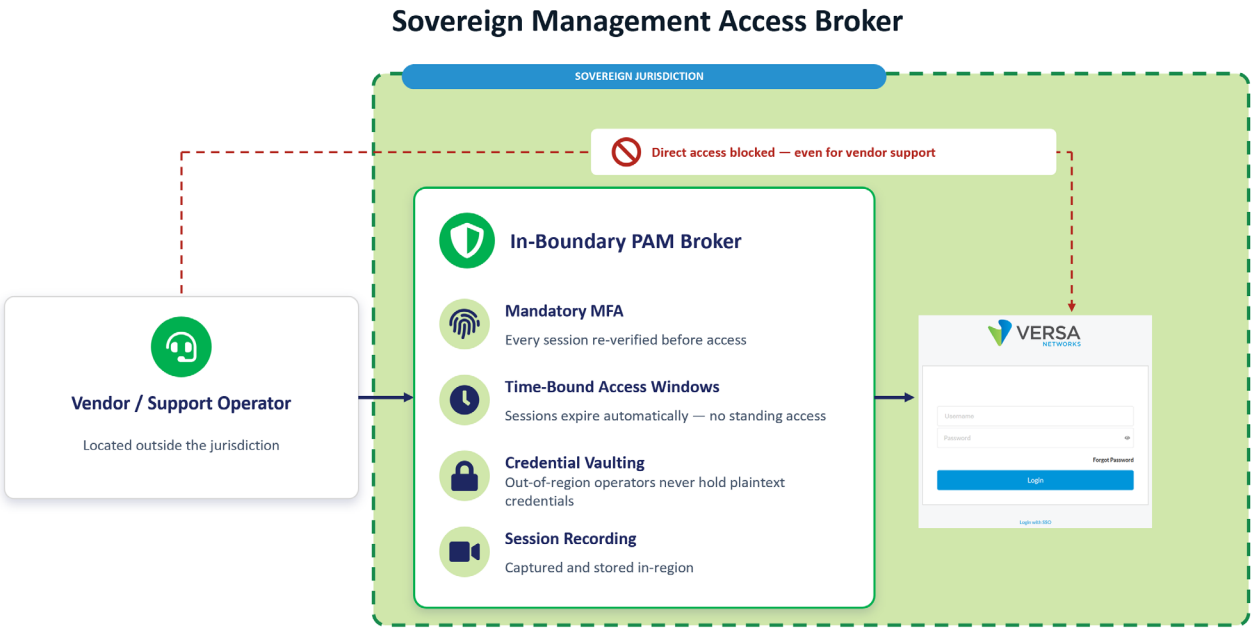

Figure 3. Vendor support access flow: remote admin session authorized in-region and proxied through the PAM broker; no direct access.

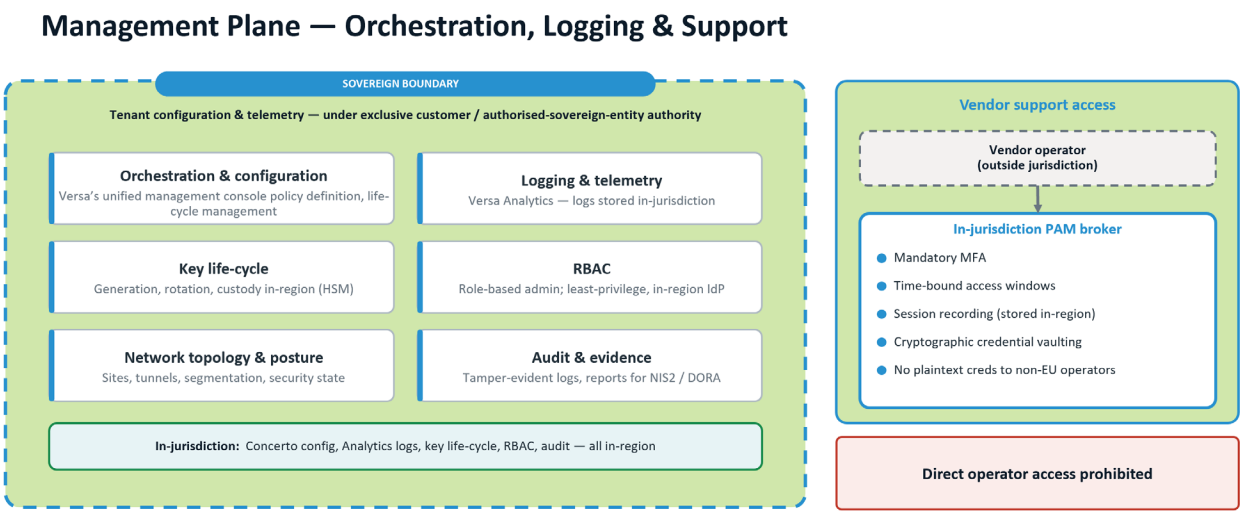

Figure 5. Management-plane architecture: configuration, logging, keys, and RBAC in-boundary; vendor support brokered through in-jurisdiction PAM.

