

Versa Sovereign SASE et conformité NIS2

Répondre à la directive européenne sur la sécurité des réseaux et de l'information avec Versa Sovereign SASE

La conformité à NIS2 impose de plus en plus une assurance au niveau architectural quant à l'endroit où les données sensibles sont traitées, à la manière dont les politiques sont appliquées, et à qui gouverne l'accès aux systèmes critiques. Versa Sovereign SASE fournit une solution SASE complète dont l'ensemble des plans de données, de contrôle et de gestion fonctionnent entièrement au sein de la juridiction de l'UE, appuyée par des certifications indépendantes et des options de déploiement flexibles adaptées aussi bien aux environnements IT qu'OT. Pour les organisations soumises aux obligations NIS2, Versa offre une voie directe vers la conformité, sans sacrifier les capacités de sécurité ni la flexibilité opérationnelle.

La directive NIS2

La directive NIS2 de l'UE (UE 2022/2555) élargit les obligations de cybersécurité et de résilience opérationnelle pour les organisations exploitant des infrastructures critiques et des services essentiels dans l'ensemble de l'UE. Au-delà de la mise en œuvre de contrôles de sécurité, NIS2 met l'accent sur la gouvernance, la gestion des risques, la notification des incidents, la sécurité de la chaîne d'approvisionnement et une responsabilité démontrable.

Les exigences clés incluent :

- Supervision de la gouvernance et responsabilité de la direction (art. 20)
- Gestion des risques de cybersécurité et mesures de résilience (art. 21)
- Notification des incidents aux autorités nationales et aux CSIRT (art. 23)
- Recours à des cadres de certification de cybersécurité reconnus (art. 24)
- Exigences de supervision réglementaire et de juridiction (art. 26)

Ces exigences poussent de plus en plus les organisations vers des architectures offrant un contrôle opérationnel clair, une visibilité sur l'application des politiques, des opérations de sécurité auditable et une assurance juridictionnelle renforcée sur les systèmes et données sensibles.

Versa Sovereign SASE

Versa Sovereign SASE est conçu spécifiquement pour répondre aux exigences opérationnelles et réglementaires de NIS2 en maintenant l'intégralité de l'architecture SASE, y compris les plans de données, de contrôle et de gestion, au sein d'environnements sous contrôle souverain. En tant que modèle de déploiement de la plateforme VersaONE Universal SASE, cette solution répond à la limite fondamentale du SASE cloud-based traditionnel : même lorsque les fournisseurs exploitent un point de présence local (PoP), l'inspection du trafic, les décisions de politique et la gestion de la plateforme continuent souvent de dépendre d'une infrastructure située hors de la juridiction visée.

Versa Sovereign SASE aligne les trois plans de l'architecture SASE au sein d'un environnement d'exploitation souverain :

- **Plan de données** : l'inspection du trafic, la protection contre les menaces et le filtrage de contenu sont exécutés au niveau des points de présence locaux, sans détournement du trafic pour traitement hors juridiction.
- **Plan de contrôle** : la validation d'identité, l'évaluation des politiques et les décisions de connexion s'effectuent au sein de l'environnement souverain désigné.
- **Plan de gestion** : l'administration de la plateforme, la journalisation, la configuration et l'accès opérationnel restent gouvernés localement.

Dans l'UE, le service Sovereign SASE-as-a-Service de Versa est disponible avec l'ensemble des opérations, du traitement des données et du support régis par le droit de l'UE, indépendamment de l'infrastructure cloud mondiale de Versa. Pour les organisations exigeant un contrôle infrastructurel complet, Versa Sovereign SASE est également disponible en déploiement sur site ou en cloud privé au sein de l'UE.

Correspondance entre les exigences NIS2 et Versa Sovereign SASE

Le tableau ci-dessous met en correspondance les exigences NIS2 pertinentes avec les capacités de Versa Sovereign SASE et les résultats de conformité qu'elles permettent d'atteindre.

