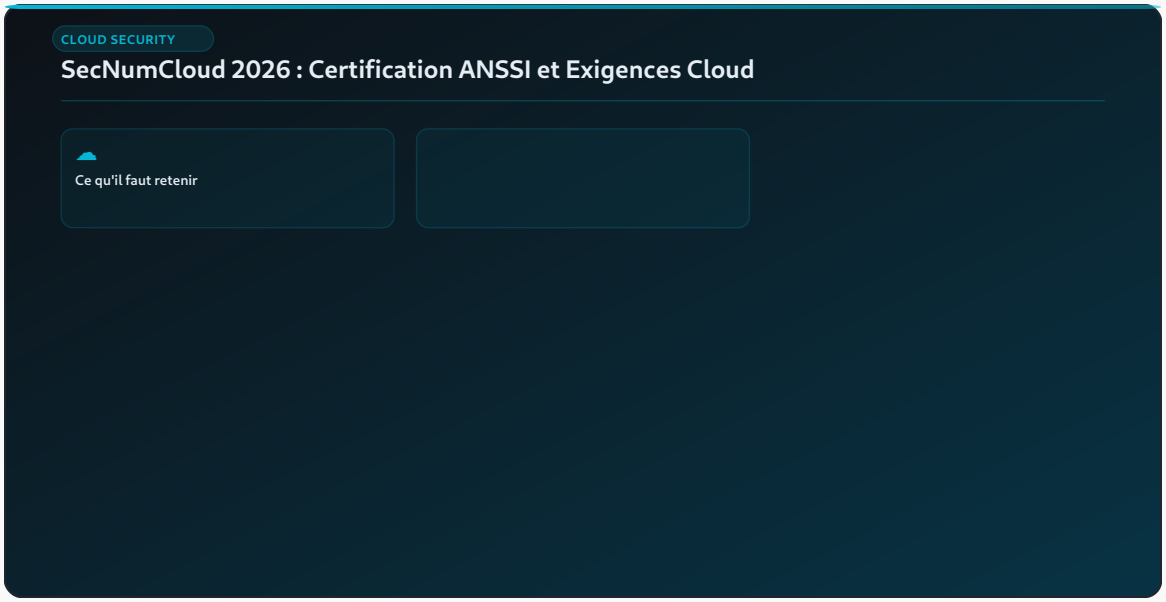
SecNumCloud 2026 : Certification Cloud ANSSI et Exigences Techniques

> Guide SecNumCloud 2026 : référentiel ANSSI v3.2, exigences techniques et organisationnelles, prestataires qualifiés et avantages pour données sensibles.

SecNumCloud est le référentiel de qualification des prestataires de services cloud publié par l'ANSSI. En 2026, sa version 3.2 est la référence incontournable pour les administrations publiques françaises et les organisations souhaitant héberger leurs données sensibles dans un environnement cloud souverain et sécurisé. Face à la prolifération des offres cloud et aux inquiétudes légitimes sur la souveraineté des données, SecNumCloud offre une garantie formelle d'indépendance vis-à-vis des droits extraterritoriaux étrangers — notamment le Cloud Act américain — et un niveau d'exigences techniques et organisationnelles significativement plus élevé que les certifications cloud classiques comme ISO 27001 ou SOC 2. Ce guide complet détaille les exigences du référentiel SecNumCloud v3.2, les prestataires qualifiés disponibles en France en 2026, les différences fondamentales avec ISO 27001 et HDS, le processus de qualification et les cas d'usage pour lesquels SecNumCloud est recommandé voire obligatoire selon les circulaires du SGDSN et les obligations NIS2. La qualification SecNumCloud est l'une des réponses françaises et européennes les plus crédibles aux enjeux de souveraineté numérique dans un contexte géopolitique où la localisation et la protection des données sont devenues des enjeux stratégiques de premier ordre pour les États, les OIV et les entreprises opérant dans les secteurs critiques de l'économie nationale.

À RETENIR



SecNumCloud v3.2 est le référentiel ANSSI le plus exigeant pour les services cloud destinés aux données sensibles des administrations et des OIV.

La protection contre les **droits extraterritoriaux** (Cloud Act, FISA) est une exigence centrale — les hyperscalers américains ne peuvent pas être qualifiés tels quels.

Les prestataires qualifiés en 2026 incluent **OVHcloud, Outscale (Dassault Systèmes) et Bleu** (Orange/Capgemini pour Microsoft 365 souverain).

SecNumCloud est **recommandé voire obligatoire** pour les OIV et les administrations traitant des données sensibles selon les circulaires SGDSN.

Le processus de qualification prend **12 à 24 mois** et représente un investissement de plusieurs centaines de milliers d'euros pour les prestataires.

L'articulation NIS2 + SecNumCloud offre la protection la plus complète pour les systèmes d'information essentiels des entités critiques françaises.

Qu'est-ce que SecNumCloud et pourquoi est-il stratégique en 2026

SecNumCloud est le *référentiel de qualification des prestataires de services cloud* établi par l'ANSSI. Il définit les exigences de sécurité et de souveraineté que doivent respecter les fournisseurs de services cloud souhaitant obtenir la qualification ANSSI — la plus haute marque de confiance pour l'hébergement de données sensibles en France. La version 3.2, publiée en 2022, renforce significativement les exigences par rapport aux versions précédentes, notamment sur la protection contre les droits extraterritoriaux étrangers.

