S3NS

Powered by THALES x Google Cloud

Who are you meeting with today ?

Blaise Vignon

Chief Product Officer, GTM

S3NS

Current trends reinforce the need for digital sovereignty

Geopolitical tensions

Extraterritoriality of international laws

Increasing regulation (esp. in Europe) & emergence of European preference

Increasing importance of digital, notably with AI

Acceleration of innovation

Increase in cyberattacks

Fundamentals of a unique partnership

THALES Google Cloud

Bilateral coherence, Strategic engagement, Technological ambition

Getting the most out of sensitive data,

increasing performance and transformation capacity

Reduce development and operating costs

within a framework of increased security requirements

Increase hybridization capabilities

with the required level of control

Protecting data & its sovereignty

in the Cloud and contributing to a future of trust

Concerns about sensitive data are holding organisations back

01 Uncertainty arising from shifting laws and global geopolitical dynamics

02 Achieving compliance, a resource-intensive yet non-negotiable requirement

03 Desire for greater control over data, operations and infrastructure

S3NS

SecNumCloud: a multilayered framework against foreign interference

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION • ANSSI •

We navigated the intricacies of the SecNumCloud qualification

S3NS

276

Requirements divided into 15 chapters

3

Main **categories** : Operations, Technology, Legal

- Information security, risk management
- Organization information security
- HR security
- Assets management
- Access control, identity management
- Cryptology
- Physical, environmental security
- Operational security
- Network security
- Acquisition, dev, maintenance
- Third-party relationship
- Security incident management
- Business continuity
- Compliance
- Protection against extraterritorial laws

ANSSI developed recommendations for Cloud hosting

- ✓ **Sensitive IS relevant to the “Cloud au Centre” doctrine of the French Government** only authorized in SecNumCloud qualified Clouds
- ✓ Recommended for **Vital Importance Operator** (OIV) and **Essential Services Operator** (OSE) **sensitive IS**
- ✓ Possible to host a **Vital Importance IS** (SIIV) subject to a reasoned risk analysis
- ✓ Possible to host a **Restricted Diffusion IS** (SIDR), by demonstrating that the solution is protected at the appropriate level

