



OBSERVATOIRE

SecNumCloud

ÉDITION SEPTEMBRE 2026

SecNumCloud : l'été où la doctrine est devenue marché

L'obligation entre en vigueur, l'offre s'élargit. Reste à savoir si la France a construit une exception nationale ou l'avant-garde d'une doctrine au milieu d'une offre de confiance qui émerge.

Le basculement juridique

L'été 2026 aura fait basculer SecNumCloud politiquement et juridiquement. L'arrêté du 12 août pris par le Premier ministre approuve le référentiel applicable aux prestataires d'informatique en nuage : SecNumCloud 3.2, dans une version qui remonte à mars 2022. Rien ne change donc fondamentalement dans les exigences. Tout change dans leur portée. Ce que l'ANSSI qualifiait devient, pour certaines données sensibles, la règle d'achat de l'État, de ses opérateurs et de six groupements d'intérêt public, en application du décret du 14 avril 2026 et de l'article 31 de la loi SREN. La séquence est désormais complète : loi de principe, décret de périmètre, arrêté de standard. La souveraineté ne relève plus seulement d'une doctrine ou d'une préférence. Elle devient, sur un périmètre défini, une contrainte d'achat.

Elle est encore incomplète. Collectivités et établissements hospitaliers ne sont pas directement intégrés à cette obligation générale alors qu'ils manipulent certaines des données les plus sensibles. Ils constituent également une part considérable de la commande publique numérique. Le décret ménage également une transition : lorsqu'une offre acceptable existe, certains projets antérieurs peuvent bénéficier d'une dérogation allant jusqu'à dix-huit mois ; lorsqu'elle n'existe pas, une dérogation d'un an peut être renouvelée jusqu'à son apparition. L'obligation est donc réelle, mais son assiette demeure étroite et son application dépend aussi de l'existence d'une offre répondant effectivement au besoin.

De la qualification au marché

Côté offre, le mouvement s'accélère. Le 1^{er} septembre, deux qualifications sont annoncées le même jour. OVHcloud obtient SecNumCloud pour SNC Cloud Platform, son offre de cloud public facturée à l'usage, troisième offre qualifiée du groupe après Bare Metal Pod et VMware on OVHcloud. Numspot, coentreprise de Bouygues Telecom, de la Banque des Territoires, de Dassault Systèmes et de Docaposte, obtient à son tour la qualification de sa plateforme de services cloud. Scaleway, de son côté, poursuit son pro-

cessus de qualification et a été sélectionné pour accueillir la future plateforme souveraine de la Plateforme des données de santé. Pris séparément, ces événements sont industriels. Pris ensemble, ils commencent à dessiner un marché. C'est probablement là que se trouve le véritable basculement de 2026. Le problème de SecNumCloud n'a jamais été uniquement le coût de la qualification. C'était celui de la demande située en face. Pendant des longs mois, les candidats ont dû financer des cycles longs, coûteux et exigeants pour accéder à un marché dont personne ne pouvait garantir la profondeur. En rendant obligatoire le recours à des offres répondant à ces exigences pour certaines données sensibles, l'État change l'équation. Il ne subventionne pas l'offre : il organise la demande.

La bataille est désormais européenne

Le débat européen a longtemps opposé deux conceptions. D'un côté, une certification cloud centrée sur la cybersécurité. De l'autre, la position française selon laquelle la confiance ne peut être réduite à la sécurité technique : elle suppose aussi de savoir quelle entreprise contrôle le service, de quel droit elle dépend et à quelles injonctions extraterritoriales elle peut être soumise. L'Europe commence à sortir de cette opposition. Le projet de Cloud and AI Development Act présenté par la Commission le 3 juin propose un cadre européen de souveraineté du cloud à quatre niveaux. Plus le niveau augmente, plus apparaissent des exigences relatives à la localisation, au contrôle de la technologie, aux personnels, aux dépendances et à l'exposition aux juridictions de pays tiers. Le déplacement est majeur : la souveraineté n'est plus seulement envisagée comme un attribut de la certification de cybersécurité. Elle devient une caractéristique autonome de l'offre et un critère de la commande publique.

C'est précisément le terrain sur lequel la France expérimente depuis plusieurs années. Deux trajectoires sont désormais possibles. SecNumCloud peut rester une exception française : exigeante, protectrice, mais limitée par la taille de son marché et progressivement contournée par des architectures européennes différentes. Ou l'expérience française peut contribuer à définir le niveau supérieur d'une architecture européenne de confiance : sécurité technique, maîtrise opérationnelle, contrôle juridictionnel et autonomie technologique. Dans le premier cas, la France aura construit une forteresse. Dans le second, elle aura construit un standard.

L'été 2026 n'a donc pas clos le débat sur SecNumCloud. Il en a changé la nature. La question est désormais de savoir si la France saura transformer une exigence nationale en marché européen.

SÉBASTIEN GARNAUT
Founder of CyberTaskForce
& Paris Cyber Summit

SecNumCloud

Quoi de neuf ?

RÉPUBLIQUE FRANÇAISE

JOURNAL OFFICIEL

LOIS ET DÉCRETS

Le référentiel **SecNumCloud** devient **obligatoire** pour les prestataires privés traitant **des données de l'État**.