⚡ Retour terrain

La configuration par défaut des providers cloud est rarement sécurisée. J'applique systématiquement un benchmark CIS au premier audit : AWS CIS Benchmark, Azure Security Benchmark, ou GCP CIS Benchmark selon le cas. Sur les 50 derniers environnements cloud audités, aucun n'atteignait le score minimal de conformité CIS niveau 1 sans intervention préalable. Les findings les plus fréquents : logging CloudTrail/ Activity Log désactivé sur certaines régions, MFA non forcé sur les comptes root/admin, et SGs/NSGs avec des règles 0.0.0.0/0 en entrée.

En 2026, SecNumCloud est stratégique pour trois raisons convergentes. La première est la **souveraineté des données** : le Cloud Act américain de 2018 permet aux autorités américaines d'accéder aux données stockées sur des serveurs gérés par des entreprises de droit américain, même si ces serveurs sont physiquement localisés en Europe. SecNumCloud exige que les prestataires qualifiés soient immunisés contre ces droits extraterritoriaux — ce qui exclut de facto les hyperscalers américains des qualifications SecNumCloud, quelle que soit la localisation physique de leurs datacenters européens. La deuxième est l'obligation réglementaire émergente : des circulaires interministérielles et recommandations du SGDSN imposent l'utilisation de services qualifiés SecNumCloud pour certaines catégories de données des administrations et OIV. La troisième est la montée en puissance de NIS2 qui renforce les exigences sur les prestataires cloud des entités essentielles.

SecNumCloud v3.2 : les 20 domaines d'exigences du référentiel

Le référentiel SecNumCloud v3.2 est organisé en **20 domaines de sécurité** couvrant l'intégralité des aspects d'un service cloud sécurisé. Ces domaines incluent la gouvernance et la gestion des risques, la gestion des actifs et des configurations, la sécurité physique des datacenters, la sécurité des réseaux et communications, la gestion des identités et des accès, la sécurité des opérations cloud, la gestion des incidents et de la continuité, le développement sécurisé des services, la gestion des vulnérabilités et des correctifs, et la conformité réglementaire. Les exigences sont classées en trois catégories : de base (applicables à tous), renforcées (pour les IaaS et PaaS) et de souveraineté.

Les **exigences de souveraineté** de la version 3.2 sont les plus structurantes et discriminantes. Le prestataire et ses actionnaires de contrôle doivent être de droit européen et ne pas être soumis à des législations extraterritoriales permettant à des États tiers d'accéder aux données des clients sans leur consentement. Les données des clients doivent être hébergées exclusivement sur le territoire de l'Union Européenne. Les équipes ayant accès aux données clients doivent être localisées en UE. Et le prestataire doit démontrer sa capacité à refuser tout accès non consenti à des autorités étrangères, avec les garanties juridiques appropriées.

Les exigences techniques incluent : des **contrôles d'accès** renforcés avec MFA obligatoire pour toutes les interfaces d'administration, une **isolation multi-tenant** garantissant qu'un client ne peut pas accéder aux données d'un autre client, un **chiffrement des données** au repos et en transit avec gestion des clés permettant au client de contrôler ses propres clés (BYOK), une **journalisation complète** de tous les accès aux données des clients, et des **sauvegardes** redondantes avec tests de restauration documentés régulièrement.

Les prestataires qualifiés SecNumCloud en 2026 : état des lieux

La liste des prestataires qualifiés SecNumCloud, publiée et maintenue par l'ANSSI, compte en 2026 un nombre encore limité d'acteurs mais s'enrichit progressivement. Les principaux prestataires qualifiés ou en cours de qualification illustrent la diversité des offres disponibles.

Prestataire	Type	Positionnement
OVHcloud	IaaS qualifié	Premier grand acteur qualifié, datacenters France, leader prix
Outscale (Dassault)	IaaS qualifié	Filiale Dassault Systèmes, industrie et défense
Bleu (Orange/ Capgemini)	IaaS/SaaS souverain Microsoft	Microsoft 365 et Azure sur infrastructure souveraine française
S3NS (Thales/Google)	IaaS/SaaS souverain Google	Google Cloud sur infrastructure souveraine gérée par Thales

SecNumCloud vs ISO 27001 vs HDS : comparatif détaillé

Les certifications cloud ISO 27001, HDS et SecNumCloud répondent à des objectifs différents et ne doivent pas être confondues. L'**ISO 27001** est une certification de système de management de la sécurité de l'information applicable à toute organisation. Elle couvre la sécurité de l'information (CID) mais n'impose aucune exigence de souveraineté. Un prestataire cloud

américain peut être certifié ISO 27001 tout en étant soumis au Cloud Act — les deux sont parfaitement compatibles. La **certification HDS** (Hébergement Données de Santé), obligatoire pour tout hébergeur de données de santé personnelles, couvre des exigences spécifiques au secteur santé mais n'impose pas d'immunité aux droits extraterritoriaux. **SecNumCloud** est le seul référentiel qui intègre explicitement les exigences de souveraineté et d'immunité aux droits extraterritoriaux, ce qui est sa valeur ajoutée distinctive et discriminante.

Les trois certifications sont cumulables : un prestataire peut être simultanément qualifié SecNumCloud, certifié ISO 27001 ET certifié HDS, offrant la couverture la plus complète pour les données les plus sensibles du secteur santé. C'est d'ailleurs la cible que visent les prestataires SecNumCloud qui souhaitent adresser le marché hospitalier et médico-social, où la certification HDS est obligatoire et où SecNumCloud est de plus en plus demandé pour les données les plus sensibles des établissements de santé soumis à NIS2.