Control Plane - Versa capabilities

Function	Versa components and roles
Configuration	Versa's unified management console handles policy authoring and lifecycle management, in-region
Logging	Logs and audit records captured and stored in-jurisdiction through the platform
Telemetry	Operational telemetry and reporting kept in-region
Administrative control	Least-privilege RBAC against an in-region IdP; vendor support brokered through an in-jurisdiction PAM system

Sovereignty red flag: Sovereignty breaks if a vendor operations team can administer the tenant, read logs, or hold plaintext credentials from outside the jurisdiction.

Jurisdiction: Legal and Operational Sovereignty

Sovereignty requirement

Jurisdiction is the dimension architecture cannot resolve on its own. The service must be governed by and operated under applicable local law, and the contracting entity must be legally domiciled within the jurisdiction. The risk comes from foreign regulations, such as the US CLOUD Act, that can compel providers domiciled in their country to produce data in their control, regardless of where it is physically stored. The key phrase is "in their control." If a foreign-headquartered vendor operates the control plane, the management plane, or the support-access infrastructure, even from an in-region data center, that infrastructure remains within potential reach of foreign law. The EU Cloud Sovereignty Framework names the CLOUD Act explicitly under its SOV-2 (Legal and Jurisdictional Sovereignty) objective as a scored evaluation criterion.

Versa sovereignty checkpoints:

- The service is governed by and operated under applicable local (EU / national) law.
- The contracting entity is legally domiciled within the jurisdiction.
- No foreign legal regime can compel access to the service, its configuration, metadata, or operational data through the vendor.

Structure

Versa's approach to the jurisdiction dimension is structural. For its EU sovereign service, contracts are executed through Versa Networks B.V., a Netherlands-domiciled EU legal entity. Service is operated from redundant ISO 27001-certified facilities run by a Sovereign SASE service provider in Germany, under EU and German law. These entities holding operational control are domiciled in-jurisdiction, removing the basis of control that regulations including the CLOUD Act rely upon.

The diagram places this legal and operational stack inside the sovereign boundary and shows foreign legal reach, such as the CLOUD Act, blocked at the boundary because no in-control vendor dependency crosses it. The right-hand panel maps the resulting assurances to the frameworks EU buyers are assessed against. Versa provides complete VersaONE feature parity across its Sovereign SASE tiers, including VersaAI processing kept within jurisdiction.