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

RECOMMANDATIONS POUR L’HÉBERGEMENT DANS LE CLOUD DES SYSTÈMES D’INFORMATION SENSIBLES

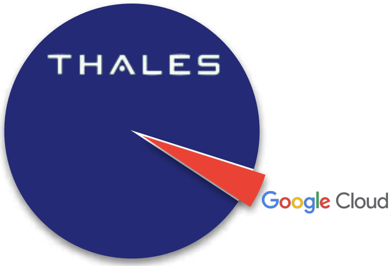
July 9th 2024

French company fully controlled by Thales

2 pillars for independence from extraterritorial laws

Shareholding

Thales is a **very large majority shareholder**

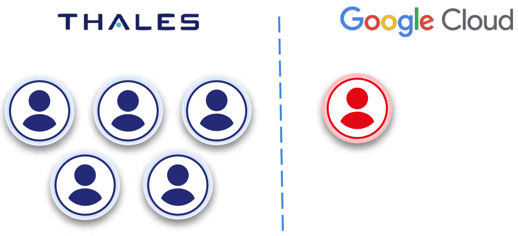


Governance

S3NS is **fully controlled by Thales**

THALES
S3NS

Google Cloud has an observer seat on the **BofD***, **without voting rights**

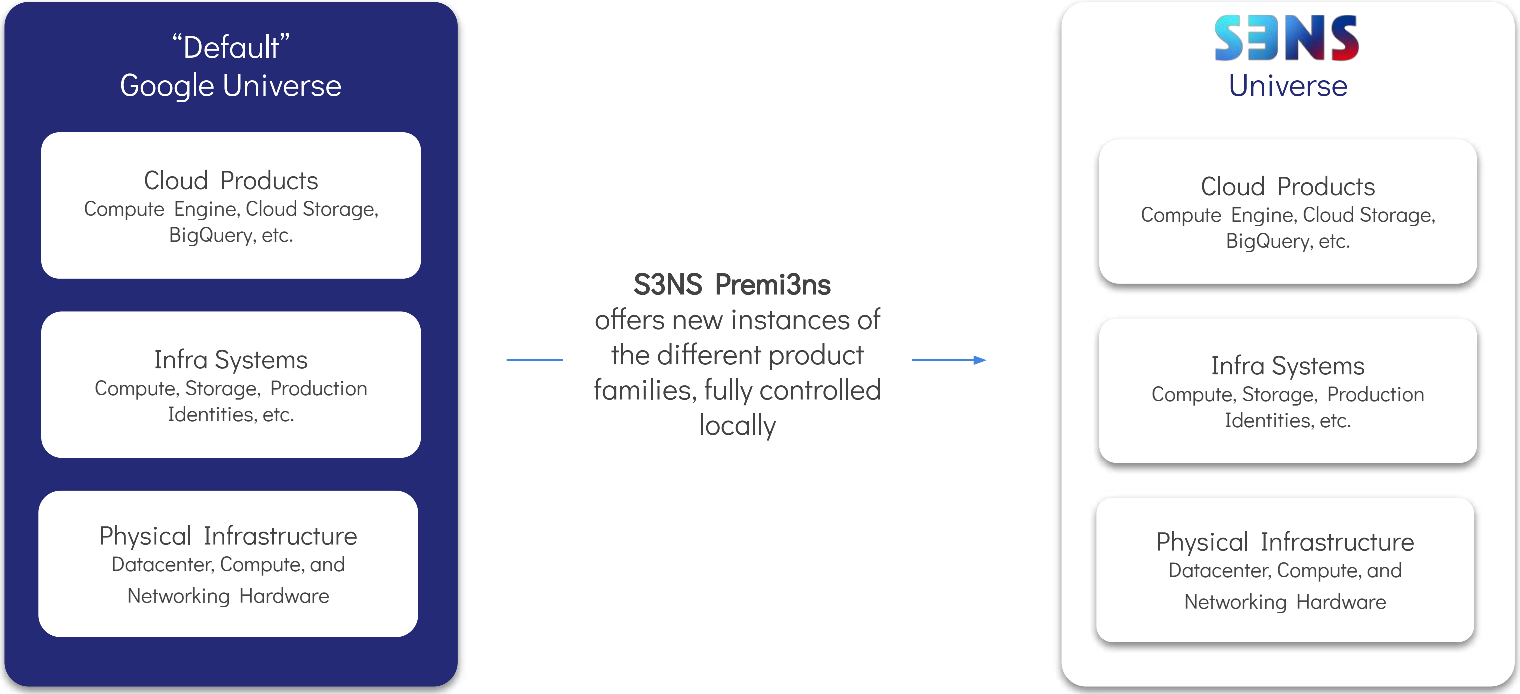


Google has no control over S3NS operations

Security
Marketing
Operations
Datacenter

* BofD : Board of Directors

We replicate the Google Cloud experience



“Default”
Google Universe

Cloud Products
Compute Engine, Cloud Storage, BigQuery, etc.

Infra Systems
Compute, Storage, Production Identities, etc.

Physical Infrastructure
Datacenter, Compute, and Networking Hardware

S3NS Premi3ns
offers new instances of the different product families, fully controlled locally

