OBSERVATOIRE

SecNumCloud

ÉDITION **FÉVRIER 2026**

OBSERVATOIRE SecNumCloud

SecNumCloud : levier marché de la Stratégie cyber française

La France bien de publier sa stratégie nationale cyber, et SecNumCloud occupe une place intéressante dans le dispositif. Avant ce texte, SecNumCloud souffrait d'un malentendu : être perçu comme un outil de l'État, comme un cloud administratif par nature. Cette lecture est réductrice et erronée. La stratégie nationale de cybersécurité 2026–2030 permet précisément d'en sortir en replaçant SecNumCloud dans sa fonction réelle : non pas servir un acteur mais qualifier un marché. Ce marché n'est ni celui du cloud en général, ni celui des usages courants. C'est le marché des organisations critiques ou détentrices d'informations sensibles, qu'elles soient publiques ou privées. SecNumCloud n'est pas un outil de propriété, c'est un outil de lisibilité et d'accès.

Un marché fondé sur la criticité, pas sur le statut

Le critère central de SecNumCloud n'est pas juridique, il est fonctionnel. Il ne distingue pas le public du privé, il distingue le critique du non critique, le sensible du grand public, le systémique de l'accessoire. Le débat s'est longtemps trompé de terrain. Dans la stratégie 2026–2030, le cloud est reconnu comme une infrastructure critique, et certaines données, certains traitements, certaines fonctions comme vitaux pour la Nation. SecNumCloud vient répondre à cette réalité : offrir un cadre d'accès adapté aux organisations qui portent une responsabilité systémique, qu'il s'agisse d'opérateurs d'importance vitale, d'acteurs de la santé, de l'énergie, de la défense industrielle, de la finance, ou de filières technologiques stratégiques. Ce n'est donc pas le cloud de l'État mais le cloud des fonctions à haute responsabilité.

SecNumCloud comme porte d'accès à un marché de la confiance

En qualifiant ce marché, SecNumCloud en devient la porte d'entrée. Il ne garantit pas un avantage commercial automatique mais il rend possible l'accès à un segment précis : celui des usages où la confiance n'est pas un argument marketing mais une condition d'opérabilité. Ce mécanisme est structurant. Il transforme une exigence de sécurité en signal de marché lisible : pour opérer sur ce segment, il faut accepter un certain niveau de contraintes, d'auditabilité et de responsabilité. En retour, les organisations clientes disposent d'un cadre clair pour arbitrer leurs choix technologiques. L'État, dans ce modèle, n'est pas le client unique, ni même central. Il est le qualificateur du seuil, celui qui définit les règles d'accès à un marché dont les bénéficiaires sont d'abord les acteurs critiques eux-mêmes, publics et privés confondus. Et ca, c'est le rôle d'une État qui exerce sa souveraineté. Il définit le cadre.

D'un outil étatique à une infrastructure d'usage stratégique

Le véritable enjeu, désormais, est d'assumer pleinement cette bascule. Tant que SecNumCloud sera perçu comme un outil "pour l'État", il restera cantonné à un rôle défensif et polémique. S'il est clairement posé comme une infrastructure de marché pour les usages sensibles, alors sa logique devient évidente : investir pour accéder, se conformer pour opérer, et monter en gamme pour durer.La stratégie 2026–2030 crée les conditions de cette clarification, mais elle appelle une doctrine d'usage explicite : quels types de données, quels niveaux de criticité, quelles chaînes de responsabilité. Sans cette explicitation, SecNumCloud restera un objet ambigu. Avec elle, il peut devenir un accélérateur de structuration, au service de la résilience nationale comme de la compétitivité des acteurs concernés.

SecNumCloud n'est pas l'outil des États. C'est l'outil des organisations qui ne peuvent pas se permettre l'approximation, et elles sont nombreuses en Europe.

