# Sovereign SASE erklärt

*Vollständiges SASE. Souverän von Grund auf.*

## Die Herausforderung

Unternehmen müssen zunehmend digitale Souveränität nachweisen – nicht nur den Schutz von Daten, sondern auch die Kontrolle darüber, wie Nutzer sich verbinden, wie der Datenverkehr inspiziert wird und wie Sicherheits- und Netzwerkplattformen betrieben werden.

Manche Organisationen haben begonnen, Workloads in regionale oder souveräne Cloud-Umgebungen zu verlagern. Netzwerk- und Sicherheitsdienste werden jedoch häufig weiterhin global betrieben. Selbst wenn die Infrastruktur lokal erscheint, können Zugriffsentscheidungen, Sicherheitsverarbeitungen oder die Plattformverwaltung weiterhin von Systemen außerhalb der vorgesehenen Betriebsumgebung abhängen.

Dadurch entsteht eine Lücke zwischen den Erwartungen an die Souveränität und der tatsächlichen Art der Sicherheitsbereitstellung. Souveränität bezieht sich längst nicht mehr nur darauf, wo Daten liegen; sie hängt auch davon ab, wer Zugriff, Inspektion und Verwaltung kontrolliert.

## Was ist Sovereign SASE?

Sovereign SASE erweitert Secure Access Service Edge (SASE), in dem die Souveränitätskontrollen in Netzwerk- und Sicherheitsarchitekturen integriert werden.

Es liefert SASE-Funktionen und stellt gleichzeitig sicher, dass die für Konnektivität, Durchsetzung und Betrieb verantwortlichen Systeme mit den festgelegten Betriebsgrenzen übereinstimmen.

Eine Sovereign-SASE-Architektur stellt sicher, dass Zugriffsentscheidungen, Traffic-Inspektion und Plattformverwaltung über die Kontroll-, Daten- und Management-Ebene hinweg innerhalb derselben Betriebsumgebung zusammenwirken. Souveränität hängt davon ab, dass alle drei Ebenen konsistent zusammenarbeiten.

## Warum herkömmliches, gemeinsam genutztes SASE nicht ausreicht

Herkömmliche, gemeinsam genutzte SASE-Plattformen wurden für globale Skalierung und zentralisierte Servicebereitstellung entwickelt. Diese Architekturen basieren auf gemeinsam genutzter Infrastruktur sowie global betriebenen Kontroll- und Managementsystemen.

Nutzer verbinden sich möglicherweise über einen nahegelegenen Point of Presence (PoP), doch das Vorhandensein eines regionalen PoPs bedeutet nicht, dass die gesamte Sicherheitsverarbeitung lokal erfolgt. In vielen gemeinsam genutzten SASE-Umgebungen werden Funktionen wie Bedrohungsschutz, Analysen oder Teile der Inspektionsabläufe an zentralisierten Standorten anderswo verarbeitet.

Wenn Datenverkehr die lokale Umgebung zur Inspektion oder Analyse verlässt, wird die Durchsetzung nicht mehr lokal geregelt, und die Souveränitätserwartungen werden nicht vollständig erfüllt.
Dieses Modell kann zudem zu Traffic-Hairpinning führen, bei dem Datenverkehr zu zentralisierten Verarbeitungssystemen umgeleitet wird, was die Latenz erhöht und demzufolge die Leistung beeinträchtigt.

Gemeinsam genutzte SASE-Architekturen wurden um zentralisierte Verarbeitungsmodelle herum entwickelt und nicht um lokalisierte operative Kontrolle.

## Warum viele Sovereign-SASE-Ansätze weiterhin zu kurz greifen

Als Reaktion auf Souveränitätsanforderungen haben einige Anbieter regionale oder souveräne Varianten von SASE eingeführt, indem sie lokale PoPs bereitstellen oder Teile der Infrastruktur isolieren.

Diese Ansätze verbessern die Lokalität des Traffic, adressieren jedoch häufig nur, wo der Datenverkehr in das Netzwerk eintritt. Sicherheitsverarbeitung, Policy-Auswertung oder operative Abläufe können weiterhin auf global gemeinsam genutzten Plattformen basieren.

Wenn Bedrohungsschutz, Analysen oder Policy-Durchsetzung außerhalb der vorgesehenen Umgebung stattfinden, bleiben die Souveränitätsziele unvollständig. Diese Architekturen können zudem weiterhin auf die Umleitung des Traffic für bestimmte Funktionen angewiesen sein, was zu denselben Hairpinning- und den Auswirkungen auf die Leistung führt, die auch bei gemeinsam genutzten SASE-Modellen auftreten.

Sovereign SASE erfordert eine Abstimmung über Kontroll-, Daten- und Management-Ebene hinweg.
Die Lokalisierung nur einzelner Teile der Architektur stellt keine vollständige Kontrolle über Zugriffsentscheidungen und Plattformbetrieb her.

