La sécurité dans le Cloud Computing

BYOK
SSPM
CWPP
CASB
SecNumCloud
EUCS
CSPM
CDR
BYOE
C5
27017

https://www.securitecloud.com/actualites/webinaire-securite-dans-le-cloud

WEBINAIRE

Jeudi 27 avril 2023 - 17h

Qui suis-je ?

Conférencier

Capgemini

ORSYS formation

+ de 10 000 personnes formées depuis 1995

- **1989** ESIGETEL Ingénieur en Sciences du Numérique
- **1993-2001 : PDG - Fondateur** ExperLAN
  - Directeur Technique
  - SSII spécialisée dans la sécurité IP
  - Société revendue à Thales en octobre 2001
- **2001-2005 : PDG - Fondateur** AXILIANCE
  - Directeur R&D
  - Editeur spécialisé dans la sécurité Web (RealSentry)
  - Société revendue à Beeware en septembre 2005
- **2006-2018 : Directeur associé** SECURIVIEW NEXT GENERATION SOC
  - Supervision sécurité SI
  - Société revendue à Linkbynet (2018) puis Accenture (2020)
- **Depuis 2009 : Président - Fondateur** VERISAFE L'EXPERTISE CYBERSÉCURITÉ
  - Audit, conseil, formation en sécurité SI
- **Depuis 2014 : Expert Judiciaire près la cour d'appel de Montpellier**

C’est quoi la « Sécurité du Cloud » ?

Double approche de Cybersécurité

Trois piliers fondamentaux

La sécurité dans le Cloud

- **Les 5 mythes de la sécurité dans le Cloud**
- **Le chiffrement dans le Cloud à l'état de l'art**
  - BYOK, HYOK et BYOE
- **Les labels de sécurité des fournisseurs**
  - ISO 27001, ISO 27017, SecNumCloud, EUCS
- **L'apport des solutions dédiées**
  - CASB, CWPP, CSPM et SSPM
- **La doctrine française du « Cloud de confiance »**

Nouvelle formation chez VERISAFE

- ✓ **Animée en présentiel ou en distanciel synchrone depuis 2011**

Les 5 mythes de la sécurité dans le Cloud

Mythe n°1

- Une infra IT « on-prem » sera toujours plus sécurisée

Les 5 mythes de la sécurité dans le Cloud

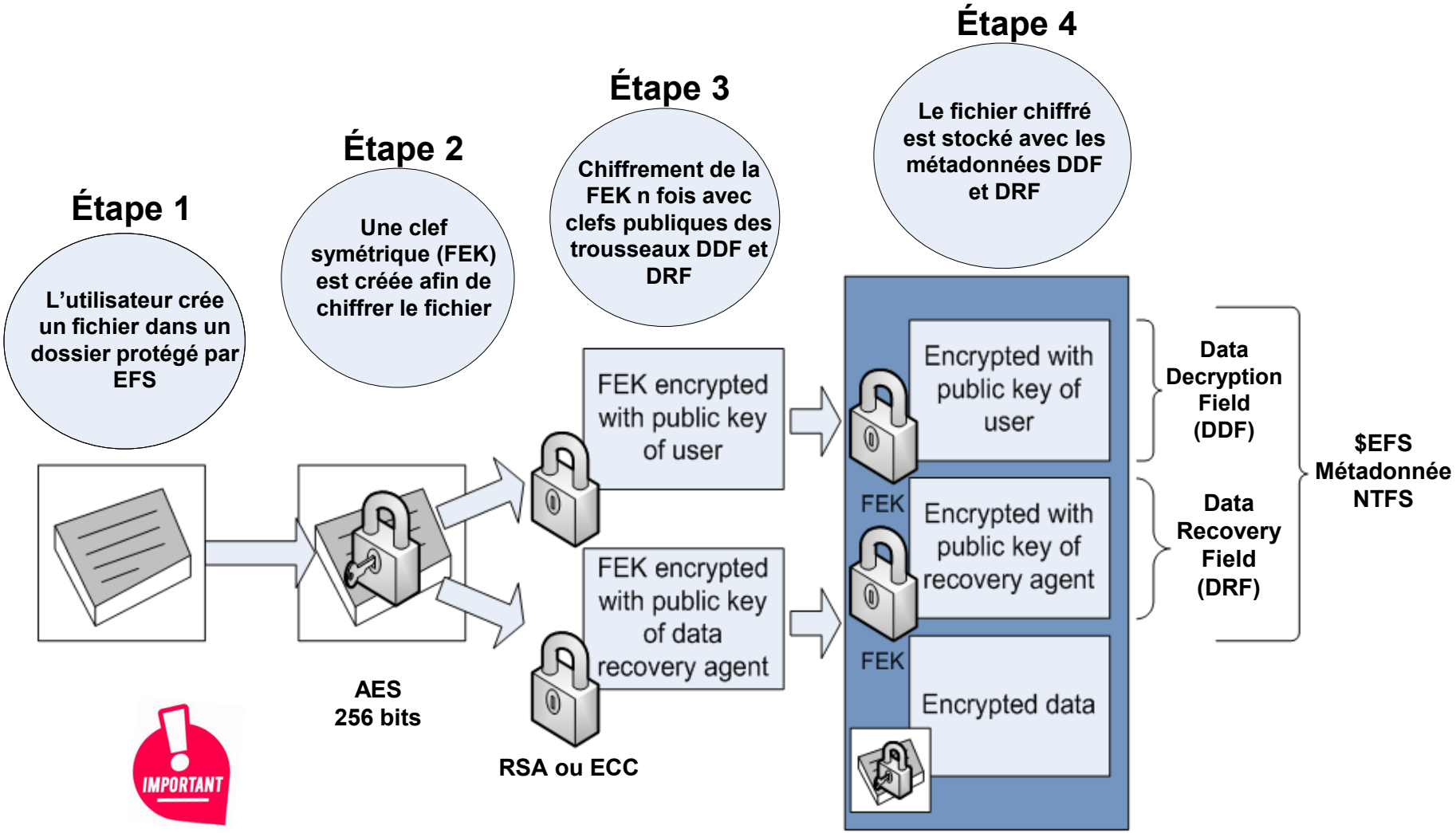
Mythe n°1

- Une infra IT « on-prem » sera toujours plus sécurisée

Mythe n°2

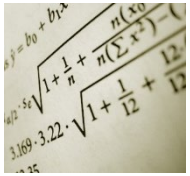
- Il n’y a aucun risque car mes données sont chiffrées

L'importance de la gestion des clés



Comment récupérer ses données en cas de problème ?
→ DRA : Agent de récupération de données
→ KRA : Agent de récupération de clés

La confiance dans le chiffrement



Choisir les bons algorithmes et longueurs de clé

- Bannir les algorithmes fragiles ou vulnérables (RC4, DES, MD5, …)
- Interdire formellement les algorithmes « personnels » ou opaques
- Suivre les recommandations (ANSSI, ENISA, NIST, Keylength.com, …)

Vérifier l'implémentation logicielle

- Faille involontaire de sécurité dans le code ou volontaire (backdoor)
- Certifications ou qualifications (ANSSI, NIST, CC-15408, …)

Surveiller l'installation & l'administration

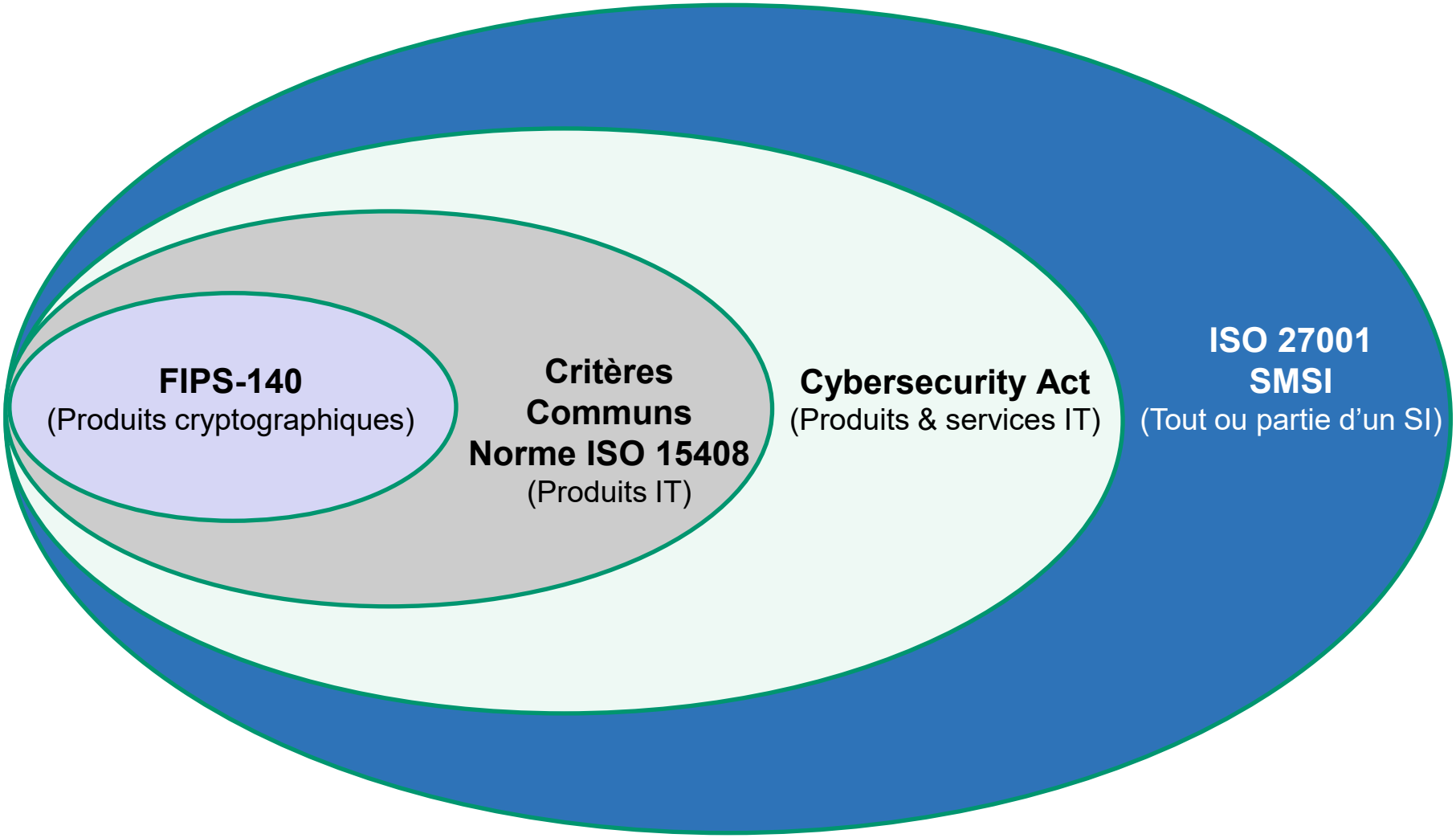
- Installation & paramétrage réalisés dans les règles de l'art ?
- Qui gère les clés ? (création, utilisation, révocation, recouvrement, …)
- Sont-elles accessibles ? (Container logiciel, HSM, carte à puce, TPM)