Le processus de qualification SecNumCloud : étapes et délais pratiques

L'obtention de la qualification SecNumCloud est un processus long et exigeant reflétant le niveau d'ambition du référentiel. Les prestataires doivent anticiper un délai de **12 à 24 mois minimum** entre le démarrage du processus et l'obtention de la qualification, selon leur maturité initiale.

La **phase de préparation** (3-12 mois) : analyse de l'écart par rapport aux exigences SecNumCloud, développement de la documentation requise (politique de sécurité, procédures, registres), déploiement des contrôles manquants, et préparation aux audits. La **phase d'audit** (2-4 mois) : un organisme d'audit qualifié PASSI réalise un audit complet couvrant tous les domaines du référentiel, incluant des tests techniques intrusifs et des inspections sur site des datacenters et des équipes. La **phase d'instruction ANSSI** (3-6 mois) : l'ANSSI instruit le dossier et émet sa décision de qualification. La qualification est valable 3 ans avec des audits de surveillance annuels. Le coût du processus pour un prestataire de taille intermédiaire est estimé entre 300 000 et 1 million d'euros, incluant les investissements de mise à niveau, les coûts d'audit et les ressources internes mobilisées.

Cas d'usage SecNumCloud : obligations et recommandations

SecNumCloud n'est pas pertinent pour tous les cas d'usage cloud. Son niveau d'exigences et les surcoûts associés (20-50 % plus cher que le cloud standard) le réservent aux situations où la souveraineté des données et le niveau de sécurité renforcé justifient cet investissement. Les cas pour lesquels SecNumCloud est **obligatoire ou fortement recommandé** : données sensibles des administrations publiques, systèmes d'information des OIV désignés par le SGDSN, entités essentielles NIS2 traitant des données critiques pour leurs services essentiels, entreprises de la BITD (Base Industrielle et Technologique de Défense), et organisations soumises à des obligations sectorielles de localisation des données en France.

Les cas d'usage **optionnels mais bénéfiques** : entreprises souhaitant démontrer à leurs clients une posture de souveraineté des données supérieure au marché, prestataires répondant à des appels d'offres publics où SecNumCloud est critère de sélection, organisations traitant des données personnelles sensibles qui veulent aller au-delà des obligations RGPD, et secteurs santé et finance cherchant à combiner HDS/DORA avec des garanties de souveraineté maximales.

Chiffrement et gestion des clés dans SecNumCloud

La gestion du chiffrement et des clés cryptographiques est l'un des domaines les plus différenciants de SecNumCloud. Le référentiel impose que les clients puissent **contrôler leurs propres clés de chiffrement** (BYOK — Bring Your Own Key) pour les données les plus sensibles, garantissant que même le prestataire qualifié ne peut pas accéder en clair aux données sans la participation active du client. Pour le plus haut niveau de protection, SecNumCloud recommande une architecture avec un **HSM (Hardware Security Module)** dédié localisé dans les locaux du client ou sous son contrôle direct.

Les algorithmes cryptographiques utilisés doivent être conformes aux recommandations ANSSI publiées dans le RGS (Référentiel Général de Sécurité) : AES-256 pour le chiffrement symétrique, RSA-4096 ou courbes elliptiques recommandées pour le chiffrement asymétrique. L'exclusion des algorithmes propriétaires dont la robustesse n'est pas publiquement validée par la

communauté cryptographique internationale est une exigence explicite. Cette conformité aux algorithmes RGS garantit également la compatibilité avec les exigences de chiffrement des systèmes d'information gouvernementaux français et facilite l'interconnexion sécurisée entre les services cloud SecNumCloud et les systèmes on-premise des administrations.

Articulation SecNumCloud avec NIS2 pour les entités essentielles

SecNumCloud et NIS2 s'articulent de manière complémentaire. NIS2 impose des mesures de sécurité pour les services cloud des entités essentielles et importantes sans imposer spécifiquement SecNumCloud. Cependant, les guides ANSSI d'application de NIS2 recommandent fortement les services qualifiés SecNumCloud pour les données sensibles des entités essentielles, et l'utilisation de SecNumCloud est valorisée lors des contrôles NIS2 comme preuve d'une approche rigoureuse de la gestion des risques cloud.

Pour les entités soumises à la fois à NIS2, DORA et HDS, la stratégie optimale de certification cloud est : SecNumCloud pour les données et systèmes les plus critiques, HDS ou PCI DSS pour les données sensibles sectorielles, et ISO 27001 + SOC 2 pour les données moins sensibles. Cette stratégie multi-niveaux optimise les coûts tout en maintenant un niveau de protection adapté à la classification des données. Notre guide NIS2 Phase 2 et notre guide HDS 2026 détaillent les articulations pratiques avec SecNumCloud.

SecNumCloud et le cloud souverain européen : EUCS et GAIA-X

SecNumCloud s'inscrit dans un mouvement de construction d'un écosystème cloud souverain européen. L'**EUCS** (European Union Cybersecurity Certification Scheme for Cloud Services) développé par l'ENISA vise un schéma harmonisé au niveau européen avec plusieurs niveaux d'assurance. Le niveau Élevé de l'EUCS devrait inclure des exigences proches de SecNumCloud sur l'immunité aux droits extraterritoriaux. SecNumCloud constitue ainsi le modèle français qui a influencé la conception de ce niveau d'assurance maximale dans le schéma européen. L'adoption

de l'EUCS permettrait une reconnaissance mutuelle entre les qualifications nationales européennes, facilitant l'accès des prestataires qualifiés SecNumCloud aux marchés d'autres États membres sans avoir à obtenir des qualifications nationales distinctes dans chaque pays.

