# Versa Sovereign SASE und NIS2-Konformität

*Die NIS2-Richtlinie der EU zu Netzwerk- und Informationssicherheit mit Versa Sovereign SASE*

Die NIS2-Konformität erfordert zunehmend eine auf Architektur-Ebene garantierte Sicherheit hinsichtlich der Frage, wo sensible Daten verarbeitet werden, wie Richtlinien durchgesetzt werden und wer den Zugriff auf kritische Systeme steuert. Versa Sovereign SASE liefert einen vollständigen SASE-Stack, bei dem sämtliche Daten-, Kontroll- und Management-Ebenen vollständig innerhalb der EU-Jurisdiktion betrieben werden – abgesichert durch unabhängige Zertifizierungen und flexible Bereitstellungsoptionen, die sowohl für IT- als auch für OT-Umgebungen geeignet sind. Für Organisationen, die NIS2-Verpflichtungen unterliegen, bietet Versa einen direkten Weg zur Konformität, ohne Abstriche bei der Sicherheitsfunktionalität oder der operativen Flexibilität zu machen.

## Die NIS2-Richtlinie

Die NIS2-Richtlinie der EU (EU 2022/2555) erweitert die Cybersicherheits- und Resilienzpflichten für Organisationen, die kritische Infrastrukturen und wesentliche Dienste innerhalb der EU betreiben. Über die Umsetzung von Sicherheitskontrollen hinaus legt NIS2 besonderen Wert auf Governance, Risikomanagement, Vorfallsmeldung, Lieferkettensicherheit und nachweisbare Rechenschaftspflicht.

Zu den zentralen Anforderungen zählen:

- Governance-Aufsicht und Rechenschaftspflicht der Geschäftsleitung (Art. 20)
- Cybersicherheits-Risikomanagement und Resilienzmaßnahmen (Art. 21)
- Meldung von Vorfällen an nationale Behörden und CSIRTs (Art. 23)
- Verwendung anerkannter Zertifizierungsrahmen für Cybersicherheit (Art. 24)
- Regulatorische Aufsicht und Zuständigkeitsanforderungen (Art. 26)

Diese Anforderungen bewegen Organisationen zunehmend zu Architekturen, die klare operative Kontrolle, Transparenz bei der Durchsetzung von Richtlinien, prüfbare Sicherheitsabläufe und eine stärkere rechtliche Absicherung sensibler Systeme und Daten bieten.

## Versa Sovereign SASE

Versa Sovereign SASE wurde gezielt entwickelt, um die operativen und regulatorischen Anforderungen von NIS2 zu erfüllen, indem die gesamte SASE-Architektur – einschließlich Daten-, Kontroll- und Management-Ebenen – innerhalb souverän kontrollierten Umgebungen verbleibt. Als Bereitstellungsmodell der VersaONE Universal SASE Platform adressiert es die grundlegende Einschränkung herkömmlicher Cloud-basierter SASE-Lösungen: Selbst wenn Anbieter einen lokalen Point of Presence (PoP) betreiben, hängen Traffic-Inspektion, Policy-Entscheidungen und Plattformverwaltung häufig weiterhin von Infrastruktur außerhalb der vorgesehenen Jurisdiktion ab.

Versa Sovereign SASE bringt alle drei Ebenen der SASE-Architektur innerhalb einer souveränen Betriebsumgebung in Einklang:

- **Datenebene: Datenverkehrsprüfung, Bedrohungsschutz und Content-Filterung werden an lokalen PoPs ausgeführt, ohne dass Datenverkehr zur Verarbeitung außerhalb der Jurisdiktion umgeleitet wird.**
- **Kontrollebene: Identitätsprüfung, Policy-Auswertung und Verbindungsentscheidungen erfolgen innerhalb der festgelegten souveränen Umgebung.**
- **Management-Ebene: Plattformverwaltung, Protokollierung, Konfiguration und operativer Zugriff bleiben lokal geregelt.**

In der EU ist Versas „Sovereign SASE-as-a-Service" verfügbar, wobei sämtliche Betriebs-, Datenverarbeitungs- und Support-Prozesse dem EU-Recht unterliegen – unabhängig von Versas globaler Cloud-Infrastruktur. Für Organisationen, die vollständige Infrastrukturkontrolle benötigen, ist Versa Sovereign SASE zudem für On-Premises- oder private EU-Cloud-Bereitstellungen verfügbar.