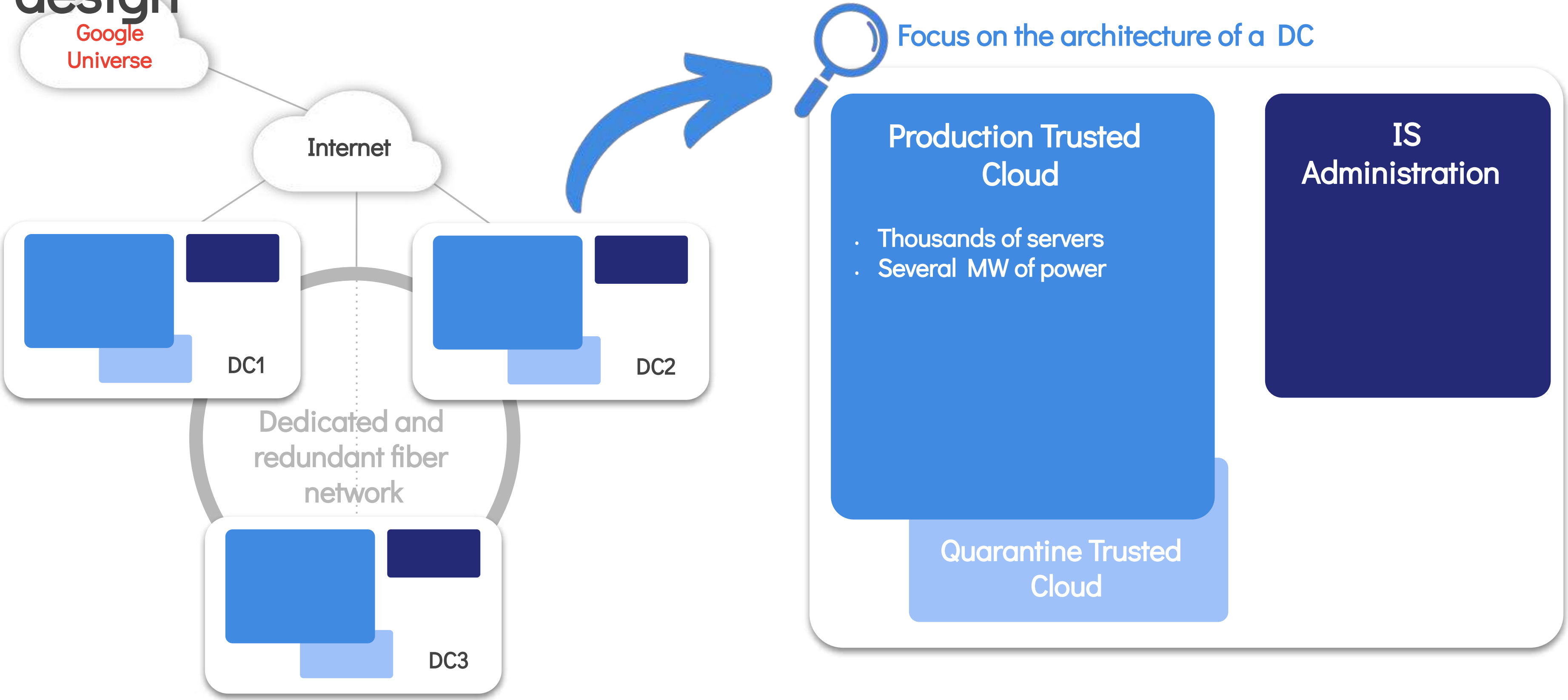
S3NS
Universe

Cloud Products
Compute Engine, Cloud Storage, BigQuery, etc.

Infra Systems
Compute, Storage, Production Identities, etc.

Physical Infrastructure
Datacenter, Compute, and Networking Hardware

Our physical infrastructure is resilient and secure by design



Google Universe

Internet

DC1

DC2

DC3

Dedicated and redundant fiber network

Focus on the architecture of a DC

Production Trusted Cloud

- Thousands of servers
- Several MW of power

IS Administration

Quarantine Trusted Cloud

Separation of Duties and Protection Against Potential Internal Malice

Key Strategies for Mitigation:

Differentiate Teams: Separate teams for setting security rules, operating the systems, and verifying compliance (SOC).

Separate Admin Perimeters: Divide administration perimeters by technical scope. Enhance Admin Activity Monitoring.

Prevent Unilateral Sensitive Actions by a single admin

Prevent Admin Access to Customer Data

Admin Activity Monitoring Requirements:

Connection Chain: No single team manages the entire connection chain (admin workstation, VPN, IDP, remote attestation, bastions, target systems). An abnormal action must be identifiable on at least 2 links.

Log Management: No single team can disable or delete logs. S3NS uses 2 SIEMs (1 internal, 1 external PDIS qualified by ANSSI). Disabling a log source must generate an alert.

Multi-Party Approval (MPA) in GCP for SREs

Supply Chain Security at S3NS

Two S3NS Perimeters

1. Admin IS (Information System - Mostly Open Source):

Automated security checks with Scorecard (vulnerabilities, maintenance, Branch Protection, SAST, code review, signed releases, etc.).

