Sovereign SASE expliqué

Un SASE complet. Souverain par conception.

Le défi

Les entreprises doivent de plus en plus démontrer leur souveraineté — non seulement la protection des données, mais aussi le contrôle sur la manière dont les utilisateurs se connectent, dont le trafic est inspecté, et dont les plateformes de sécurité et de réseau sont exploitées.

Certaines organisations ont commencé à déplacer leurs charges de travail vers des environnements cloud régionaux ou souverains. Cependant, les services de réseau et de sécurité restent souvent exploités à l'échelle mondiale. Même lorsque l'infrastructure semble locale, les décisions d'accès, le traitement de la sécurité ou la gestion de la plateforme peuvent continuer à dépendre de systèmes situés en dehors de l'environnement d'exploitation visé.

Cela crée un écart entre les attentes en matière de souveraineté et la manière dont la sécurité est réellement fournie. La souveraineté ne se limite plus à l'emplacement des données ; elle dépend également de qui contrôle l'accès, l'inspection et la gestion.

Qu'est-ce que le Sovereign SASE ?

Le Sovereign SASE étend le Secure Access Service Edge (SASE) en intégrant des contrôles de souveraineté dans l'architecture réseau et sécurité.

Il fournit les capacités du SASE tout en garantissant que les systèmes responsables de la connectivité, de l'application des politiques et de l'exploitation sont alignés sur des frontières opérationnelles définies.

Une architecture de SASE souverain garantit que les décisions d'accès, l'inspection du trafic et la gestion de la plateforme fonctionnent ensemble au sein des plans de contrôle, de données et de gestion, dans le même environnement d'exploitation. La souveraineté dépend de la cohérence de fonctionnement de ces trois couches.

Pourquoi le SASE mutualisé traditionnel ne suffit pas

Les plateformes SASE mutualisées traditionnelles ont été conçues pour une échelle mondiale et une fourniture de services centralisée. Ces architectures reposent sur une infrastructure partagée ainsi que sur des systèmes de contrôle et de gestion exploités à l'échelle mondiale.

Les utilisateurs peuvent se connecter via un point de présence (PoP) situé à proximité, mais la présence d'un PoP régional ne signifie pas que l'ensemble du traitement de sécurité s'effectue localement. Dans de nombreux environnements SASE mutualisés, des fonctions telles que la protection contre les menaces, l'analyse ou certaines étapes de l'inspection sont traitées dans des emplacements centralisés ailleurs.

Lorsque le trafic quitte l'environnement local pour être inspecté ou analysé, l'application des politiques n'est plus gouvernée localement, et les attentes en matière de souveraineté ne sont pas pleinement satisfaites. Ce modèle peut également entraîner un effet de « hairpinning » du trafic, où celui-ci est redirigé vers des systèmes de traitement centralisés, ce qui augmente la latence et affecte la performance.

Les architectures SASE mutualisées ont été conçues autour de modèles de traitement centralisés plutôt que d'un contrôle opérationnel localisé.

Pourquoi de nombreuses approches Sovereign SASE restent insuffisantes

En réponse aux exigences de souveraineté, certains fournisseurs ont introduit des variantes régionales ou souveraines du SASE en déployant des PoP locaux ou en isolant certaines parties de leur infrastructure.

Ces approches améliorent la localité du trafic, mais ne traitent souvent que le point d'entrée du trafic dans le réseau. Le traitement de la sécurité, l'évaluation des politiques ou les workflows opérationnels peuvent continuer à reposer sur des plateformes mutualisées à l'échelle mondiale.

Si la protection contre les menaces, l'analyse ou l'application des politiques s'effectuent en dehors de l'environnement visé, les objectifs de souveraineté restent incomplets. Ces architectures peuvent également continuer à dépendre de la redirection du trafic pour certaines fonctions, entraînant les mêmes effets de hairpinning et les mêmes impacts sur la performance que dans les modèles SASE mutualisés.

Le Sovereign SASE nécessite un alignement entre le plan de contrôle, le plan de données et le plan de gestion. Localiser seulement certaines parties de l'architecture ne permet pas d'établir un contrôle complet sur les décisions d'accès et l'exploitation de la plateforme.

