VERSATILITY

Versa Sovereign SASE

SASE solutions that meet sovereignty requirements

Anuj Dutia

VP Global Solutions

Prasad T

Field CISO

Topics

Versa SASE Flavors Overview

What’s New – Sovereign SASE as a Service

Why Sovereign Security Is a Board Mandate?

What Every Compliance Framework Demands

How Versa SASE Delivers Global Sovereign Compliance

Sovereign SASE competitive landscape

Sovereign SASE Use Case Review

VERSATILITY

Versa SASE Flavors

Versa SASE-as-a-Service ™

- Versa Infrastructure
- Versa Operations

Versa Sovereign SASE ™ - SaaS

- Versa Infrastructure
- Your Jurisdictions
- Versa Operations

NEW

Versa Sovereign SASE™

- Your Infrastructure
- Your Jurisdictions
- Your Operations

Sovereign SASE flavors – Summary of Deployment Models

Component	Sovereign SASE as a Service	Sovereign SASE On Premises
SASE Gateway & Management	VERSA	Enterprise/MSP
Hosting infrastructure (*Hardware, datacenter, cloud, network*)	VERSA	Enterprise/MSP
Deployment model	Shared Sovereign Cloud	Dedicated on premises gateway
Enterprise / End User Management	Enterprise / MSP	Enterprise / MSP
Software & Service Components	SASE Gateway	SASE Gateway & SASE HE

Full Universal SASE Stack

Core Features

- Stateful Firewall (Layer 3 & 4)
- Deep Packet Inspection (DPI)
- Zero Trust Access for Private Apps
- Reputation and Filtering (File, URL & IP)
- Antivirus
- Malware Protection
- Inline DLP
- Inline CASB

Add-ons*

- Advanced Threat Protection (ATP)
- Advanced DLP
- Remote Browser Isolation
- API based CASB

VERSATILITY

Sovereign SASE Consumption Models

Versa SASE service delivered from locally deployed shared SASE Gateways & controllers hosted and managed by Versa

Sovereign SASE as a Service (Dedicated)

Versa SASE service delivered from locally deployed Sovereign SASE Gateways & controllers hosted and managed by Versa

