Versa Sovereign SASE and NIS2 Compliance

Addressing the EU's Network and Information Security Directive with Versa Sovereign SASE

NIS2 compliance increasingly drives the need for architecture-level assurance over where sensitive data is processed, how 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 EU jurisdiction, backed by independent certifications and flexible deployment options suited to both IT and OT environments. For organizations subject to NIS2 obligations, Versa offers a direct path to compliance without sacrificing security capability or operational flexibility.

The NIS2 directive

The EU's NIS2 Directive (EU 2022/2555) expands cybersecurity and operational resilience obligations for organizations operating critical infrastructure and essential services across the EU. Beyond implementing security controls, NIS2 emphasizes governance, risk management, incident reporting, supply chain security, and demonstrable accountability.

Key requirements include:

- Governance oversight and management accountability (Art. 20)
- Cybersecurity risk management and resilience measures (Art. 21)
- Incident reporting to national authorities and CSIRTs (Art. 23)
- Use of recognized cybersecurity certification frameworks (Art. 24)
- Regulatory oversight and jurisdiction requirements (Art. 26)

These requirements increasingly push organizations toward architectures that provide clear operational control, policy enforcement visibility, auditable security operations, and stronger jurisdictional assurance over sensitive systems and data.

Versa Sovereign SASE

Versa Sovereign SASE is purpose-built to address NIS2 operational and regulatory requirements by keeping the full SASE architecture, including data, control, and management planes, within sovereign-controlled environments. A deployment model of the VersaONE Universal SASE Platform, it addresses the fundamental limitation of traditional cloud-based SASE: even when vendors operate a local point of presence (PoP), traffic inspection, policy decisions, and platform management often still depend on infrastructure outside the intended jurisdiction.

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

- **Data plane:** Traffic inspection, threat protection, and content filtering are executed at local PoPs, with no traffic hair-pinned outside the jurisdiction for processing.

- **Control plane:** Identity validation, policy evaluation, and connection decisions occur within the designated sovereign environment.
- **Management plane:** Platform administration, logging, configuration, and operational access remain locally governed.

In 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.

NIS2 requirements mapped to Versa Sovereign SASE

The table below maps relevant NIS2 requirements to Versa Sovereign SASE capabilities and the compliance outcomes they support.

NIS2 requirement	Versa Sovereign SASE capability	Outcome
Governance & management accountability (Art. 20)	Centralized policy management gives management bodies unified visibility and control over the organization's cybersecurity posture; role-based access with separation of duties ensures appropriate oversight; automated compliance reporting delivers management-ready evidence of cybersecurity status	Enables management bodies to approve, oversee, and demonstrate compliance with NIS2 cybersecurity obligations; supports personal accountability requirements
Risk management policy (Art. 21(2)(a))	Centralized policy management via Versa Director with single-pane-of-glass visibility; continuous UEBA and AI-driven risk assessment; version-controlled security baselines	Supports documented, risk-based security policies with auditable baselines aligned to NIS2 obligations
Incident detection & response (Art. 21(2)(b))	Real-time IDS/IPS, ATP with MITRE ATT&CK mapping, automated containment playbooks, SIEM integrations	Supports rapid detection and containment of security incidents in line with Art. 21(2)(b) incident handling obligations
Business continuity (Art. 21(2)(c))	Active-active HA clustering with sub-second failover; SD-WAN multi-path resilience (MPLS, broadband, LTE/4G/5G); automated config backup and restore; contractual SLAs	Maintains critical service availability during hardware failures, site outages, or active attacks
Supply chain security (Art. 21(2)(d))	EU supply chain with full bill-of-materials disclosure; ZTNA-enforced fine-grained third-party access; application-level micro-segmentation; NIS2-aligned contractual DPA obligations for subprocessors; all data, metadata, logs, and telemetry processed within EU-governed operational environments	Addresses NIS2 ICT supply chain requirements with auditable, least-privilege supplier access controls; reduces exposure to cross-border regulatory and jurisdictional complexity
Secure system acquisition (Art. 21(2)(e))	Secure-by-design SASE architecture; all components subject to security review and patch management; automated patch deployment and threat intelligence feeds	Demonstrates security-first acquisition practices with ongoing vulnerability management
Effectiveness assessment (Art. 21(2)(f))	Automated compliance reporting aligned to NIS2 requirements; real-time dashboards across all security domains; immutable, tamper-evident audit logs; GRC platform integration	Provides measurable evidence of security control effectiveness; supports internal and external audits