Merci et à bientôt,
SÉBASTIEN GARNAULT

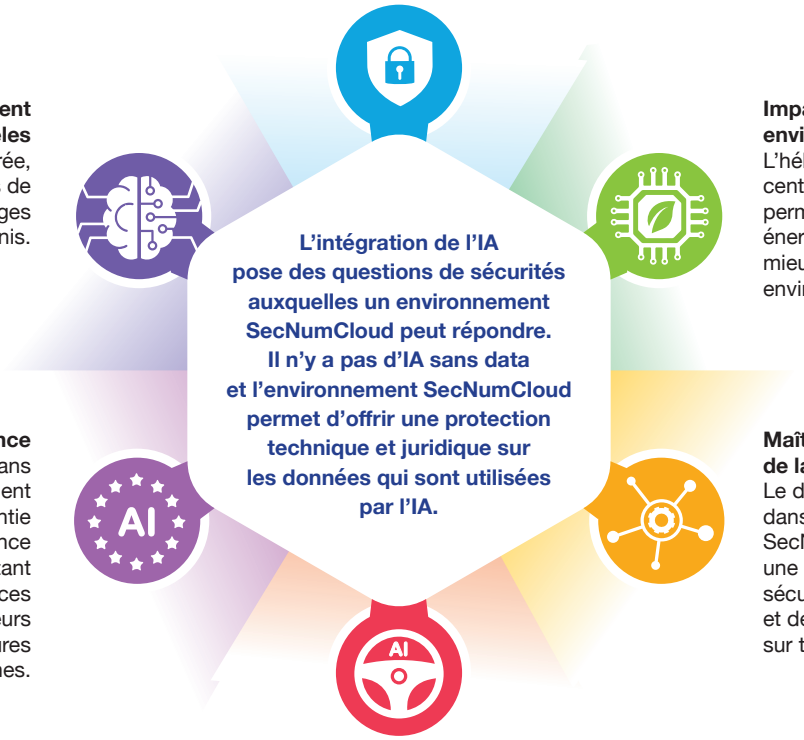
Focus : Déployer l'IA en environnement SecNumCloud

Avec SecNumCloud, une IA sécurisée et à l'échelle

Protection des données / Respect du RGPD
SecNumCloud permet de réconcilier innovation IA et exigences de protection des données, y compris pour les informations sensibles ou critiques.

Entraînement des modèles
Une IA mieux calibrée, alignée aux besoins de l'entreprise, aux usages plus définis.

Impact environnemental de l'IA
L'hébergement des data centers SecNumCloud permet de bénéficier du mix énergétique français et mieux mesurer l'impact environnemental de l'IA.



L'intégration de l'IA pose des questions de sécurités auxquelles un environnement SecNumCloud peut répondre. Il n'y a pas d'IA sans data et l'environnement SecNumCloud permet d'offrir une protection technique et juridique sur les données qui sont utilisées par l'IA.

Résilience
L'usage de l'IA dans un environnement SecNumCloud garantie une meilleure résilience opérationnelle, en limitant les dépendances critiques à des acteurs ou infrastructures extra-européennes.

Maîtrise de la chaîne IA
Le déploiement de l'IA dans un environnement SecNumCloud garanti une cohérence de sécurité, de gouvernance et de responsabilité sur toute la chaîne.

Gouvernance des usages IA
Grâce à des mécanismes, de contrôle des droits, de segmentation des environnements, les organisations peuvent mettre en place une gouvernance claire et traçable des usages de l'IA. L'IA devient un outil piloté, et non une pratique diffuse.

Les stratégies d'intégration

Offre 1

L'infrastructure IA : le GPU dans SecNumCloud une offre technique qui permet de répondre à des besoins importants en IA.

Bleu
CLOUD TEMPLE
NumSpot
Business
Scaleway
S3NS

Offre 2

La plateforme IA : Un logiciel d'IA sur un environnement SecNumCloud une solution où le cloud provider est un facilitateur.
> **Offre LLM as a service (opérée par le cloud provider)**
> **Offre opérée par le client avec un logiciel d'IA dédié**

CLOUD TEMPLE
NumSpot
Business
OUTSCALE

Offre 3

Les modèles d'IA : La clef est d'offrir une intégration d'IA qui soit modèle-agnostique afin de permettre une flexibilité dans le choix et le changement de modèles.