Vérifier l'utilisation

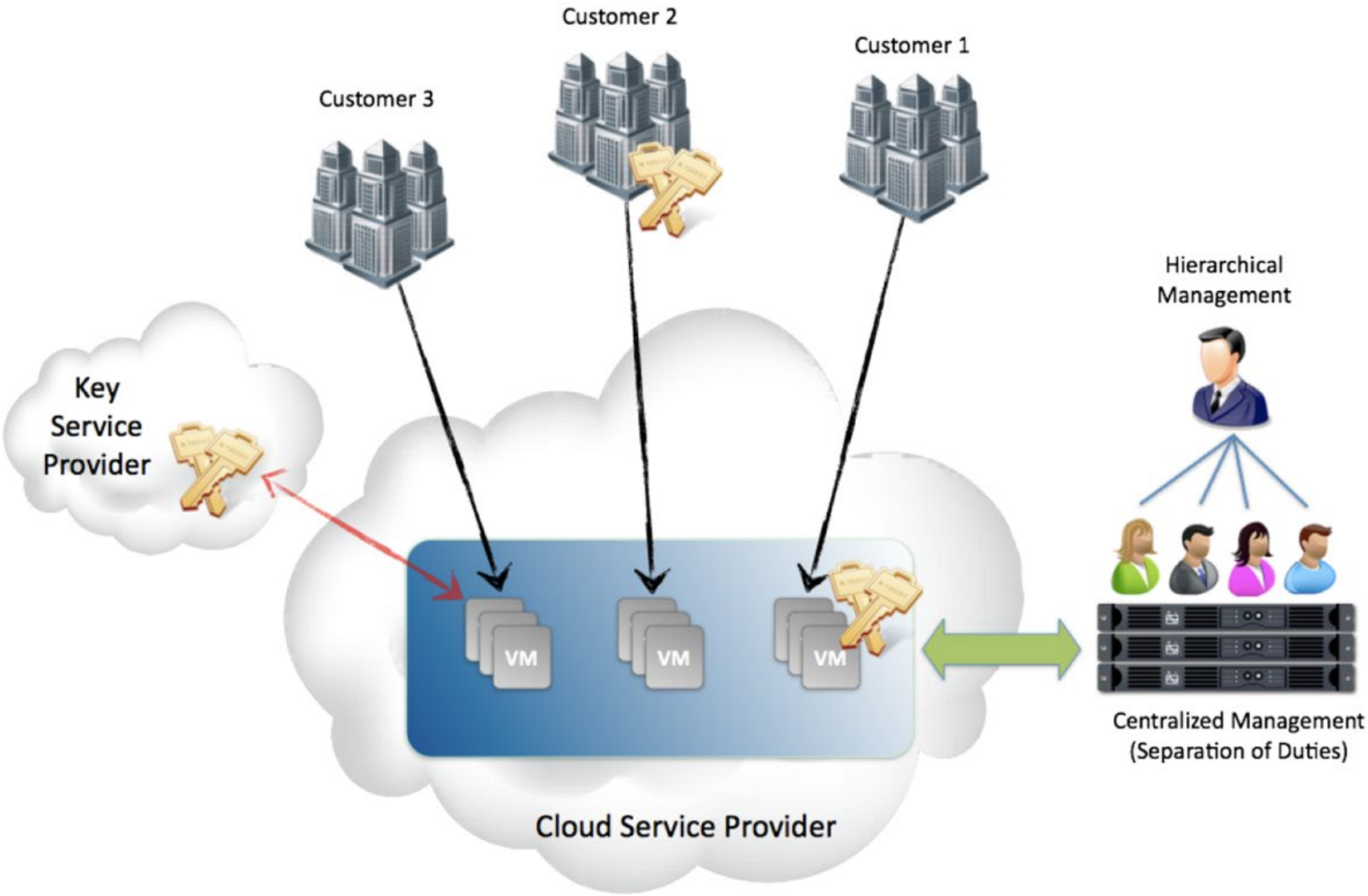
- Formaliser les procédures (révocation, recouvrement, incidents sécurité)
- Sensibilisation du personnel (utilisateur, développeur, DBA, …)

« *Encryption works ! Properly implemented, strong crypto systems are one of the few things that you can rely on. Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it* » **Edward Snowden**

Les certifications de sécurité



Les 3 options de gestion des clés



La gestion des clés dans le Cloud

Le fournisseur fournit le service de chiffrement

- **Les clés sont gérées via un service (SSM) sous le contrôle du CSP**
  - Le client fait totalement confiance au CSP
- **Les clés sont gérées via un HSM sous le contrôle des clients**
  - Le CSP n'a pas (à priori) accès aux clés des clients

Le client utilise ses propres clés ou service de chiffrement

- **BYOK (Bring Your Own Keys) ou HYOK (Hold Your Own Keys)**
  - Exemple HSM on-premise avec synchro sur HSM off-premise
- **BYOE (Bring Your Own Encryption)**
  - BYOK + module de chiffrement tiers
  - Exemples : Revolve (Deveoteam), CipherTrust (Thalès)
- **CASB (Cloud Access Security Broker)**
  - Exemple : CipherCloud (https://CipherCloud.com)

Le client s'appuie sur un service tiers de gestion des clés

- **Key Management as a Service (KMaaS)**
  - Problèmes potentiels d'interopérabilité
  - Exemples : CipherTrust Cloud Key Manager (Thalès), SvKMS (StorMagic)

Produits HSM chez Thalès

Luna USB (Luna G5)

(FIPS-140-2 L2)

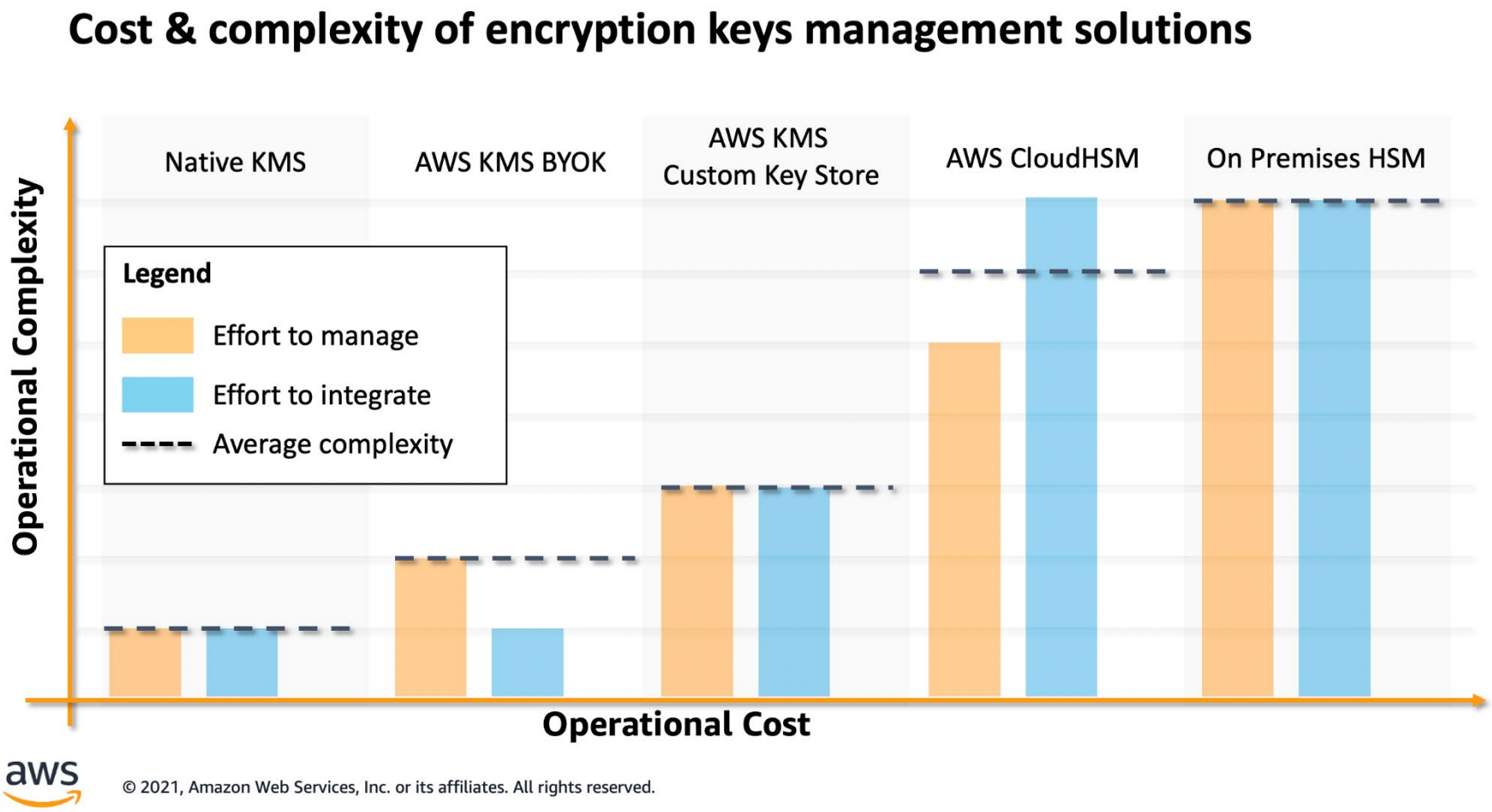
Luna PCIe

(FIPS-140-2 L3)

Luna Network HSM7

(FIPS-140-2 L3 & CC EAL4+)

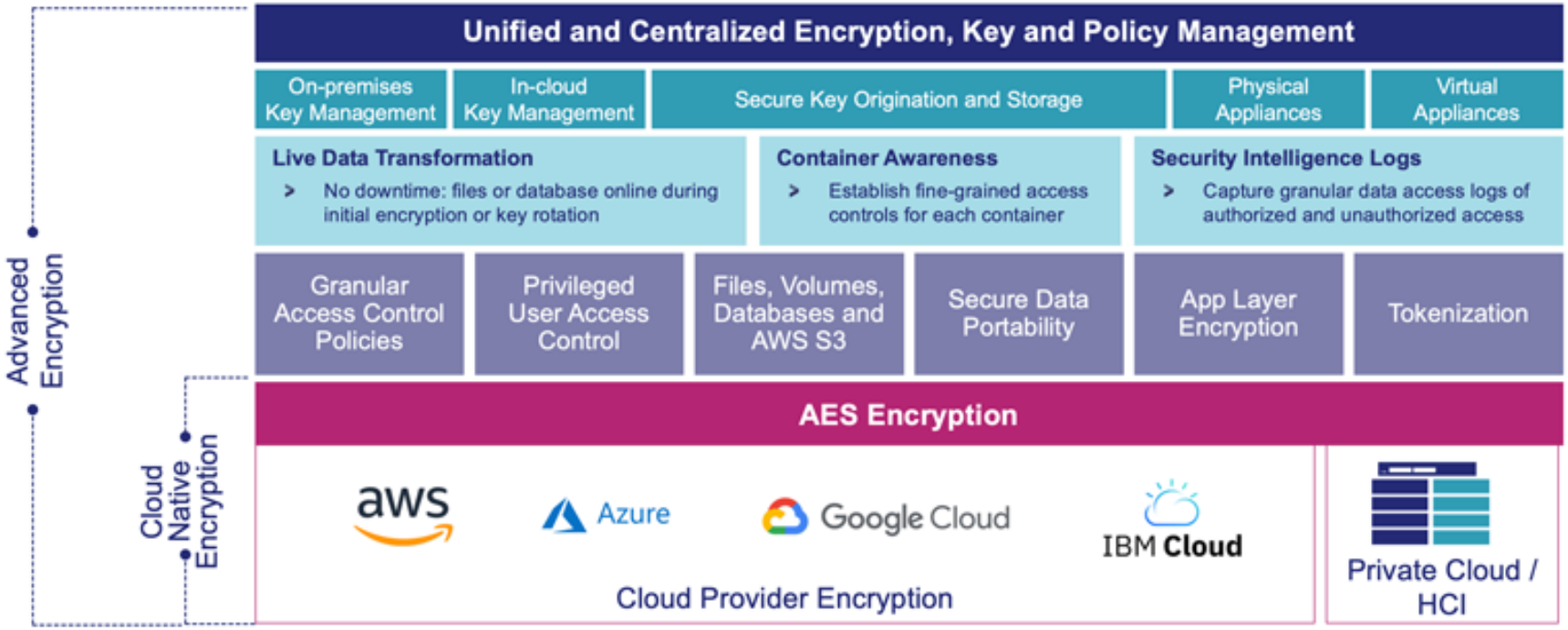
Coûts & complexité de mise en oeuvre



Source : https://aws.amazon.com/fr/blogs/security/demystifying-kms-keys-operations-bring-your-own-key-byok-custom-key-store-and-ciphertext-portability

Bring Your Own Encryption (BYOE)

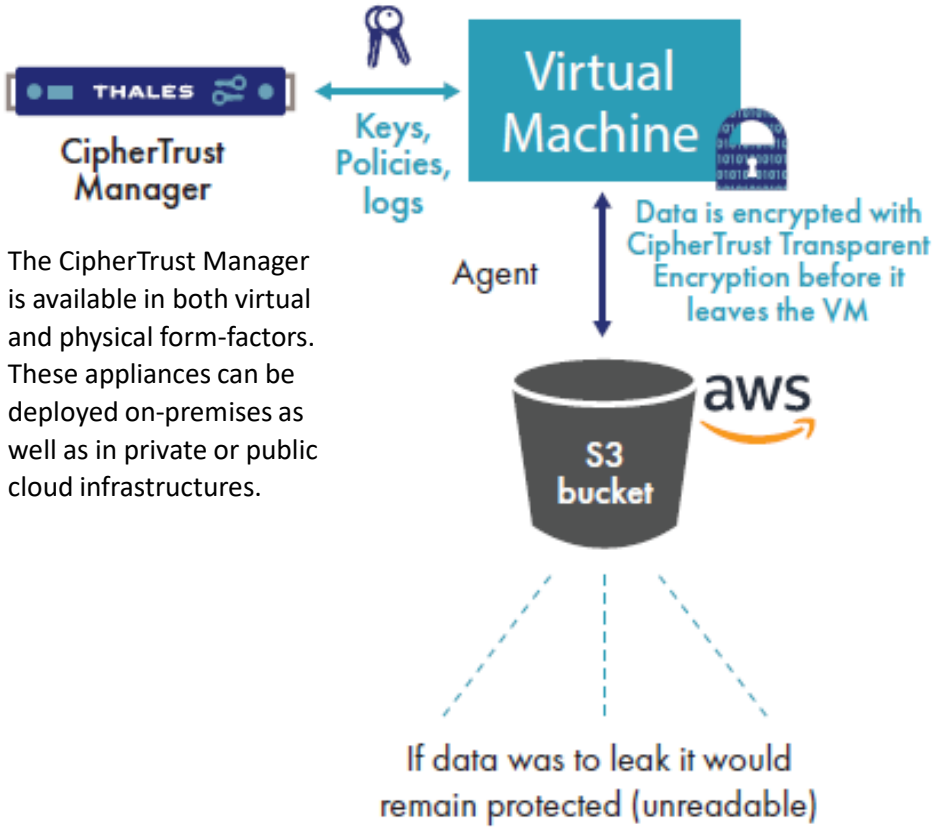
Avec le BYOE, on va encore plus loin qu'avec l'approche BYOK/HYOK puisqu'en plus de la gestion des clés, on utilise un module cryptographique complémentaire non fourni par le CSP



Source : https://cpl.thalesgroup.com/encryption/bring-your-own-encryption

Le manque de normes implique des solutions spécifiques pour chaque services Cloud

Exemple : Sécurité S3 (Thalès)



The CipherTrust Manager is available in both virtual and physical form-factors. These appliances can be deployed on-premises as well as in private or public cloud infrastructures.