NIS2 requirement	Versa Sovereign SASE capability	Outcome
Cybersecurity hygiene (Art. 21(2)(g))	Enforced security baselines across all users, devices, and workloads; automated patch deployment; integrated threat intelligence feeds; continuous posture assessment	Maintains consistent security hygiene at scale, reducing attack surface across the organization
Cryptography & encryption (Art. 21(2)(h))	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 NIS2 encryption obligations for data in motion and at rest within sovereign boundaries
Access control & HR security (Art. 21(2)(i))	ZTNA with continuous posture assessment; RBAC with separation of duties; native MFA; integration with enterprise identity providers (Azure AD, Okta, ADFS); audit trail of privileged operations	Enforces least-privilege access across users, devices, and applications; eliminates standing third-party access
MFA & secure communications (Art. 21(2)(j))	Native MFA for all user and administrator access; continuous, post-authentication trust evaluation based on device posture and user behavior; all communications encrypted end-to-end	Supports NIS2 MFA and secure communications requirements across users and workloads
Incident reporting timelines (Art. 23)	Detailed, timestamped and tamper-evident event logs; SIEM integration and NIS2-ready reporting templates for competent authority and CSIRT notification; pre-built incident response playbooks with automated alerting to support structured reporting workflows	Supports mandatory 24-hour early warning, 72-hour incident notification, and 1-month final report timelines to national CSIRTs and competent authorities
Cybersecurity certification schemes (Art. 24)	ISO/IEC 27001:2022, SOC 2 Type II, BSI C5, ISO/IEC 27017, and ISO/IEC 27018 certifications; alignment with ENISA Cybersecurity Certification Framework under the EU Cybersecurity Act	Supports demonstration of NIS2 compliance through certification schemes aligned with Article 24 and the EU Cybersecurity Act
Jurisdiction & territoriality (Art. 26)	All operations, data processing, and support governed under EU law via Versa Sovereign SASE-as-a-Service; EU-resident operational staff; no third-country infrastructure dependencies	Ensures supervisory jurisdiction remains cleanly within the designated EU member state authority, with no extraterritorial complications

OT/ICS environments

For NIS2-obligated entities in the energy, transport, water, and manufacturing sectors, securing operational technology environments is a distinct challenge. Versa Sovereign SASE extends NIS2 security controls into OT environments without disrupting operational processes:

- **Purdue Model-aware segmentation:** Enforce zone-based access controls aligned with IEC 62443 and the Purdue Reference Model for industrial networks.
- **Industrial protocol inspection:** Deep packet inspection for OT protocols (Modbus, DNP3, IEC 60870-5, PROFINET) enables anomaly detection without operational disruption.
- **Passive OT asset discovery:** Identify and inventory OT assets across IT/OT convergence environments without active scanning and requiring additional sensors.

Why NIS2-obligated organizations choose Versa

As the first-to-market vendor, Versa Sovereign SASE is purpose-built for jurisdictional, regulatory, and operational sovereignty. Unlike platforms that rely on global infrastructure behind localized gateways, Versa keeps the full SASE stack within sovereign-controlled environments by design.

This architecture helps organizations address growing NIS2 expectations around risk management, operational resilience, governance, and control over critical digital infrastructure.

Versa addresses all three sovereignty planes (data, control, and management) without dependencies on foreign infrastructure or trade-offs in security capability. NIS2-obligated entities receive the complete VersaONE platform in a fully sovereign architecture, with flexible deployment options ranging from Sovereign SASE-as-a-Service to private EU cloud and on-premises.

By enforcing sovereignty across data, control, and management planes supporting NIS2-aligned security and governance objectives, Versa gives entities a clear, 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-NIS2-CMP-01.0