CYBER TASK FORCE

OBSERVATOIRE

SecNumCloud

ÉDITION **JUIN 2026**

L'EDITO SecNumCloud

L'approche danoise : pragmatisme et ouverture sécurisée

Joen Magieres
Senior Policy Advisor, Danish Chamber of Commerce.

Le débat européen sur la souveraineté numérique s'est considérablement intensifié ces dernières années. La montée des tensions géopolitiques, des menaces cyber, des préoccupations autour des infrastructures critiques et des dépendances stratégiques a replacé les politiques numériques au cœur de l'agenda européen.

Dans le même temps, les décideurs européens font face à un exercice d'équilibre complexe : renforcer la résilience et réduire les dépendances stratégiques sans fragmenter davantage un marché unique numérique européen déjà particulièrement complexe.

Du point de vue danois, cet équilibre est essentiel. Les décideurs publics et les organisations professionnelles danoises considèrent de plus en plus la cybersécurité, la résilience et la sécurité des chaînes d'approvisionnement comme des priorités stratégiques. Pourtant, les entreprises danoises peinent à se développer et à changer d'échelle sur le marché européen, et cherchent donc leurs opportunités de croissance ailleurs.

En réalité, huit des douze licornes danoises ont déplacé leur siège social à l'étranger depuis le début des années 2000, illustrant la difficulté de construire des champions mondiaux depuis l'Europe.

En matière de confiance cloud, le Danemark a toutefois adopté une approche décentralisée et fondée sur le risque, centrée sur la protection des données, la résilience et la sécurité. Plutôt que de construire un régime unique de certification de cloud souverain similaire à SecNumCloud, la responsabilité des choix cloud repose largement sur chaque organisation.

Dans les faits, les administrations publiques comme les entreprises privées sont tenues de conduire leurs propres évaluations de risques, procédures d'achat et analyses de conformité, en fonction de la sensibilité des données et des services concernés.

Pour les données personnelles, l'Autorité danoise de protection des données fournit des lignes directrices sur l'usage conforme du cloud. Sur le volet cybersécurité, la directive NIS2 joue un rôle croissant. Le ministère de la Résilience et de la Préparation coordonne sa mise en œuvre, tandis que treize autorités sectorielles supervisent la conformité. L'Agence danoise pour le gouvernement numérique est, quant à elle, chargée de superviser les fournisseurs cloud, les centres de données et certaines infrastructures numériques relevant de NIS2.

À la différence de l'initiative française SecNumCloud, le Danemark n'applique aucune forme d'exclusion formelle des hyperscalers. L'accès au marché demeure globalement ouvert et le débat porte moins sur la nationalité des acteurs que sur la gestion des risques, de la résilience et des dépendances. Les décisions reposent généralement sur des critères tels que la nature des données concernées, les garanties contractuelles, les mesures de cybersécurité, la conformité au RGPD, les risques liés à la chaîne d'approvisionnement ou encore les exigences de passation des marchés publics.

Pour autant, la dynamique en faveur de la compétitivité danoise et européenne gagne en intensité — et pour de bonnes raisons. Au-delà du rapport souvent cité de Draghi, ceux de Letta et de Niinistö ont eux aussi mis en lumière une réalité préoccupante : ni le marché

européen, ni notre compétitivité, ni notre résilience ne sont aujourd'hui dans une situation satisfaisante. Les solutions européennes sont donc de plus en plus recherchées, même lorsqu'elles impliquent une approche moins strictement nationale.

Comme l'exprime l'actuel ministre danois des Affaires étrangères : « Nous ne pouvons pas être un pays gagnant dans une région perdante. »

C'est dans cette logique que la Chambre de commerce danoise a proposé un Marché unique numérique plus intégré et moins fragmenté, une harmonisation accrue de la réglementation numérique, une généralisation du principe du « Only Once », ainsi qu'une approche européenne davantage coordonnée en matière de certification cybersécurité, d'infrastructures numériques et de résilience.

La cybersécurité et les secteurs critiques au centre des priorités

La cybersécurité est devenue un élément de plus en plus central du débat. Le Danemark est l'une des sociétés les plus numérisées au monde — et donc également l'une des plus dépendantes et vulnérables sur le plan numérique. Les pouvoirs publics comme les industriels considèrent désormais les infrastructures cloud comme des infrastructures critiques à part entière.