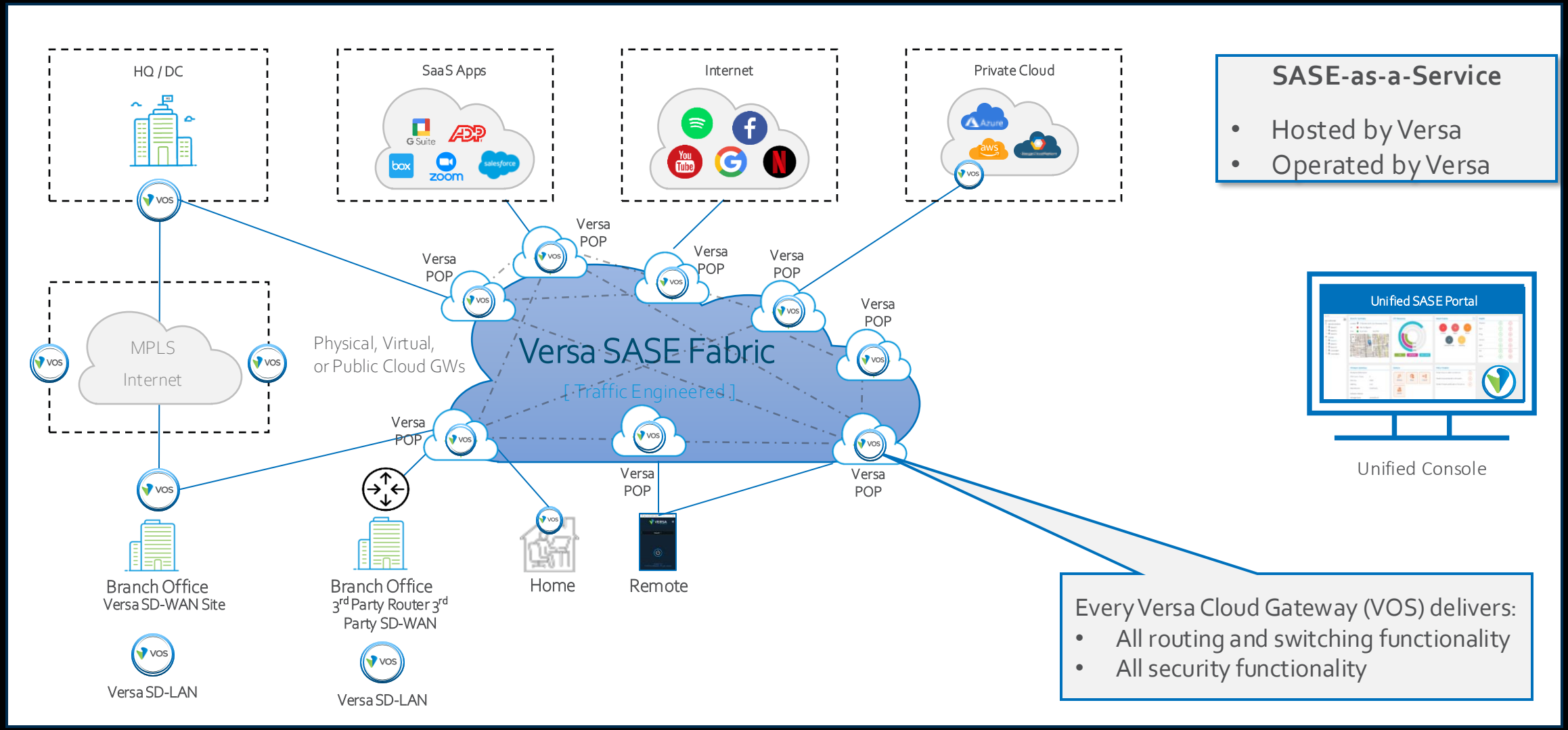
Sovereign SASE as a Service (Multi-tenant)

Full ownership of SASE gateways and data plane for regulatory, government, or military-grade requirements