GAIA-X, le projet d'infrastructure cloud fédérée européenne, a évolué vers un cadre de certification et d'interopérabilité. OVHcloud est l'un des membres fondateurs et plusieurs prestataires SecNumCloud y participent activement. La double appartenance à GAIA-X et la qualification SecNumCloud positionnent ces prestataires comme les champions de la souveraineté numérique européenne, un argument commercial de plus en plus puissant dans les appels d'offres publics où les critères de souveraineté gagnent du poids dans les grilles d'évaluation.

Retours terrain : migration vers SecNumCloud en pratique

Les organisations ayant réalisé une migration vers un environnement cloud qualifié SecNumCloud partagent des retours convergents. Le premier défi est la **disponibilité des services** : le catalogue de services des prestataires SecNumCloud est plus restreint que celui des hyperscalers. Certains services cloud avancés (IA générative, analytics grande échelle, services IoT complexes) ne sont pas encore disponibles en version qualifiée SecNumCloud. Le deuxième défi est le **surcoût** de 20-50 % par rapport aux offres standard, justifié par les exigences plus élevées mais représentant un frein pour les budgets IT contraints.

Un retour terrain particulièrement illustratif : lors de l'accompagnement d'une Direction Régionale ministérielle dans sa migration vers SecNumCloud pour ses systèmes RH, le principal point de friction n'était pas technique mais organisationnel — la nécessité de re-valider tous les niveaux de confidentialité des données gérées. Cet exercice de classification, perçu initialement comme une contrainte administrative, s'est révélé être un bénéfice inattendu conduisant à une réorganisation globale de la protection des données RH bien au-delà du seul choix du prestataire cloud. La démarche SecNumCloud a ainsi agi comme catalyseur d'une gouvernance des données plus rigoureuse dans l'ensemble de la direction régionale.

Perspectives SecNumCloud 2027 : évolution du référentiel et du marché

L'ANSSI a signalé une révision du référentiel SecNumCloud pour 2026-2027 afin d'intégrer les enseignements des premières qualifications v3.2, d'adapter les exigences aux nouvelles technologies (conteneurs, Kubernetes, edge computing, IA dans les services cloud) et de s'aligner sur l'EUCS. Le marché des prestataires qualifiés devrait s'élargir avec l'arrivée de nouveaux acteurs : prestataires sectoriels (santé, défense), filiales françaises d'acteurs européens (Thales, Atos T-Systems), et offres hybrides innovantes comme Bleu et S3NS.

La demande institutionnelle pour la souveraineté numérique, portée par NIS2, DORA et les circulaires interministérielles, devrait accélérer cette expansion. Le surcoût SecNumCloud par rapport au cloud standard devrait se réduire progressivement avec l'augmentation du nombre de prestataires qualifiés et l'économie d'échelle qui en découle. Les ressources officielles SecNumCloud sont disponibles sur cyber.gouv.fr/secnumcloud et les orientations EUCS sur le site de l'ENISA. Pour les entités cherchant à optimiser leur architecture cloud au-delà de SecNumCloud, notre guide AWS Well-Architected Security offre une perspective complémentaire sur les bonnes pratiques de sécurité cloud dans les environnements non-qualifiés SecNumCloud.

Sécurité des APIs et des interfaces cloud dans SecNumCloud

La sécurité des interfaces de programmation (APIs) et des consoles d'administration cloud est une exigence centrale de SecNumCloud v3.2. Les prestataires qualifiés doivent imposer des mécanismes d'authentification forte (MFA obligatoire) sur toutes les interfaces d'administration et d'accès aux données des clients, des politiques de rotation régulière des clés d'API et des jetons d'accès, des limitations de débit (rate limiting) sur les APIs pour prévenir les abus et les attaques par force brute, et une journalisation exhaustive de tous les appels API avec conservation sécurisée des logs pendant une durée minimale définie.

Les clients des services SecNumCloud bénéficient de garanties sur la sécurité des APIs qu'ils ne peuvent pas toujours obtenir auprès des hyperscalers américains : les API Gateway des prestataires qualifiés sont auditées lors du processus de qualification et font l'objet de tests de pénétration réguliers par des auditeurs PASSI indépendants. Cette assurance sur la sécurité des interfaces cloud est particulièrement importante pour les administrations et OIV qui exposent des données sensibles via des APIs à leurs partenaires ou à leurs applications mobiles — chaque endpoint API représente un vecteur d'attaque potentiel qui doit être sécurisé et audité régulièrement dans le contexte d'une qualification SecNumCloud maintenue à jour.

Gestion des incidents dans un environnement SecNumCloud

SecNumCloud impose des exigences spécifiques sur la **gestion des incidents de sécurité** qui vont au-delà des obligations ISO 27001 standard. Les prestataires qualifiés doivent notifier leurs clients dans des délais définis (typiquement 4 heures pour les incidents majeurs affectant des données clients) et coopérer avec l'ANSSI et le CERT-FR lors d'incidents significatifs. La chaîne de notification entre le prestataire SecNumCloud, le client, l'ANSSI et les autorités sectorielles doit être documentée et testée régulièrement.

