Versa Sovereign SASE and KRITIS Compliance

Addressing Germany's critical infrastructure requirements with Versa Sovereign SASE

Maintaining KRITIS compliance goes beyond strong cybersecurity. It requires verifiable architecture-level control over where data is processed, where policies are enforced, and who governs access to critical systems. Versa Sovereign SASE delivers a complete SASE stack with all data, control, and management planes operating entirely within German and EU jurisdiction, backed by BSI-aligned certifications and flexible deployment options suited to both IT and OT environments. For organizations subject to KRITIS obligations, Versa offers a direct path to compliance without sacrificing the security capabilities or operational flexibility that modern critical infrastructure demands.

Germany's KRITIS framework

The KRITIS framework (Kritische Infrastrukturen) designates operators across ten sectors as subject to heightened cybersecurity obligations. Key obligations include implementing state-of-the-art technical and organizational measures (TOMs), mandatory incident reporting to the BSI within defined timeframes, regular audits and compliance evidence, supply chain security requirements, and data localization controls for sensitive operational data.

Versa Sovereign SASE

Against this regulatory backdrop, Versa Sovereign SASE delivers an architecture purpose-built to meet stringent operational, security, and governance requirements, providing full networking and security capabilities while keeping data, control, and operations within sovereign boundaries.

A deployment model of the VersaONE Universal SASE Platform, it addresses a key limitation of traditional cloud SASE: even with local points of presence, traffic inspection, policy decisions, and platform management may still depend on infrastructure outside the intended jurisdiction.

Versa Sovereign SASE aligns all three planes of the SASE architecture within a sovereign operating environment:

- **Control plane:** Identity validation, policy evaluation, and connection decisions occur within the designated sovereign environment.
- **Data plane:** Traffic inspection, threat protection, and content filtering are executed at local PoPs, with no traffic hairpinned outside the jurisdiction for processing.
- **Management plane:** Platform administration, logging, configuration, and operational access remain locally governed.

In Germany and the EU, Versa's Sovereign SASE-as-a-Service is available with all operations, data processing, and support governed under EU law, independent of Versa's global cloud infrastructure. For organizations requiring complete infrastructure control, Versa Sovereign SASE is also available for on-premises or private EU cloud deployment.

KRITIS requirements mapped to Versa Sovereign SASE

Below are the KRITIS requirements mapped to Versa Sovereign SASE offerings.

KRITIS requirement	Versa Sovereign SASE capability	Outcome
State-of-the-art security measures (TOMs)	Full SASE stack including ZTNA, NGFW, SWG, CASB, DLP, IPS, ATP, SD-WAN operating within sovereign EU infrastructure	Demonstrates technical security maturity aligned with BSI standards and KRITIS TOM obligations
Attack detection systems (IT-SiG 2.0)	Real-time IDS/IPS, UEBA with MITRE ATT&CK mapping, automated containment playbooks, and SIEM integration	Supports IT-SiG 2.0 attack detection and continuous monitoring requirements across IT and OT environments
Mandatory incident reporting to BSI	Automated alerting, pre-built incident response playbooks, detailed event logs, and BSI-ready reporting	Supports mandatory BSI incident notification within defined KRITIS reporting timeframes
Access control & privileged access management	ZTNA with continuous posture assessment, RBAC with separation of duties, native MFA, and integration with enterprise identity providers	Enforces least-privilege access across users, devices, and applications; reduces persistent third-party access exposure
Data residency & jurisdictional sovereignty	All data, metadata, logs, and telemetry stored and processed within EU member states; no third-country access	Supports organizations seeking stronger jurisdictional control over operational and security data; limits exposure to extraterritorial regulations such as the U.S. CLOUD Act
Logging, auditability & BSI compliance evidence	Immutable, tamper-evident audit logs; IPFIX/Syslog/Netflow/PCAP support; automated compliance reports aligned to BSI requirements; GRC platform integration	Supports centralized audit evidence collection and preparation for BSI compliance review
Business continuity & resilience	Active-active HA clustering with sub-second failover, SD-WAN multi-path resilience (MPLS, broadband, 4G/5G), automated config backup and restore, contractual SLAs	Maintains critical service availability during hardware failures, site outages, or active attacks
Supply chain security	Vetted EU supply chain with full bill-of-materials disclosure; ZTNA-enforced fine-grained third-party access; application-level micro-segmentation; contractual DPA obligations for subprocessors	Addresses KRITIS ICT supply chain requirements with auditable, least-privilege supplier access controls
Encryption & cryptographic controls	TLS 1.3 and IPsec with AES-256 for all data in transit; AES-256 encryption at rest with EU-resident key management; HSM-backed key storage; full SSL/TLS inspection	Supports KRITIS state-of-the-art encryption requirements for protecting sensitive data in transit and at rest
OT/ICS security (energy, water, transport sectors)	Purdue Model-aware segmentation aligned to IEC 62443; deep packet inspection for OT protocols (Modbus, DNP3, IEC 60870-5, PROFINET); passive OT asset discovery	Extends security visibility and segmentation into OT environments while supporting operational continuity

Why KRITIS-regulated organizations choose Versa

KRITIS focuses on ensuring the security, availability, and resilience of essential services through strong technical and organizational controls aligned with BSI guidance.

As the first-to-market vendor, Versa Sovereign SASE helps organizations meet these requirements with a deployment model purpose-built for control, transparency, and operational independence. Versa's full SASE stack can be deployed within customer- or sovereign-controlled environments, supporting strict data protection and governance needs without reducing capability.

Unlike platforms that rely on globally distributed infrastructure, Versa keeps the full SASE stack (including data, control, and management planes) within sovereign-controlled environments by design, reducing external dependencies while maintaining performance and flexibility.

By combining sovereign-aligned deployment with security controls aligned to BSI guidance, Versa gives KRITIS-aligned organizations a practical path to compliance without sacrificing capability, performance, or flexibility.

Request a demo to see Versa Sovereign SASE in action.

Explore Versa Sovereign SASE.

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.

Part# SB_SOV-SASE-KRISTIS-CMP-01.0