



**OBSERVATORY**

# SecNumCloud

FEBRUARY 2026 EDITION

### ***SecNumCloud: A Market Lever in France's Cyber Strategy***

---

France has just published its national cybersecurity strategy, and SecNumCloud occupies a particularly interesting position within it. Until now, SecNumCloud has suffered from a persistent misunderstanding: it has often been perceived as a tool of the State, an “administrative cloud” by nature. This interpretation is both reductive and misleading.

The 2026–2030 National Cybersecurity Strategy can help move beyond this confusion by restoring SecNumCloud to its true function: not serving a specific actor, but qualifying a market. That market is neither the cloud sector as a whole nor everyday digital uses. It is the market for organizations that are critical or handle sensitive information, public or private. SecNumCloud is not an instrument of ownership; it is an instrument of clarity and access.

#### ***A market defined by criticality, not by status***

---

The central criterion of SecNumCloud is not legal, but functional. It does not distinguish between public and private actors; it distinguishes between critical and non-critical activities, between sensitive functions and mass-market uses, between systemic responsibilities and peripheral ones. For too long, the debate has been framed on the wrong terrain.

In the 2026–2030 strategy, cloud infrastructure is explicitly recognized as critical infrastructure, and certain data, processing activities, and functions are identified as vital to the Nation. SecNumCloud responds directly to this reality by providing an access framework tailored for organizations that bear systemic responsibility—whether operators of vital importance, actors in health-care, energy, industrial defense, finance, or strategic technology sectors. This is not the State's cloud; it is the cloud for high-responsibility functions.

### ***SecNumCloud as a gateway to a trust-based market***

---

By qualifying this market, SecNumCloud becomes its gateway. It does not guarantee automatic commercial advantage, but it makes access to a specific segment possible: one in which trust is not a marketing claim, but a condition of operability. This mechanism is structurally significant. It transforms a security requirement into a clear market signal: to operate in this segment, providers must accept a certain level of constraint, auditability, and accountability. In return, client organizations gain a transparent framework for making their technology choices.

In this model, the State is neither the sole customer nor even the central one. It is the body that defines the threshold—the actor that sets the rules for access to a market whose primary beneficiaries are critical organizations themselves, public and private alike. This is precisely the role of a State exercising sovereignty: defining the framework.

#### ***From a State tool to strategic-use infrastructure***

---

The real challenge now is to fully embrace this shift. As long as SecNumCloud is seen as a tool “for the State,” it will remain confined to a defensive and often polemical role. If it is clearly positioned as market infrastructure for sensitive uses, its logic is self-evident: invest to gain access, comply to operate, and move up the value chain to endure. The 2026–2030 strategy creates the conditions for this clarification, but it also calls for an explicit doctrine of use: which types of data, which levels of criticality, which chains of responsibility. Without this clarity, SecNumCloud will remain ambiguous. With it, it can become a powerful structuring accelerator—serving both national resilience and the competitiveness of the actors concerned.

SecNumCloud is not a tool for States. It is a tool for organizations that cannot afford approximation, and there are many of them in Europe.

**Thank you, and see you soon,**  
SÉBASTIEN GARNAULT

# Focus: Deploying AI in a SecNumCloud Environment

## SecNumCloud: Secure, Scalable AI



## Integration Strategies

Offer 1	Offer 2	Offer 3
<p><b>AI Infrastructure: GPU infrastructure within SecNumCloud — a technical offering designed to meet high-intensity AI computing needs.</b></p> <div style="text-align: center;"> </div>	<p><b>AI Platforms:</b> AI software deployed on SecNumCloud — with the cloud provider acting as an enabler.</p> <ul style="list-style-type: none"> <li>&gt; LLM-as-a-Service operated by the cloud provider</li> <li>&gt; Client-operated solutions using dedicated AI software</li> </ul> <div style="text-align: center;"> </div>	<p><b>AI Models:</b> The key is model-agnostic integration, ensuring flexibility in model selection and the ability to switch over time.</p> <ul style="list-style-type: none"> <li>&gt; Open models: users retain control over model evolution</li> <li>&gt; Proprietary models: controlled by their owners and often more powerful</li> </ul>

# SecNumCloud

## What is it?

SecNumCloud is the ANSSI framework that defines security and sovereignty requirements for cloud computing services used by administrations and businesses in France.

### The difference between qualification and certification

A **qualification** verifies a provider's or service's ability to meet a need (trust, skills, expected level).

A **certification**, issued by a third-party organization, attests to conformity with a specific standard or framework.