Exigences clés pour le Sovereign SASE

Les déploiements SASE peuvent être évalués au regard d'exigences qui traitent conjointement les plans de contrôle, de données et de gestion.

Contrôle d'accès localisé (plan de contrôle)

Les décisions d'accès doivent s'effectuer au sein de l'environnement souverain. La validation d'identité, l'évaluation des politiques et les décisions de connexion ne doivent pas reposer sur des systèmes de contrôle mutualisés à l'échelle mondiale, situés en dehors de la frontière opérationnelle visée.

Inspection du trafic localisée (plan de données)

Les fonctions d'inspection du trafic et de protection — y compris la prévention des menaces et l'analyse du trafic — doivent s'effectuer au niveau de points de présence souverains, sans rediriger le trafic vers des environnements de traitement externes.

Gestion de la plateforme localisée (plan de gestion)

L'administration, la surveillance, la journalisation, la configuration et l'accès opérationnel doivent rester gouvernés localement, afin que la supervision de la plateforme reste alignée sur les attentes de souveraineté. Cela inclut à la fois l'administration par le client et l'accès opérationnel du fournisseur, en évitant toute dépendance à des systèmes de gestion mondiaux centralisés.

Modèle de prestation de service et cadre juridique d'exploitation

L'architecture technique seule ne détermine pas si un déploiement répond aux attentes de souveraineté. Les organisations doivent également évaluer la manière dont le service est fourni et exploité sur le plan juridique, y compris quelle entité juridique régionale fournit le service et comment la responsabilité opérationnelle est structurée. L'alignement entre l'architecture de déploiement et le modèle d'exploitation du service contribue à garantir que la gouvernance et la prestation de service restent cohérentes avec les objectifs de souveraineté.

Capacité SASE complète (sur l'ensemble des plans)

Une solution Sovereign SASE comprend les capacités SASE fondamentales telles que la connectivité SD-WAN, le Zero Trust Network Access, le Firewall as a Service, la passerelle Web sécurisée (Secure Web Gateway), ainsi qu'une politique et une visibilité unifiées, opérant sur l'ensemble des plans de contrôle, de données et de gestion.

Versa Sovereign SASE

Versa Sovereign SASE fournit des capacités SASE complètes, avec la souveraineté intégrée dans l'architecture de la plateforme.
Les décisions d'accès, l'inspection du trafic et le traitement de la sécurité restent localisés, tandis que la gestion et l'exploitation de la plateforme s'alignent sur le modèle d'exploitation visé.

En traitant conjointement les plans de données, de contrôle et de gestion — et en évitant toute dépendance à des environnements d'inspection ou de gestion externes — Versa Sovereign SASE élimine les écarts créés lorsque seules certaines parties d'une architecture SASE sont localisées.

Versa Networks, Inc.
2550 Great America Way, Suite 350
Santa Clara, CA 95054
Tél. : +1 408.385.7660
E-mail : info@versa-networks.com
Site web : www.versa-networks.com

À propos de Versa

Versa, un leader mondial du SASE, permet aux organisations de créer des réseaux auto-protecteurs qui simplifient et automatisent radicalement leur infrastructure réseau et sécurité. Propulsée par l'IA, la plateforme VersaONE Universal SASE offre des solutions convergentes SSE, SD-WAN et SD-LAN qui protègent les données et défendent contre les cybermenaces, tout en offrant une expérience numérique supérieure. Des milliers de clients dans le monde, avec des centaines de milliers de sites et des millions d'utilisateurs, font confiance à Versa pour leurs réseaux et leur sécurité critiques.

© 2026 Versa Networks, Inc. Tous droits réservés. Certains produits Versa sont protégés par des brevets Versa, ainsi que par des brevets en instance. Versa Networks et VOS sont des marques commerciales ou déposées de Versa Networks, Inc. Toutes les autres marques utilisées ou mentionnées dans ce document appartiennent à leurs propriétaires respectifs.
Réf. DS_SOVSASEEXP-01 26-0218