- **Transparent object storage encryption in the cloud**

Provides transparent encryption of sensitive data stored in Amazon S3 buckets.

- **Customer-owned key security**

Maintain control and ownership of encryption keys on-premises or in the cloud with a FIPS 140-2 compliant solution.

- **Fast deployment and implementation**

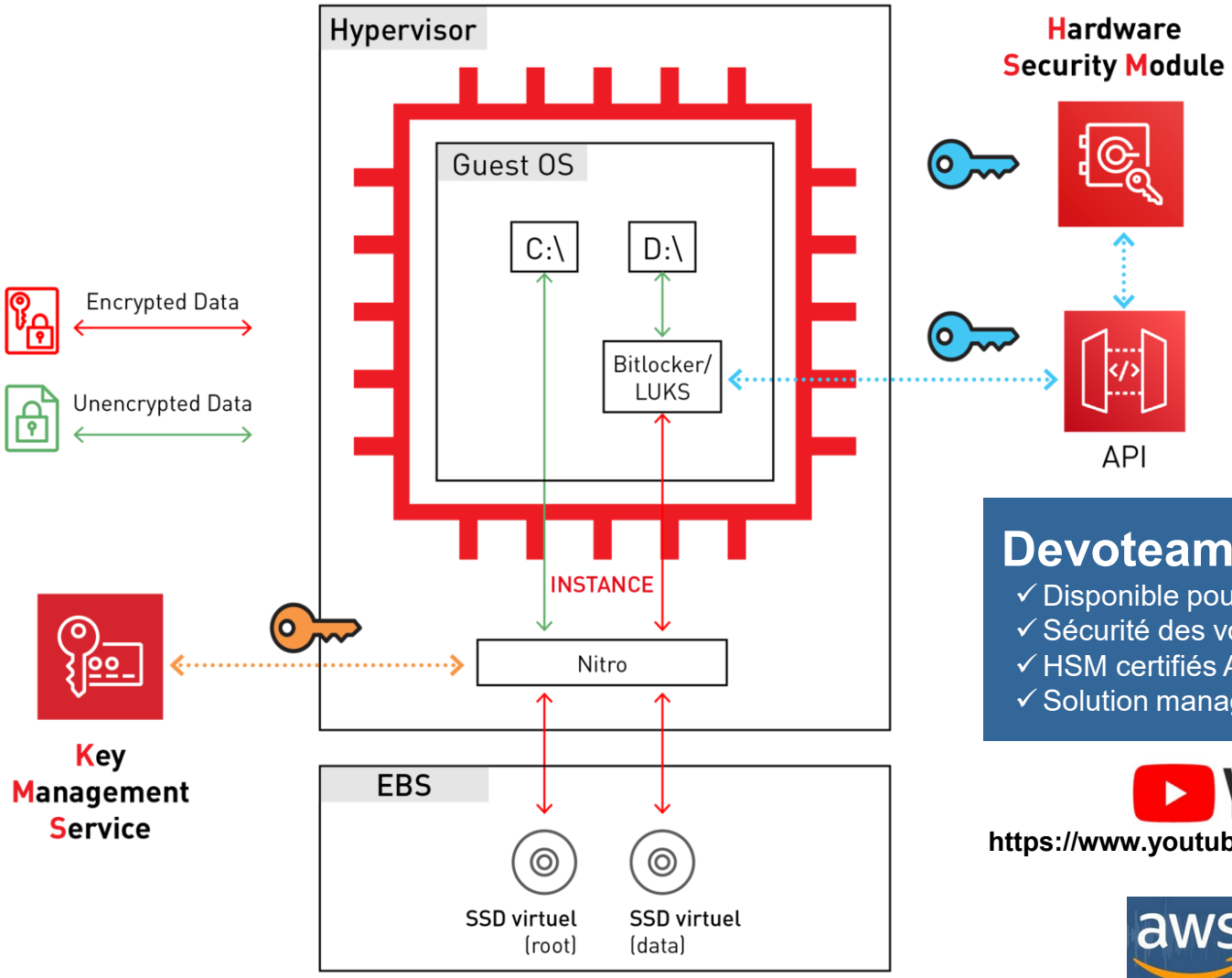
Easy to deploy agents run on Amazon EC2 and on-premises servers with no need to change applications or database schema.

- **Segregation of duties**

Add granular access management and privileged user access controls controlled by the security team.

Source : https://cpl.thalesgroup.com/resources/encryption/amazon-s3-with-ciphertrust-transparent-encryption-solution-brief

Exemple : Sécurité EBS (Devoteam)



Devoteam Revolve

- ✓ Disponible pour EC2 (vm) & ECS (container)
- ✓ Sécurité des volumes EBS (Block storage)
- ✓ HSM certifiés ANSSI & hébergés par Thalès
- ✓ Solution managée par Devoteam

YouTube

https://www.youtube.com/watch?v=JcvnpGnMGqI

aws le podcast en français

https://aws.amazon.com/fr/blogs/france/podcast_2021/#071

Source : https://revolve.team/chiffrement-cloud-aws

Les 5 mythes de la sécurité dans le Cloud

Mythe n°1

- Une infra IT « on-prem » sera toujours plus sécurisée

Mythe n°2

- Il n'y a aucun risque car mes données sont chiffrées

Mythe n°3

- Je suis rassuré car mon CSP est certifié ISO 27001

Le SMSI dans l'ISO 27001

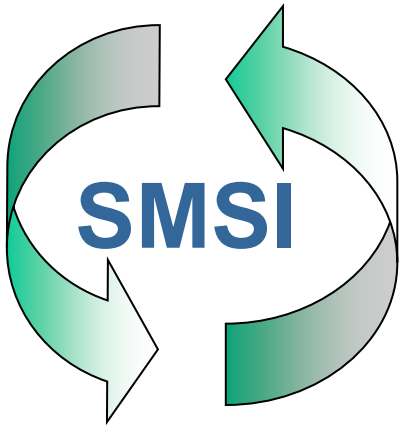
Exigences de sécurité

PLAN (Préparer / Planifier)

Définition du périmètre, Politique de sécurité de l'information, appréciation des risques, plan de traitement des risques

DO (Déployer)

Traitement des risques,
Mise en oeuvre des mesures de sécurité,
Allocation des ressources,
Formation, Sensibilisation,…



Act (Actualiser / Améliorer)

Amélioration, correction des non-conformités, actions préventives et correctives, documentation,…

Check (Contrôler)

Contrôle des mesures,
Veille externe,
Audit interne,
Analyse des non-conformités,…

Amélioration continue de la sécurité

Usage de la certification ISO 27001

Doctolib

bsi ISO 27001 Hébergeurs de données de santé CERTIFIED

Levallois-Perret, le 17 novembre 2021

COMMUNIQUÉ DE PRESSE

Doctolib obtient la certification ISO 27001, démontrant ainsi son engagement en matière de sécurité de l'information.

Doctolib obtient une nouvelle certification majeure : ISO 27001. Cette certification a été délivrée par BSI Group, organisme habilité et reconnu en France et à l'international. Elle atteste que Doctolib adopte les meilleures pratiques en termes de sécurité de l'information.

Intérêt de la norme ISO 27001 ?

L'ISO 27001 ne garantit pas un niveau de sécurité !

- Aucune garantie sur la pertinence de l'analyse de risque
- Aucune garantie sur l'adéquation des mesures de sécurité

Un certificat ISO 27001 donne très peu d'informations

- Quelles sont concrètement les mesures de sécurité déployées ?
- Quelle est niveau d'acceptation des risques résiduels ?
- Le SMSI traite les risques SSI du fournisseur
  - **Pas à la sécurité des données clients chez le CSP**
    - Exemple : backups chez OVH

Une certification 27001 donne une énorme crédibilité en sécurité

- Elément marketing important pour tous les CSP
- Ne pas être ISO 27001 aujourd'hui serait un énorme handicap pour un CSP
  - Seuls les tout-petits fournisseurs ne le sont pas encore

QUID des certifications 27017 et 27018 ?

afaq
AFNOR CERTIFICATION

Certificat
Certificate

N° 2018/81509.3 — **Page 1 / 2**

AFNOR Certification certifie que le système de management mis en place par :
AFNOR Certification certifies that the management system implemented by:

ORANGE BUSINESS SERVICES

pour les activités suivantes :
for the following activities:

CONCEPTION, INGENIERIE, VENTE, DEPLOIEMENT ET SUPPORT DE SERVICES INFORMATIQUES ET DE SOLUTIONS DE COMMUNICATION, DE SERVICES CLOUD POUR LES ENTREPRISES ET DE CONTRATS D'OUTSOURCING
Déclaration d'applicabilité : v 9R1

DESIGN, ENGINEERING, SALES, DEPLOYMENT AND SUPPORT OF INFORMATION AND COMMUNICATION TECHNOLOGY SERVICES, BUSINESS CLOUD SERVICES AND OUTSOURCING CONTRACTS
Statement of applicability : v 9R1

a été évalué et jugé conforme aux exigences requises par :
has been assessed and found to meet the requirements of :

ISO 27017 : 2015

et est déployé sur les sites suivants :
and is developed on the following locations:

6 rue de la Touche Lambert FR-35510 CESSON SEVIGNE CEDEX

Liste des sites certifiés en annexe / *List of certified locations on appendix*

Ce certificat est valable à compter du (année/mois/jour) *This certificate is valid from (year/month/day)* **2021-12-21** Jusqu'au *Until* **2023-12-17**

Ce document est signé électroniquement. Il constitue un original électronique à valeur probatoire.
This document is electronically signed. It stands for an electronic original with probationary value.

Julien NIZRI
Directeur Général d'AFNOR Certification
Managing Director of AFNOR Certification

Flashez ce QR Code pour vérifier la validité du certificat

Seul le certificat électronique, consultable sur www.afnor.org, fait foi en temps réel de la certification de l'organisme. *The electronic certificate only, available at www.afnor.org, attests in real-time that the company is certified.* AFAQ est une marque déposée.*AFAQ is a registered trademark.* CERT. F 0696 fr 070320

afaq
AFNOR CERTIFICATION

Certificat
Certificate

N° 2018/81507.3 — **Page 1 / 2**

AFNOR Certification certifie que le système de management mis en place par :
AFNOR Certification certifies that the management system implemented by:

ORANGE BUSINESS SERVICES

pour les activités suivantes :
for the following activities:

CONCEPTION, INGENIERIE, VENTE, DEPLOIEMENT ET SUPPORT DE SERVICES INFORMATIQUES ET DE SOLUTIONS DE COMMUNICATION, DE SERVICES CLOUD POUR LES ENTREPRISES ET DE CONTRATS D'OUTSOURCING
Déclaration d'applicabilité : v 9R1

DESIGN, ENGINEERING, SALES, DEPLOYMENT AND SUPPORT OF INFORMATION AND COMMUNICATION TECHNOLOGY SERVICES, BUSINESS CLOUD SERVICES AND OUTSOURCING CONTRACTS
Statement of applicability : v 9R1

a été évalué et jugé conforme aux exigences requises par :
has been assessed and found to meet the requirements of :

ISO 27018 : 2019

et est déployé sur les sites suivants :
and is developed on the following locations:

6 rue de la Touche Lambert FR-35510 CESSON SEVIGNE CEDEX

Liste des sites certifiés en annexe / *List of certified locations on appendix*

Ce certificat est valable à compter du (année/mois/jour) *This certificate is valid from (year/month/day)* **2021-12-21** Jusqu'au *Until* **2023-12-17**

Ce document est signé électroniquement. Il constitue un original électronique à valeur probatoire.
This document is electronically signed. It stands for an electronic original with probationary value.