Cette évolution s'est encore accélérée depuis l'invasion de l'Ukraine par la Russie, la montée des tensions géopolitiques et l'augmentation significative des cyberattaques visant les pays européens. Les décideurs publics et économiques danois sont de plus en plus préoccupés par la résilience, la continuité d'activité et les dépendances au sein des chaînes d'approvisionnement numériques.

Les considérations de sécurité nationale deviennent déterminantes lorsqu'il s'agit d'infrastructures critiques, de fonctions publiques sensibles ou d'informations classifiées. Dans ces cas, les autorités et les opérateurs sont tenus d'évaluer avec attention leur exposition géopolitique, les risques liés à la chaîne d'approvisionnement et les dépendances opérationnelles.

Le Danemark dispose également du D-Seal, un label volontaire portant sur la sécurité informatique et l'usage responsable des données. Bien qu'il ne constitue ni un régime de certification de cloud souverain ni une condition obligatoire d'accès au marché, la Chambre de commerce danoise estime que certains éléments du modèle pourraient inspirer de futures approches européennes en matière d'infrastructures numériques de confiance, notamment dans le cadre d'une révision du Cyber Security Act et du Cyber Security Certification Framework.

Entre hybridation et souveraineté numérique

L'approche danoise ne conduit donc pas à un modèle strictement souverainiste du cloud, mais plutôt à une approche hybride et pragmatique. La Chambre de commerce danoise recommande explicitement une stratégie cloud différenciée combinant hyperscalers, modèles hybrides, fournisseurs locaux et partenariats stratégiques.

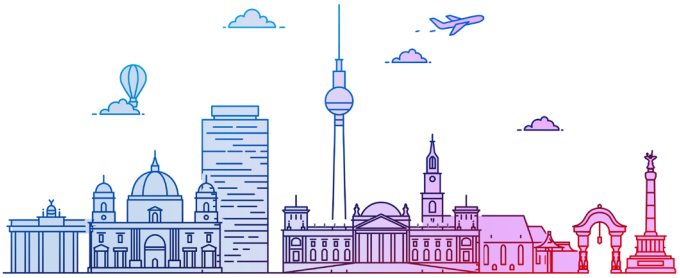
Le marché danois demeure néanmoins fortement dépendant des fournisseurs cloud non européens. Selon une récente analyse de la Chambre de commerce danoise, 88 % des entreprises membres utilisant des services cloud s'appuient sur au moins un fournisseur non européen. Dans le même temps, 52 % souhaitent réduire, au moins partiellement, cette dépendance, principalement en raison des enjeux géopolitiques, des préoccupations de conformité et des exigences de résilience des chaînes d'approvisionnement.

Plutôt que de poursuivre une souveraineté numérique stricte, l'approche émergente du Danemark pourrait ainsi être mieux définie comme une « ouverture sécurisée » : maintenir l'accès aux technologies mondiales tout en renforçant la résilience, la cybersécurité et la maîtrise des risques stratégiques liés à leur utilisation.

OBSERVATOIRE

SecNumCloud
Quoi de neuf ?

Hallo Deutschland!



THALES Google Cloud

Google Cloud et Thales annoncent la création d'une entité jumelle de SENS en Allemagne.

Ce nouveau cloud souverain allemand, offert par une entité controlée par Thales Allemagne, répondra aux normes allemandes, notamment le nouveau référentiel C3A et les critères C5. Cette annonce reflète la réalité européenne du marché du cloud souverain. Les acteurs privés sont actifs dans un marché à l'échelle européenne, et développent des offres réplicables en dehors des seules frontières du marché national initial.

blue. | J1

Blue valide son J1 et progresse dans sa qualification SecNumCloud.

Scalingo

Scalingo demande à l'ANSSI la qualification SecNumCloud de son offre PaaS.

Le projet s'appuie sur l'infrastructure SecNumCloud qualifiée de OUTSCALE, illustrant la structuration progressive d'un écosystème PaaS souverain reposant sur des couches IaaS déjà qualifiées.

C:YLLENE

Cyllène ne fait plus partie des acteurs en cours de qualification par l'ANSSI.

