OBSERVATORY

SecNumCloud

APRIL 2026 EDITION

EDITORIAL SecNumCloud

Artificial intelligence is not just reshaping the threat landscape, it is redefining its tempo.

As Gérôme Billois, Partner at Wavestone, recently noted: "In 2018, it took an average of 2.3 years for a vulnerability to be exploited after disclosure. In 2025, it's 23 days. In 2026… 1.6 days." At the same time, a cyberattack occurs every 39 seconds worldwide, and every 14 seconds when it comes to ransomware. We are therefore under constant attack. AI is accelerating attackers. It is also accelerating defenders. By enabling continuous anomaly detection, large-scale correlation of weak signals, and automated response, AI is shrinking exposure windows and compressing incident cycles. This is no longer a reactive model of protection; it is an anticipatory capability operating in continuous time. This compression of time in cybersecurity reveals a broader transformation. If security can now operate in the system's real time, it is because infrastructure performance itself is changing in nature, not only in its technical parameters, but in its temporal dimension.

Redefining performance: from technical metrics to tempo

Until recently, cloud infrastructure performance was defined by well-established metrics: computing power, availability, elasticity, and cost optimization. These remain essential, but they are no longer sufficient. Performance is now measured by the ability to operate at the speed of the market. And that speed is accelerating. Organizations must adapt to shorter decision cycles, faster deployments, and constant adjustment to unstable environments. AI directly addresses this challenge by narrowing the gap between analysis, decision, and execution. It does not merely enhance performance, it aligns performance with the real-time tempo of the economy. Performance, in this sense, becomes temporal.

A market shift: a new purchasing equation

This shift has direct implications for market structure. As performance becomes inseparable from speed, purchasing criteria are evolving at a fundamental level. Decision-makers are no longer comparing solutions based solely on technical specifications. They are now evaluating a more demanding equation: the ability to deliver performance in a faster and more secure environment, while ensuring a high level of control, accountability, responsibility, and predictability. In this equation, one begins to recognize attributes traditionally associated with sovereignty, long the exclusive remit of states. It is no longer just about moving fast. It is about moving fast without losing control, echoing a long-standing principle: speed is nothing without control. This is the logic of the ZeroTrustMarket: an environment where trust is no longer assumed, but continuously demonstrated through verifiable and auditable architectures, embedded governance guarantees, and operational traceability. In such a market, security becomes the structural condition for access, and a key differentiator conferring competitive advantage.

SecNumCloud: an accelerating market standard

This evolution finds its most concrete expression in managed security services: what is being purchased is no longer a tool, but the capability to operate continuously in a state of persistent attack. As the Cyber Excellence Hub recently emphasized, "European companies need performance, resilience, and security." Value is shifting toward those who can combine all three, such as Thales and Cloud Temple, both SecNumCloud-qualified providers. Performance is not sacrificed within SecNumCloud, on the contrary, the qualification acts as a performance enabler within the ZeroTrustMarket. It also helps explain the growing criticism directed at ANSSI and at players like Thales, which has successfully integrated Google Cloud AI solutions without relinquishing control. When competition becomes difficult to match on substance, the temptation is to target the player instead of the play. In that context, ANSSI's head, Vincent Strubel, has at times had to step in as referee to restate the rules of the game.

SecNumCloud is not a political tool

The qualification establishes a verified baseline of trust upfront, reducing subsequent due diligence cycles, simplifying sovereignty requirements in sensitive tenders, and accelerating deployment in regulated environments. The cost is upfront; the benefit is continuous. In an environment shaped by artificial intelligence, this capability becomes decisive. With SecNumCloud offerings, the challenge is no longer to trade off performance against security, but to ensure that performance remains governable under acceleration. Tomorrow, market leaders will not be defined by technological performance alone. They will be defined by their ability to operate at the speed of the market without losing control. Organizations that build verifiable trust architectures, and providers capable of sustaining them, will hold a structural advantage.

SecNumCloud AI is controlled speed.