Julien NIZRI
Directeur Général d'AFNOR Certification
Managing Director of AFNOR Certification

Flashez ce QR Code pour vérifier la validité du certificat

Seul le certificat électronique, consultable sur www.afnor.org, fait foi en temps réel de la certification de l'organisme. *The electronic certificate only, available at www.afnor.org, attests in real-time that the company is certified.* AFAQ est une marque déposée.*AFAQ is a registered trademark.* CERT. F 0696 fr 070320

Cryptographie - Norme ISO 27017

10.1.2 Key management

Control 10.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should identify the cryptographic keys for each cloud service, and implement procedures for key management. Where the cloud service provides key management functionality for use by the cloud service customer, the cloud service customer should request the following information on the procedures used to manage keys related to the cloud service: – type of keys; – specifications of the key management system, including procedures for each stage of the key life-cycle, i.e., generating, changing or updating, storing, retiring, retrieving, retaining and destroying; – recommended key management procedures for use by the cloud service customer. The cloud service customer should not permit the cloud service provider to store and manage the encryption keys for cryptographic operations when the cloud service customer employs its own key management or a separate and distinct key management service.	(no additional implementation guidance)

A propos de l'incendie OVH (Strasbourg)

1. **Les datacenters Strasbourg 1 et Strasbourg 4 devaient être fermés**
2. **Le datacenter SBG4 n'était pas indépendant énergétiquement**
3. **SBG3 n'avait pas sa propre salle réseau**
4. **Des backups étaient réalisés sur le même datacenter**
5. **Les planchers du datacenter SBG2 étaient en bois**
6. **L'absence de système d'extinction automatisé sur SBG2**

La gestion des backup dans l'offre OVHcloud Private Cloud

(Offre certifiée ISO 27001 et qualifiée SecNumCloud)

Au sein de son offre de cloud privé managé (Private Cloud), OVH ne proposait pas de service de backup déporté avant avril 2020. Ses clients ayant souscrit à cette offre auparavant ne disposent donc pas de la nouvelle option.

L'ensemble des utilisateurs de Private Cloud localisés sur SBG2 semblent être dans ce cas. OVH a en effet clairement indiqué que leur sauvegarde était irrécupérable.

Idem pour ceux adossés à SBG1. Octave Klaba le confirme sur Twitter : "Les sauvegardes gratuites et payantes de Private Cloud dans SBG1 étaient hébergées dans une autre salle du centre de données. Les deux sont détruites.

Source : www.journaldunet.com - 29 mars 2021

Calcul du risque par OVHcloud

Quel risque pour OVH en cas de perte de données clients ?

- Le contrat limite la responsabilité d'OVH à verser une somme maximale de 6 mois d'abonnement en cas de perte des données → Pénalités !
  - Les pénalités viennent sanctionner le client ou le prestataire lorsqu'il est à l'origine du non-respect du SLA
  - Les indemnités viennent réparer le préjudice subi par le client ou le prestataire lorsqu'une autre partie est à l'origine du non-respect des SLA

2 condamnations pour OVHcloud

- **Contrat Cloud = Contrat d'adhésion**
  - Un contrat d'adhésion est défini comme « celui qui comporte un ensemble de clauses non négociables, déterminées à l'avance par l'une des parties »
- **Article 1171 du code civil**
  - « Toute clause non négociable, déterminée à l'avance par l'une des parties, qui crée un déséquilibre significatif entre les droits et obligations des parties au contrat est réputée non écrite »
- **2 condamnations à ce jour**
  - 100 000 € pour France Bati Courtage (26/01/2023)
  - 144 836 € pour Bluepad (09/03/2023)
- **+ Un recours collectif (actuellement en cours)**
  - Cabinet Ziegler Associés
  - Application de l'article 1231-1 du code civil

Le référentiel ANSSI SecNumCloud

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

Agence nationale de la sécurité des systèmes d'information

Prestataires de services d'informatique en nuage (SecNumCloud)

référentiel d'exigences

Version 3.2 du 8 mars 2022

HISTORIQUE DES VERSIONS

DATE	VERSION	EVOLUTION DU DOCUMENT	REDACTEUR
30/07/2014	1.3	*Version publiée pour commentaires.*	ANSSI
20/03/2015	2.0	*Version intermédiaire utilisée pour la procédure expérimentale*	ANSSI
08/12/2016	3.0	*Première version applicable.* Modifications principales : • création d'un référentiel par niveau de qualification ; • clarifications apportées à certaines exigences ; • refonte des chapitres 9, 10, 13 et des annexes ; • intégration plus précise des labels PASSI, PRIS et PDIS.	ANSSI
11/06/2016	3.1	*Version prenant en compte le Règlement général sur la protection des données (RGPD).* Modifications principales : • mise en conformité avec le RGPD ; • retrait de la mention d'un niveau de qualification avancé. • précision concernant l'hébergement externe partagé	ANSSI
08/03/2022	3.2	*Version intégrant principalement des critères de protection vis-à-vis du droit extra-européen.* *Modifications apportées aux chapitres 1.3.1, 3.2, 3.3.2, 4, 5.3, 6.1,7.1, 7.2, 8.1, 9.1, 9.5, 9.7, 10.2, 11.2.1, 11.5, 12.10, 12.13, 12.14, 17.1, 18.2.3, 19.1, 19.6, Annexes 1 et 2.*	ANSSI

- **Version 1.3 - Publiée le 30/07/2014**
  - Appel à commentaires
  - Clôture de réception des commentaires le 3/11/2014
  - 2 niveaux définis dans le même document :
    - élémentaire & standard
- **Version 2.0 - 20/03/2015 - Non publiée**
  - Version intermédiaire utilisée pour la procédure expérimentale
    - Secure Cloud & Secure Cloud plus
- **Version 3.0 - Publiée le 08/12/2016**
  - 2 niveaux définis dans 2 documents distincts :
    - SecNumCloud – niveau essentiel
    - SecNumCloud – niveau avancé
- **Version 3.1 - Publiée le 11/06/2018**
  - Mise en conformité avec le RGPD
  - Suppression du niveau de qualification avancé
- **Version 3.2 - Publiée le 08/03/2022**
  - Ajout de critères de protection vis-à-vis du droit extra-européen
    - CLOUD act et FISA en ligne de mire…
  - Diverses modifications apportées

V3.1 : 15 domaines & 233 exigences

CONTROLE D'ACCES ET GESTION DES IDENTITES (32)

GESTION DES ACTIFS (8)

CRYPTOLOGIE (14)

SECURITE DES RESSOURCES HUMAINES (10)

SECURITE PHYSIQUE ET ENVIRONNEMENTALE (33)

ORGANISATION DE LA SECURITE DE L'INFORMATION (10)

SECURITE LIEE A L'EXPLOITATION (32)

POLITIQUES DE SECURITE ET GESTION DU RISQUE (13)

SecNumCloud

SECURITE DES COMMUNICATIONS (8)

EXIGENCES SUPPLEMENTAIRES (25)

ACQUISITION, DEVELOPPEMENT, MAINTENANCE (12)

CONFORMITE (9)

CONTINUITE D'ACTIVITE (5)

RELATIONS AVEC LES TIERS (9)

GESTION DES INCIDENTS SECURITE (13)

mais aussi **7 recommandations à destination des commanditaires** (Annexe 2)

Le principal ajout de la version 3.2

19.6. Protection vis-à-vis du droit extra-européen

a) Le siège statutaire, administration centrale et principal établissement du prestataire doivent être établis au sein d'un État membre de l'Union Européenne.

b) Le capital social et les droits de vote dans la société du prestataire ne doivent pas être, directement ou indirectement :
- individuellement détenus à plus de 24% ;
- et collectivement détenus à plus de 39% ;
par des entités tierces possédant leur siège statutaire, administration centrale ou principal établissement au sein d'un État non membre de l'Union européenne.

Si le capital détenu par ces entités tierces se présente sous la forme d'actions admises aux négociations sur un marché réglementé, ces susdites entités tierces sont celles déclarées conformément au I de l'article L.233-7 du code de commerce.
Ces entités tierces susmentionnées ne peuvent pas individuellement ou collectivement :
- en vertu d'un contrat ou de clauses statutaires, disposer d'un droit de véto ;
- en vertu d'un contrat ou de clauses statutaires, désigner la majorité des membres des organes d'administration, de direction ou de surveillance du prestataire.

c) En cas de recours par le prestataire, dans le cadre des services fournis au commanditaire, aux services d'une société tierce - y compris un sous-traitant - possédant son siège statutaire, administration centrale ou principal établissement au sein d'un État non membre de l'Union Européenne ou appartenant ou étant contrôlée par une société tierce domiciliée en dehors l'Union Européenne, cette susdite société tierce ne doit pas avoir la possibilité technique d'obtenir les données opérées au travers du service. Ces données visées sont celles qui sont confiées au prestataire par les commanditaires ainsi que toutes données techniques (identités des bénéficiaires et des administrateurs de l'infrastructure technique, données manipulées par le Software Defined Network, journaux de l'infrastructure technique, annuaire, certificats, configuration des accès, etc.) comprenant des informations sur les commanditaires.

Pour les besoins du présent article, la notion de contrôle est entendue comme étant celle mentionnée au II de l'article L233-3 du code de commerce.

d) Dans le cadre de l'exigence 19.6.c, toute société tierce à laquelle le prestataire recourt pour fournir tout ou partie du service rendu au commanditaire, doit garantir au prestataire une autonomie d'exploitation continue dans la fourniture des services d'informatique en nuage qu'il opère ou doit être qualifié SecNumCloud.

Pour les besoins du présent article, la notion d'autonomie d'exploitation est entendue comme étant la capacité de maintenir la fourniture du service d'informatique en nuage en faisant appel aux compétences propres du prestataire ou en recourant à des prestations disponibles auprès d'au moins deux sociétés tierces.

e) Le service fourni par le prestataire doit respecter la législation en vigueur en matière de droits fondamentaux et les valeurs de l'Union relatives au respect de la dignité humaine, à la liberté, à l'égalité, à la démocratie et à l'État de droit. Il peut être pris en considération pour l'appréciation de la conformité susmentionnée, le fait que le prestataire entretienne des liens avec un gouvernement ou un organisme public étrangers.

f) Le prestataire doit informer formellement le commanditaire, et dans un délai d'un mois, de tout changement juridique, organisationnel ou technique pouvant avoir un impact sur la conformité de la prestation aux exigences du chapitre 19.6.

Prestataires qualifiés SecNumCloud

	Date de début de la qualification	Date de fin de la qualification	Niveau de recommandation	IaaS	PaaS	SaaS	Référence de la qualification
Informatique en nuage (SecNumCloud)							
Cloud Temple							
Secure Temple	15/03/2022	15/03/2025	✓	x			569
Oodrive							
Oodrive_platform avec le service Oodrive_collaborate	17/03/2022	22/01/2025	✓			x	596
Oodrive_platform avec le service Oodrive_meeting	17/03/2022	22/01/2025	✓			x	597
Oodrive_platform avec le service Oodrive_share	17/03/2022	22/01/2025	✓			x	598
Outscale SAS							
Iaas Cloud on Demand	16/12/2022	12/06/2023	✓	x			2679
OVH							
Private Cloud	16/12/2022	24/06/2023	✓	x			2678
Worldline							
Worldline Cloud Services - Secured IaaS	22/10/2021	22/10/2024	✓	x			2686

Source : ANSSI (avril 2023)

Prestataires en cours de qualification

Prestataire	Service(s)	Localisation
Cloud Solutions 112 Rue Réaumur 75002 Paris Tel : + 33 (0)1 76 44 01 97 mél : sales[at]cloud-solutions.fr	**Wimi Entreprise (SaaS)** Plateforme de travail collaboratif (Partage et co-édition de documents, Gestion de projet, visioconférence, chat)	France
IDNOMIC (Keynectis) 175, rue Jean-Jacques Rousseau 92130 Issy-les-Moulineaux tel : 01.55.64.22.00 mél : sales[at]idnomic.com https://www.idnomic.com ↗	**ID-PKI en mode SaaS**	France
Index Education 2-8, rue Georges Charpak 13013 Marseille Tél : 04 96 15 21 70 https://www.index-education.com/fr/ ↗	**Service SaaS (Pronote, Pronote primaire, HyperPlanning et Edt)**	France
cegedim.cloud 137 Rue d'Aguesseau 92100 Boulogne-Billancourt Tél : 01 49 09 22 00 Mél : contact@cegedim.cloud www.cegedim.cloud ↗	**CegNumCloud Secured IaaS**	France
Whaller 3 rue Salomon de Rothschild 92150 Suresnes Tél : +33 1 47 92 82 18 Mél : contact@whaller.com whaller.com ↗	**Whaller DONJON SaaS** Plateforme de communication et de collaboration(Réseau social d'entreprise, outils collaboratifs, gestion de fichiers, visioconférence, Intranet)	France
Orange Business 1 Place des Droits de l'Homme 93210 Saint-Denis La Plaine Mél : cloudstore@orange-business.com cloud.orange-business.com ↗	**Cloud Avenue** Cloud Privé Virtuel – IaaS	France

Source : ANSSI (avril 2023)

Aide de 180 K€ pour les « petits » CSP

GUICHET D'ACCÈS AU DISPOSITIF D'ACCOMPAGNEMENT À LA QUALIFICATION
SECNUMCLOUD

GOUVERNEMENT — FRANCE 2030 — bpifrance

1 Audit initial

- Evaluer et mesurer le niveau cyber
- Montant de l'aide : 40k€

Plan de développement à une démarche de qualification

Plan de préparation à la qualification SecNumCloud.