#### It aims to attest

- 1 The quality and robustness of a cloud service
- 2 The competence of the cloud operator
- 3 The trust that can be placed in the operator

#### It establishes a multi-dimensional framework

- 1 Technical
- 2 Operational
- 3 Legal



### Technical Criteria

- > **Documented risk assessment** covering the entire scope of the service.
- > **Annual updating** of information security and business continuity plans.
- > **Obligation to inform** the client in the event of a personal data breach.
- > **Appointment** of an information systems security manager.
- > **Appointment** of a physical security manager.
- > **Daily data backup** policy.



### Operational Criteria

- > **Strong multi-factor authentication** to access administration interfaces.
- > **Nominative accounts** for users.
- > **An encryption mechanism** that prevents data recovery in the event of a resource or physical support reallocation.
- > **Segregation of network flows** (logical/physical/encrypted).
- > **Active monitoring** to manage technical vulnerabilities and evaluate risk exposure.



### Legal Criteria

- > The provider's statutory headquarters, central administration, and principal establishment **must be established within an EU Member State.**
- > **Limits on the holding of capital and voting rights** by non-EU entities: 24% individually, 39% collectively.
- > **Storage and processing of data within the EU.**
- > **Justified compliance with GDPR principles** (legitimate purposes, limited data retention period).
- > The service agreement must include a **reversibility clause** providing for the secure restitution and erasure of the client's data upon contract termination or for any other cause.



## The Qualification Procedure

- J0** Application for qualification submitted to ANSSI
- J1** Evaluation work accepted
- J2** Evaluation strategy accepted
- J3** Qualification decision by ANSSI.



- > Detailed description of the services submitted for qualification
- > Demonstration of conformity to the SecNumCloud framework
- > Selection of a qualified auditor responsible for conducting the J2 audits

- > Validation by ANSSI of the audit plan proposed by the evaluation body
- > Roadmap for J2 audits

- > Technical and organizational audits are conducted on-site by the accredited organization.
- > The report is transmitted to ANSSI for analysis.

- > ANSSI reviews the J2 audit report
- > Potential requests for corrective actions
- > Potential request for additional information or validation of the certification qualification

## The Main Evaluation Criteria



### Technical Criteria

- > Documented risk assessment covering the entire scope of the service.
- > Annual updating of information security and business continuity plans.
- > Obligation to inform the client in the event of a personal data breach.
- > Appointment of an information systems security manager.
- > Appointment of a physical security manager.
- > Daily data backup policy.



### Operational Criteria

- > Strong multi-factor authentication to access administration interfaces.
- > Nominative accounts for users.
- > An encryption mechanism that prevents data recovery in the event of a resource or physical support reallocation.
- > Segregation of network flows (logical/physical/encrypted).
- > Active monitoring to manage technical vulnerabilities and evaluate risk exposure.



### Legal Criteria

- > The provider's statutory headquarters, central administration, and principal establishment must be established within an EU Member State.
- > Limits on the holding of capital and voting rights by non-EU entities: 24% individually, 39% collectively.
- > Storage and processing of data within the EU.
- > Justified compliance with GDPR principles (legitimate purposes, limited data retention period).
- > The service agreement must include a reversibility clause providing for the secure restitution and erasure of the client's data upon contract termination or for any other cause.

# SecNumCloud

## Who is it?

### Services Under Review for Qualification

	IN PROGRESS		QUALIFIED	
	Applicants	Offering	Provider	Offering
IaaS	<b>Adista</b> <b>Bleu</b> <b>Cyllene ITS</b> <b>Ecritel</b> <b>Gip Mipih (Numih France)</b> <b>ITS Integra</b> <b>Numspot</b> <b>Orange Business</b> <b>OVH SAS</b> <b>Prolival - Groupe Tenexa</b> <b>Scaleway</b> <b>Bretagne Télécom</b>	dista Secure Cloud Cloud de Confiance Bleu IaaS SecNumCloud Ecritel Secure Cloud Cloud Premier Souverain IT SecureCloud Plateforme des services cloud Cloud Avenue SecNum Dynamic SNC Cloud Platform Horizon SecNumCloud Scaleway SecNumCloud Blue Secure Cloud	<b>Cegedim</b> <b>Cloud Temple</b> <b>OVH</b> <b>OVH</b>  <b>Orange Business</b> <b>Outscale</b> <b>Worldline</b> <b>S3NS</b>	CegNumCloud Secured IaaS IAAS Secure Temple Bare Metal Pod Hosted Private Cloud powered by VMware CloudAvenueSecNum IaaS Worldline Cloud Services Cloud de Confiance PREMI3NS
Caas	<b>Bleu</b> <b>ITS Integra</b>	Cloud de Confiance Bleu ITSecureKube	<b>S3NS</b>	Cloud de Confiance PREMI3NS
PaaS	<b>Bleu</b> <b>OVH SAS</b> <b>Scaleway</b>	Cloud de Confiance Bleu SNC Cloud Platform Scaleway SecNumCloud	<b>Cloud Temple</b> <b>S3NS</b>	PaaS Openshift Cloud de Confiance PREMI3NS
SaaS	<b>Ecritel Solutions</b> <b>NetExplorer</b> <b>Cloud Solutions</b>	Ecritel Secure Backup Share and Workspace Wimi	<b>Index Education</b> <b>Index Education</b> <b>Index Education</b> <b>Index Education</b> <b>Oodrive</b> <b>Oodrive</b> <b>Oodrive</b> <b>Oodrive</b> <b>Whaller</b>	EDT Hyperplanning Pronote Pronote Primaire Oodrive_Work_Share Oodrive_Work Oodrive_Meet Whaller Donjon SaaS