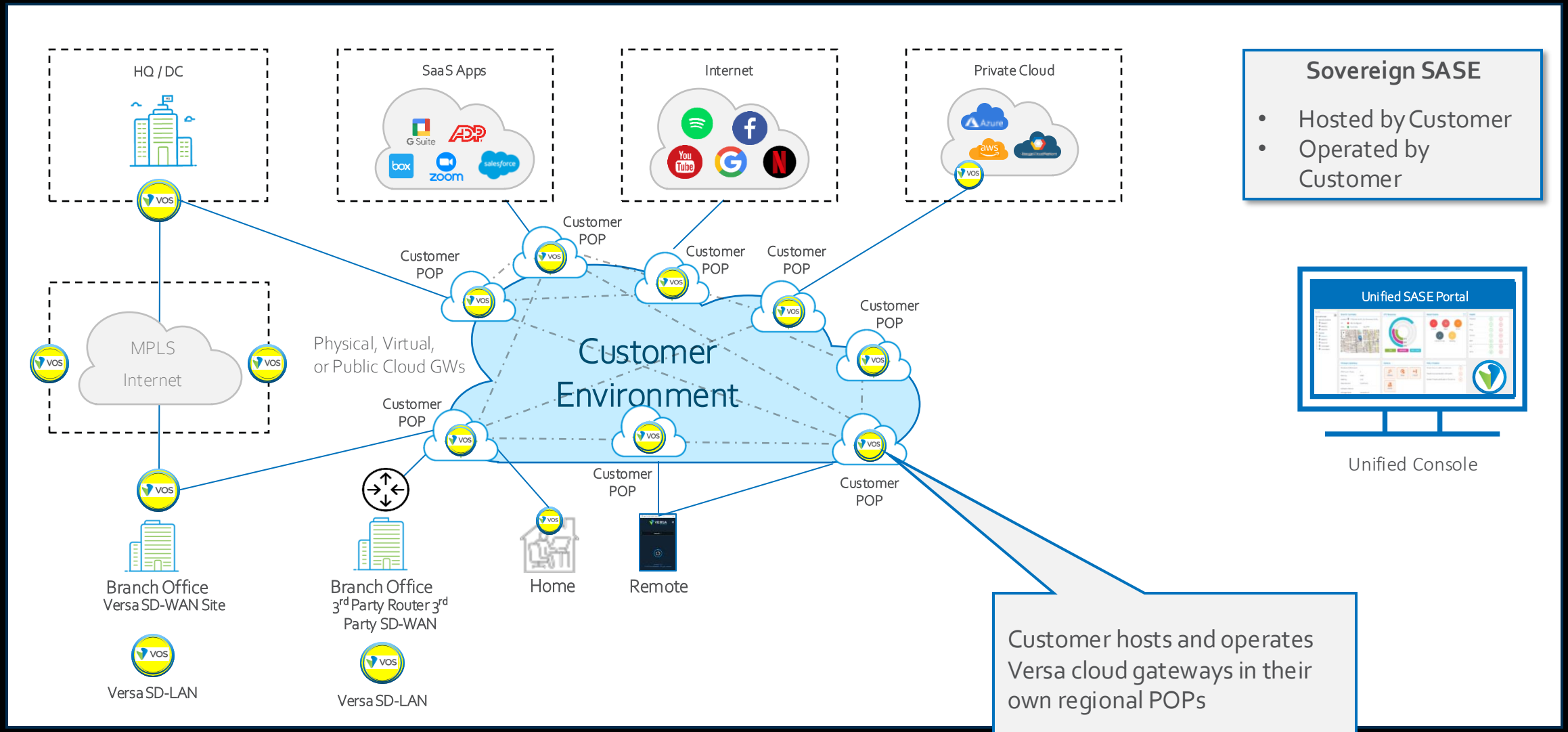
Sovereign SASE

VERSATILITY

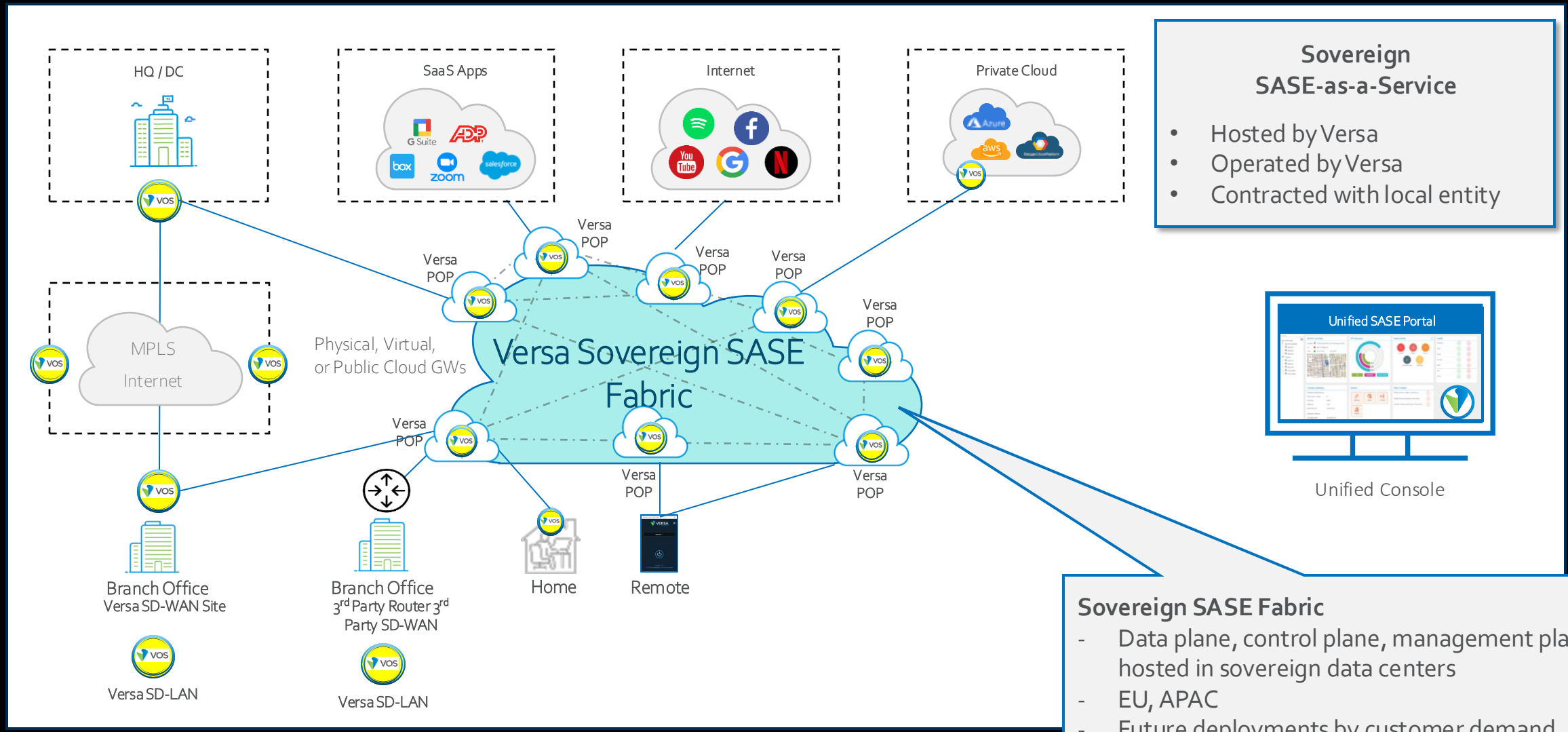
Versa SASE as a Service *(Versa Cloud Delivered)*