2 FORMULE TRANSFORMATION

- Référence au Guide d'hygiène de l'ANSSI
- Intégration d'actions cyber dans le fonctionnement technique et organisationnel de l'entreprise
- Montant de l'aide : 60k€

SI durci par des mesures et des pratiques formalisées

3 FORMULE CONFORMITE

- Audit de qualification à blanc
- Les entreprises doivent formaliser leurs pratiques et appliquer les guides de l'ANSSI
- Montant de l'aide : 40k€

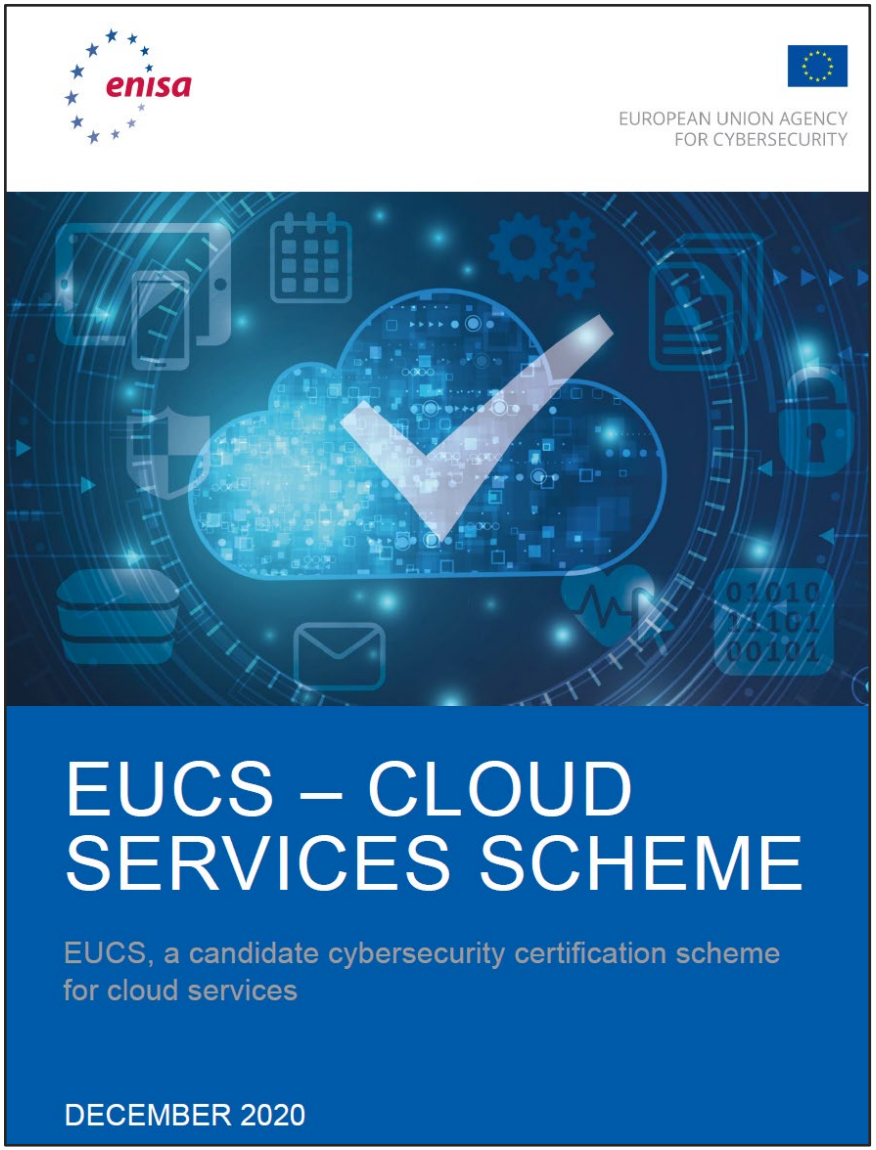
Une offre Cloud alignée avec les exigences du référentiel SecNumCloud

4 Qualification SECNUMCLOUD

- Démarche de qualification mature de l'entreprise
- Respect et application des règles du référentiel
- Reconnaissance via le Visa de sécurité ANSSI
- Montant de l'aide : 40k€

Aide réservée aux PME (au sens du règlement européen 364/2004) : moins de 250 personnes et CA annuel < 50 M€

La certification européenne EUCS



A.1 Organisation of information security

OIS-01 INFORMATION SECURITY MANAGEMENT SYSTEM

Objective

The CSP operates an information security management system (ISMS). The scope of the ISMS covers the CSP's organisational units, locations and processes for providing the cloud service.

Requirements

Ref	Description	Ass. Level
OIS-01.1	The CSP shall define, implement, maintain and continually improve an information security management system (ISMS), covering at least the operational units, locations and processes for providing the cloud service	Basic
OIS-01.2	The ISMS shall be in accordance to ISO/IEC 27001	Substantial
OIS-01.3	The ISMS shall have a valid certification according to ISO/IEC 27001 or to national schemes based on ISO 27001	High
OSI-01.4	The CSP shall document the measures for documenting, implementing, maintaining and continuously improving the ISMS	Basic
OIS-01.5	The documentation shall include at least: • Scope of the ISMS (Section 4.3 of ISO/IEC 27001); • Declaration of applicability (Section 6.1.3), and • Results of the last management review (Section 9.3).	Substantial

A.8 Identity and Access control Mgt

IAM-07 AUTHENTICATION MECHANISMS

Objective

Adequate authentication mechanisms are used in to be granted access to any environment and when needed within an environment.

Requirements

Ref	Description	Ass. Level
IAM-07.1	The CSP shall document and implement a policy and procedures about authentication mechanisms, covering at least the following aspects: • The selection of mechanisms suitable for every type of account and each level of risk; • The protection of credentials used by the authentication mechanism; • The generation and distribution of credentials for new accounts; • Rules for the renewal of credentials, including periodic renewals, renewals in case of loss or compromise; and • Rules on the required strength of credentials, together with mechanisms to communicate and enforce the rules;	Basic
IAM-07.2	The access to all environments of the CSP shall be authenticated, including non-production environments	Substantial
IAM-07.3	The access to the production environment of the CSP shall require strong authentication	High
IAM-07.4	The access to all environments of the CSP containing CSC data shall require strong authentication	High
IAM-07.5	Within an environment, user authentication shall be performed through passwords, digitally signed certificates or procedures that achieve at least an equivalent level of security	Substantial
IAM-07.6	For access to non-personal shared accounts, the CSP shall implement measures that require the users to be authenticated with their personal account before being able to access these technical accounts	Substantial
IAM-07.7	All authentication mechanisms shall include a mechanism to block an account after a predefined number of unsuccessful attempts	Basic

A.9 Cryptography and Key Management

CKM-03 ENCRYPTION OF DATA AT REST

Objective

The CSP has established procedures and technical safeguards to prevent the disclosure of cloud customers' data during storage.

Requirements

Ref	Description	Ass. Level
CKM-03.1	The CSP shall document and implement procedures and technical safeguards to encrypt cloud customers' data during storage	Basic
CKM-03.2	The private and secret keys used for encryption shall be known only to the cloud customer in accordance with applicable legal and regulatory obligations and requirements, with the possibility of exceptions	Substantial
CKM-03.3	The procedures for the use of private and secret keys, including a specific procedure for any exceptions, shall be contractually agreed with the cloud customer	Substantial
CKM-03.4	The private and secret keys used for encryption shall be known exclusively by the cloud customer and without exceptions in accordance with applicable legal and regulatory obligations and requirements	High

Exemples de certifications : AWS

CSA

Contrôles Cloud Security Alliance

CyberGRX

Gestion de risque par des tiers

CyberVadis

Gestion de risque par des tiers

ISO 9001

Norme de qualité mondiale

ISO 22301

Sécurité et résilience

ISO 27001

ISO 27017

ISO 27701

ISO 27018

PCI DSS, niveau 1

SOC 1

Rapport de contrôles d'audit

SOC 2

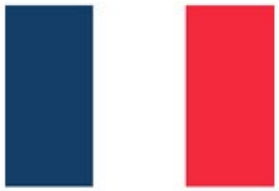
Rapport de sécurité, de disponibilité et de confidentialité

SOC 3

Rapport des contrôles généraux

Source : https://aws.amazon.com/fr/compliance/programs

Autres certifications AWS (Europe)



HDS

Protection des données personnelles de santé (France)

C5

Attestation de sécurité opérationnelle (Allemagne)

CISPE

Coalition des fournisseurs de services d'infrastructure cloud en Europe

Cyber Essentials Plus

Protection contre les cybermenaces au Royaume-Uni

ENS High

Normes gouvernementales (Espagne)

Source : https://aws.amazon.com/fr/compliance/programs

Les 5 mythes de la sécurité dans le Cloud

Mythe n°1

- Une infra IT « on-prem » sera toujours plus sécurisée

Mythe n°2

- Il n'y a aucun risque car mes données sont chiffrées

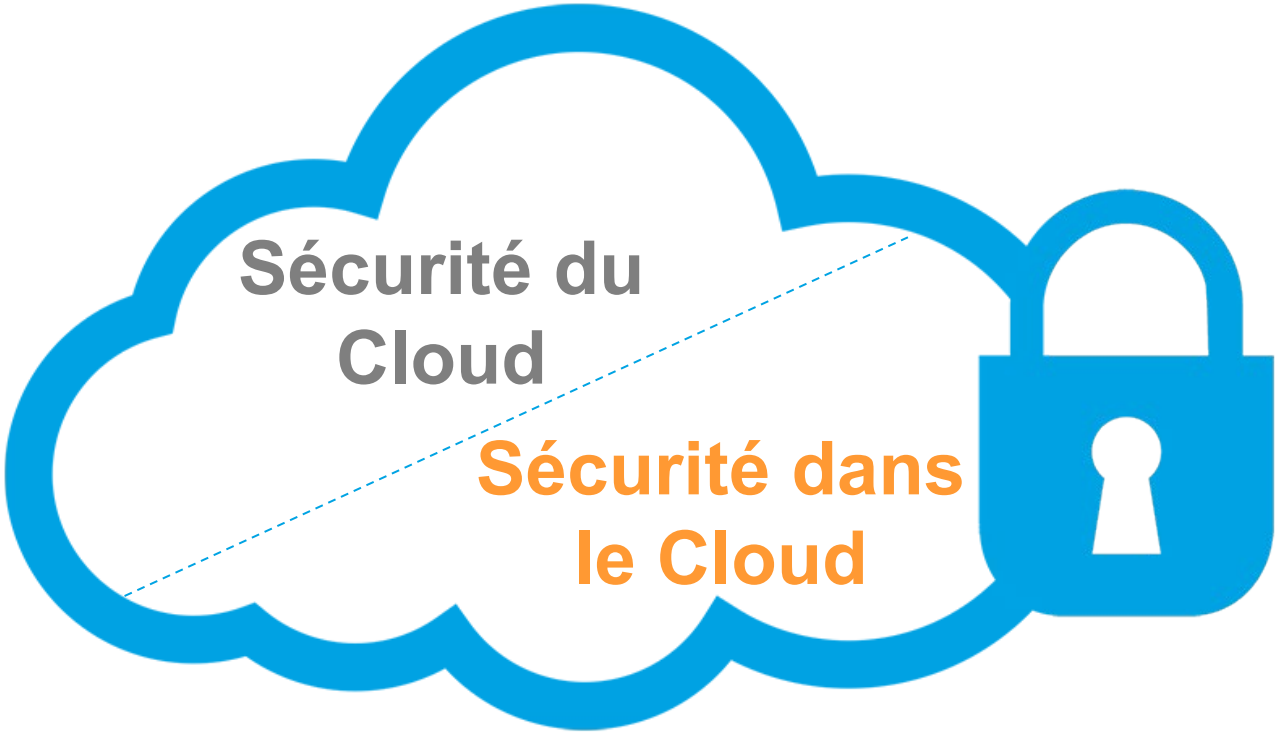
Mythe n°3

- Je suis rassuré car mon CSP est certifié ISO 27001

Mythe n°4

- La sécurité c'est essentiellement l'affaire de mon CSP

Modèle de responsabilité partagé



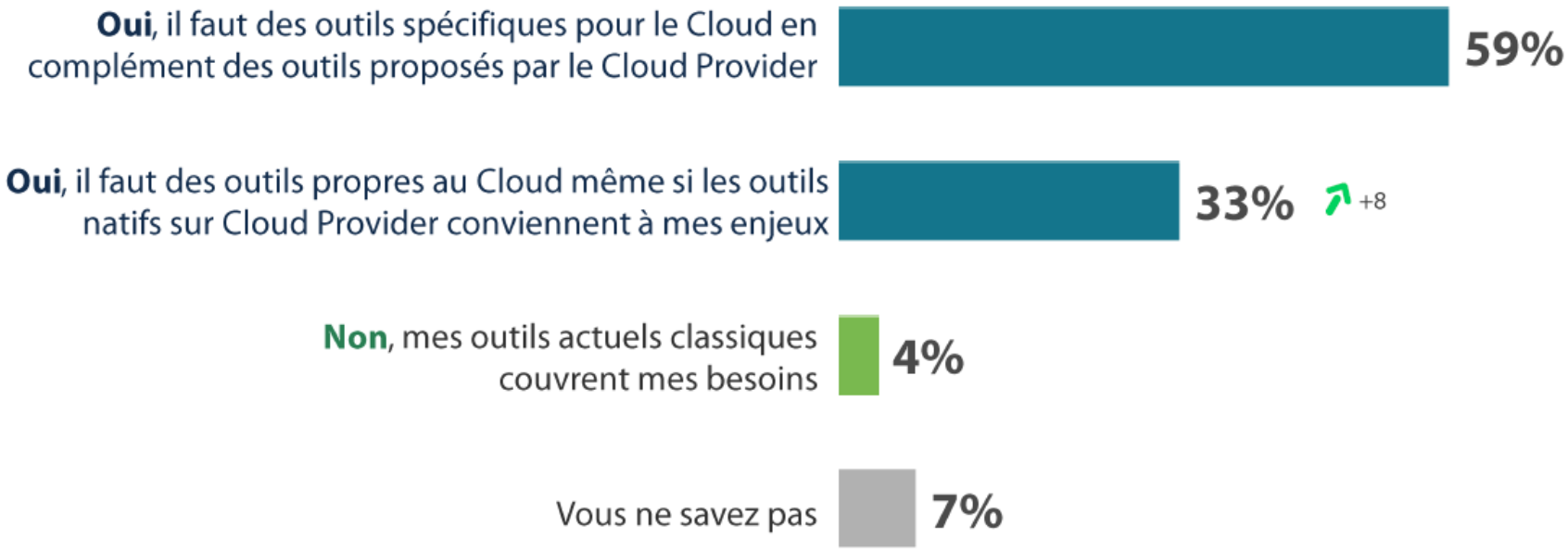
Mais **Qui** est **responsable** de **Quoi** ?