Zoom du mois de mai : cloud souverain à l'échelle européene

OVHcloud

dans son alliance
avec Post Telecom
et CleverCloud

Scaleway

S3NS

dans son partenariat
avec Proximus,
Clarence et Mistral

L'appel d'offre couvre la fourniture de services de cloud pour les institutions, organes et organismes de l'UE pour un montant maximal de 180 millions d'euros sur une période de six ans. Les fournisseurs retenus ont été sélectionnés sur la base de leur adéquation avec le cadre de souveraineté de l'informatique en nuage de la Commission Européenne.

Zoom du mois de février : 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.

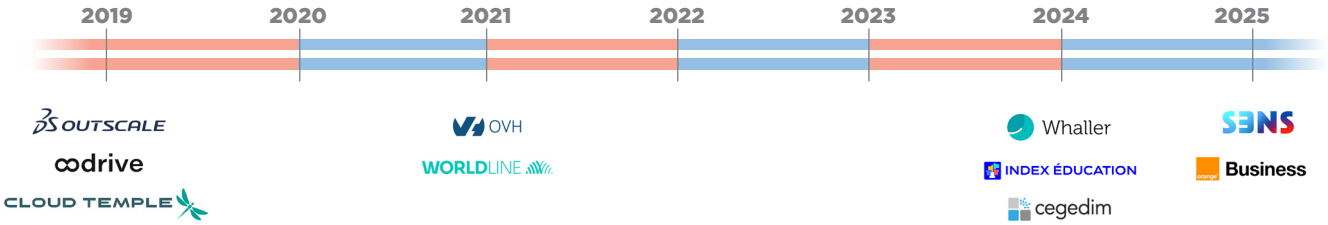
> **Ouverts : l'usager contrôle l'évolution du modèle**

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

Zoom du mois de janvier : les qualifiés

La qualification : un engagement d'entreprise inscrit dans la durée

Les entreprises qualifiées SecNumCloud ont été précurseures pour engager le processus de qualification. L'engagement quasi-citoyen de ces entreprises démontre un fort alignement entre les valeurs de l'entreprise et les ambitions de sécurité et de confiance du référentiel SecNumCloud.



Les offres qualifiées

	TYPE DE CLOUD	PART DE L'OFFRE QUALIFIÉE	CLIENTS CIBLES	NOMBRE DE SERVICES MANAGES	HORIZON GEOGRAPHIQUE	PRINCIPE DE COMPOSITION	AMBITION D'EXTENSION
OUTSCALE	Mutualisé	30 50 80 100	Secteur privé OIV/OSE Secteur public	10+	Europe	Facilitateur	✓
cegedim		Informations non disponibles					
CLOUD TEMPLE	Mutualisé	30 50 80 100	Secteur privé OIV/OSE Secteur public	20+	France	Facilitateur	✓
INDEX ÉDUCATION		Informations non disponibles					
cloudrive		Informations non disponibles					
Business		Informations non disponibles					
OVH	Dédié	30 50 80 100	PME/TPE Secteur privé OIV/OSE Secteur public	20+	France	Facilitateur	✓
S3NS	Mutualisé	30 50 90 100	PME/TPE Secteur privé OIV/OSE Secteur public	50+	Europe	Facilitateur	✓
WORLDLINE	Dédié & Mutualisé	30 50 80 100	Secteur privé Secteur public	10+	France	Facilitateur	✓
Whaller	Mutualisé	30 50 80 100	PME/TPE Secteur public	10+	Monde	Bénéficiaire	✓

Cloud Mutualisé : Les ressources matérielles sont partagées entre plusieurs clients
Cloud Dédié : Les ressources matérielles sont réservées à un seul client

Zoom du mois de décembre : le PaaS

Périmètre du PaaS et critères d'analyse

Le PaaS est une brique stratégique: elle permet de déployer des **services managés**. Ces services managés sont un élément clef pour comprendre la maturité des offres des différents acteurs qualifiés ou en cours de qualification SecNumCloud.