> **Ouverts : l'usager contrôle l'évolution du modèle**

> **Propriétaires : le modèle est contrôlé par le propriétaire, souvent ces modèles sont plus puissants**

OBSERVATOIRE

SecNumCloud *c'est quoi ?*

SecNumCloud est le référentiel de l'ANSSI qui définit les exigences de sécurité et de souveraineté pour les services d'informatique en nuage (cloud) utilisés par les administrations et entreprises en France.

La différence entre qualification et certification

La qualification vérifie l'aptitude d'un prestataire ou d'un service à répondre à un besoin (confiance, compétences, niveau attendu).

La certification atteste officiellement, via un organisme tiers, la conformité à une norme ou un référentiel précis.

Il vise à attester

1. de la qualité et de la robustesse d'un service cloud
2. de la compétence de l'opérateur de cloud
3. ainsi que de la confiance pouvant lui être accordée

Il établit un cadre

1. technique
2. opérationnel
3. juridique

Critères **Techniques**

- **Appréciation des risques** documentée couvrant l'ensemble du périmètre du service
- **Révision annuelle** des plans de sécurité de l'information et de continuité d'activité
- **Obligation d'information** du commanditaire en cas de violation de données à caractère personnel
- **Désignation** d'un responsable de la sécurité des systèmes d'information
- **Désignation** d'un responsable de la sécurité physique
- **Politique de sauvegarde** quotidienne des données

Critères **Opérationnels**

- **Authentification multifacteurs** fort pour l'accès aux interfaces d'administration
- **Comptes nominatifs** pour les utilisateurs
- **Mécanisme de chiffrement** empêchant la récupération de données lors de la réallocation d'une ressource ou d'un support physique
- **Cloisonnement des flux** réseau (logique/physique/chiffré)
- **Veille active** pour gérer les vulnérabilités techniques, évaluer l'exposition aux risques

Critères **Juridiques**

- **Doivent être établis au sein d'un État membre de l'UE** : le siège statutaire, l'administration centrale et le principal établissement du prestataire
- **Limites sur la détention du capital** et des droits de vote par des entités hors UE: 24% individuellement, 39% collectivement
- **Stockage et traitement des données au sein de l'UE**
- **Justification du respect des principes du RGPD** (finalités légitimes, durée de conservation des données limitée)
- **Une clause de réversibilité** doit être contenue dans la convention de service prévoyant la restitution et l'effacement sécurisé des données du commanditaire en fin de contrat ou pour toute autre cause

La procédure de qualification

- **J0** Demande de qualification auprès de l'ANSSI
- **J1** Stratégie d'évaluation acceptée
- **J2** Travaux d'évaluation acceptés
- **J3** Décision de qualification par l'ANSSI

J0

- Description détaillée des services soumis à qualification
- Démonstration de la conformité au référentiel SecNumCloud
- Choix d'un auditeur qualifié chargé de mener les audits J2

J1

- Validation par l'ANSSI du plan d'audit proposé par l'organisme d'évaluation
- Fixation de la feuille de route des audits J2

J2

- Audits techniques et organisationnels sur site par l'organisme agréé
- Transmission du rapport à l'ANSSI pour analyse

J3

- Étude du rapport d'audit J2 par l'ANSSI
- Demande d'éventuelles actions correctives par l'ANSSI
- Potentielle demande de compléments d'information ou validation de la certification

Les principaux critères d'évaluation

Critères **Techniques**

- Appréciation des risques documentée couvrant l'ensemble du périmètre du service
- Établissement et actualisation annuelle des plans de sécurité de l'information et de continuité d'activité
- Obligation d'information du commanditaire en cas de violation de données à caractère personnel
- Désignation d'un responsable de la sécurité des systèmes d'information
- Désignation d'un responsable de la sécurité physique
- Politique de sauvegarde quotidienne des données

Critères **Opérationnels**

- Authentification multifacteurs fort pour l'accès aux interfaces d'administration
- Comptes nominatifs pour les utilisateurs
- Mécanisme de chiffrement empêchant la récupération lors d'une réallocation de ressource ou d'un support physique
- Cloisonnement des flux réseau (logique/physique/chiffré)
- Veille active pour gérer les vulnérabilités techniques, évaluer l'exposition aux risques