Faut-il des outils spécifiques ?

D'après vous, la sécurisation des données stockées dans le Cloud requiert-elle des outils ou dispositifs spécifiques ?

… 89% estiment que la sécurisation des données stockées dans le Cloud requiert des outils spécifiques

Rappel Vague 7 : 86%



Source : Baromètre de la cybersécurité des entreprises - CESIN (janvier 2023)

Quels risques dans le Cloud ?

Risques liés au fournisseur

- Risques physiques (accès aux datacenters, incendies,…)
- Risques techniques liés à l'infrastructure (Hyperviseur, Kubernetes, API, SDN,…)
- Malveillance interne
- Risques juridiques (Patriot Act, Cloud Act,…)

Risques liés à l'usage (surfacturation / Shadow IT,…)

- Monitoring des accès et de l'activité des utilisateurs (CASB)

Risques liés aux Workloads

- Surveillance et protection des charges de travail dans le Cloud (CWPP)

Risques liés à la configuration des services Cloud

- Gestion de la posture de sécurité IaaS (CSPM)
- Gestion de la posture de sécurité SaaS (SSPM)

CASB : Les 4 fonctionnalités

Cloud Access Security Broker

Visibilité

- Permet d'avoir une vision globale de l'utilisation des applications cloud sous forme de tableaux de bord: Quels sont les services Cloud utilisés ? Qui les utilisent ? Comment les applications Cloud sont utilisées ?
- Permet d'observer les tendances des usages internes et peuvent les aider à détecter des comportements suspicieux voire des menaces.
- Permet de lutter contre le shadow IT.
- Analyse beaucoup plus granulaire qu'avec un SWG ou un firewall NG (possibilité de définir entre 40 et 100 critères sur plusieurs milliers d'applications Cloud)

Gestion d'identité

- Permet de fournir pour toutes les applications cloud un système d'authentification unifié.
- La solution peut s'appuyer sur des annuaires internes ou faire appel à un Cloud Identity Provider externe (couplage possible avec des solutions tierces de SSO ou d'authentification OTP)

Contrôle d'accès

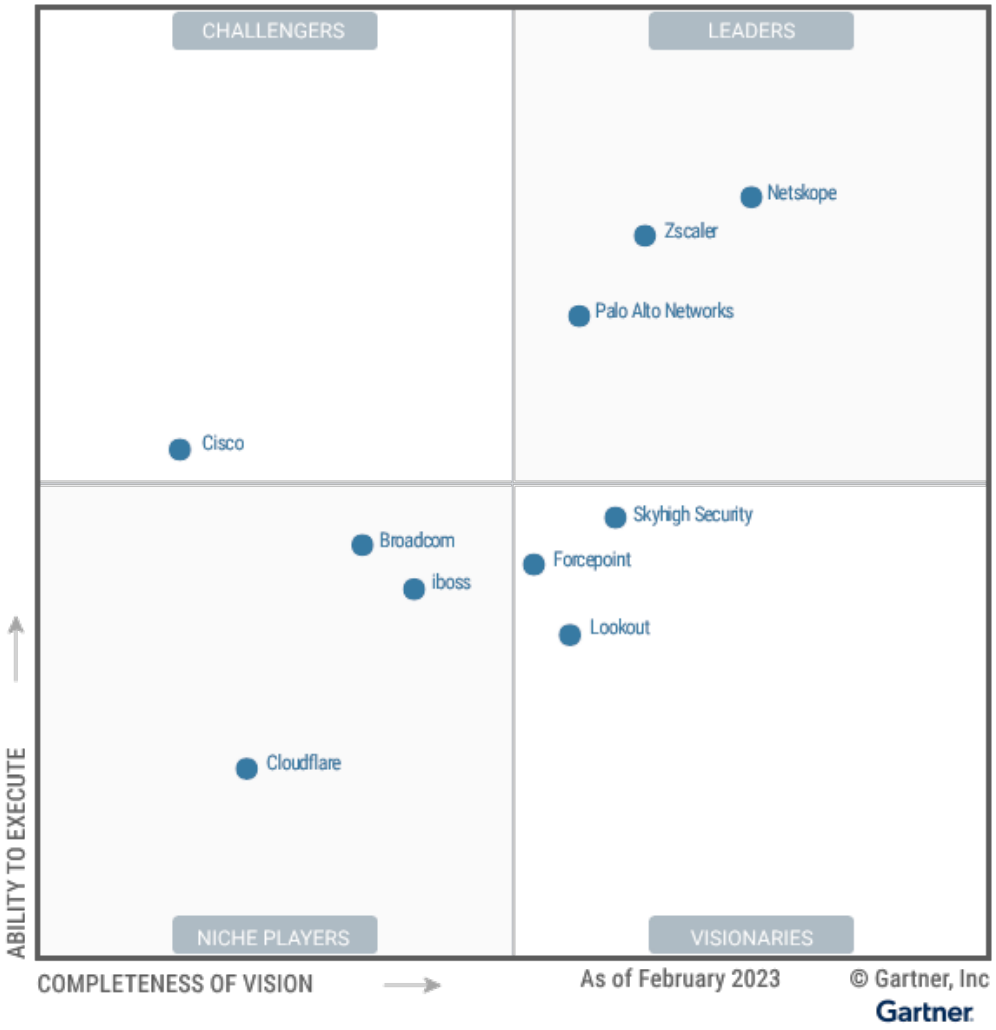
- Permet de définir les habilitations d'accès aux applications Cloud.
- Typiquement, le contrôle d'accès est basé sur le modèle RBAC sur lequel on peut y adjoindre en complément un contrôle de conformité sur le device (type, OS, localisation, …)

Protection des données

- Chiffrement des données avec des spécificités propres au Cloud : chiffrement sélectif (ne chiffre que les données sensibles), chiffrement avec préservation de format, tokenisation, …
- Permet de protéger contre la fuite d'informations sensibles ou réglementée. En pratique c'est une solution de DLP adaptée aux applications dans le Cloud.

Magic Quadrant for SSE (Gartner)

Le CASB est un composant du Security Service Edge (SSE)



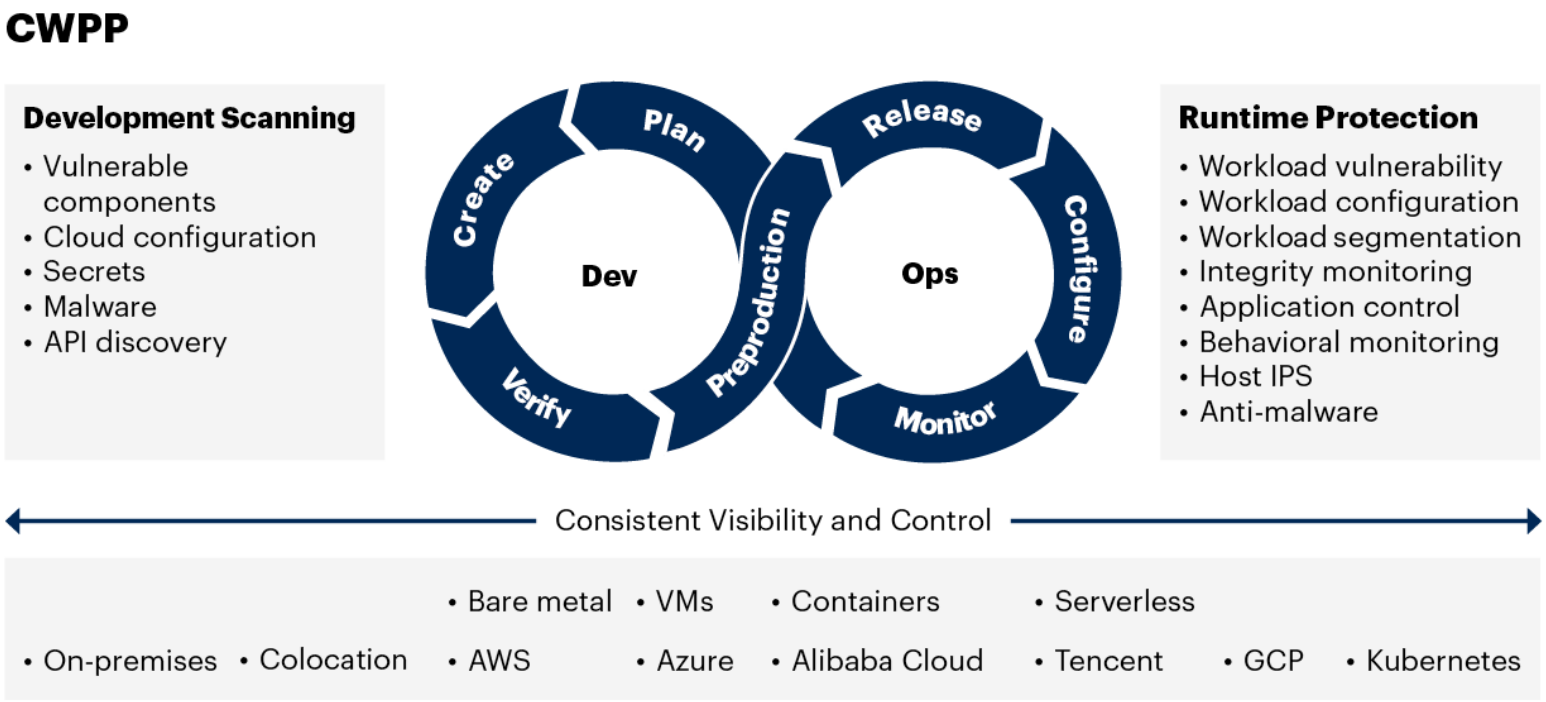
Source : Gartner - février 2023

Cloud Workload Protection Platform (CWPP)