Versa Sovereign SASE *(Your Infrastructure)*



Versa Sovereign SASE as a Service



Sovereign SASE-as-a-Service

- Hosted by Versa
- Operated by Versa
- Contracted with local entity

Unified Console

Sovereign SASE Fabric

- Data plane, control plane, management plane all hosted in sovereign data centers
- EU, APAC
- Future deployments by customer demand

Sovereign

SASE

Compliance, Governance & Architectural Control
for a Regulated Global Enterprise

"Sovereignty is not where your data sits …
it is where control, enforcement, and accountability truly reside."

GDPR	CCPA / CPRA	HIPAA	ISO 27001	NIST CSF 2.0	EU AI Act

VERSATILITY

The Compliance Pressure: Why Sovereign Security Is a Board Mandate

Regulators across every region are tightening sovereignty requirements — and penalties are existential

GDPR
European Union

- Data residency & cross-border controls
- Processing accountability (Art.5, 25)
- Fines up to €20M or 4% global revenue
- 72-hour breach notification

CCPA / CPRA
California / USA

- Consumer data rights & opt-out
- Purpose limitation on data use
- $7,500 per intentional violation
- Mandatory risk assessments (CPRA)

HIPAA
United States

- PHI confidentiality & integrity
- Access control & audit controls
- BAA requirements for vendors
- Penalties: $100–$1.9M per category

ISO 27001
International

- Risk-based information security
- Supplier & third-party governance
- Continuous improvement mandate
- Annex A controls (A.5 – A.18)

NIST CSF 2.0
United States / Global

- Govern → Identify → Protect → Detect
- Respond and Recover functions
- GV.OC: organisational context
- DE.CM: continuous monitoring

EU AI Act
European Union

- AI system transparency (Art.13)
- Human oversight requirements (Art.14)
- Logging of AI-driven decisions
- Fines up to 6% global turnover

VERSATILITY

What Every Compliance Framework Demands: Four Universal Obligations

Strip away jurisdiction-specific language — every regulation converges on these four control themes

01

Data Control & Residency

Data must stay within defined sovereign boundaries. Cross-border transfers require explicit legal basis. Purpose limitation and minimisation apply.

GDPR Art.5,44-49 · HIPAA §164.312 · CCPA §1798

02

Auditability & Transparency

All actions — human and machine — must be logged, timestamped, and accessible to the data controller. AI decisions require explainability.