Free Pro is also undergoing qualification, but no public information is available on the type of qualification requested.

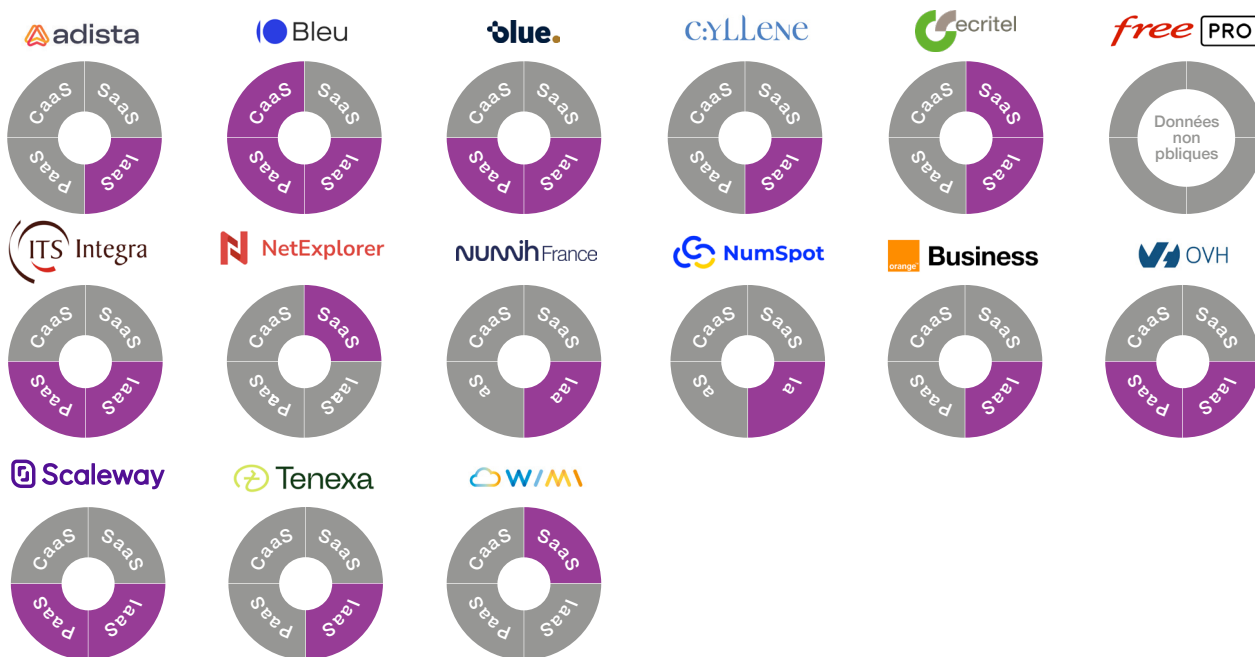
### The candidates

IaaS	
Caas	
PaaS	
SaaS	

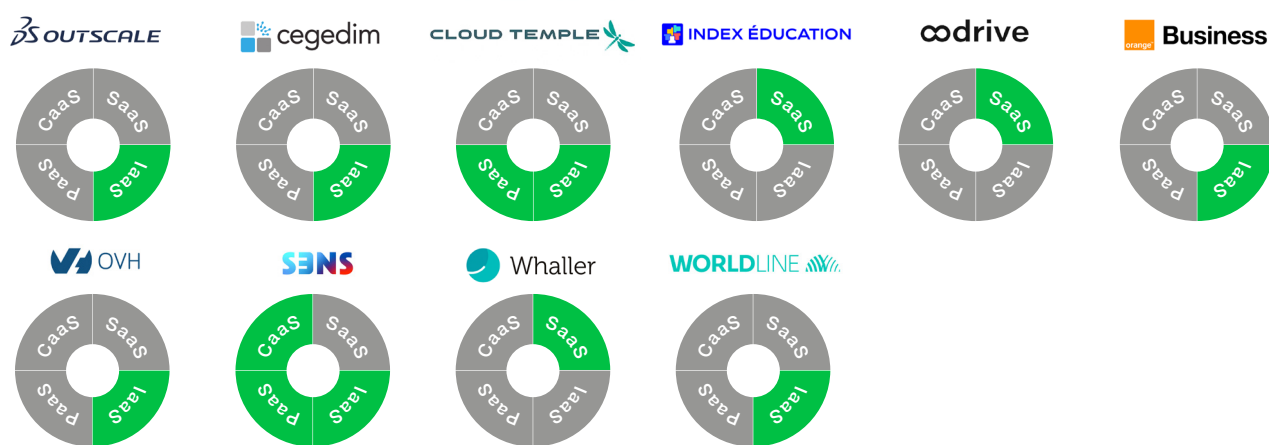


## Scope of the qualification

### IN PROGRESS



### QUALIFIED PROVIDERS



## Status of candidates

- J0** Application for qualification submitted to ANSSI
- J1** Evaluation work accepted
- J2** Evaluation strategy accepted
- J3** Qualification decision by ANSSI



# Glossary of Cloud Offerings



## IaaS (Infrastructure as a Service)

- > Provision of physical computing resources.
- > **The provider owns** the physical infrastructure and rents it or makes it available to a user.
- > **The client builds** his activity on this platform
- > **The provider** owns all the physical material, including machines, network, and storage.
- > **The client** builds the services according to his needs, decides the scope/perimeter, and determines the possible uses on the leased infrastructure.

### The Specifics of IaaS

- **Strict segregation** between users.
- To prevent data recovery during resource reallocation or physical support recovery, **encryption (of the disk, file system, or by volume) with a key per client is required**

## CaaS (Container as a Service)

- > Provision of tools allowing **the deployment, management, and orchestration of application** containers.
- > **A container** is like a small, isolated box that contains everything necessary for an application to function (libraries, code, tools, etc.), without interfering with others.
- > **The provider** manages the underlying infrastructure (servers, storage, network, operating system).
- > **The client** controls the containers and the technical elements related to their applications

### The Specifics of CaaS

- **Strict segregation** between clients.
- **Recommended cryptography:** encryption by volume (one key/client).
- **Secure obliteration** at the end of the contract means the secure erasure of the encryption keys for the client's storage spaces.
