SNC Cloud Platform

All the potential of the public cloud secured to the highest level

SecNumCloud

For a cloud service with top-tier security

The **SecNumCloud** qualification is based on thorough assessment of cloud providers.Nearly **1,200 requirements** are reviewed by an independent evaluator under the authority of ANSSI.

They cover the entire cloud value chain, from **infrastructure to governance, including operations, security, and organisation.**

The objective is clear:

To enable the hosting of **sensitive applications**, without critical dependency or legal risk.

SecNumCloud primarily focuses on:

- protection against extraterritorial access to data;
- autonomy in the use of technologies;
- the location of infrastructures and operations within the EU;
- strong isolation and advanced cybersecurity defences.

Permettre l'hébergement d'usages sensibles, sans dépendance critique ni exposition juridique.

Cloud security: a principle of proportional uses

Robust security is not always necessary or automatically required. It ultimately comes down to the **scenario, issues**, and perceived level of risk. For some organisations, SecNumCloud is a logical option. For others, it is **strategic**.

Your scenario as a starting point

Often, this decision is guided by the regulatory landscape, e.g., implementing the NIS2 directive, cloud-first approach, military programming laws, etc. If you are a government body, a key player, or more broadly an **organisation subject to these regulations, robust security is not optional.**

It is an operational necessity, or even a core building block for achieving higher levels of confidentiality, for instance, through controlled distribution.

A market-driven requirement

Beyond the regulatory framework, the market itself raises its standards.Software publishers, SaaS platforms, and service providers are now required **to demonstrate their ability to protect the sensitive data entrusted to them** by both public and private clients.
Here, security becomes much more than a technical prerequisite. It serves as **a mark of credibility, a means of standing out, or** even a strong selling point.

Protecting what matters most

Some things are non-negotiable: your business continuity; the protection of your critical data; the confidentiality of your industrial, scientific, or strategic secrets.
In such scenarios, the question is no longer just «*Do I need SecNumCloud?*», but rather «*Can I realistically afford to ignore it?*»

PROBALILITY 1 > 5	IMPACT 1 > 16	PI SCORES	1 > 80	COUNT
1- RARE	1- INSIGNICANT	1- 2	NEGLIGIBLE	0
2 - UNLIKELY	2 - MINOR	3 - 8	MINOR	7
3 - POSSIBLE	4 - MODERATE	10 - 16	MODERATE	4
4 - LIKELY	8 - MAJOR	20 - 32	HIGH	1
5 - ALMOST CERTAIN	16 - SEVERE	40 - 80	CRITICAL	2