Pour les clients entités essentielles NIS2, la gestion des incidents dans un environnement SecNumCloud s'intègre naturellement dans les procédures de notification ANSSI requises par NIS2 : le prestataire SecNumCloud notifie le client en moins de 4 heures, et le client dispose ensuite d'un maximum de 24 heures pour transmettre son alerte précoce à l'ANSSI conformément aux exigences NIS2. Cette articulation fluide entre la gestion des incidents côté prestataire et les obligations de notification côté client est l'un des avantages opérationnels concrets de l'utilisation d'un prestataire cloud qualifié SecNumCloud pour les entités soumises à NIS2 — elle facilite le respect des délais de notification réglementaires en garantissant une information rapide et complète du client sur tout incident affectant ses données hébergées dans le cloud souverain.

FAQ — SecNumCloud 2026

Un prestataire cloud américain peut-il obtenir la qualification SecNumCloud ?

Non. SecNumCloud v3.2 exige que le prestataire et ses actionnaires de contrôle ne soient pas soumis à des législations extraterritoriales permettant à des États tiers d'accéder aux données clients sans consentement. Cela exclut de facto les entreprises de droit américain soumises au Cloud Act et au FISA. AWS, Microsoft Azure et Google Cloud ne peuvent pas obtenir la qualification SecNumCloud directement. Des solutions hybrides comme Bleu (Orange/ Capgemini pour Microsoft) et S3NS (Thales pour Google) cherchent à résoudre cette contrainte via des structures juridiques innovantes où des entités françaises gèrent l'infrastructure, mais leur qualification reste soumise à l'analyse complète de l'ANSSI.

SecNumCloud est-il obligatoire pour toutes les administrations françaises ?

Non, mais des circulaires interministérielles et instructions du SGDSN le rendent obligatoire pour certaines catégories : systèmes d'information des OIV traitant des données sensibles, données relevant du secret professionnel gouvernemental, SIIV (Systèmes d'Information d'Importance Vitale). Pour les autres administrations, SecNumCloud est fortement recommandé pour les données de niveau sensible avec une obligation de documenter et justifier l'utilisation d'alternatives non-qualifiées dans une analyse de risques approuvée par les autorités de tutelle.

Combien coûte un service cloud qualifié SecNumCloud comparé au cloud standard ?

Les services SecNumCloud qualifiés sont généralement 20 à 50 % plus chers que les offres cloud standard équivalentes. Ce surcoût reflète les investissements requis : infrastructures dédiées ou isolées, équipes certifiées, audits réguliers, certifications multiples, et restrictions sur la mutualisation des ressources. Ce surcoût doit être mis en perspective avec le coût d'un incident de souveraineté ou de sécurité sur des données sensibles, qui peut être plusieurs fois supérieur au différentiel de coût cloud annuel. Les marchés cadre interministériels permettent aux administrations de mutualiser les achats et de bénéficier de tarifs négociés avec les prestataires qualifiés.

SecNumCloud couvre-t-il les services SaaS ou seulement l'infrastructure IaaS ?

SecNumCloud couvre les trois modèles de service : IaaS, PaaS et SaaS. En pratique, les premières qualifications concernaient principalement l'IaaS. Le SaaS qualifié est plus rare car il impose l'audit de l'application elle-même en plus de l'infrastructure. L'initiative Bleu vise à proposer Microsoft 365 qualifié SecNumCloud — une avancée majeure pour les administrations utilisant massivement les outils Microsoft qui pourront ainsi bénéficier des fonctionnalités M365 avec les garanties de souveraineté SecNumCloud.

Comment articuler SecNumCloud avec les obligations RGPD pour les données personnelles ?

SecNumCloud et RGPD sont complémentaires. SecNumCloud garantit la souveraineté et la sécurité de l'hébergement, tandis que le RGPD régule le traitement des données personnelles quelle que soit leur localisation. Un environnement SecNumCloud facilite la conformité RGPD en garantissant que les données restent dans l'UE, que les sous-traitants sont des entités européennes, et que les droits d'accès des autorités étrangères sont bloqués — trois points sensibles dans les analyses RGPD sur les transferts de données hors UE. La combinaison SecNumCloud + accord de sous-traitance RGPD avec le prestataire constitue le standard de protection le plus élevé pour les données personnelles sensibles hébergées en cloud.

Continuité d'activité et reprise après sinistre dans SecNumCloud

SecNumCloud impose des exigences strictes de **continuité d'activité et de reprise après sinistre** qui dépassent significativement les obligations ISO 27001 standard. Les prestataires qualifiés doivent maintenir des **SLAs de disponibilité** élevés (typiquement 99,9 % voire 99,99 % pour les services essentiels) avec des garanties contractuelles sur les pénalités en cas de non-respect, des architectures redondantes sur plusieurs datacenters géographiquement séparés mais tous localisés en France ou dans l'UE, des plans de reprise après sinistre testés au moins annuellement avec documentation des résultats, et des délais de restoration des données (RPO et RTO) définis et garantis contractuellement.

La continuité d'activité dans un environnement SecNumCloud inclut également la gestion des dépendances critiques du prestataire lui-même : ses propres sous-traitants (électricité, connectivité réseau, maintenance des équipements) doivent respecter des critères de localisation et de sécurité cohérents avec la qualification SecNumCloud. Cette exigence de traçabilité de la chaîne d'approvisionnement du prestataire est analogue aux obligations supply chain NIS2 et DORA pour les entités financières — elle garantit que la souveraineté et la résilience SecNumCloud ne sont pas compromises par un maillon faible dans la chaîne de dépendances opérationnelles du prestataire qualifié.