- Administration and supervision operations must be carried out **from within the European Union**

## PaaS (Platform as a Service)

- > Provision of a **technical platform ready for use** to develop, host, and run applications.
- > **The provider** manages the entire infrastructure part (network, servers, storage, operating system, etc.).
- > **The client** focuses on the development and management of their own applications

### The Specifics of PaaS

- The provider has a **duty to inform** the client in case of modification to the software elements that the provider controls.
- **Strict segregation** between clients interfaces: the resources allocated for the use of one client must not be accessible to other clients

## SaaS (Software as a Service)

- > Provision of **ready-to-use applications**, hosted in the cloud and fully managed by the provider.
- > The user simply accesses the application via the Internet—without having to install, host, or maintain anything.
- > **The provider** manages all the technical aspects requiring IT skills.
- > **The client** does not control the cloud platform but can modify configuration settings within the application.

### The Specifics of SaaS

- **Multi-factor authentication** for end-user access.
- **Segregation** between the administration interfaces made available to clients and the interfaces allowing end-user access



---

**of Cloud Temple**

<https://www.cloud-temple.com/en/large-language-model-as-a-service-llmaas/>

---

**of SENS**

<https://documentation.s3ns.fr/compute/docs/gpus?hl=fr#a3-series>

---

**of Bleu**

<https://www.bleucloud.fr/telechargement-liste-des-services-azure/>

---

**of NumSpot**

<https://numspot.com/en/produit/sovereign-data-aisovereign-data-ai/>

---

**of Orange Business Services**

<https://www.orange.com/en/press-release/orange-business-launches-new-trusted-genai-offers-end-to-end-for-french-customers-233858?>

---

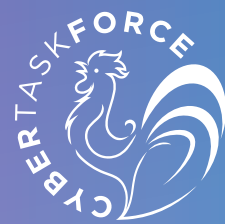
**of Scaleway**

<https://www.scaleway.com/en/custom-built-clusters/>

---

**of Outscale**

<https://en.outscale.com/cloud-experience/sovereign-cloud/>



FEBRUARY  
2026  
EDITION