GDPR Art.30 · CCPA §999.317 · EU AI Act Art.13-14 · NIST DE.CM

03

Access Control & Governance

Least-privilege access enforced at every layer. Vendor boundaries defined and auditable. Identity-aware policy, role-based controls, BAA/DPA agreements.

HIPAA §164.308 · ISO 27001 A.9 · NIST PR.AC · SOC 2 CC6

04

Accountability & Jurisdiction

Operations governed by designated law. Conformity assessments for AI. Incident response within mandated SLAs. Third-party risk owned by the controller.

GDPR SCCs · EU AI Act Art.9,17 · NIST GV.OC · ISO A.15

These four obligations are universal — they apply regardless of which framework governs your organisation.

VERSATILITY

VERSATILITY

Versa's Architectural Answer: Five Sovereign Control Pillars

Sovereignty requires ALL five layers under compliant control simultaneously — not just data storage

Each pillar directly addresses one or more of the Four Universal Obligations

01

Sovereign Data Inspection & Policy Enforcement

In-region TLS inspection, DLP, and CASB inline. Data never exits the sovereign boundary for processing. No shared inspection PoP.

Obligations 1 + 2

GDPR · HIPAA

02

Sovereign Control & Management

Customer-owned orchestration and control plane. Vendor access scoped, role-restricted, and fully auditable against SLA boundaries.

Obligations 2 + 3

ISO 27001 · NIST

03

Sovereign Data & Log Storage

Logs, flow records, and metadata retained in-region. Customer-controlled encryption keys (BYOK). No shared log plane or telemetry egress.

Obligations 1 + 2

GDPR · CCPA

04

Sovereign Operations Center

Security monitoring and incident response by regionally-cleared personnel. SOC access gated, role-controlled, and audit-logged end-to-end.

Obligation 3

SOC 2 · HIPAA

05

Sovereign Jurisdiction & Legal Boundary

Operations governed by designated national or regional law. Contracts aligned to SCCs, adequacy decisions, and local data protection authority requirements.

Obligation 4

GDPR · EU AI Act

VERSATILITY

Key point: Most vendors satisfy 1–2 pillars. Versa delivers all five — on a single unified platform.

VERSATILITY

How Versa Delivers Sovereignty: Three Deployment Models

Same unified Versa VOS platform — three distinct sovereignty postures to match your regulatory requirement

VERSATILITY

Model 1

Sovereign SASE as a Service — Dedicated

Dedicated SASE Gateways and Controllers, locally deployed and managed by Versa within the customer's sovereign region. Full tenant isolation — no shared infrastructure.

Best fit:

Regulated enterprises requiring data residency and managed ops without owning infrastructure

Data Inspection ✓· Control & Management ✓· Log Storage ✓· Operations Center ✓· Jurisdiction ✓ (Versa-managed, within sovereign boundary)

Model 2

Sovereign SASE as a Service — Multi-tenant

Locally deployed Sovereign SASE Gateways and Controllers hosted by Versa in a sovereign regional PoP. Shared infrastructure — sovereign data boundary maintained per tenant.

Best fit:

Organisations needing sovereign data plane and operational scale without dedicated infrastructure

Data Inspection ✓· Log Storage ✓· Jurisdiction ✓ | Control & Management (partial) | Operations Center (regionally scoped)

Model 3

Sovereign SASE — Full Customer Ownership

Customer or partner owns and operates all SASE Gateways, Controllers, and the complete data plane. Designed for government, defence, or military-grade sovereign requirements. Full air-gap capable.

Best fit:

Government, Defence, Critical National Infrastructure — highest security classification or regulatory requirement

All five pillars ✓✓— Data Inspection · Control & Management · Log Storage · Operations Center · Jurisdiction — customer owns every layer

All three models run on Versa VOS — the same unified platform, adapting to your sovereignty posture without re-architecture.