## NIS2-Anforderungen im Abgleich mit Versa Sovereign SASE

Die folgende Tabelle ordnet relevante NIS2-Anforderungen den Funktionen von Versa Sovereign SASE sowie den damit unterstützten Compliance-Ergebnissen zu.

| NIS2-Anforderung | Versa Sovereign SASE-Funktion | Ergebnis |
|---|---|---|
| Governance und Rechenschaftspflicht der Geschäftsleitung (Art. 20) | Zentralisiertes Policy-Management verschafft der Geschäftsleitung einheitliche Sichtbarkeit und Kontrolle über die Cybersicherheitslage der Organisation; rollenbasierter Zugriff mit Aufgabentrennung gewährleistet eine angemessene Aufsicht; automatisierte Compliance-Berichterstattung liefert für die Geschäftsleitung aufbereitete Nachweise zum Cybersicherheitsstatus | Ermöglicht es der Geschäftsleitung, die Einhaltung der NIS2-Cybersicherheitspflichten zu genehmigen, zu überwachen und nachzuweisen; unterstützt die Anforderungen an die persönliche Rechenschaftspflicht |
| Risikomanagement-Richtlinie (Art. 21 Abs. 2 Buchstabe a) | Zentralisiertes Richtlinien-Management über Versa Director und Concerto mit Single-Pane-of-Glass-Sichtbarkeit; kontinuierliche UEBA und KI-gestützte Risikobewertung; versionskontrollierte Sicherheits-Baselines | Unterstützt dokumentierte, risikobasierte Sicherheitsrichtlinien mit prüfbaren Baselines im Einklang mit den NIS2-Pflichten |
| Erkennung und Reaktion auf Vorfälle (Art. 21 Abs. 2 Buchstabe b) | Echtzeit-IDS/IPS, ATP mit MITRE-ATT&CK-Zuordnung, automatisierte Eindämmungs-Playbooks, SIEM-Integrationen | Unterstützt die schnelle Erkennung und Eindämmung von Sicherheitsvorfällen gemäß den Vorgaben zur Vorfallsbehandlung nach Art. 21 Abs. 2 Buchstabe b |
| Betriebskontinuität (Art. 21 Abs. 2 Buchstabe c) | Active-Active-HA-Clustering mit Failover im Sub-Sekundenbereich; SD-WAN-Multipath-Resilienz (MPLS, Breitband, LTE/4G/5G); automatisiertes Konfigurations-Backup und -Restore; vertragliche SLAs | Gewährleistet die Verfügbarkeit kritischer Dienste bei Hardwareausfällen, Standortausfällen oder aktiven Angriffen |
| Sicherheit der Lieferkette Art. 21 Abs. 2 Buchstabe d) | Versa kann nachweisen, dass die Sovereign-SASE-Bereitstellung in der EU vollständig souverän ist bzw. über eine ausschließlich EU-basierte Lieferkette verfügt.; durch ZTNA erzwungener, fein abgestufter Zugriff für Dritte; Mikrosegmentierung auf Anwendungsebene; NIS2-konforme vertragliche AVV-Pflichten für Unterauftragsverarbeiter; sämtliche Daten, Metadaten, Protokolle und Telemetrie werden innerhalb EU-geregelter Betriebsumgebungen verarbeitet | Adressiert die NIS2-Anforderungen an die IKT-Lieferkette durch überprüfbare, nach dem Least-Privilege-Prinzip gestaltete Lieferantenzugriffskontrollen; reduziert die Exposition gegenüber grenzüberschreitender regulatorischer und rechtlicher Komplexität |

