



**RÉPUBLIQUE
FRANÇAISE**

*Liberté
Égalité
Fraternité*

TLP:GREEN



CLOUD SECURITY OVERVIEW

ANSSI - FRENCH CYBERSECURITY AGENCY

SEPTEMBER 2026

ANSSI



Agence nationale de la sécurité des systèmes d'information (French Cybersecurity Agency) created in 2009



National authority for cyber security and cyber defence



Government organisation that reports to the General Secretariat for Defence and National Security (SGDSN)



Defensive mission (not offensive)

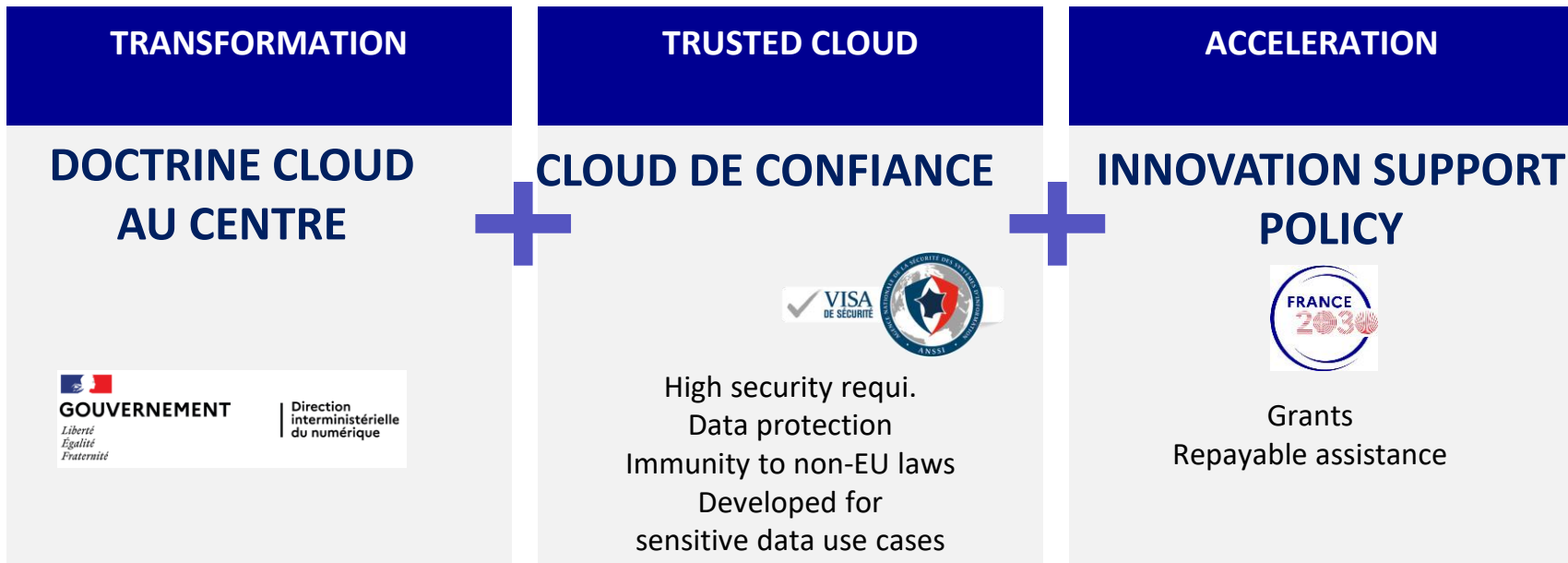


Role: to protect the nation from cyber attacks



Primary targets: Operators of critical national infrastructures ("OIV"), operators of essential services ("OES") and administrations

The 3 pillars of national cloud strategy

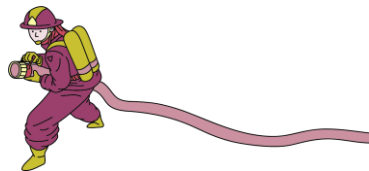


CERT-FR - French Computer Emergency Response Team

- CERT-FR is the national government agency responsible for the operational implementation of the function of defending digital systems of national interest, a role assigned to ANSSI.

  PUBLICATIONS • SERVICES • RÉSEAU DE CERT • RECHU LIAISON • À PHOTOS • ALERTES			
ALERTES DE SÉCURITÉ <i>Les alertes de sécurité sont des documents destinés à prévenir d'un danger immédiat</i>			
31 mars 2026	C2-H11H-2026-ALE-004	Vulnérabilité dans FS BIG IP Access Policy Manager	Alerte en cours
20 mars 2026	CERTFR 2026 ALE 003	Note d'alerte - Châssés des messages instantanés	Alerte en cours
30 janvier 2026	CERTFR 2026 ALE 001	[Mis.] Multiples vulnérabilités dans l'outil Fingerprint Manager Mobile	Alerte en cours
25 février 2026	C2-H11H-2026-ALE-002	[Mis.] Vulnérabilité dans Cisco Catalyst SD-WAN	Clôturée le 26/02/26
05 décembre 2025	C2-H11H-2025-ALE-014	[Mis.] Vulnérabilité dans Raccor Server Components	Clôturée le 12/02/26
VOIR TOUTES LES ALERTES >>			

- It primarily responds to incidents occurring within government ministries and agencies, operators of critical infrastructure, and providers of essential services, but may be called upon to take action throughout the entire country.
- Anssi assumes a cyber firefighter role.