Exigence NIS2	Capacité Versa Sovereign SASE	Résultat
Supervision de la gouvernance et responsabilité de la direction (art. 20)	La gestion centralisée des politiques offre aux organes de direction une visibilité et un contrôle unifiés sur la posture de cybersécurité de l'organisation ; l'accès basé sur les rôles avec séparation des tâches garantit une supervision adéquate ; le reporting de conformité automatisé fournit des preuves prêtes pour la direction sur l'état de la cybersécurité	Permet aux organes de direction d'approuver, de superviser et de démontrer la conformité aux obligations de cybersécurité NIS2 ; soutient les exigences de responsabilité personnelle
Politique de gestion des risques (art. 21, § 2, a)	Gestion centralisée des politiques via Versa Director avec visibilité en un seul volet ; UEBA continue et évaluation des risques pilotée par IA ; référentiels de sécurité sous contrôle de version	Soutient des politiques de sécurité documentées et fondées sur le risque, avec des référentiels auditable conformes aux obligations NIS2
Détection et réponse aux incidents (art. 21, § 2, b)	IDS/IPS en temps réel, ATP avec cartographie MITRE ATT&CK, playbooks de confinement automatisés, intégrations SIEM	Soutient la détection et le confinement rapides des incidents de sécurité, conformément aux obligations de traitement des incidents de l'art. 21, § 2, b
Continuité des activités (art. 21, § 2, c)	Clustering haute disponibilité actif-actif avec basculement en moins d'une seconde ; résilience multi-chemins du SD-WAN (MPLS, haut débit, LTE/4G/5G) ; sauvegarde et restauration automatisées de la configuration ; SLA contractuels	Maintient la disponibilité des services critiques en cas de panne matérielle, d'interruption de site ou d'attaque active
Sécurité de la chaîne d'approvisionnement (art. 21, § 2, d)	Chaîne d'approvisionnement européenne avec divulgation complète de la nomenclature ; accès tiers finement contrôlé et appliqué par ZTNA ; micro-segmentation au niveau applicatif ; obligations contractuelles de sous-traitance conformes à NIS2 pour les sous-traitants ultérieurs ; l'ensemble des données, métadonnées, journaux et données de télémétrie sont traités au sein d'environnements d'exploitation régis par l'UE	Répond aux exigences NIS2 relatives à la chaîne d'approvisionnement TIC grâce à des contrôles d'accès fournisseurs auditable et fondés sur le moindre privilège ; réduit l'exposition à la complexité réglementaire et juridictionnelle transfrontalière

Acquisition sécurisée des systèmes (art. 21, § 2, e)	Architecture SASE sécurisée dès la conception ; l'ensemble des composants fait l'objet d'un examen de sécurité et d'une gestion des correctifs ; déploiement automatisé des correctifs et flux de renseignement sur les menaces	Démontre des pratiques d'acquisition axées sur la sécurité, avec une gestion continue des vulnérabilités
Évaluation de l'efficacité (art. 21, § 2, f)	Reporting de conformité automatisé aligné sur les exigences NIS2 ; tableaux de bord en temps réel sur l'ensemble des domaines de sécurité ; journaux d'audit immuables et inviolables ; intégration à une plateforme GRC	Fournit des preuves mesurables de l'efficacité des contrôles de sécurité ; soutient les audits internes et externes
Hygiène de cybersécurité (art. 21, § 2, g)	Référentiels de sécurité appliqués à l'ensemble des utilisateurs, équipements et charges de travail ; déploiement automatisé des correctifs ; flux de renseignement sur les menaces intégrés ; évaluation continue de la posture	Maintient une hygiène de sécurité cohérente à grande échelle, réduisant la surface d'attaque de l'ensemble de l'organisation
Cryptographie et chiffrement (art. 21, § 2, h)	TLS 1.3 et IPsec avec AES-256 pour l'ensemble des données en transit ; chiffrement AES-256 des données au repos avec gestion des clés résidant dans l'UE ; stockage des clés sécurisé par HSM ; inspection SSL/TLS complète	Soutient les obligations NIS2 de chiffrement des données en transit et au repos au sein de frontières souveraines
Contrôle d'accès et sécurité RH (art. 21, § 2, i)	ZTNA avec évaluation continue de la posture ; RBAC avec séparation des tâches ; MFA native ; intégration avec les fournisseurs d'identité d'entreprise (Azure AD, Okta, ADFS) ; piste d'audit des opérations privilégiées	Applique l'accès selon le principe du moindre privilège pour les utilisateurs, équipements et applications ; élimine les accès tiers permanents
MFA et communications sécurisées (art. 21, § 2, j)	MFA native pour l'ensemble des accès utilisateurs et administrateurs ; évaluation continue de la confiance post-authentification basée sur la posture des équipements et le comportement des utilisateurs ; toutes les communications chiffrées de bout en bout	Soutient les exigences NIS2 en matière de MFA et de communications sécurisées pour les utilisateurs et les charges de travail
Délais de notification des incidents (art. 23)	Journaux d'événements détaillés, horodatés et inviolables ; intégration SIEM et modèles de rapport conformes à NIS2 pour la notification aux autorités compétentes et aux CSIRT ; playbooks de réponse aux incidents préconfigurés avec alertes automatisées, en appui à des processus de notification structurés	Soutient les délais obligatoires : alerte précoce sous 24 heures, notification d'incident sous 72 heures, et rapport final sous un mois, auprès des CSIRT nationaux et des autorités compétentes
Régimes de certification de cybersécurité (art. 24)	Certifications ISO/IEC 27001:2022, SOC 2 Type II, BSI C5, ISO/IEC 27017 et ISO/IEC 27018 ; alignement avec le cadre de certification de cybersécurité de l'ENISA au titre du règlement européen sur la cybersécurité	Soutient la démonstration de la conformité NIS2 par le biais de régimes de certification conformes à l'article 24 et au règlement européen sur la cybersécurité
Juridiction et territorialité (art. 26)	L'ensemble des opérations, du traitement des données et du support est régi par le droit de l'UE via Versa Sovereign SASE-as-a-Service ; personnel d'exploitation résidant dans l'UE ; aucune dépendance à une infrastructure de pays tiers	Garantit que la compétence de supervision demeure clairement du ressort de l'autorité de l'État membre de l'UE désigné, sans complication extraterritoriale