OBSERVATORY

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

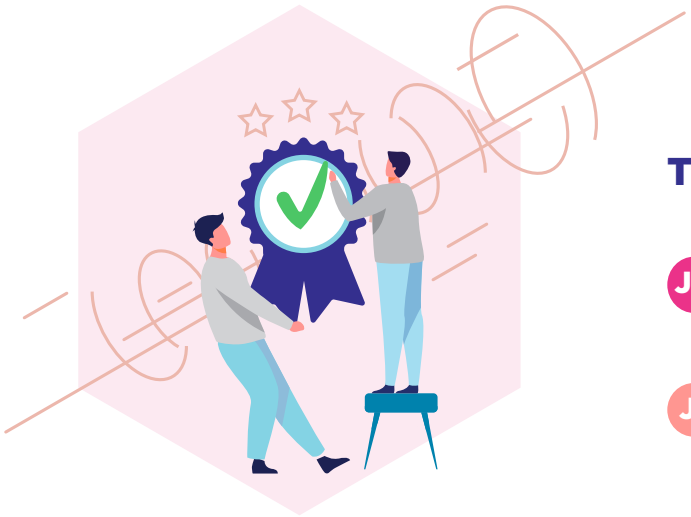
> **Documented risk assessment** covering the entire scope of the service.
> **Annual updating** of information security and business continuity plans.
> **Obligation to inform** the client in the event of a personal data breach.
> **Appointment** of an information systems security manager.
> **Appointment**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

J0

- 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

J1

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

J2

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

J3

- 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.

OBSERVATORY

SecNumCloud
Who is it?

Services Under Review for Qualification

	IN PROGRESS		QUALIFIED	
	Applicants	**Offering**	**Provider**	**Offering**
IaaS	**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 is also undergoing qualification, but no public information is available on the type of qualification requested.

The candidates

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

Scope of the qualification

IN PROGRESS

adista — CaaS, SaaS, PaaS, IaaS

Bleu — CaaS, SaaS, PaaS, IaaS

blue. — CaaS, SaaS, PaaS, IaaS

CYLLENE — CaaS, SaaS, PaaS, IaaS

ecritel — CaaS, SaaS, PaaS, IaaS

free PRO — Données non publiques

ITS Integra — CaaS, SaaS, PaaS, IaaS

NetExplorer — CaaS, SaaS, PaaS, IaaS

NUMIH France — CaaS, SaaS, PaaS, IaaS

NumSpot — CaaS, SaaS, PaaS, IaaS

orange Business — CaaS, SaaS, PaaS, IaaS

OVH — CaaS, SaaS, PaaS, IaaS

Scaleway — CaaS, SaaS, PaaS, IaaS

Tenexa — CaaS, SaaS, PaaS, IaaS

WIMI — CaaS, SaaS, PaaS, IaaS

QUALIFIED PROVIDERS

OUTSCALE — CaaS, SaaS, PaaS, IaaS

cegedim — CaaS, SaaS, PaaS, IaaS

CLOUD TEMPLE — CaaS, SaaS, PaaS, IaaS

INDEX ÉDUCATION — CaaS, SaaS, PaaS, IaaS

odrive — CaaS, SaaS, PaaS, IaaS

orange Business — CaaS, SaaS, PaaS, IaaS

OVH — CaaS, SaaS, PaaS, IaaS

S3NS — CaaS, SaaS, PaaS, IaaS

Whaller — CaaS, SaaS, PaaS, IaaS

WORLDLINE — CaaS, SaaS, PaaS, IaaS

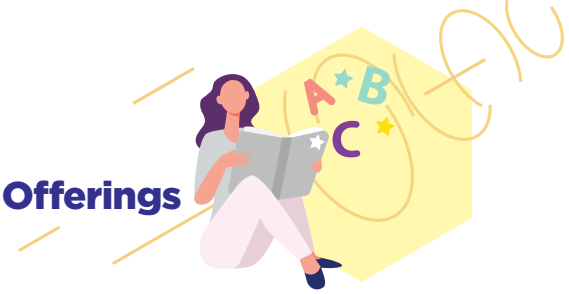
Status of candidates

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

J0 — ITS Integra, Tenexa

J1 — Bleu, ecritel, NetExplorer, NumSpot, Scaleway, S3NS

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 swithin 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*

APRIL 2026
EDITION