Critères **Juridiques**

- Le siège statutaire, l'administration centrale et le principal établissement du prestataire doivent être établis au sein d'un État membre de l'UE
- Limites sur la détention du capital et des droits de vote par des entités hors UE: **24% individuellement, 39% collectivement**
- Stockage et traitement des données au sein de l'UE
- Respect des principes du RGPD justifié (finalités légitimes, durée de conservation limitée)
- La convention de service doit inclure une clause de réversibilité prévoyant la restitution et l'effacement sécurisé des données du commanditaire en fin de contrat ou pour toute autre cause

OBSERVATOIRE

SecNumCloud *c'est qui ?*

Les services soumis à la qualification

EN COURS

	Candidat	Offre
IaaS	**Adista**	dista Secure Cloud
	Bleu	Cloud de Confiance Bleu
	Cyllene ITS	IaaS SecNumCloud
	Ecritel	Ecritel Secure Cloud
	Gip Mipih (Numih France)	Cloud Premier Souverain
	ITS Integra	IT SecureCloud
	Numspot	Plateforme des services cloud
	Orange Business	Cloud Avenue SecNum Dynamic
	OVH SAS	SNC Cloud Platform
	Prolival - Groupe Tenexa	Horizon SecNumCloud
	Scaleway	Scaleway SecNumCloud
	Bretagne Télécom	Blue Secure Cloud
CaaS	**Bleu**	Cloud de Confiance Bleu
	ITS Integra	ITSecureKube
PaaS	**Bleu**	Cloud de Confiance Bleu
	OVH SAS	SNC Cloud Platform
	Scaleway	Scaleway SecNumCloud
SaaS	**Ecritel Solutions**	Ecritel Secure Backup
	NetExplorer	Share and Workspace
	Cloud Solutions	Wimi

LES QUALIFIÉS

	Entreprises	Offre
IaaS	**Cegedim**	CegNumCloud Secured IaaS
	Cloud Temple	IAAS Secure Temple
	OVH	Bare Metal Pod
	OVH	Hosted Private Cloud powered by VMware
	Orange Business	CloudAvenueSecNum
	Outscale	IaaS
	Worldline	Worldline Cloud Services
	S3NS	Cloud de Confiance PREMI3NS
CaaS	**S3NS**	Cloud de Confiance PREMI3NS
PaaS	**Cloud Temple**	PaaS Openshift
	S3NS	Cloud de Confiance PREMI3NS
SaaS	**Index Education**	EDT
	Index Education	Hyperplanning
	Index Education	Pronote
	Index Education	Pronote Primaire
	Oodrive	Oodrive_Work _Share
	Oodrive	Oodrive_Work
	Oodrive	Oodrive_Meet
	Whaller	Whaller Donjon SaaS

