Versa Sovereign SASE und KRITIS-Konformität

Adressierung der Anforderungen an kritische Infrastrukturen in Deutschland mit Versa Sovereign SASE

Die Einhaltung von KRITIS erfordert mehr als starke Cybersicherheit. Sie erfordert eine überprüfbare Kontrolle auf Architekturebene darüber, wo Daten verarbeitet werden, wo Richtlinien durchgesetzt werden und wer den Zugriff auf kritische Systeme kontrolliert. Versa Sovereign SASE stellt einen vollständigen SASE-Stack bereit, dessen Daten-, Kontroll- und Verwaltungsebenen vollständig innerhalb der deutschen und EU-Jurisdiktion betrieben werden, unterstützt durch BSI-orientierte Zertifizierungen und flexible Bereitstellungsoptionen für IT- und OT-Umgebungen. Für Organisationen, die KRITIS-Verpflichtungen unterliegen, bietet Versa einen direkten Weg zur Konformität, ohne auf die Sicherheitsfähigkeiten oder die operative Flexibilität zu verzichten, die moderne kritische Infrastrukturen erfordern.

Der KRITIS-Rahmen in Deutschland

Der KRITIS-Rahmen (Kritische Infrastrukturen) verpflichtet Betreiber in zehn Sektoren zu erhöhten Cybersicherheitsauflagen. Zu den wichtigsten Pflichten zählen die Umsetzung dem Stand der Technik entsprechender technischer und organisatorischer Maßnahmen (TOMs), verpflichtende Meldungen von Vorfällen an das BSI innerhalb festgelegter Fristen, regelmäßige Audits und Compliance-Nachweise, Anforderungen an die Lieferkettensicherheit sowie Kontrollen zur Datenlokalisierung für sensible Betriebsdaten.

Versa Sovereign SASE

Vor diesem regulatorischen Hintergrund liefert Versa Sovereign SASE eine Architektur, die speziell für strenge betriebliche, sicherheitstechnische und governance-bezogene Anforderungen entwickelt wurde, und bietet volle Netzwerk- und Sicherheitsfunktionalität, während Daten, Kontrolle und Betrieb innerhalb souveräner Grenzen bleiben.

Als Bereitstellungsmodell der VersaONE Universal SASE Platform adressiert es eine zentrale Einschränkung von herkömmlichem Cloud-SASE: Selbst mit lokalen Points of Presence können Verkehrsprüfung, Richtlinienentscheidungen und Plattformverwaltung weiterhin von Infrastruktur außerhalb der vorgesehenen Jurisdiktion abhängen.

Versa Sovereign SASE richtet alle drei Ebenen der SASE-Architektur innerhalb einer souveränen Betriebsumgebung aus:

- **Kontrollebene:** Identitätsprüfung, Richtlinienbewertung und Verbindungsentscheidungen erfolgen innerhalb der festgelegten souveränen Umgebung.
- **Datenebene:** Verkehrsprüfung, Bedrohungsschutz und Inhaltsfilterung werden an lokalen PoPs ausgeführt, ohne dass Datenverkehr zur Verarbeitung außerhalb der Jurisdiktion umgeleitet wird.
- **Verwaltungsebene:** Plattformadministration, Protokollierung, Konfiguration und operativer Zugriff bleiben lokal gesteuert.

In Deutschland und 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 auch für On-Premises- oder private EU-Cloud-Bereitstellungen verfügbar.

KRITIS-Anforderungen zugeordnet zu Versa Sovereign SASE

Nachfolgend sind die KRITIS-Anforderungen den Versa Sovereign SASE Angeboten zugeordnet.

