

OBSERVATOIRE

SecNumCloud

ÉDITION **AVRIL 2026**

L'EDITO SecNumCloud

L'intelligence artificielle ne transforme pas seulement le profil des menaces, elle en reconfigure le tempo.

Gérôme Billois, Partner chez Wavestone, rappelait récemment qu' «En 2018, il fallait en moyenne 2,3 ans pour qu'une vulnérabilité soit exploitée après sa divulgation. En 2025, c'est 23 jours. En 2026… 1,6 jour ». Dans le même temps, une attaque informatique survient toutes les 39 secondes dans le monde, c'est toutes les 14 secondes pour les ransomwares. Nous sommes donc sous attaque permanente, l'IA accélère les attaquants. Elle accélère aussi les défenseurs. En permettant une détection continue des anomalies, une corrélation des signaux faibles à grande échelle et une réponse automatisée, l'IA réduit les fenêtres d'exposition et contracte les cycles d'incident. Ce n'est plus une logique de protection réactive : c'est une capacité d'anticipation opérant dans un temps continu. Cette compression temporelle dans la sécurité est le révélateur d'une transformation plus large. Si la sécurité peut désormais s'exercer dans le temps réel du système, c'est que la performance des infrastructures est en train de changer de nature, non plus seulement dans ses paramètres techniques, mais dans sa dimension temporelle.

Une redéfinition de la performance : de la technique au tempo

Jusqu'à présent, la performance des infrastructures cloud reposait sur des critères établis : puissance de calcul, disponibilité, élasticité, optimisation des coûts. Ces éléments demeurent essentiels, mais ils ne suffisent plus. La performance se mesure désormais à la capacité à opérer dans le temps réel du marché. Or ce temps s'accélère. Les organisations doivent intégrer des cycles de décision plus courts, des déploiements plus rapides et une adaptation permanente à des environnements instables. L'IA permet précisément de répondre à cette exigence en réduisant la distance entre analyse, décision et exécution. Elle ne se contente pas d'améliorer la performance : elle aligne la performance sur le tempo réel de l'économie. La performance devient ainsi temporelle.

Le basculement du marché : une nouvelle équation d'achat

Cette évolution a des conséquences directes sur la structure du marché. Si la performance devient indissociable de la vitesse, les critères d'achat évoluent en profondeur. Les décideurs n'arbitrent plus entre solutions sur la base de leurs caractéristiques techniques. Ils arbitrent désormais une équation plus exigeante : la capacité à délivrer de la performance dans un environnement accéléré et plus securisé, tout en garantissant un haut niveau de maîtrise, de contrôle, de responsabilité et de prévisibilité. On reconnait d'ailleurs les attributs de la Souveraineté, monopole des États. Il ne s'agit plus seulement d'aller vite. Il s'agit d'aller vite sans perdre la maîtrise, comme Ronaldo le rappelait en 2000 dans sa pub Pirelli. C'est ce que désigne la logique du ZeroTrustMarket : un environnement où la confiance ne se présume plus, mais se démontre en continu par des architectures vérifiables et auditables. des garanties de gouvernance intégrées et une traçabilité opérationnelle. Dans ce marché, la sécurité devient une la condition structurante d'accès, le différenciant donnant un avantage concurrentiel.

SecNumCloud : un standard de marché en accélération

Cette évolution trouve sa traduction la plus concrète dans les services managés de sécurité : ce n'est plus l'outil qui est acheté, mais la capacité à opérer en continu dans un environnement d'attaque permanent. Le Pôle d'excellence cyber rappelait récemment que « les entreprises européennes ont besoin de performance, de résilience et de sécurité ». La valeur se déplace vers ceux qui savent combiner les trois comme Thalès ou CloudTemple, tous deux qualifiés Secnumcloud. La performance n'est pas sacrifiée dans SecNumCloud. Au contraire, la qualification s'inscrit précisément comme un levier de performance pour le ZeroTrustMarket. C'est aussi ce qui explique les attaques de certains sur l'ANSSI et Thalès, qui a su intégrer les solutions IA de Google Cloud sans perdre la main. Quand on ne ne peut pas jouer le ballon, par peur de la concurrence, on joue le bonhomme. Vincent Strubel en a été contraint de rappeler les règles en tant qu'arbitre, pour certains mauvais joueurs.

SecNumCloud n'est pas un outil politique

La qualification établit une base de confiance vérifiée en amont, ce qui réduit ensuite les cycles de due diligence contractuelle, simplifie les exigences de souveraineté dans les appels d'offres sensibles et accélère le déploiement dans les environnements réglementés. Le coût est initial et le bénéfice est continu. Dans un environnement structuré par l'intelligence artificielle, cette capacité devient déterminante. Avec les offres SecNumCloud, l'enjeu n'est plus d'opposer performance et sécurité mais de s'assurer que la performance reste gouvernable dans l'accélération. Demain, les acteurs ne seront pas départagés par leur seule performance technologique. Ils le seront par leur capacité à tenir dans le temps réel du marché sans perdre le contrôle. Les organisations qui auront construit des architectures de confiance vérifiable et les fournisseurs capables de les soutenir disposeront d'un avantage structurel.

L'IA de SecNumCloud, c'est la vitesse maîtrisée.

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

adista



Bleu



Blue.



CYLLENE



ecritel



free PRO



ITS Integra



NetExplorer



NUMIH France



NumSpot



orange Business



OVH



Scaleway



Tenexa



WIMI



LES QUALIFIÉS

DS OUTSCALE



cegedim



CLOUD TEMPLE



INDEX ÉDUCATION



∞drive



orange Business



OVH



S3NS



Whaller



WORLDLINE



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



J0 : ITS Integra, Tenexa, Blue., adista

J1 : Bleu, ecritel, NetExplorer, NumSpot, Scaleway

J3 : S3NS

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*



CYBER TASK FORCE

ÉDITION
AVRIL 2026