Environnements OT/ICS

Pour les entités soumises à NIS2 dans les secteurs de l'énergie, des transports, de l'eau et de l'industrie manufacturière, la sécurisation des environnements de technologie opérationnelle constitue un enjeu spécifique. Versa Sovereign SASE étend les contrôles de sécurité NIS2 aux environnements OT sans perturber les processus opérationnels :

- **Segmentation tenant compte du modèle de Purdue:** application de contrôles d'accès basés sur des zones, conformes à la norme IEC 62443 et au modèle de référence de Purdue pour les réseaux industriels.
- **Inspection des protocoles industriels:** l'inspection approfondie des paquets (DPI) pour les protocoles OT (Modbus, DNP3, IEC 60870-5, PROFINET) permet une détection des anomalies sans perturbation opérationnelle.
- **Découverte passive des actifs OT:** identification et inventaire des actifs OT dans les environnements de convergence IT/OT, sans balayage actif ni capteurs supplémentaires requis.

Pourquoi les organisations soumises à NIS2 choisissent Versa

En tant que premier fournisseur à avoir lancé le Sovereign SASE sur le marché, Versa Sovereign SASE est conçu spécifiquement pour la souveraineté juridique, réglementaire et opérationnelle. Contrairement aux plateformes qui s'appuient sur une infrastructure mondiale derrière des passerelles localisées, Versa maintient, par conception, l'intégralité de la solution SASE au sein d'environnements sous contrôle souverain.

Cette architecture aide les organisations à répondre aux attentes croissantes de NIS2 en matière de gestion des risques, de résilience opérationnelle, de gouvernance et de contrôle des infrastructures numériques critiques.

Versa couvre les trois plans de souveraineté (données, contrôle et gestion) sans dépendance à une infrastructure étrangère ni compromis sur les capacités de sécurité. Les entités soumises à NIS2 bénéficient de la plateforme VersaONE complète au sein d'une architecture entièrement souveraine, avec des options de déploiement flexibles allant du Sovereign SASE-as-a-Service au cloud privé de l'UE et au déploiement sur site.

En appliquant la souveraineté sur l'ensemble des plans de données, de contrôle et de gestion, au service d'objectifs de sécurité et de gouvernance conformes à NIS2, Versa offre aux entités une voie claire et concrète vers la conformité, sans sacrifier les capacités, la performance ou la flexibilité.

Demandez une démonstration pour voir Versa Sovereign SASE en action.

Découvrez Versa Sovereign SASE.



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.