| | | |
|---|---|---|
| Sichere Systembeschaffung (Art. 21 Abs. 2 Buchstabe e) | „Secure-by-Design"-SASE-Architektur; alle Komponenten unterliegen Sicherheitsprüfungen und Patch-Management; automatisierte Patch-Bereitstellung und Threat-Intelligence-Feeds | Demonstriert „Security-First"-Beschaffungspraktiken mit fortlaufendem Schwachstellenmanagement |
| Wirksamkeitsbewertung (Art. 21 Abs. 2 Buchstabe f) | Automatisierte Compliance-Berichte gemäß NIS2-Anforderungen; Echtzeit-Dashboards über alle Sicherheitsbereiche hinweg; unveränderliche, manipulationssichere Audit-Protokolle; Integration in GRC-Plattformen | Liefert messbare Nachweise zur Wirksamkeit der Sicherheitskontrollen; unterstützt interne und externe Audits |
| Cyberhygiene (Art. 21 Abs. 2 Buchstabe g) | Durchgesetzte Sicherheits-Baselines über alle Nutzer, Geräte und Workloads hinweg; automatisiertes Patch Deployment; integrierte Bedrohungsdaten-Feeds; kontinuierliche Bewertung des Sicherheitsstatus | Gewährleistet ein einhetliches Sicherheitsmanagement im großen Maßstab und reduziert so die Angriffsfläche im gesamten Unternehmen |
| Kryptografie und Verschlüsselung (Art. 21 Abs. 2 lit. h) | TLS 1.3 und IPsec mit AES-256 für sämtliche Daten während der Übertragung; AES-256-Verschlüsselung ruhender Daten mit Schlüsselverwaltung in der EU; HSM-gestützte Schlüsselspeicherung; vollständige SSL/TLS-Inspektion | Unterstützt die NIS2-Verschlüsselungspflichten für Daten während der Übertragung und im Ruhezustand innerhalb souveräner Grenzen |
| Zugriffskontrolle und Personalsicherheit (Art. 21 Abs. 2 lit. i) | ZTNA mit kontinuierlicher Sicherheitsbewertung; RBAC mit Aufgabentrennung; native MFA; Integration mit Unternehmens-Identitätsanbietern (Azure AD, Okta, ADFS); Audit-Trail privilegierter Vorgänge | Setzt Least-Privilege-Zugriff über Nutzer, Geräte und Anwendungen hinweg durch; beseitigt dauerhaften Drittanbieterzugriff |
| MFA und sichere Kommunikation (Art. 21 Abs. 2 lit. j) | Native MFA für sämtlichen Nutzer- und Administratorzugriff; kontinuierliche, auf Geräte-Posture und Nutzerverhalten basierende Vertrauensbewertung nach der Authentifizierung; sämtliche Kommunikation Ende-zu-Ende verschlüsselt | Unterstützt die NIS2-Anforderungen an MFA und sichere Kommunikation über Nutzer und Workloads hinweg |
| Fristen für die Vorfallsmeldung (Art. 23) | Detaillierte, mit Zeitstempel versehene und manipulationssichere Ereignisprotokolle; SIEM-Integration und NIS2-konforme Berichtsvorlagen für die Meldung an zuständige Behörden und CSIRTs; vorgefertigte Incident-Response-Playbooks mit automatisierter Alarmierung zur Unterstützung strukturierter Meldeprozesse | Unterstützt die verpflichtenden Fristen von 24 Stunden für die Frühwarnung, 72 Stunden für die Vorfallsmeldung und einem Monat für den Abschlussbericht gegenüber nationalen CSIRTs und zuständigen Behörden |
| Cybersicherheits-Zertifizierungssysteme (Art. 24) | Zertifizierungen nach ISO/IEC 27001:2022, SOC 2 Type II, ISO/IEC 27017 und ISO/IEC 27018; Ausrichtung am ENISA-Rahmenwerk für Cybersicherheitszertifizierung im Rahmen des EU-Cybersicherheitsgesetzes | Unterstützt den Nachweis der NIS2-Konformität durch Zertifizierungssysteme im Einklang mit Artikel 24 und dem EU-Cybersicherheitsgesetz |
| Zuständigkeit und Territorialität (Art. 26) | Sämtliche Betriebs-, Datenverarbeitungs- und Support-Prozesse unterliegen über Versa Sovereign SASE-as-a-Service dem EU-Recht; EU-ansässiges Betriebspersonal; keine Abhängigkeiten von Infrastruktur in Drittstaaten | Stellt sicher, dass die Aufsichtszuständigkeit eindeutig bei der festgelegten Behörde des jeweiligen EU-Mitgliedstaats verbleibt, ohne extraterritoriale Komplikationen |