5 piliers permettant de lire l'offre PaaS

1 IA
Capacité à développer, entraîner et déployer des modèles d'intelligence artificielle dans un environnement cloud qualifié SecNumCloud.
> *Stade 1 : GPU*
> *Stade 2 : IA Native ou LLM as a Service*

2 DATABASE MANAGÉE
Capacité à héberger, exploiter, sécuriser un moteur de base de données sans que le client ait à gérer les serveurs ou l'administration quotidienne dans un environnement cloud qualifié SecNumCloud.
> *Stade 1 : SQL*
> *Stade 2 : no-SQL*

3 ANALYTICS MANAGÉS
Capacité à collecter, stocker, traiter et visualiser des données à des fins d'analyse, sans administration de l'infrastructure sous-jacente par le client dans un environnement cloud qualifié SecNumCloud.
> *Stade 1 : Visualisation et requête simples*
> *Stade 2 : Big Data*

4 STOCKAGE MANAGÉ
Capacité à assurer le provisionnement, la disponibilité, le monitoring et la sécurité des données stockées, sans intervention du client sur l'infrastructure, le tout dans un environnement cloud qualifié SecNumCloud
> *Stade 1 : Block Storage*
> *Stade 2 : File Storage*

5 INTEROPÉRABILITÉ AVEC DES ÉDITEURS TIERS (ISV)
Capacité de la plateforme à permettre le déploiement de services par des éditeurs indépendants dans un environnement cloud qualifié SecNumCloud.

L'Observatoire complète son analyse par un critère de **disponibilité géographique** de l'offre PaaS.
L'analyse des offres a été réalisée au regard des informations publiques disponibles, et suivant les services soumis à qualification. A l'avenir les acteurs peuvent élargir l'offre PaaS qualifiée SecNumCloud.

Les offres PaaS

	CLOUD TEMPLE	Bleu	Scaleway	S3NS
	Offre cloud unique certifié SecNumCloud depuis 2022 Double qualification obtenue : IaaS et PaaS	Offre les services de Microsoft Azure et Microsoft 365 dans un environnement SecNumCloud Triple qualification en cours : IaaS, CaaS, PaaS		Offre les services de Google dans un environnement SecNumCloud Triple qualification en cours : IaaS, CaaS, PaaS
Analytics managés	STADE 2	STADE 2		STADE 2
Database managée	STADE 2	STADE 2		STADE 2
Stockage managé	STADE 2	STADE 2		STADE 2
Plateforme IA	STADE 2	STADE 1		STADE 1
Interopérabilité *éditeurs tiers (ISV)*				
Géographie	FRANCE	FRANCE	EUROPE	EUROPE

Qualification obtenue

Indisponible
Disponible mais non incluse dans le périmètre de qualification SecNumCloud
Disponible et incluse dans le périmètre de qualification SecNumCloud

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

IaaS

EN COURS		LES QUALIFIÉS	
Candidat	**Offre**	**Entreprises**	**Offre**
Adista	dista Secure Cloud	**Cegedim**	CegNumCloud Secured IaaS
Bleu	Cloud de Confiance Bleu	**Cloud Temple**	IAAS Secure Temple
Cyllene ITS	IaaS SecNumCloud	**OVH**	Bare Metal Pod
Ecritel	Ecritel Secure Cloud	**OVH**	Hosted Private Cloud powered by VMware
Gip Mipih (Numih France)	Cloud Premier Souverain	**Orange Business**	CloudAvenueSecNum
ITS Integra	IT SecureCloud	**Outscale**	IaaS
Numspot	Plateforme des services cloud	**Worldline**	Worldline Cloud Services
Orange Business	Cloud Avenue SecNum Dynamic	**S3NS**	Cloud de Confiance PREMI3NS
OVH SAS	SNC Cloud Platform		
Prolival - Groupe Tenexa	Horizon SecNumCloud		
Scaleway	Scaleway SecNumCloud		
Bretagne Télécom	Blue Secure Cloud		

CaaS

Bleu	Cloud de Confiance Bleu	**S3NS**	Cloud de Confiance PREMI3NS
ITS Integra	ITSecureKube		

PaaS

Bleu	Cloud de Confiance Bleu	**Cloud Temple**	PaaS Openshift
OVH SAS	SNC Cloud Platform	**S3NS**	Cloud de Confiance PREMI3NS
Scaleway	Scaleway SecNumCloud		

SaaS

Ecritel Solutions	Ecritel Secure Backup	**Index Education**	EDT
NetExplorer	Share and Workspace	**Index Education**	Hyperplanning
Cloud Solutions	Wimi	**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.


cegedim


ecritel


free PRO


ITS Integra


Scalingo


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 — Tenexa, adista

J1 — ITS Integra, Bleu, ecritel, Blue., NetExplorer, NumSpot, Scaleway

J2 —

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*

ÉDITION
JUIN 2026