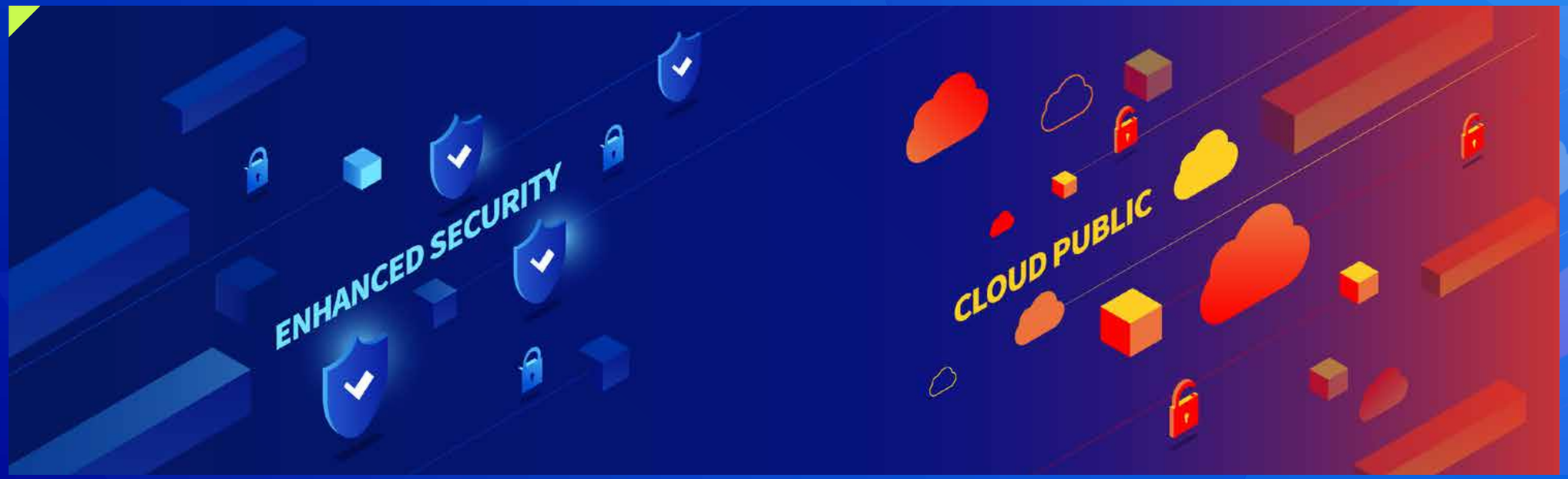
The maturity of high-security solutions

For a long time, highly demanding security environments have **evolved on the fringes of the rest of IT**. Although primarily designed to protect, these systems significantly restricted usage and limited teams' agility.

In parallel, public cloud transformed IT through **automation, on-demand services**, and **new development modes**.

These two trends, once at odds, are now **converging**.

With security standards becoming more **structured**, requirements **more clearly defined**, and cloud platforms **maturing**, organisations can achieve a better balance between risk and benefit.



The age of informed choice

Successfully managing digital risks is now a **strategic issue** for organisations.

Due to new regulations, increasing cyber threats, and past experiences, cloud adoption strategies are **becoming more structured and deliberate**.

There is no one-size-fits-all solution.

Every organisation faces its unique realities, whether in terms of data type, service criticality, compliance requirements, team expertise, or technological setups.

Opportunity alone is no longer the deciding factor when choosing cloud solutions.

They are **developed** by separating what can be standardised from what needs closer management.

Within this scenario, decisions are best made through a structured, deliberate approach guided by a proven framework.

- Identifying the risks.
- Understanding the limitations.
- Measuring the impacts.
- Deciding based on current priorities.

Strategic autonomy then becomes a key factor among many in this decision-making process. Not as an end, but as **a lever to ensure freedom of action.**