## OT-/ICS-Umgebungen

Für NIS2-verpflichtete Einrichtungen in den Sektoren Energie, Transport, Wasser und verarbeitendes Gewerbe stellt die Absicherung operativer Technologieumgebungen eine eigenständige Herausforderung dar. Versa Sovereign SASE erweitert die NIS2-Sicherheitskontrollen auf OT-Umgebungen, ohne die Betriebsprozesse zu stören:

- **Purdue-Modell-bewusste Segmentierung:** Durchsetzung zonenbasierter Zugriffskontrollen im Einklang mit IEC 62443 und dem Purdue-Referenzmodell für industrielle Netzwerke.
- **Inspektion industrieller Protokolle:** Deep Packet Inspection für OT-Protokolle (Modbus, DNP3, IEC 60870-5, PROFINET) ermöglicht Anomalieerkennung ohne Betriebsstörungen.
- **Passive OT-Asset-Erkennung:** Identifizierung und Inventarisierung von OT-Assets in IT/OT-Konvergenzumgebungen ohne aktives Scannen und ohne zusätzliche Sensoren.

## Warum sich NIS2-verpflichtete Organisationen für Versa entscheiden

Als First-to-Market-Anbieter wurde Versa Sovereign SASE gezielt für rechtliche, regulatorische und operative Souveränität entwickelt. Anders als Plattformen, die sich auf globale Infrastruktur hinter lokalisierten Gateways stützen, hält Versa den gesamten SASE-Stack von vornherein innerhalb souverän kontrollierter Umgebungen.

Diese Architektur unterstützt Organisationen dabei, den wachsenden NIS2-Erwartungen in Bezug auf Risikomanagement, operative Resilienz, Governance und Kontrolle über kritische digitale Infrastruktur gerecht zu werden.

Versa adressiert alle drei Souveränitätsebenen (Daten, Kontrolle und Management) ohne Abhängigkeiten von ausländischer Infrastruktur oder Kompromisse bei der Sicherheitsfunktionalität. NIS2-pflichtige Unternehmen erhalten die vollständige VersaONE-Plattform in einer vollständig souveränen Architektur, mit flexiblen Bereitstellungsoptionen von Sovereign SASE-as-a-Service bis hin zu privater EU-Cloud und On-Premises.

Durch die Durchsetzung von Souveränität über Daten-, Kontroll- und Management-Ebenen hinweg, die NIS2-konforme Sicherheits- und Governance-Ziele unterstützen, bietet Versa Organisationen einen klaren, praktikablen Weg zur Compliance, ohne dabei auf Funktionalität, Performance oder Flexibilität verzichten zu müssen.

**Fordern Sie eine Demo an, um Versa Sovereign SASE in Aktion zu sehen.**

**Entdecken Sie Versa Sovereign SASE.**

Versa Networks, Inc
2550 Great America Way, Suite 350
Santa Clara, CA 95054
Tel: +1 408.385.7660
info@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 Plattform 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.

©2026 Versa Networks, Inc. Alle Rechte vorbehalten. Teile der Versa-Produkte sind durch Versa-Patente sowie angemeldete Patente geschützt. Versa Networks und FlexVNF sind Marken oder eingetragene Marken der Versa Networks, Inc. Alle anderen hierin verwendeten oder erwähnten Marken sind Eigentum ihrer jeweiligen Inhaber. Teil-Nr.
SB_SOV-SASE-NIS2-CMP-01.0