Versa SASE Delivers Global Sovereign Compliance

Every compliance obligation traceable to an enforced architectural control — audit-ready, by design

VERSATILITY

Regulation	Obligation	Sovereign Pillar	Versa Control (Governance · Accountability · Jurisdiction called out)	Evidence for Auditors
GDPR / CCPA	Data residency, cross-border controls & consumer data rights	**Data Inspection · Jurisdiction**	In-region TLS inspection; no egress to shared PoP. CCPA: data subject rights honoured via access-controlled log plane. Jurisdiction: SCCs / adequacy decisions. Accountability: DPA names Versa as processor.	*Data flow map, DPA/SCCs, consumer rights log, inspection records*
GDPR / CCPA	Audit logs & processing transparency	**Control & Management · Log Storage**	Governance: customer-accessible audit trails; immutable log chain. Log Storage: in-region, BYOK encryption. Accountability: processing register maintained.	*Log retention policy, access records, encryption key audit*
HIPAA	PHI access control, BAA, transmission security	**Data Inspection · Operations Center**	Identity-aware policy; RBAC enforced inline. Operations Center: SOC staffed by cleared analysts. Accountability: BAA-ready architecture; signed BAA with customer.	*BAA, RBAC config, SOC access logs, session records*
ISO 27001	Third-party governance & vendor risk	**Control & Management**	Governance: customer-owned orchestration; vendor access SLA-bounded and auditable. Accountability: supplier risk register; Annex A.15 controls documented.	*Vendor access logs, SLA evidence, control plane config*
NIST CSF 2.0	Govern, detect, respond, continuous monitoring	**Control & Management · Operations Center**	Governance (GV.OC): policy-driven architecture with defined roles. Operations Center: regional SOC; SIEM-integrated; continuous monitoring. Accountability: governance dashboards.	*SOC runbooks, SIEM logs, governance reports*
EU AI Act	AI transparency, human oversight, decision logging	**Control & Management · Jurisdiction**	Governance: observable ML pipeline; every AI decision logged. Accountability: human override enforced; conformity assessment documented. Jurisdiction: AI system governed under designated law.	*AI decision audit log, override records, conformity docs*

"Sovereignty is not a checkbox — it is the architectural foundation for compliance, risk management, and trust."

** Emerging country-specific frameworks also apply: PDPA (Thailand/Singapore), PDPL (Saudi Arabia), DPDP (India), LGPD (Brazil), POPIA (South Africa) — Versa's five pillars are designed to satisfy all.*

The Difference That Makes It Sovereign

Sovereign Capabilities	VERSA	Primary Competitor	Other SASE Vendors
	Data, Policy & Control Plane		
In Region Data & Policy Controls	High Flexibility across deployment models	Available	Limited
Customer Controlled Mgmt. Plane options	Strong support	Partial	Limited to in-region data residency
E2E Operations & Control	Complete operational Flexibility	Partial	No
	Deployment Options		
Data Sovereignty & Log Storage	Strong customer and regional control options	Available	Available
Jurisdiction & Deployment Flexibility	Very Flexible (customer owned, dedicated, aaS)	Moderate	Limited
Dedicated Sovereign Deployment	Available	Available	Limited
	Architecture		
Unified SASE with Sovereign Deployment	Native unified platform approach	Partial integration model	Cloud native - SSE focus
Best fit for highly regulated/ sovereign Environment	Strong fit for hybrid/enterprise/federal	Suited for hybrid environments	Only SaaS centric environment

Sovereign SASE Use Case Summary

Why	What	How
➢ We need data sovereignty, predictable SLAs and enterprise-class security-without having to build, host or manage the infrastructure ourselves.	 Local hosted Sovereign SASE GWs with **dedicated** infrastructure	 *Dedicated Sovereign SASE aaS (Versa Hosted & Managed)*
➢ We want sovereign infrastructure, but rely on Versa's expertise to operate, secure, optimize SASE fabric end-to-end.	 Local hosted Sovereign SASE GWs with **shared** infrastructure	 *Sovereign SASE aaS (Versa Hosted & Managed)*
➢ We need complete sovereignty over our data, gateways and operations because of regulatory requirements-we must run everything ourselves.	 Customer hosts and manages the whole SASE stack	 *Sovereign SASE (Customer Hosted & Managed)*

Thank You