The SNC Cloud Platform approach

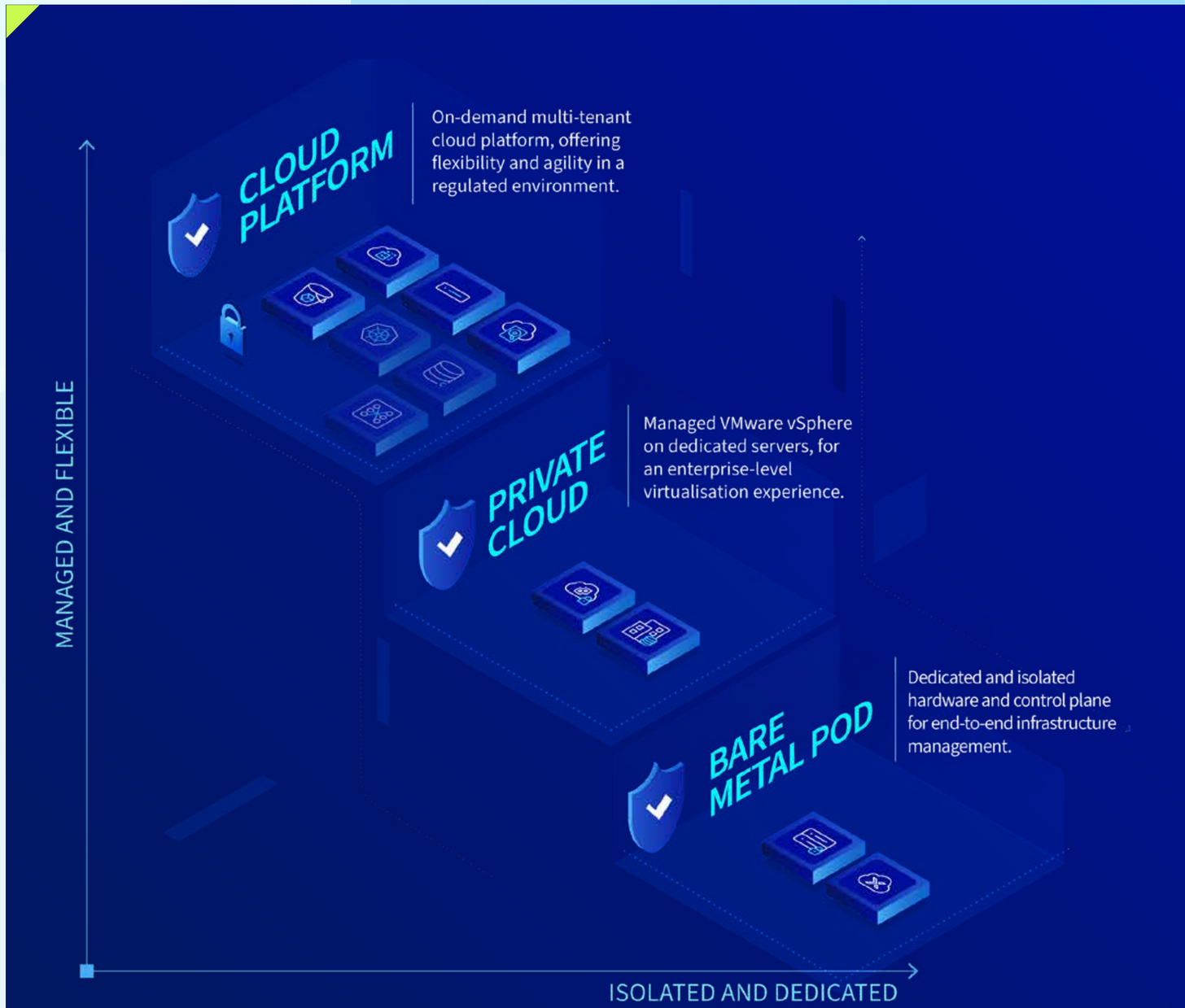
OVHcloud was among the first providers to have its cloud services qualified to the SecNumCloud standard. Having qualified its Private Cloud environment, OVHcloud took the next step of qualifying Bare Metal Pod, its infrastructure base.

This is the base upon which **SNC Cloud Platform** was built.

This managed services platform provides access to **public cloud benefits** (on-demand, flexible, scalable, and industrialised services), all within a highly secure environment.

SNC Cloud Platform is built around three structural pillars:

- **security as a core component**
- **next-generation services**
- **a carefully orchestrated solution**



SNC Cloud Platform

Ensuring a highly secure cloud

Security as a core component
By their very design, flexible and scalable cloud services rely on resource pooling. Despite this being a fundamental cloud principle, it remains **a major concern when hosting sensitive applications**, particularly those handling your critical data and services.

As a result, environments are rigidly isolated, with advanced segmentation and a lack of implicit trust between clients, services, and workloads, to maintain the integrity and confidentiality of your environments.