2. Cloud Infrastructure (GCP Technology):

Use of a Quarantine Cloud Region for updates provided by Google.

Cloud Update Analysis Process

- The update is first installed in quarantine where S3NS performs:
  - A system and network behavior analysis (simulated representative client deployments)
  - An automatic binary analysis (searches for prohibited characteristics, e.g., obfuscated code).
  - A manual binary analysis (on samples).
- When all controls are successful, S3NS authorizes its deployment in client production.

Source code Transparency & Inspection

S3NS operates its own Cloud infrastructure, powered by GCP technology

As a key security measure, Google shares the GCP source code with S3NS, representing a unique and major transparency effort from a private player.

3 axes of Source Code Analysis:

- **Security Function Verification:**
  - Check the correct implementation of security-critical functions (virtualization, sandboxing, encryption, network filtering).
- **Automated Software Inspectability:**
  - Goal: Source code access enables S3NS to create faster and more accurate automated analysis tools.
- **Anomaly Investigation:**
  - Use Case: If automated analysis identifies a potentially abnormal behavior, the source code is a crucial investigation tool for efficient doubt resolution.

We are ready to serve enterprises and the public sector

01. **The Trusted Cloud** represents a **significant market opportunity**, in both **France** and **Europe**

02. **S3NS** is the **first European hyperscaler**, leveraging both **Google Cloud technology** and **Thales' expertise**

03. **S3NS is spearheading this effort**:
    - The **broadest service portfolio** among **all SecNumCloud** qualified (or soon-to-be qualified) offers
    - **SecNumCloud qualified the 17th December 2025 and GA since mid-October**

Third-Party Support Management

- S3NS performs all operations.

- Support from Google Cloud to S3NS is strictly managed in two ways:
  - **Upstream Metric Filtering** : S3NS defines ultra-granular filtering policies for shared metrics. This ensures no client data is exposed, only information strictly necessary for infrastructure health and function.
  - **During an Intervention** (Read-Only Access):

    A bastion allows an S3NS Site Reliability Engineer (SRE) to share only a read-only view with the Google SRE.

    The Google SRE can guide, but has no action capability.

    Only technical information regarding the infrastructure's Control Plane is shared.

    Crucially, S3NS SREs also do not have access to client data, which is the best way to ensure it cannot be leaked to a third party, including Google.

Premi3ns by S3NS calendar

● Physical installation ● Software Dev. ● Training ● *Handoff*

Q1 2025	Q2 2025	Q3 2025	Q4 2025	Q1 2026	Q2 2026
Google Cloud services availability (wave 1) SRE training completed Handoff process begins	Infrastructure compliant with SNC requirements				Google Cloud services availability (wave 2)
Early Adoption Program					
Milestone 1 ✓ December 2024			General Availability 15th October SecNumCloud Qualification	ISO 27001 & HDS	
PASSI audits		Representative operations			

THALES GROUP LIMITED DISTRIBUTION

Do not share - Communicate under NDA

What services are on PREMI3NS

Compute

- Compute Engine
- Cloud GPUs

Storage

- Cloud Storage

Data Analytics

- BigQuery Edition Enterprise
- Pub/Sub

Operations

- Cloud Monitoring
- Cloud Logging

Networking

- Cloud DNS
- Cloud Interconnect
- Cloud Load Balancing
- Cloud NAT
- Private Service Connect
- Cloud Router
- Virtual Private Cloud
- Cloud VPN
- Cloud Armor
- Premium Network Tier
- Cloud Firewall Rules
- Service Directory

Available Services

Management Tools

- Cloud SDK
- Cloud IAM

Security

- Cloud Resource Manager
- Key Management Service

Containers

- GKE Autopilot
- Artifact Registry

Databases

- Cloud SQL Enterprise Plus

Products unavailable pending release and certification

Security

- Secret Manager
- Admin Access Transparency
- Identity Aware Proxy

Storage

- Storage Transfer Service
- Filestore

Operations

- Cloud Asset Inventory

Compute

- Confidential VMs

Containers

- Cloud Run
- Cloud Build

Databases

- Cloud Spanner
- Cloud Bigtable

Data Analytics

- Dataproc
- Cloud Composer

Networking

- Partner Interconnect