Définition du Gartner

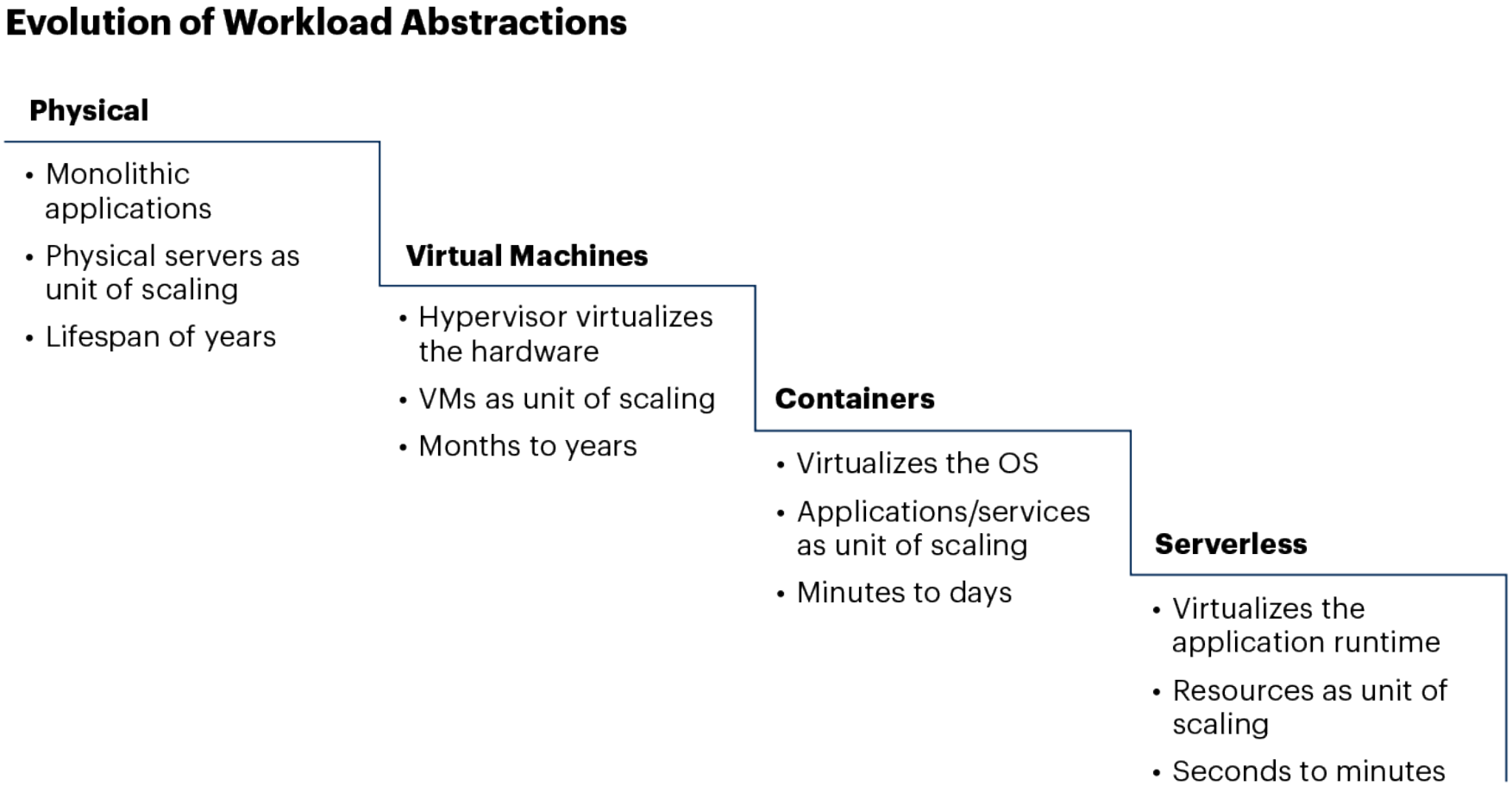
- CWPPs are workload-centric security products that **protect server workloads in hybrid, multicloud** data center environments
- CWPPs provide consistent visibility and control for **physical machines, virtual machines (VMs), containers and serverless workloads**, regardless of location
- CWPP offerings protect workloads using a combination of **system integrity protection, application control, behavioral monitoring, intrusion prevention and optional anti-malware protection at runtime**
- CWPP offerings should also include **scanning for workload risk proactively in the development pipeline**

Cloud Workload Protection Platform



Source : Gartner - 07/2021
Market Guide for Cloud Workload Protection Platforms

Abstraction des charges de travail



Source : Gartner - 07/2021
Market Guide for Cloud Workload Protection Platforms

Principales fonctionnalités

- Détection en exécution
  - Détecter et bloquer les comportements suspects pendant l'exécution des VM, conteneurs et microservices
- Gestion des vulnérabilités
  - Détecter les vulnérabilités liées ou non à l'OS à partir des images de conteneurs stockées dans les pipelines CI/CD et les registres avant le déploiement en production
- Sécurité réseau
  - Visualiser le trafic réseau à l'intérieur des VM, conteneurs et de Kubernetes et appliquer la segmentation réseau Kubernetes native
- Conformité
  - Valider la conformité des VM et conteneurs et assurer la surveillance de l'intégrité des fichiers
- Réponse aux incidents
  - Faciliter les investigations et la réponse aux incidents pour les VM, conteneurs et Kubernetes

Le problème n°1 dans le Cloud…

Gartner

« Through 2023, at least 99% of cloud security failures will be the customer's fault. »

L'utilisation d'outils (CSPM / SSPM) permettent d'atténuer une des menaces les plus courantes en matière de sécurité dans le cloud :

les erreurs de configuration !

Quels risques dans le Cloud ?

Selon vous, les facteurs suivants représentent-ils un risque faible, modéré ou fort en ce qui concerne l'utilisation du Cloud ?

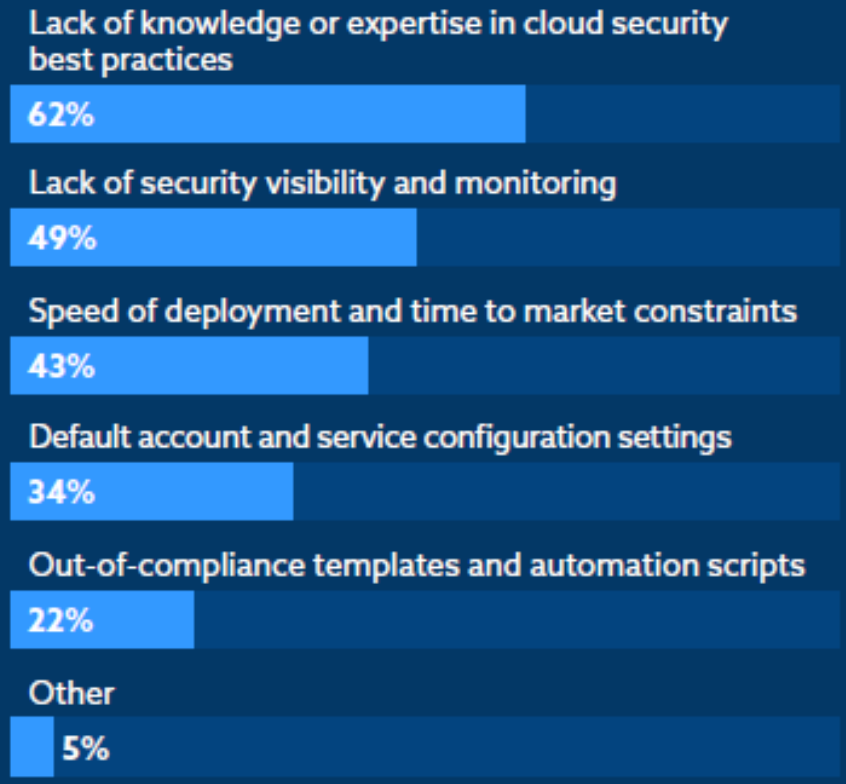
Rappel classement 2021	% Un risque fort	
1	51%	**Non maîtrise de la chaîne de sous-traitance de l'hébergeur**
2	49%	**Difficulté de contrôler les accès par des administrateurs de l'hébergeur**
3	43%	Expertise encore trop rare, attendue de la part des architectes et des administrateurs
	42%	Stockage des données en France/Europe mais assuré et/ou opéré par des prestataires étrangers où la loi du pays d'origine s'applique également
	40%	Difficulté de mener des audits (test d'intrusion, contrôle des configurations, visite sur site)
4	40%	Mauvaise visibilité de l'inventaire des ressources qu'il y a dans le cloud
	37%	Stockage des données dans des datacenters à l'étranger, hors du droit français
	36%	Non-effacement des données par l'hébergeur en fin de contrat (normal ou anticipé) alors que c'est prévu contractuellement
	35%	Non-maîtrise des paramètres de sécurité / chiffrement faible de la part de l'hébergeur
	35%	Maîtrise difficile de l'utilisation qui en est faite par les salariés de votre entreprise
	32%	Difficulté ou impossibilité d'alimenter le SIEM par des logs provenant du Cloud
	32%	Indisponibilité des données / de l'application due à une attaque de l'hébergeur
	32%	Forte fréquence des nouvelles versions mises en ligne avec des potentielles évolutions non contrôlées des principes ou paramètres de sécurité
5	31%	Confidentialité des données vis-à-vis de l'hébergeur
	31%	Non-effacement des données au cours de l'usage, les suppressions et purges opérées par le client n'étant pas réellement effectives
	29%	Attaque par rebond depuis l'hébergeur
	27%	Défaut de cloisonnement entre les différents clients de l'hébergeur
	27%	Traitement et exploitation des données par l'hébergeur à l'insu de ses clients
	26%	Propagation systémique des attaques et erreurs humaines qui surviendraient au niveau de l'hébergeur
	23%	Non-restitution des données par l'hébergeur en fin de contrat (normal ou anticipé) alors que c'est prévu contractuellement
	16%	Piégeage d'une application hébergée

Source : Baromètre de la cybersécurité des entreprises - CESIN (janvier 2023)

Causes des mauvaises configurations

Causes of Cloud Misconfigurations

The primary cause of misconfigurations in organizations was "lack of knowledge or expertise in cloud security best practices" (62%). This is unsurprising since this was noted as a major security barrier earlier. Somewhat more surprising was the second most selected response, "lack of security visibility and monitoring" (49%), since visibility wasn't noted as a primary barrier for resolving security concerns previously in the survey. This could indicate that organizations are not prioritizing resolving challenges around visibility and as a result, visibility is a leading cause of misconfigurations.



Source : CSA - 09/2021
The State of Cloud Security Risk, Compliance and Misconfigurations

Les mauvaises pratiques dans AWS

CloudGoat is used to deploy (and shutdown) a vulnerable set of AWS resources, designed to teach AWS security risks. We ensure that all vulnerabilities we include are only exploitable by someone with access to the given AWS account. This includes white listing access to sensitive resources to a personal IP address you supply where possible.

- **Une dizaine de services AWS mal configurés : EC2, S3, IAM, Lambda,...**
- **Plus d'une vingtaine de vulnérabilités exploitables**
  - Elévation de privilège, SSRF, clés API statiques dans code ou fichier conf, mauvaises conf de services,…

Source : https://rhinosecuritylabs.com/aws/cloudgoat-vulnerable-design-aws-environment

Cloud Security Posture Management

Principales fonctionnalités

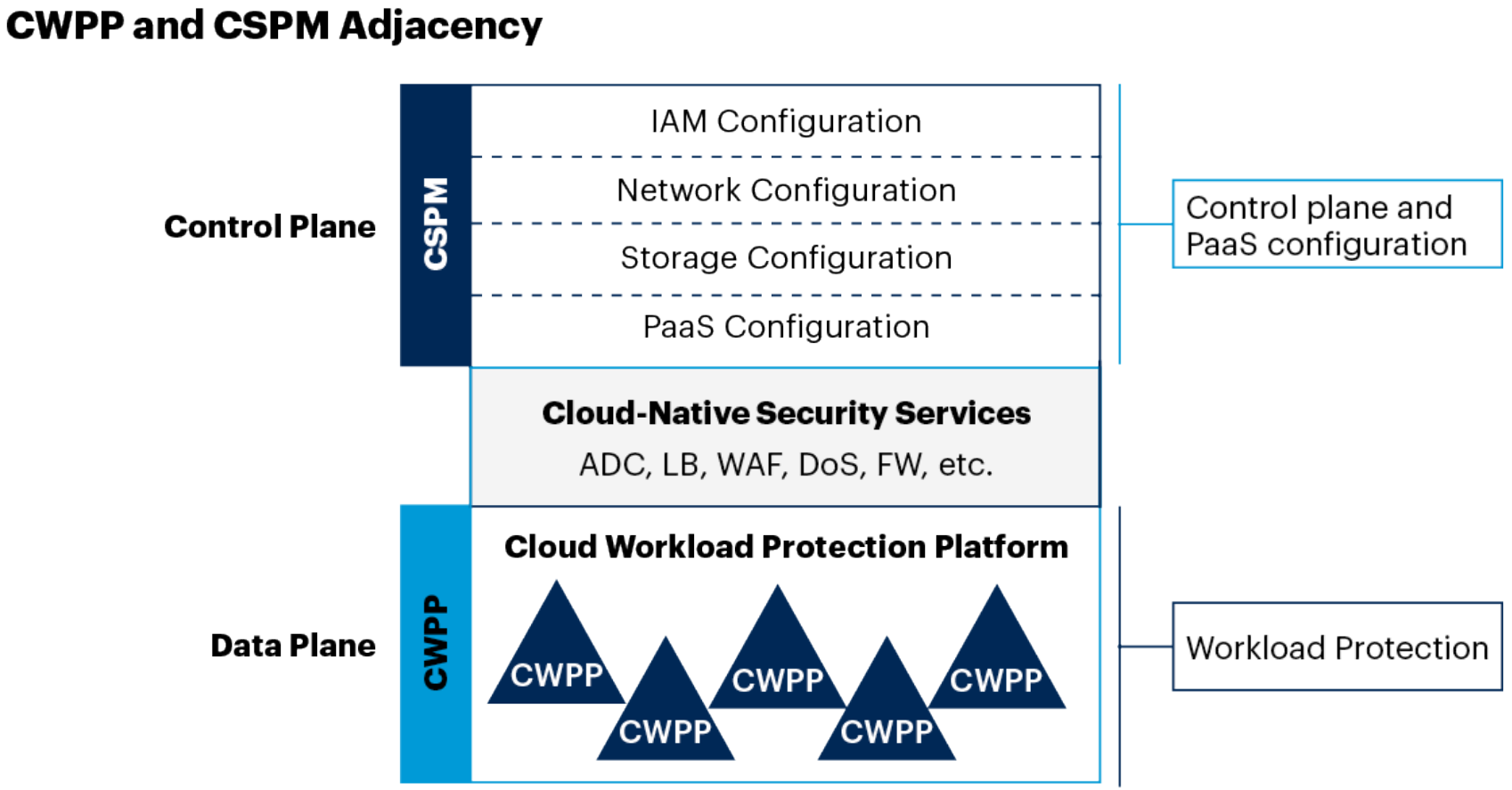
- **Inventaire des actifs cloud**
  - Un outil CSPM s'appuie généralement sur des intégrations API avec un ou plusieurs fournisseurs cloud afin de détecter automatiquement les ressources dans le cloud
- **Contrôle des configurations**
  - Un CSPM permet de détecter et parfois de corriger automatiquement les erreurs de configuration
  - Il maintient un inventaire des meilleures pratiques pour différentes configurations et services cloud
- **Gestion de la conformité**
  - Vérification des configurations par rapport à de nombreux référentiels
    - Benchmarks CIS, GDPR, HIPAA, ISO-27001, NIST-800-53, PCI-DSS, SOC 2, …

Exemples de solutions

- Palo Alto Networks (Prisma Cloud)
- Trend Micro (Cloud One Conformity)
- Zcaler (Zcaler CSPM)
- Orca (Orca Security)
- Etc..