Built-in security at all levels

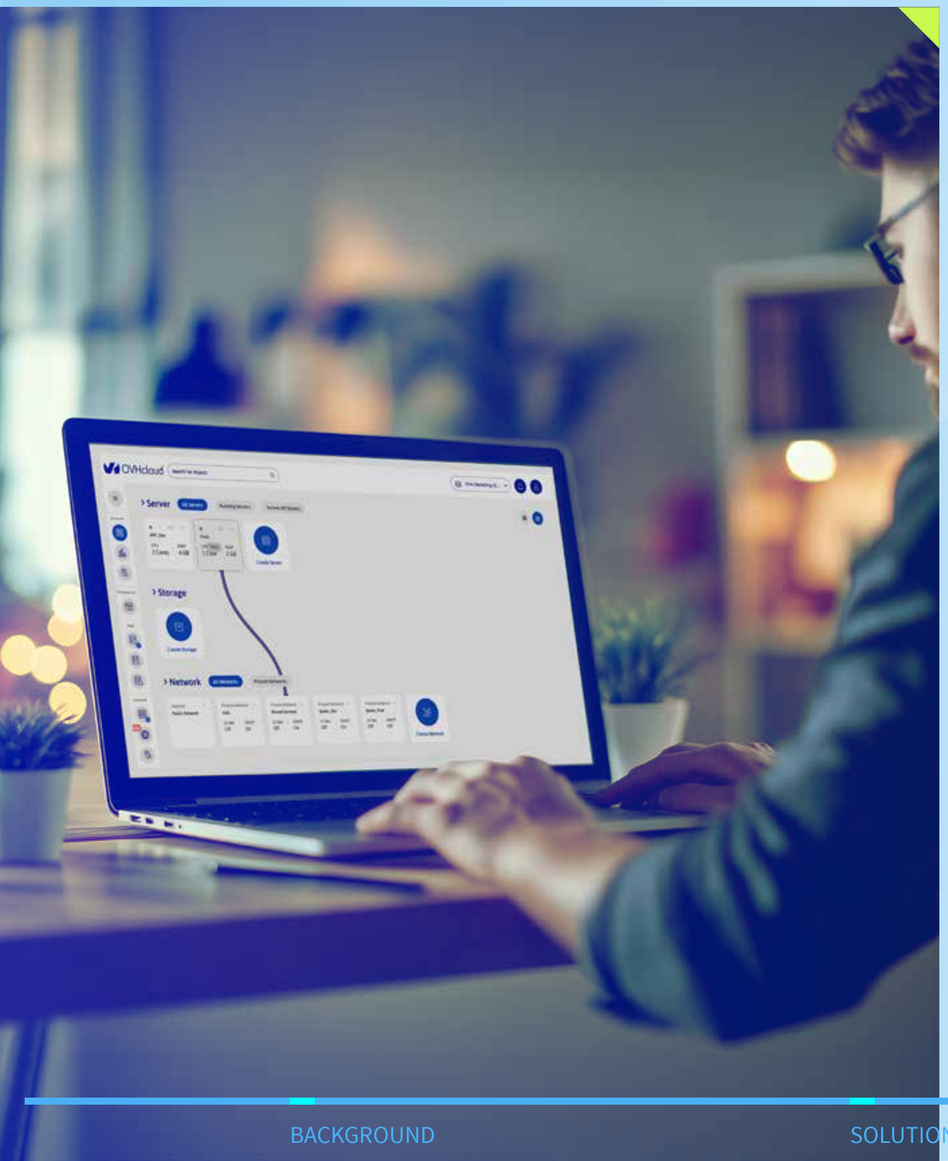
Comprehensive and integrated security
Multi-layer controls cover the infrastructure, network, and operations to limit risks and reduce attack surfaces – without limiting your uses.

Strict isolation of environments
Workloads run in a strictly isolated execution environment, with robust containment mechanisms ensuring no uncontrolled interaction between workloads.

Fortified infrastructure
Attack vectors are minimised through hardened systems, isolated execution layers, and protected critical components.

Continuous compliance and monitoring
The platform's integrated permanent controls, logging, and monitoring enable rapid incident detection and timely response, ensuring your operations continue uninterrupted.

This comprehensive, integrated, and controlled approach to security is why **SNC Cloud Platform** seamlessly aligns with a **SecNumCloud qualification process**, meeting the framework's requirement across the entire value chain.



SNC Cloud Platform

Next-generation services

The hurdle for both IT and product teams is integrating advanced cloud capabilities seamlessly, without added complexity and disruption to existing uses.

Designed for security, **SNC Cloud Platform** delivers an experience that closely mirrors that of the public cloud.Services are available whenever you need them, environments can scale rapidly, and access to resources is standardised and industrialised.

The platform provides **next-generation cloud services**, tailored to meet the current needs of organisations, whether for hosting critical applications, processing data, or supporting innovative projects.

Built on modern, proven cloud standards, these services harness cloud-native approaches, automation, and containerised solutions. They also rely on data-ready environments and AI, without unnecessary complexity.
As technology advances and the platform's capabilities expand, the services services evolve accordingly.

