

Extending Versa Sovereign SASE with Advanced Security Capabilities

Executive Summary

Organizations turn to Versa Sovereign Secure Access Services Edge (SASE) when security alone is not enough; they also need explicit control over how and where security decisions are made, enforced, and governed. That includes keeping the control plane, inspection, logging, and policy management inside clearly defined organizational or jurisdictional boundaries, rather than relying on opaque, shared cloud infrastructure.

However, many “sovereign” SASE approaches still push advanced protections - such as API security and data protection (API-DP), remote browser isolation (RBI), and advanced threat protection (ATP) - into external clouds, which weakens the sovereignty model and creates operational fragmentation. Versa addresses this gap by extending Sovereign SASE with Advanced Security Cloud (ASC) capabilities that run on customer-owned infrastructure, so the same environment that enforces access can also deliver high-value, cloud-grade protections as and when needed.

This gives customers a single strategy for sovereignty and security depth. Versa delivers a full-stack, sovereignty-aware SASE architecture on customer premises, helping organizations meet jurisdictional, operational, and resilience requirements without compromising on advanced security capabilities. A key differentiator is that customers can maintain control-plane authority and advanced security processing within defined jurisdictional boundaries when required.

Why Customers Choose Sovereign SASE

Organizations adopt Sovereign SASE when they need tighter control over data protection, data processing, security enforcement, operational accountability, and platform management than a conventional shared-cloud model can offer. In this context, sovereignty is not only about where data sits; it is also about who operates the control plane, where policy decisions are made, and how access, inspection, management, and governance remain within defined operating boundaries across the service lifecycle.

This matters for enterprises and service providers operating under regulatory, contractual, or national-infrastructure obligations. Sovereign SASE helps them align with data-protection and critical-infrastructure

expectations worldwide - for example, General Data Protection Regulation (GDPR), Network and Information Security Directive (NIS2), Digital Operational Resilience Act (DORA), and comparable data-protection, sectoral, and resilience requirements in the UK, the Americas, Asia-Pacific, and other regions - by keeping control-plane functions, access decisions, enforcement, and management within defined operating boundaries.

		VERSA	Other Vendors
The Sovereign difference	Data Inspection & Policy Enforcement	✓	✓
	Control & Management	✓	✗
	Data & Log Storage	✓	✓
	Operations Center	✓	✗
	Jurisdiction	✓	✗

For many enterprises, sovereignty is also a trust, resilience, and business continuity decision. They want private or jurisdictionally controlled infrastructure, clearer governance, and the ability to preserve architectural independence in highly regulated, sensitive, or even air-gapped environments across sectors such as government, financial services, healthcare, manufacturing, and service providers.

Why Advanced Security Features Matter

A sovereign architecture is only complete if it includes the security capabilities customers actually plan to use. If core SASE functions stay inside sovereign boundaries but advanced services must be consumed from elsewhere, the operating model becomes split, and sovereignty becomes harder to defend in practice.

That is why ASC capabilities matter. Customers increasingly expect a SASE platform to provide not only core access and inspection controls, but also advanced protections that support modern applications, digital services, and high-assurance operating environments.

When those functions run outside the sovereign environment, customers are left with an incomplete answer: some traffic and controls remain local, while higher-value security functions still depend on an external platform. Extending Sovereign SASE with ASC capabilities closes that gap and preserves architectural consistency.

Versa’s Sovereign SASE

Versa’s Sovereign SASE delivers the full scope of modern SASE, with sovereignty designed into the platform rather than bolted on as a workaround. The objective is not merely to claim sovereign deployment, but to make sovereignty practical across control-plane authority, policy control, inspection, logging, operations, and advanced protection services. As the architecture view illustrates, control plane placement and jurisdictional alignment are central to that design.

That is the strategic value of extending Versa Sovereign SASE to include ASC capabilities such as RBI, API-DP, and ATP on customer premises. Customers can consume advanced security services without stepping outside their sovereign or jurisdictionally controlled operating model.

This is especially important for organizations that selected sovereign deployment because they do not want critical control-plane, inspection, enforcement, or management functions to depend on a third-party shared cloud. A sovereign design is stronger when advanced capabilities can run inside the customer’s own environment whenever policy, risk, or operational requirements demand it.

Why Extend Sovereign SASE with On Premises Advanced Security

Customer requirement	Why it matters	Versa Sovereign response
Keep inspection and enforcement within sovereign boundaries	Sovereignty is weakened when advanced processing must leave the controlled environment.	Versa extends Sovereign SASE so advanced security capabilities can run on customer-controlled infrastructure.
Maintain one consistent operating model	Separate architectures for core SASE and advanced services create complexity, governance overhead, and integration friction.	VersaONE provides a unified platform approach instead of forcing a split between sovereign access and non-sovereign advanced security.
Support highly regulated or sensitive environments	Some customers require on-premises or jurisdictionally controlled infrastructure for operational, regulatory, or national-infrastructure reasons.	Versa supports deployment on customer infrastructure, including high-compute security functions, for high-security and air-gapped environments.
Avoid compromise between sovereignty and security depth	Customers should not be forced into a trade-off between local or jurisdictional control and modern protection capabilities.	Versa positions Sovereign SASE as full-stack SASE, extended to include advanced security capabilities on premises.

Summary

Customers choose Sovereign SASE because they want control, accountability, jurisdictional alignment, and architectural independence in how security is delivered - not simply a promise about where data is stored. The value of sovereignty increases when advanced security capabilities can operate inside the same controlled environment as core SASE services.

Extending Sovereign SASE to include ASC capabilities is therefore essential to a complete sovereign architecture. Versa enables organizations to bring cloud-grade advanced security onto customer-controlled infrastructure, so they can pursue sovereignty and security depth as part of the same strategy rather than as competing priorities.



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, a global leader in SASE, 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 delivering 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.

©2026 Versa Networks, Inc. All rights reserved. Portions of Versa products are protected under Versa patents, as well as patents pending. Versa Networks and FlexVNF are trademarks or registered trademarks of Versa Networks, Inc. All other trademarks used or mentioned herein belong to their respective owners.

Part# TB_SOVSASE-ADVSEC-01.0