Pour les clients des services SecNumCloud, les SLAs et garanties de continuité contractualisées fournissent une base solide pour la rédaction des plans de continuité d'activité NIS2 et DORA : les engagements du prestataire (RTO, RPO, disponibilité minimale) peuvent être directement intégrés dans les PCA/PRA comme hypothèses de base pour les scénarios d'incident cloud, réduisant l'incertitude dans la planification de la reprise d'activité après un incident majeur affectant l'infrastructure cloud hébergeant les systèmes critiques de l'entité.

Audit et traçabilité dans les environnements SecNumCloud

La **journalisation complète et la traçabilité** de toutes les opérations sur les données des clients est une exigence non-négociable de SecNumCloud. Contrairement aux services cloud standards où les logs peuvent être limités ou non accessibles aux clients, les prestataires SecNumCloud doivent fournir à leurs clients un accès complet et continu aux logs de toutes les opérations réalisées sur leurs données : accès (qui a accédé à quoi, quand et depuis où), modifications (quelles données ont été modifiées par qui), opérations administratives (redémarrage de VMs, modification de configuration, création/suppression de ressources), et opérations de sauvegarde et de restauration.

Cette traçabilité exhaustive est indispensable pour les entités soumises aux obligations d'audit NIS2 et DORA : lors d'un incident de sécurité, la capacité à reconstruire une timeline précise des opérations sur les données hébergées dans le cloud est critique pour la réponse à l'incident, la notification réglementaire et l'investigation forensique. Les prestataires SecNumCloud doivent conserver ces logs pendant une durée minimale (typiquement 12 mois) dans un stockage sécurisé

et immuable, garantissant qu'ils ne peuvent pas être modifiés ou supprimés par le prestataire ou par un attaquant ayant compromis les systèmes de gestion du prestataire.

Les clients ont également le droit de réaliser des audits de leurs environnements cloud SecNumCloud, soit directement soit via des auditeurs mandatés. Ce droit d'audit contractuel — l'une des clauses DORA les plus difficiles à obtenir des hyperscalers américains — est intrinsèque à la qualification SecNumCloud : les prestataires s'engagent à permettre des audits des clients dans le cadre du processus de qualification et doivent maintenir cette coopération pendant toute la durée de la qualification. Notre bilan DORA 2026 souligne l'importance cruciale de ce droit d'audit pour la conformité du secteur financier.

SecNumCloud pour les établissements de santé : HDS et souveraineté

Le secteur santé présente un cas d'usage particulièrement riche pour SecNumCloud, à l'intersection de multiples obligations réglementaires. Les établissements de santé soumis à NIS2 comme entités essentielles, qui doivent obligatoirement faire appel à des prestataires certifiés HDS pour héberger les données de santé personnelles, ont tout intérêt à choisir des prestataires à la fois certifiés HDS et qualifiés SecNumCloud pour les systèmes les plus sensibles.

La combinaison HDS + SecNumCloud offre une protection maximale pour les données médicales : la certification HDS garantit la conformité aux exigences spécifiques du secteur santé (disponibilité pour la continuité des soins, intégration dans le parcours de soins, confidentialité médicale), tandis que SecNumCloud garantit la souveraineté des données et leur protection contre les droits extraterritoriaux étrangers. Cette combinaison est particulièrement pertinente pour les CHU et centres hospitaliers régionaux qui traitent des données médicales hautement sensibles et qui sont des cibles prioritaires des cyberattaques — notamment des groupes ransomware qui ont causé plusieurs incidents majeurs dans les hôpitaux français ces dernières années.

L'ANS (Agence du Numérique en Santé) travaille avec l'ANSSI pour développer un référentiel sectoriel articulant HDS et SecNumCloud, permettant aux établissements de santé de conduire

un processus de qualification et de certification consolidé plutôt que deux démarches parallèles. Cette harmonisation, attendue pour 2026-2027, réduira la charge administrative des établissements de santé tout en garantissant un niveau de protection maximale pour les données médicales hébergées dans le cloud souverain français. Consultez notre guide HDS 2026 pour les détails de la certification hébergement données de santé et son articulation avec SecNumCloud et NIS2.

Intégration DevSecOps dans un environnement SecNumCloud

Pour les équipes de développement déployant des applications dans des environnements SecNumCloud, l'intégration des pratiques DevSecOps est une nécessité pour maintenir la vitesse de développement tout en respectant les exigences de sécurité du référentiel. SecNumCloud n'impose pas une méthodologie de développement spécifique, mais les exigences sur la sécurité du développement, la gestion des vulnérabilités et la traçabilité des déploiements sont compatibles avec les approches CI/CD modernes dès lors qu'elles intègrent les contrôles de sécurité requis.

Les pipelines CI/CD dans un environnement SecNumCloud doivent intégrer des **scans de sécurité automatisés** à chaque étape : SAST (Static Application Security Testing) sur le code source, SCA (Software Composition Analysis) pour identifier les vulnérabilités dans les dépendances open source, DAST (Dynamic Application Security Testing) sur les applications déployées dans l'environnement de test, et scan des images conteneurs avant leur déploiement en production. La traçabilité de ces scans et de leurs résultats doit être maintenue pour démontrer lors des audits SecNumCloud que chaque déploiement en production a été soumis aux contrôles de sécurité requis.