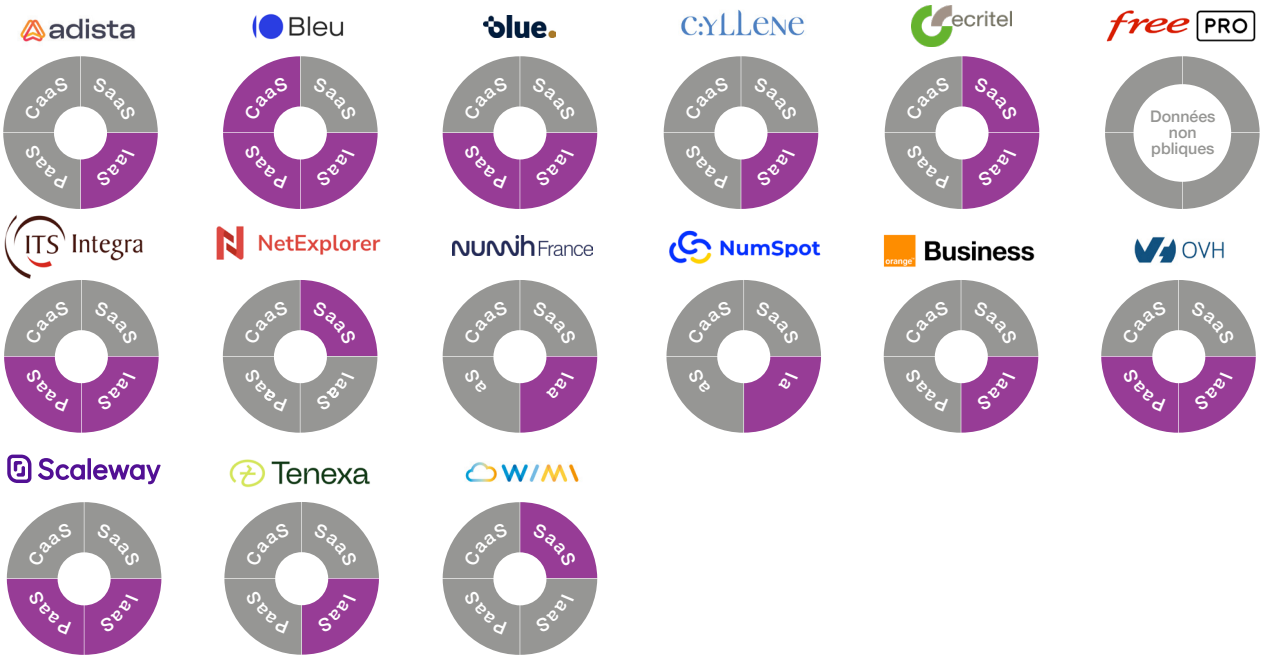
Free Pro est également en cours de qualification mais aucune information publique n'est disponible sur le type de qualification demandée

Les candidats

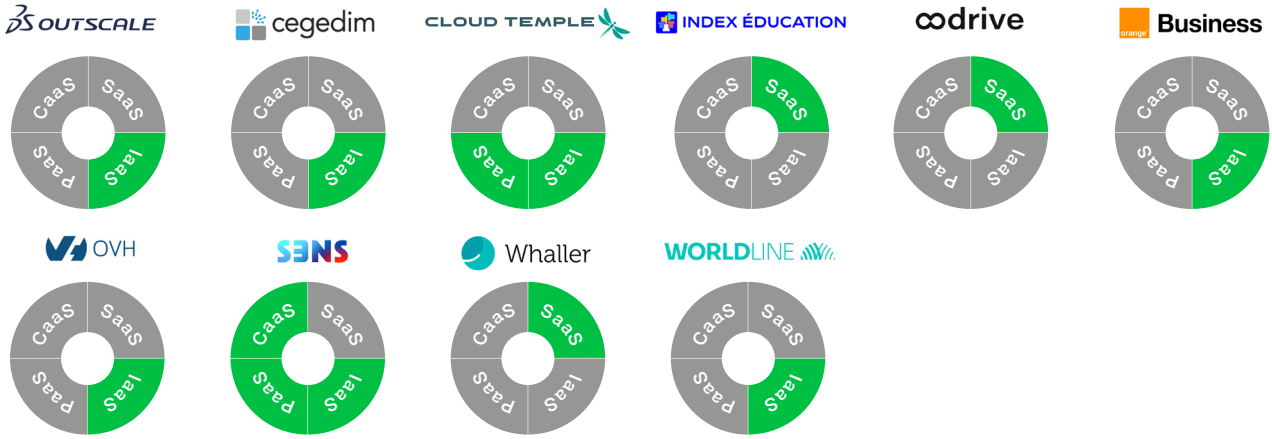
IaaS	adista, Bleu, blue., Business, CYLLENE, ecritel, ITS Integra, NUMIH France, NumSpot, OVH, Scaleway, Tenexa
CaaS	Bleu, ITS Integra
PaaS	Bleu, OVH, Scaleway
SaaS	ecritel, NetExplorer, WIMI

Périmètre de la qualification

EN COURS



LES QUALIFIÉS



Statut des candidats à la qualification

J0 Demande de qualification auprès de l'ANSSI

J1 Stratégie d'évaluation acceptée

J2 Travaux d'évaluation acceptés

J3 Décision de qualification par l'ANSSI

Lexique

IaaS (Infrastructure as a Service)

> Mise à disposition de ressources informatiques physiques.
> **Le prestataire détient** l'infrastructure physique et la loue/la met à disposition d'un utilisateur.
> **Le client construit** son activité sur cette plateforme.