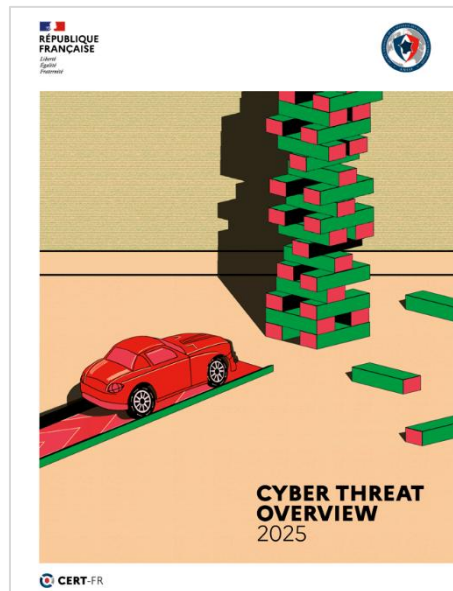


Cyber Threat Overview 2025

ANSSI published each year a cyber threat overview.

On the 2025 report, ANSSI notes that the level of cyber threat remains high, spares no one, and is the work of attackers who are becoming increasingly difficult to track. The boundaries between state actors and cybercriminals are blurring. ANSSI provided a focus on the compromise of cloud environments*.

ANSSI also published a cloud computing threat status**.



As a result of the growing use of cloud services amongst many organisations, cases of compromise affecting the data hosted within these environments are regularly observed. Several cases of ransomware attacks involving the encryption of data hosted on cloud resources were notably reported to ANSSI in 2025, which suggests that numerous malicious actors are conscious of this development. The generalisation of cloud-hosted solutions represents an opportunity for these actors to acquire the data of several different entities by compromising a single service provider. In October of 2025, ANSSI was informed of a ransomware attack which resulted in the encryption of resources linked to a French vendor's Software-as-a-Service solution which had been hosted on an Amazon Web Services cloud environment.

* <https://cyber.gouv.fr/en/publications/cyber-threat-overviews/cyber-threat-overview-2025/> (see page 50)

** <https://www.cert.ssi.gouv.fr/cti/CERTFR-2025-CTI-001/>

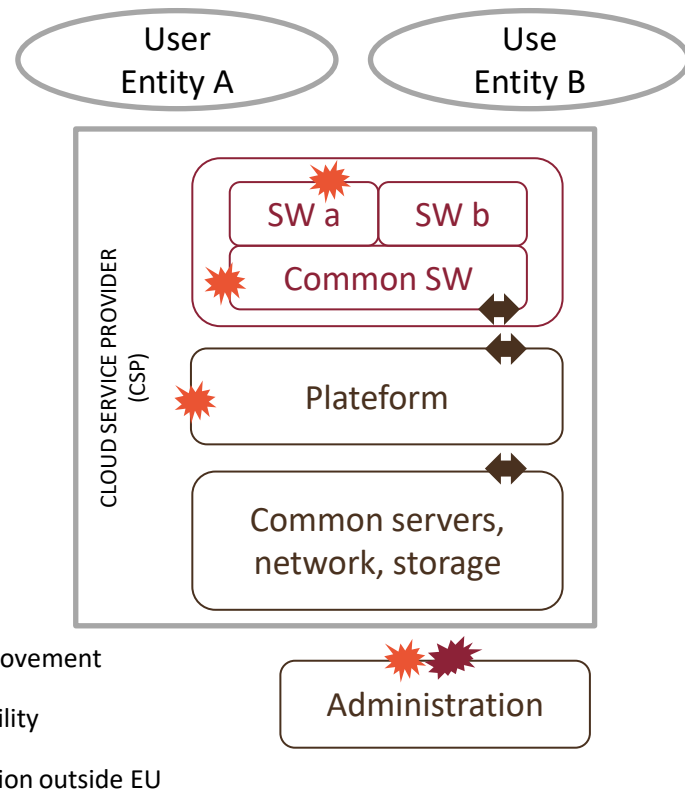
Risks

TECHNICAL RISKS AT EACH STACK LAYER

RISKS ASSOCIATED WITH OUTSOURCING AND POOLING RESOURCES

LEGAL RISKS

- Customers data under non EU regulations
- Kill switch
- Localization outside EU



ANSSI certifies and qualifies

- Cybersecurity solutions are many and varied, but not all of them offer the same level of effectiveness, robustness and trust. The security visas issued by ANSSI make it easy to identify the most reliable of them, recognised as such following an assessment carried out by approved laboratories using a rigorous and proven methodology.
- Security certification and qualification are the two processes that enable ANSSI to assess products and services. The choice of one or the other depends on the customer needs of the company wishing to have its offer evaluated. They respond to different needs and objectives.



SecNumCloud Qualification

- Security qualification delivered by ANSSI for cloud service provider's solution occurred after a deep analysis.
 - A 3-year visa.
 - A set of technical, operational and legal requirements.
 - Solution which aim to protect the hosting and processing sensitive data.
 - All SecNumCloud qualified offers provide an equivalent level of security.
 - Anssi provides guidelines for entities which may be considering a switch to cloud solutions for their restricted information systems.
-

SecNumCloud Themes

- Access control and identity management (chap. 09)
- Cryptology (chap.10)
- Operational Security (chap.12)
- Communications security (chap.13)
- Acquisition, development and maintenance of Information System (chap. 14)
- Relations with stakeholders (chap. 15)

- Management of incidents (chap. 16)
- Business continuity (chap. 17)
- Compliance (chap. 18)
- Additional requirements (chap. 19)

Addressing risks generated by non-EU laws

Datacenters have to be located in an EUMS