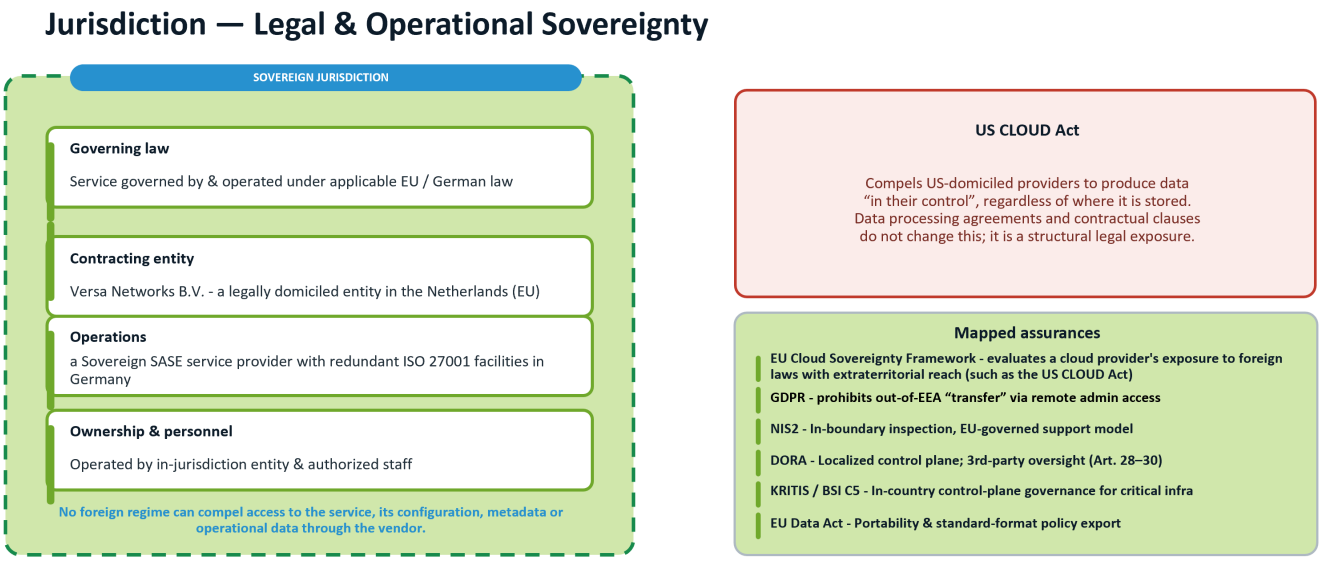

Figure 6. Jurisdiction: EU-domiciled contracting and in-country operations under local law; foreign legal reach blocked.

Jurisdiction – Mapped Versa approach

Function	Versa components and roles
Corporate ownership	Contracting through Versa Networks B.V., Versa's Netherlands-based EU legal entity
Logging	Operated under EU and national law by a sovereign SASE service provider running ISO 27001-certified facilities in Germany
Legal basis	Governed under applicable EU and national law

Sovereignty red flag: Sovereignty breaks if any plane or the support-access path is controlled by a provider based in a foreign jurisdiction. Customer data and environments then stay within reach of foreign law through the vendor, an exposure that contractual assurances alone cannot close.

Sovereignty for Each Tier

Versa offers its sovereignty controls as a spectrum on the VersaONE platform, so organizations can pick a tier based on their sovereignty needs and migrate without re-architecting. The tiers serve enterprises, service providers, and governments, with typical fits mapped below.

Tier	What it is	Sovereignty characteristics	Typical fit
Unified SASE	Shared, global cloud SASE	Data residency options on shared infrastructure	General enterprise, lowest operational overhead
Private SASE	Dedicated, single-customer gateways	Isolation from multi-tenant infrastructure	Regulated enterprises needing dedicated tenancy
Sovereign SASE-as-a-Service	Managed service in-region (e.g., by a Sovereign SASE service provider)	All four planes governed in-jurisdiction under an EU entity	EU enterprises requiring full-stack sovereignty
Sovereign SASE On-Premises	Customer or partner-hosted, air-gap capable	Full architectural and operational control	Government, defense, critical infrastructure

Regulatory & Framework Mapping

The four-plane model is intended to support the obligations typical buyers are assessed against. The mapping below is a general guide. Customers should validate each control against their specific deployment and legal review.

Framework	What it emphasizes	How Versa responds
EU Cloud Sovereignty Framework	Flags foreign-government access, such as the US CLOUD Act, as a scored risk (SOV-2: Legal and Jurisdictional Sovereignty)	Jurisdiction plane: locally domiciled entity and in-country operations
GDPR / EU Data Act	Treats remote access from outside the region (EEA) as a data transfer; requires portability	Management plane: in-region administration and logs, with support brokered through in-region access controls (PAM)
NIS2	Requires in-region inspection, tamper-evident logs, and locally governed support	Data and management planes: local inspection and log storage
DORA	Requires a local control plane and oversight of third-party providers (Art. 28–30)	Control plane in-boundary, under a local (EU) contracting entity
KRITIS / BSI C5	Requires in-country governance of controls for critical infrastructure	Control and management planes governed in-region (Germany / EU)

To see how Versa Sovereign SASE fits your sovereignty requirements, visit versa-networks.com/products/sovereign-sase/ or reach out to your Versa sales representative.

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

About Versa

Versa, the global leader in unified networking and security, enables organizations to create self-protecting networks that radically simplify and automate their network and security infrastructure. Powered by AI, the VersaONE Universal SASE Platform delivers converged SSE, SD-WAN, and SD-LAN solutions that protect data and defend against cyberthreats while providing a superior digital experience. Thousands of customers globally, with hundreds of thousands of sites and millions of users, trust Versa with their mission-critical networks and security. Versa is privately held and funded by investors such as Sequoia Capital, Mayfield, and BlackRock. For more information, visit https://www.versa-networks.com and follow Versa on LinkedIn and X (Twitter) @versanetworks.