The backbone of cloud services

- Management
- Computing
- Storage
- Connectivity

An expanding service catalogue

- Containers
- Managed MySQL databases
- Artificial intelligence
- Advanced network services

SNC Cloud Platform

A carefully orchestrated solution

Control is not limited to security, it also means having **real control over the technologies used and clear visibility into costs**.

As mentioned earlier, **SNC Cloud Platform** is based on technologies fully designed, built, and operated **by OVHcloud, from server assembly to the integration of open-source components and software development.**

It limits dependence on critical third-party technologies and forms the bedrock for lasting **strategic autonomy**.

The platform is evolving along a controlled trajectory, **independent of external roadmaps**. With this, you gain autonomy, reversibility, and operational control.

Economic control goes hand-in-hand with this **technological oversight**. With SNC Cloud Platform's end-to-end value chain control, you benefit from secure cloud services at very **competitive and predictable** prices.

Costs can be controlled through infrastructure industrialisation and operational optimisation, while **ensuring that security and service quality are not compromised.**

SNC Cloud Platform

Strengths and opportunities

SNC Cloud Platform is aimed at organisations seeking to balance **robust security**, technological control, and **cloud usage agility**.

It is a pragmatic approach based on well-thought-out choices and a deep understanding of regulatory, operational, and economic challenges.

The platform's strengths

- a highly secure cloud designed for sensitive uses
- end-to-end controlled technologies
- a modern cloud experience, without disruption to your existing uses
- controlled costs through complete value chain oversight

Proven approach

- capitalising on OVHcloud's expertise from its SecNumCloud-qualified services
- a tightly controlled service scope that ensures consistency and security
- the gradual scaling of advanced cloud services, aligned with the platform and your needs

Potential applications

- hosting sensitive workloads in a trusted cloud setup
- complying with stricter regulations and standards
- making security a market differentiator
- introducing new digital uses without compromising risk management

Key benefits

- technological and operational independence
- control over data and its uses
- cost predictability and control
- access to next-gen cloud technologies
- environment flexibility and scalability

What is SNC Cloud platform used for?

Cloud solutions adapted for the most critical uses

SNC Cloud Platform is designed for scenarios where standard public cloud services fall short.

It enables the management of sensitive or critical environments that require robust security, strict regulatory compliance, and modern cloud technologies.

You can use the platform to migrate your current setups to the cloud without losing oversight, and adopt cloud-native approaches within a controlled environment. It also supports the launch and scaling of new digital services while maintaining compliance.

Sectors where it is most applicable

Local authorities

- Digital public services
- Critical business platforms
- Infrastructure pooling

Industry and energy

- Industrial and business applications
- Production data
- Critical environments
- Command and control (C2)

Health and public sectors

- Sensitive and regulated data
- Critical applications
- Service continuity

Software publishing (ISV)

- SaaS applications
- Secure cloud environments
- Data and cost control
- Scientific computing

Financial services and billing

- Paperless billing
- Sensitive financial data
- Highly available environments

Use case #01

Hosting public services and sensitive data

Public bodies are responsible for ensuring the continuity of essential services, protecting sensitive data, and complying with strict laws and regulations.

In parallel, they aim to **modernise** their information systems, **achieve greater agility**, and **streamline** their infrastructures, all without giving up control or creating critical dependency.

SNC Cloud Platform features

- Highly secure cloud hosting for digital public services
- Support for critical business platforms (finance, HR, civil registration, GIS).
- Shared infrastructure across entities or regions, with strong isolation and control.

Key benefits

- Compliance with security, sovereignty, and data residency requirements.
- Service continuity for essential public uses.
- Gradual modernisation of information systems without disruption or legal risk.

SNC Cloud Platform

Public bodies can rely on SNC Cloud Platform for **trusted managed cloud services** that meet high regulatory requirements, ensure operational security, and support phased IT modernisation.

This pragmatic strategy is designed to fit the public sector environment and its most critical use cases.