La gestion des secrets dans un pipeline CI/CD SecNumCloud est particulièrement critique : les clés d'API, mots de passe de base de données, certificats TLS et autres secrets ne doivent jamais être stockés en clair dans les dépôts de code source ou dans les variables d'environnement des pipelines CI/CD. Des solutions de gestion des secrets (HashiCorp Vault, AWS Secrets Manager sur les offres cloud qualifiées, Azure Key Vault via Bleu) permettent de centraliser et sécuriser ces secrets avec audit trail complet — une exigence directe du référentiel SecNumCloud qui

impose la traçabilité de tous les accès aux données et ressources sensibles hébergées dans l'environnement qualifié.

Formation et certification des équipes sur SecNumCloud

L'utilisation efficace d'un environnement SecNumCloud nécessite que les équipes DSI et sécurité de l'organisation cliente soient formées aux spécificités du référentiel et aux bonnes pratiques de configuration sécurisée dans l'environnement qualifié. Cette formation couvre plusieurs domaines : la compréhension des exigences SecNumCloud et leur traduction en configurations pratiques dans l'environnement cloud, la gestion sécurisée des identités et des accès dans le contexte SecNumCloud (MFA obligatoire, rotation des clés, gestion des comptes de service), la configuration du chiffrement BYOK et de la gestion des clés avec HSM, et les procédures de notification d'incidents spécifiques à l'environnement SecNumCloud.

Les prestataires qualifiés SecNumCloud proposent généralement des formations et des certifications spécifiques à leurs plateformes pour les équipes de leurs clients. OVHcloud, par exemple, propose des certifications de niveau professionnel sur son offre cloud qualifiée, permettant aux équipes DSI d'acquérir les compétences nécessaires pour administrer et sécuriser leurs environnements de manière conforme aux exigences SecNumCloud. Ces certifications prestataires complètent les certifications cloud générales (AWS Certified Security, Azure Security Engineer) en apportant la dimension souveraineté et conformité SecNumCloud spécifique aux besoins des administrations et des OIV français.

La sensibilisation à la souveraineté numérique doit également atteindre les utilisateurs métiers des administrations et OIV utilisant des services SaaS qualifiés SecNumCloud : comprendre pourquoi les restrictions d'accès depuis des territoires hors UE sont imposées, pourquoi certains services populaires disponibles sur le cloud non-qualifié ne sont pas disponibles dans l'environnement SecNumCloud, et pourquoi les processus d'authentification sont plus contraignants dans SecNumCloud que dans les environnements cloud grand public. Cette sensibilisation réduit les comportements de contournement (shadow IT utilisant des services cloud non-qualifiés) qui constituent le principal vecteur de compromission de la souveraineté numérique des organisations pourtant engagées dans une démarche SecNumCloud.

La politique de sécurité des systèmes d'information (PSSI) des administrations et OIV utilisant SecNumCloud doit être mise à jour pour intégrer explicitement les règles d'usage des services cloud qualifiés : catégories de données autorisées à être hébergées dans SecNumCloud, procédures d'autorisation pour les nouveaux services cloud, règles de classification des données avant migration vers le cloud, et obligations de notification en cas d'incident sur les données hébergées. Cette mise à jour de la PSSI est généralement réalisée en parallèle du déploiement de SecNumCloud et constitue un livrable attendu lors des audits NIS2 et des contrôles ANSSI, démontrant que l'utilisation du cloud souverain est gouvernée de manière cohérente avec la politique globale de sécurité de l'information de l'organisation.

La gestion du cycle de vie des données dans SecNumCloud inclut également des obligations spécifiques sur la **destruction sécurisée des données** en fin de contrat ou lors de la résiliation du service. SecNumCloud impose que les prestataires qualifiés fournissent des garanties de suppression effective et irrécupérable des données des clients lors de la résiliation du contrat cloud, avec une attestation documentée de la destruction. Cette exigence est particulièrement importante pour les administrations et OIV dont les données sensibles doivent être protégées même après leur sortie de l'environnement cloud — un risque souvent négligé lors de la migration vers le cloud mais critique lors de la migration hors d'un prestataire cloud en fin de contrat ou suite à un incident. La possibilité de récupérer les données dans un format portable avant leur destruction est également garantie par SecNumCloud, facilitant les transitions entre prestataires qualifiés sans risque de perte de données ou d'enfermement propriétaire.

Pour les organisations qui souhaitent approfondir leur compréhension de l'écosystème de sécurité cloud en France et en Europe, les ressources disponibles sur le site officiel de l'ANSSI (cyber.gouv.fr/secnumcloud) constituent la référence primaire, complétées par la documentation EUCS de l'ENISA et les orientations sectorielles publiées par les ministères pour leurs administrations sous tutelle. Le marché SecNumCloud en 2026 est encore en développement mais la tendance est clairement à l'accélération, portée par la convergence des réglementations NIS2, DORA et des circulaires interministérielles sur la souveraineté numérique — une convergence qui rend l'investissement dans SecNumCloud de plus en plus rationnel économiquement pour les organisations dont les données et systèmes d'information sont au cœur de leur mission et de leur valeur stratégique pour la France et pour l'Union Européenne.