> **Le prestataire** détient tout le matériel physique: les machines, le réseau et le stockage ...
> **Le client** (commanditaire) :
- construit les services en fonction de ses besoins
- décide du champ d'application/périmètre
- décide des usages rendus possibles sur l'infrastructure loué.

Les points spécifiques *"IaaS"*

- ***Cloisonnement** strict entre les utilisateurs*
- *Pour empêcher la récupération des données en cas de réallocation de ressource ou de récupération du support physique => **chiffrement du disque ou du système de fichier ou chiffrement par volume avec une clé par commanditaire***

CaaS (Container as a Service)

> Mise à disposition d'outils permettant de **déployer, gérer et orchestrer des conteneurs** d'applications.
> **Un conteneur** est comme une petite boîte isolée qui contient tout le nécessaire pour faire fonctionner une application (bibliothèques, code, outils...), sans interférer avec les autres.

> **Le prestataire** gère l'infrastructure sous-jacente (serveurs, stockage, réseau, système d'exploitation).
> **Le client** (commanditaire) :
- contrôle les conteneurs et les éléments techniques liés à ses applications.

Les points spécifiques *"CaaS"*

- ***Cloisonnement strict** entre les commanditaires*
- ***Cryptologie recommandée** : chiffrement par volume une clé/ commanditaire)*
- ***Effacement sécurisé** à la fin du contrat = effacement sécurisé des clés de chiffrement des espaces de stockage du commanditaire.*
- *Les opérations d'administration et de supervision doivent être réalisées **depuis l'Union Européenne**.*

PaaS (Platform as a Service)

> Mise à disposition d'une **plateforme technique prête à l'emploi** pour développer, héberger et faire fonctionner des applications.

> **Le prestataire** gère toute la partie infrastructure (réseau, serveurs, stockage, système d'exploitation, etc.).
> **Le client** (commanditaire) :
- se concentre sur le développement et la gestion de ses propres applications.

Les points spécifiques *"PaaS"*

- ***Devoir d'information** par le prestataire en cas de modification sur les éléments logiciels qu'il maîtrise.*
- ***Cloisonnement strict** entre les interfaces des commanditaires: les ressources affectées à l'usage d'un prestataire ne doivent pas être accessibles à d'autres commanditaires.*

SaaS (Software as a Service)

> Mise à disposition d'**applications prêtes à l'emploi**, hébergées dans le cloud et gérées entièrement par le prestataire.
> L'utilisateur accède simplement à l'application via Internet — sans avoir à installer, héberger ou maintenir quoi que ce soit.

> **Le prestataire** gère l'ensemble des aspects techniques requérant des compétences informatiques.
> **Le client** (commanditaire) :
- Ne maîtrise pas la plateforme en nuage.
- Peut d'effectuer quelques paramétrages dans l'application.

Les points spécifiques *"SaaS"*

- ***Moyens d'authentification à multiples facteurs** pour l'accès des utilisateurs finaux*
- ***Cloisonnement** entre les interfaces d'administration mises à disposition des commanditaires et les interfaces permettant l'accès des utilisateurs finaux*

The Sources of February

Les solutions IA

de **Cloud Temple**
https://www.cloud-temple.com/en/large-language-model-as-a-service-llmaas/

de **SENS**
https://documentation.s3ns.fr/compute/docs/gpus?hl=fr#a3-series

de **Bleu**
https://www.bleucloud.fr/telechargement-liste-des-services-azure/

de **NumSpot**
https://numspot.com/produit/data-intelligence-artificielle-souveraine/

de **Orange Business Services**
https://www.orange.com/fr/communiques/orange-business-lance-en-france-de-nouvelles-offres-pour-mener-des-projets-dia-generative-de-bout-en-bout-et-de-confiance-232094?

de **Scaleway**
https://www.scaleway.com/en/custom-built-clusters/

d'**Outscale**
https://fr.outscale.com/cloud-experience/cloud-souverain/

ÉDITION
FÉVRIER
2026