Use case #02

Securing industrial and R&D environments

Companies in the industrial sector manage highly strategic data, including production data, research results, engineering models, and information about their operational processes.
In today's highly digital and networked landscape, protecting this data is **critical to a company's competitive edge, sovereignty, and business continuity.**

SNC Cloud Platform features

- Highly secure cloud hosting for sensitive industrial and business applications.
- Storage and processing of production and R&D data.
- Isolated cloud environments for engineering, research, and innovation projects.

Key benefits

- Enhanced protection for industrial secrets and expertise, without dependence on critical technologies.
- Full control for the most sensitive project environments.
- Flexible cloud usage without critical technological or legal dependency.

SNC Cloud Platform

Industrial sector companies can use SNC Cloud Platform for **secure, managed cloud services**, tailored to protect strategic data and drive innovation projects, while ensuring long-term strategic autonomy.

Use case #03

Securing digital environments for the energy and nuclear industries

Energy sector companies, with a specific focus on nuclear power, utilise crucial information systems. These systems handle operational and safety data, inputs from control systems, simulations, scientific models, and production infrastructure sensors.

Ensuing the security of these digital environments is crucial for safety, uninterrupted services, and national sovereignty. This is all in light of the elevated risks of cyberattacks, strict regulatory requirements, and the need for high resilience.

SNC Cloud Platform features

- Highly secure and sovereign cloud hosting for critical energy applications.
- Storage and processing of sensitive industrial and safety data within a controlled, auditable framework.
- Isolated cloud environments for simulation, R&D, and innovation projects.
- Update of existing systems with no impact on business continuity or safety requirements.

Key benefits

- Strategic and safety data protection, free from critical technological or legal dependency risks.
- Management and control for highly sensitive environments, compliant with critical infrastructure operator standards.
- Service continuity and enhanced resilience for key energy production systems.
- Innovation security, in line with stringent regulatory and sovereign requirements.

SNC Cloud Platform

SNC Cloud Platform offers energy companies a **secure, autonomous cloud base**, built to safeguard critical systems, ensure uninterrupted operations, and foster innovation – without compromising safety or control.

Use case #04

Deploy sovereign SaaS solutions

To meet their clients' growing demand for data protection, data residency, and sovereignty, software publishers must deliver SaaS solutions that are reliable, secure, and compliant.

They also need to **effectively manage** infrastructure **costs** and **maintain an adaptable architecture** to support new service launches.

SNC Cloud Platform features

- Highly secure cloud hosting for cloud-based SaaS applications.
- Control over data, its location and operating conditions.
- SecNumCloud-qualified industrial cloud foundation (open and controlled), with no critical dependency on third-party providers.

Key benefits

- Stronger credibility with public and private clients with high expectations.
- Differentiation through security and strategic autonomy.
- A controlled, predictable and sustainable operating model, compatible with a long-term SaaS trajectory.

SNC Cloud Platform

SNC Cloud Platform enables publishers to build **secure, sovereign, and controlled SaaS solutions**, based on a cloud foundation designed for sensitive use cases. All this without compromising the ability to freely and flexibly choose their technology.

Use case #05

Hosting e-invoicing and financial platforms

Billing platforms, financial processing, or sensitive flow management operate in highly regulated environments.

They are required to ensure robust security, consistent availability, and clear traceability, while keeping pace **with ever-changing regulations and standards**.

SNC Cloud Platform features

- Hosting for e-invoicing and sensitive financial applications.
- Storage and processing of financial data in a highly secure cloud environment.
- Robust infrastructure designed for critical uses and controlled operations.

Key benefits

- Reduced operational, legal, and compliance risks.
- Service continuity for critical financial processing.
- Secure cloud environments designed to meet high security, sovereignty, and governance requirements.

SNC Cloud Platform

SNC Cloud Platform delivers a **managed, secure, and controlled cloud foundation, perfect for mission-critical** financial systems. It enables financial organisations to meet regulatory requirements, maintain operational resilience, and gain greater control over their operations.

SNC Cloud Plateform

A one-size-fits-all approach cannot be effective when the stakes are high.

A unique strategy is required for each scenario, constraint, or application.

It is by aligning business needs with cloud capabilities that the most relevant paths forward take shape.

Explore, build, and adapt!
There is no shortage of use cases.
Together, we can figure out what really works for your environments.

ovhcloud.com