L'adoption de SecNumCloud par le secteur privé en dehors des OIV et des administrations est une tendance émergente en 2026, portée par plusieurs facteurs convergents. D'abord, les grandes

entreprises du CAC 40 prennent conscience que leurs données stratégiques (brevets, plans de développement, contrats majeurs, données personnelles de leurs clients) présentent une valeur suffisante pour justifier le surcoût SecNumCloud face au risque de cyber-espionnage économique. La France a connu plusieurs affaires notoires d'espionnage économique ciblant des données industrielles françaises via des compromissions d'environnements cloud — les noms des cibles ne sont pas publics mais les autorités françaises ont multiplié les alertes sur ce risque. Ensuite, les acteurs du secteur de la défense et de l'aérospatiale français, soumis à des règles strictes de protection du patrimoine scientifique et technique, adoptent SecNumCloud pour leurs activités de R&D et leurs systèmes de conception, où les données peuvent avoir une sensibilité stratégique sans être formellement classifiées défense. Enfin, les cabinets d'avocats d'affaires et conseils fiscaux, dépositaires d'informations particulièrement sensibles de leurs clients entreprises, commencent à s'intéresser à SecNumCloud pour différencier leur offre sur le marché de la protection de la confidentialité des données — un argument commercial de poids dans un contexte où la confidentialité des échanges avec les conseils juridiques est une exigence fondamentale du droit à la défense et du secret professionnel de l'avocat.

La stratégie de communication de l'ANSSI autour de SecNumCloud a évolué en 2025-2026 pour adresser non seulement les administrations et les OIV traditionnels mais aussi ce marché émergent du secteur privé hors obligation réglementaire. Des guides sectoriels adaptés aux PME et ETI françaises ont été publiés, permettant à des organisations plus modestes d'accéder au référentiel SecNumCloud sans nécessiter les ressources d'un grand groupe. Cette démocratisation progressive de SecNumCloud est essentielle pour construire un véritable écosystème de cloud souverain français qui dépasse les seuls marchés publics et les OIV pour atteindre la masse critique nécessaire à la viabilité économique à long terme des prestataires qualifiés et à la réduction progressive des surcoûts qui constituent aujourd'hui le principal frein à l'adoption plus large du référentiel dans l'économie française.

L'interopérabilité entre environnements SecNumCloud de différents prestataires est un enjeu pratique croissant pour les organisations multi-fournisseurs. SecNumCloud ne définit pas de standards d'interopérabilité entre prestataires qualifiés, ce qui peut créer des frictions lors de transferts de données d'un prestataire SecNumCloud à un autre. Le projet GAIA-X travaille sur des standards d'interopérabilité pour les services cloud européens qui devraient bénéficier aux prestataires SecNumCloud dans les prochaines années, facilitant la portabilité des données et des applications entre prestataires qualifiés différents. En attendant, les organisations qui utilisent

plusieurs prestataires SecNumCloud doivent gérer manuellement les transferts de données en s'assurant que ceux-ci respectent les exigences SecNumCloud tout au long du transit — notamment le chiffrement bout-en-bout et la localisation exclusivement en UE de toutes les étapes du transfert de données entre les environnements qualifiés des différents prestataires. Cette contrainte d'interopérabilité manuelle est un coût caché de l'écosystème SecNumCloud actuel que les organisations multi-prestataires doivent anticiper dans leurs projets d'architecture cloud souveraine et dans leurs plans de migration entre prestataires qualifiés en cas de changement contractuel ou de fin de qualification d'un prestataire existant.

L'émergence d'outils d'automatisation spécifiques à la conformité SecNumCloud est une tendance notable en 2026 : des solutions de Cloud Security Posture Management (CSPM) adaptées aux environnements SecNumCloud permettent aux équipes sécurité de monitorer en continu la conformité de leurs configurations cloud aux exigences du référentiel, d'identifier automatiquement les dérives de configuration qui créeraient des non-conformités lors d'un audit, et de générer des rapports de conformité automatisés facilitant la préparation des audits annuels de surveillance SecNumCloud. Ces outils CSPM spécialisés SecNumCloud réduisent significativement la charge manuelle de gestion de la conformité et permettent aux petites équipes sécurité de maintenir un niveau de conformité élevé sans ressources dédiées à la conformité cloud à temps plein. Ils constituent un investissement essentiel pour les organisations qui ont adopté SecNumCloud et souhaitent maintenir leur qualification sans accident de conformité qui risquerait de compromettre leur accréditation et d'interrompre leurs activités cloud souverain le temps d'un audit de requalification correctif.

SecNumCloud représente en définitive bien plus qu'une certification technique : c'est le symbole d'une volonté politique et industrielle française de construire un écosystème numérique souverain capable de résister aux pressions géopolitiques et aux législations extraterritoriales qui menacent la confidentialité des données stratégiques. L'histoire de SecNumCloud est celle d'un pari audacieux — imposer des standards de souveraineté élevés dans un marché cloud dominé par des acteurs dont les États d'origine peuvent légalement accéder aux données qu'ils gèrent — et d'une réussite progressive dont les premiers fruits sont visibles en 2026 avec plusieurs prestataires qualifiés proposant des offres compétitives dans les segments IaaS et SaaS. Le chemin restant à parcourir est encore long pour faire de SecNumCloud la norme pour l'ensemble des données sensibles françaises et européennes, mais la direction est clairement tracée et soutenue par des réglementations (NIS2, DORA, circulaires interministérielles) et une prise de conscience

croissante des risques de dépendance numérique qui renforcent chaque année la pertinence et l'attractivité du référentiel SecNumCloud comme standard de confiance pour le cloud souverain en France et dans l'Union Européenne.