KRITIS-Anforderung	Versa Sovereign SASE Fähigkeit	Ergebnis
Dem Stand der Technik entsprechende Sicherheitsmaßnahmen (TOMs)	Vollständiger SASE-Stack inklusive ZTNA, NGFW, SWG, CASB, DLP, IPS, ATP, SD-WAN, betrieben innerhalb souveräner EU-Infrastruktur	Weist technische Sicherheitsreife gemäß BSI-Standards und KRITIS-TOM-Pflichten nach
Systeme zur Angriffserkennung (IT-SiG 2.0)	Echtzeit-IDS/IPS, UEBA mit MITRE-ATT&CK-Mapping, automatisierte Eindämmungs-Playbooks und SIEM-Integration	Unterstützt die Anforderungen an Angriffserkennung und kontinuierliches Monitoring gemäß IT-SiG 2.0 in IT- und OT-Umgebungen
Verpflichtende Meldung an das BSI	Automatisierte Alarmierung, vorgefertigte Incident-Response-Playbooks, detaillierte Ereignisprotokolle und BSI-fertige Berichte	Unterstützt die verpflichtende BSI-Meldung innerhalb der festgelegten KRITIS-Fristen
Zugriffskontrolle & privilegierte Zugriffsverwaltung	ZTNA mit kontinuierlicher Statusbewertung, RBAC mit Aufgabentrennung, native MFA und Integration mit Enterprise-Identity-Providern	Setzt Least-Privilege-Zugriff über Nutzer, Geräte und Anwendungen durch; reduziert dauerhafte Drittanbieter-Zugriffsrisiken
Datenresidenz & jurisdiktionelle Souveränität	Alle Daten, Metadaten, Protokolle und Telemetriedaten werden innerhalb von EU-Mitgliedstaaten gespeichert und verarbeitet; kein Zugriff durch Drittstaaten	Unterstützt Organisationen, die stärkere jurisdiktionelle Kontrolle über Betriebs- und Sicherheitsdaten suchen; begrenzt die Exposition gegenüber extraterritorialen Regelungen wie dem U.S. CLOUD Act
Protokollierung, Nachvollziehbarkeit & BSI-Compliance-Nachweise	Unveränderliche, manipulationssichere Audit-Logs; Unterstützung von IPFIX/Syslog/Netflow/PCAP; automatisierte, an BSI-Anforderungen ausgerichtete Compliance-Berichte; GRC-Plattformintegration	Unterstützt die zentrale Sammlung von Audit-Nachweisen und die Vorbereitung auf BSI-Compliance-Prüfungen
Geschäftskontinuität & Resilienz	Active-Active-HA-Clustering mit Failover unter einer Sekunde, SD-WAN-Multipfad-Resilienz (MPLS, Breitband, 4G/5G), automatisierte Konfigurationssicherung und -wiederherstellung, vertragliche SLAs	Erhält die Verfügbarkeit kritischer Dienste bei Hardwareausfällen, Standortausfällen oder aktiven Angriffen aufrecht
Lieferkettensicherheit	Versa kann nachweisen, dass die Sovereign-SASE-Bereitstellung in der EU vollständig souverän ist bzw. über eine ausschließlich EU-basierte Lieferkette verfügt.; ZTNA-gesteuerter, feingranularer Drittanbieterzugriff; anwendungsbasierte Mikrosegmentierung; vertragliche DPA-Verpflichtungen für Subunternehmer	Adressiert die KRITIS-Anforderungen an die IKT-Lieferkettensicherheit mit auditierbaren, least-privilege-basierten Lieferantenzugriffskontrollen
Verschlüsselung & kryptografische Kontrollen	TLS 1.3 und IPsec mit AES-256 für alle Daten während der Übertragung; AES-256-Verschlüsselung im Ruhezustand mit EU-ansässiger Schlüsselverwaltung; HSM-gestützte Schlüsselspeicherung; vollständige SSL/TLS-Inspektion	Unterstützt die dem Stand der Technik entsprechenden KRITIS-Verschlüsselungsanforderungen zum Schutz sensibler Daten während der Übertragung und im Ruhezustand

OT-/ICS-Sicherheit (Energie, Wasser, Verkehr)	Purdue-Modell-orientierte Segmentierung gemäß IEC 62443; Deep Packet Inspection für OT-Protokolle (Modbus, DNP3, IEC 60870-5, PROFINET); passive OT-Asset-Erkennung	Erweitert die Sicherheitssichtbarkeit und Segmentierung in OT-Umgebungen bei gleichzeitiger Aufrechterhaltung der Betriebskontinuität

Warum KRITIS-regulierte Organisationen auf Versa setzen

KRITIS zielt darauf ab, die Sicherheit, Verfügbarkeit und Resilienz essenzieller Dienste durch starke technische und organisatorische Kontrollen gemäß BSI-Vorgaben sicherzustellen.

Als First-to-Market-Anbieter unterstützt Versa Sovereign SASE Organisationen dabei, diese Anforderungen mit einem Bereitstellungsmodell zu erfüllen, das eigens für Kontrolle, Transparenz und operative Unabhängigkeit entwickelt wurde. Versas vollständiger SASE-Stack kann innerhalb kunden- oder souverän kontrollierter Umgebungen bereitgestellt werden und unterstützt strenge Datenschutz- und Governance-Anforderungen, ohne die Funktionalität einzuschränken.

Anders als Plattformen, die auf global verteilter Infrastruktur beruhen, hält Versa den vollständigen SASE-Stack (einschließlich Daten-, Kontroll- und Verwaltungsebene) architektonisch innerhalb souverän kontrollierter Umgebungen und reduziert dadurch externe Abhängigkeiten bei gleichbleibender Leistung und Flexibilität.

Durch die Kombination aus souveräner Bereitstellung und an BSI-Vorgaben ausgerichteten Sicherheitskontrollen bietet Versa KRITIS-konformen Organisationen einen praktikablen Weg zur Compliance, ohne auf Funktionalität, Leistung oder Flexibilität zu verzichten.

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. Angetrieben durch KI liefert die VersaONE Universal SASE Plattform konvergente SSE-, SD-WAN- und SD-LAN-Lösungen, die Daten schützen und vor Cyberbedrohungen verteidigen und gleichzeitig ein hervorragendes digitales Nutzererlebnis bieten. Tausende Kunden weltweit, mit Hunderttausenden von Standorten und Millionen von Nutzern, vertrauen Versa ihre geschäftskritischen Netzwerke und Sicherheit an.

©2026 Versa Networks, Inc. Alle Rechte vorbehalten.
Teilenr. SB_SOV-SASE-KRITIS-CMP-01.0