Par un décret du 14 août, le Premier Ministre Sébastien Lecornu rend obligatoire la qualification SecNumCloud pour les prestataires privés traitant des données de l'Etat, de ses opérateurs et aux groupements d'intérêt publics.

L'arrêté donne force obligatoire au référentiel technique, qui jusqu'à présent était un ensemble de bonnes pratiques que les administrations étaient encouragées à suivre.

Le référentiel lui n'a pas été modifié.



SecNumCloud

Quoi de neuf ?



**Wimi valide son J3
et obtient sa qualification
SecNumCloud**



**NumSpot valide son J3
et obtient sa qualification
SecNumCloud
pour son offre IaaS***



**OVH valide son J3
et obtient sa qualification
SecNumCloud pour
son offre SNC Cloud Platform
(PaaS et IaaS)***

*Ces obtentions ont été publiquement annoncées par les acteurs mais ne sont pas encore reflétées dans le catalogue officiel de l'ANSSI



**NRB demande
à l'ANSSI la qualification
SecNumCloud
de son offre IaaS.**



**Interstis demande
à l'ANSSI la qualification
SecNumCloud
de son offre SaaS.**

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 procédure de la qualification

J0

Demande de qualification auprès de l'ANSSI

J1

Stratégie d'évaluation acceptée

J2

Travaux d'évaluation acceptés

J3

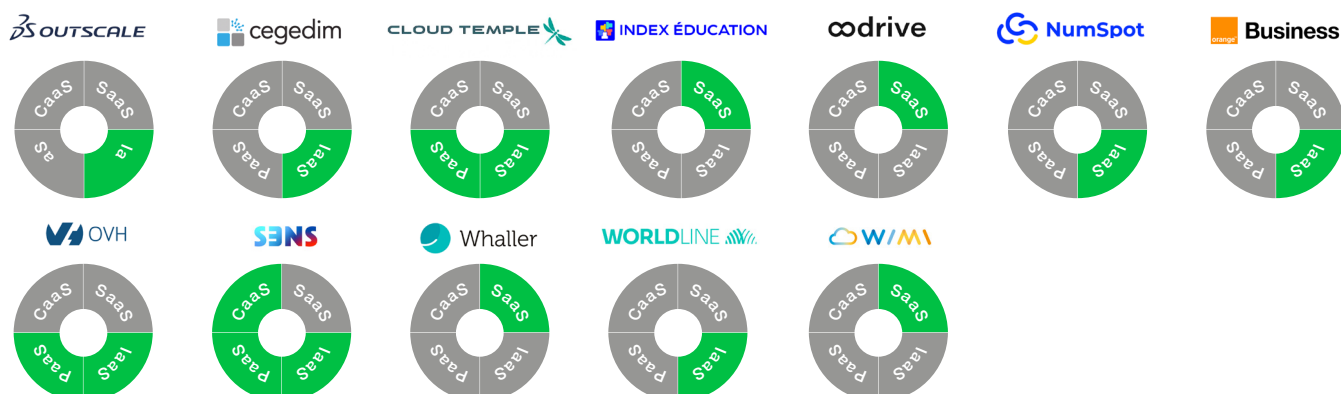
Décision de qualification par l'ANSSI



EN COURS



LES QUALIFIÉS



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"

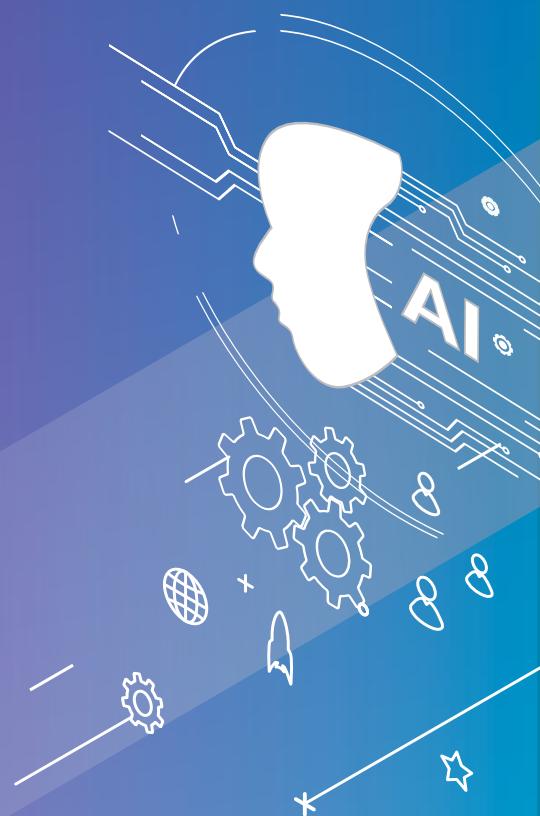
- **Devoir d'information** par le prestataire en cas de modification sur les éléments logiciels qu'il maîtrise.
- **Cloisonnement strict** entre les interfaces des commanditaires: les ressources affectées à l'usage d'un prestataire ne doivent pas être accessibles à d'autres commanditaires.

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



ÉDITION
SEPTEMBRE
2026