## Zentrale Anforderungen an Sovereign SASE

SASE-Bereitstellungen lassen sich anhand von Anforderungen bewerten, die Kontroll-, Daten- und Management-Ebene gemeinsam berücksichtigen.

### Lokalisierte Zugriffskontrolle (Kontrollebene)

Zugriffsentscheidungen sollten innerhalb der souveränen Umgebung erfolgen. Identitätsprüfung, Policy-Auswertung und Verbindungsentscheidungen sollten nicht von global gemeinsam genutzten Kontrollsystemen außerhalb der vorgesehenen Betriebsgrenze abhängen.

### Lokalisierte Traffic-Inspektion (Datenebene)

Traffic-Inspektion und Schutzfunktionen – einschließlich Bedrohungsprävention und Traffic-Analyse – sollten an souveränen Points of Presence erfolgen, ohne den Datenverkehr zur Verarbeitung an externe Umgebungen umzuleiten.

### Lokalisierte Plattformverwaltung (Management-Ebene)

Administration, Monitoring, Protokollierung, Konfiguration und operativer Zugriff sollten lokal geregelt bleiben, damit die Plattformaufsicht den Souveränitätserwartungen entspricht. Dies umfasst sowohl den administrativen Zugriff des Kunden als auch den operativen Zugriff des Anbieters, um eine Abhängigkeit von zentralisierten globalen Managementsystemen zu vermeiden.

### Servicebereitstellung und rechtliches Betriebsmodell

Die technische Architektur allein bestimmt nicht, ob eine Bereitstellung den Souveränitätserwartungen entspricht. Organisationen sollten zudem bewerten, wie der Dienst rechtlich erbracht und betrieben wird, einschließlich welche regionale juristische Einheit den Dienst bereitstellt und wie die operative Verantwortung strukturiert ist. Die Abstimmung zwischen Bereitstellungsarchitektur und Service-Betriebsmodell trägt dazu bei, dass Governance und Servicebereitstellung mit den Souveränitätszielen im Einklang bleiben.

## Vollständige SASE-Funktionalität (über alle Ebenen hinweg)

Eine Sovereign-SASE-Lösung umfasst zentrale SASE-Funktionen wie SD-WAN-Konnektivität, Zero Trust Network Access, Firewall as a Service, Secure Web Gateway sowie einheitliche Richtlinien und Sichtbarkeit über die Kontroll-, Daten- und Management-Ebene hinweg.

## Versa Sovereign SASE

Versa Sovereign SASE liefert vollständige SASE-Funktionen, bei denen Souveränität in die Plattformarchitektur integriert ist.

Zugriffsentscheidungen, Traffic-Inspektion und Sicherheitsverarbeitung bleiben lokalisiert, während Plattformverwaltung und -betrieb dem vorgesehenen Betriebsmodell entsprechen.

Durch die gemeinsame Betrachtung von Daten-, Kontroll- und Management-Ebene – und den Verzicht auf externe Inspektions- oder Verwaltungsumgebungen – schließt Versa Sovereign SASE die Lücken, die entstehen, wenn nur Teile einer SASE-Architektur lokalisiert werden.

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

Über Versa

Versa, ein globaler Marktführer im Bereich SASE, ermöglicht es Organisationen, selbstschützende Netzwerke aufzubauen, die ihre Netzwerk- und Sicherheitsinfrastruktur radikal vereinfachen und automatisieren. Die KI-gestützte VersaONE Universal SASE Platform bietet konvergente SSE-, SD-WAN- und SD-LAN-Lösungen, die Daten schützen und vor Cyberbedrohungen verteidigen und dabei ein hervorragendes digitales Nutzererlebnis liefern. Tausende Kunden weltweit, mit Hunderttausenden Standorten und Millionen Nutzern, vertrauen Versa ihre unternehmenskritischen Netzwerke und ihre Sicherheit an. Versa befindet sich in Privatbesitz und wird von Investoren wie Sequoia Capital, Mayfield und BlackRock finanziert. Weitere Informationen finden Sie unter https://www.versa-networks.com; folgen Sie Versa außerdem auf LinkedIn und X (Twitter) unter @versanetworks.

© 2026 Versa Networks, Inc. Alle Rechte vorbehalten. Teile der Versa-Produkte sind durch Versa-Patente sowie angemeldete Patente geschützt. Versa Networks und VOS sind Marken oder eingetragene Marken der Versa Networks, Inc. Alle anderen hierin verwendeten oder erwähnten Marken sind Eigentum ihrer jeweiligen Inhaber.
*Teil-Nr. SB_SOVEREIGNSASEMSP-02 26-0217*