Les benchmarks CIS

Complémentarité CSPM & CWPP



Source : Gartner - 07/2021
Market Guide for Cloud Workload Protection Platforms

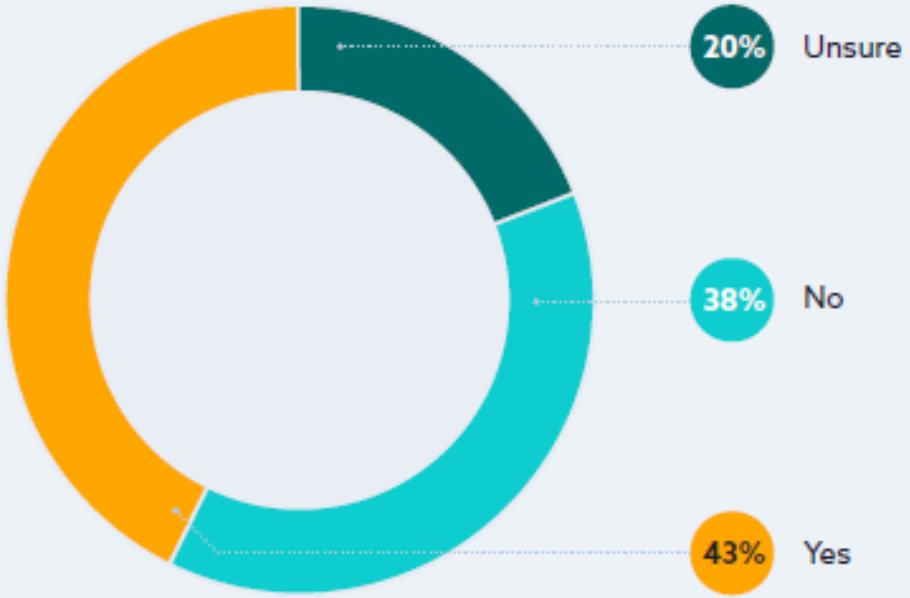
Mauvaises configurations SaaS (1/4)

Key Finding 1

SaaS misconfigurations are leading to security incidents

Security Incidents due to SaaS security misconfigurations within the past year

Reducing the timeline to detect and correct a SaaS security misconfiguration is crucial to preventing a security incident. Unfortunately for 43% of organizations, these misconfigurations did lead to a security incident. However, this could be as high as 63% due to the number of unsure respondents.



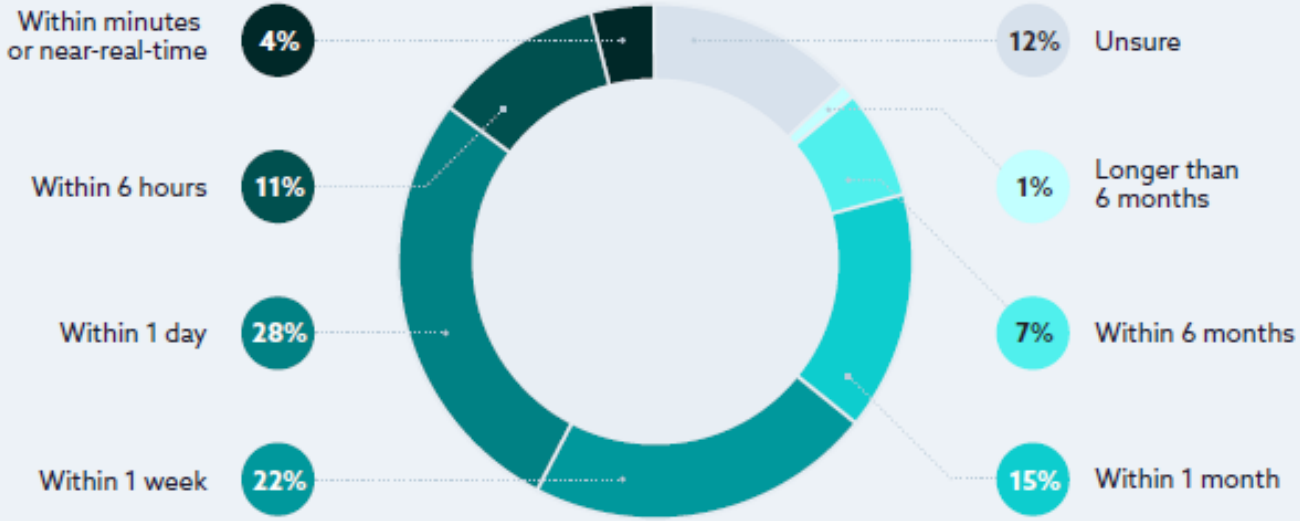
Source : CSA - 04/2022
2022 SaaS Security Survey Report

Mauvaises configurations SaaS (4/4)

Key Finding 4

Manually detecting and remediating SaaS misconfigurations is leaving organizations exposed

Correcting misconfigurations takes about one day (28%) or one week (22%) for most organizations. A nearly equal number of organizations take a month or more (23%). For users of SSPM, however, the timeline is reduced. Nearly ¾ of organizations using an SSPM can resolve the misconfiguration within one day.



Source : CSA - 04/2022
2022 SaaS Security Survey Report

Devenir Expert AWS

Débutant | **Avancé** | **Expert**

Devenir Expert Sécurité Cloud

Vendor-neutral

CISSP® Certified Information Systems Security Professional

Vendor-neutral

CCSK™ Certificate of Cloud Security Knowledge

ou

CCSP® Certified Cloud Security Professional

Vendor-specific

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

ou

aws certified Security Specialty

ou

Google Cloud Certified PROFESSIONAL CLOUD SECURITY ENGINEER

Certification CCSK ou CCSP ?

CCSK™ Certificate of Cloud Security Knowledge

CCSP® Certified Cloud Security Professional

	CCSK	CCSP
Organisme	Cloud Security Alliance (CSA)	(ISC)^2
Type de certification	Vendor-neutral	Vendor-neutral
Programme	100% Sécurité Cloud	20% Cybersécurité 80% Sécurité Cloud
Langues de l'examen	Anglais, Espagnol, Japonais	Anglais, Japonais
Type d'examen	En ligne (open book)	En centres agréés (ISC)^2 ou Pearson Vue (PVTC)
Nombre de questions	60	125
Durée	1,5 heures	3 heures
Score Requis	80%	70%
Difficulté	Moyenne (-)	Moyenne (+)
Prix	380 € (2 passages)	550 € (un passage)
Durée de validité	Illimitée	3 ans (30 CPE / an)
Frais annuels de maintien	Aucun	125 $ / an (0$ si déjà CISSP)
Pré-requis	Aucun	être déjà certifié CISSP ou avoir 5 ans d'expérience au moins 3 ans dans la Cybersécurité au moins 1 an dans un des 6 domaines du CBK (ou être CCSK)

2 formations chez VERISAFE

- ✓ **Formation sécurité Cloud**
- ✓ **Formation Prépa CCSK**
- ✓ **Token CCSK (2 passages)**

Les 5 mythes de la sécurité dans le Cloud

Mythe n°1

- Une infra IT « on-prem » sera toujours plus sécurisée

Mythe n°2

- Il n'y a aucun risque car mes données sont chiffrées

Mythe n°3

- Je suis rassuré car mon CSP est certifié ISO 27001

Mythe n°4

- La sécurité c'est essentiellement l'affaire de mon CSP

Mythe n°5

- Le graal de la sécurité du Cloud c'est un Cloud souverain

Cloud souverain ???

Cloudwatt FAILED

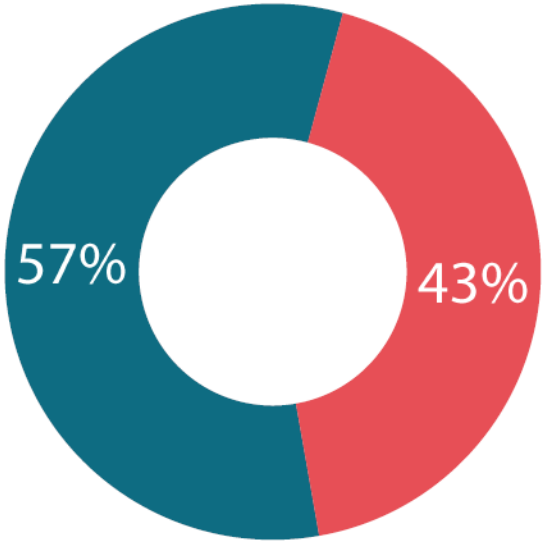
NUMERGY FAILED

GAIA-X FAILED

Souveraineté et Cloud de confiance

De nombreuses initiatives ont récemment vu le jour en matière de souveraineté et de Cloud de confiance. Vous sentez-vous concerné par ces sujets ?

Oui, c'est un sujet de préoccupation pour mon entreprise



Non, mon entreprise ne se sent pas concernée par ces sujets

Source : Baromètre de la cybersécurité des entreprises - CESIN (janvier 2023)

Cloud de confiance

À défaut d'une souveraineté totale, impossible en raison de l'avance technologique d'Amazon (AWS), Microsoft (Azure) et Google (GCP), le gouvernement français mise désormais sur une autre stratégie : un Cloud « encadré »

- Stratégie nationale pour le Cloud (mai 2021)
- Bruno Lemaire, Amélie de Montchalin et Cédric O

Cette stratégie sera mise en œuvre via la création d'un label, baptisé « Cloud de confiance » qui sera délivré aux prestataires remplissant un cahier des charges strict

- d'un point de vue technique : les fournisseurs doivent proposer des solutions sécurisées (SecNumCloud)
- d'un point de vue juridique : les solutions labellisées ne doivent pas être soumises à des règlementations autres que celles de la France et de l'Europe
  - En ligne de mire : Freedom Act, FISA 702, et CLOUD act

2 candidats au Cloud de confiance

BLEU
BEYOND THE CLOUD
Capgemini orange Microsoft

Bleu, le cloud de confiance de Capgemini et Orange à la sauce Microsoft

Dominique Filippone , publié le 27 Mai 2021

10 Réaction

Quelques jours après l'annonce du gouvernement de réorienter la stratégie nationale pour le cloud, Capgemini et Orange annoncent la création de Bleu. Visant le secteur public, les OIV et les OSE, elle fournira des services Microsoft 365 et Azure annoncés comme étant protégés de tout risque d'extraterritorialité.

Bleu poussera auprès de ses futurs clients incluant OIV et OSE des services Microsoft 365 et Azure. (crédit : Tumisu)

10 jours seulement après l'annonce du gouvernement de sa stratégie nationale pour le cloud passant par la délivrance du label cloud de confiance, Capgemini et Orange annoncent Bleu. Cette nouvelle société, créée conjointement par les deux acteurs français, devrait disposer de ses propres ressources et infrastructures ainsi que d'une autonomie opérationnelle complète. « Tous les services cloud, y compris le support client, seront entièrement opérés depuis la France par les ressources de la société et sous son contrôle », nous a expliqué un porte-parole de Capgemini.

La qualification de cloud de confiance n'est pas anodine et signifie que l'ANSSI est bien dans la boucle pour veiller au respect de plusieurs engagements de ce prochain entrant.

SUIVRE TOUTE L'ACTUALITÉ

Newsletter

Recevez notre newsletter comme plus de 50 000 professionnels de l'IT!

JE M'ABONNE

Plus de simplification pour gagner en efficacité

1 La dématérialisation au coeur de la simplification des processus

2 L'automatisation avec IA, une aide précieuse pour la simplification

3 ...

LIRE LE DOSSIER

S3NS

CLOUD COMPUTING

CLOUD DE CONFIANCE

Thalès et Google Cloud s'associent dans un cloud de confiance

le 12-10-2021
Par Cyrille Chausson

Thalès et Google Cloud ont annoncé la création d'une offre de Cloud de Confiance qui sera opérée par une société de droit français détenue majoritairement par Thalès. Le dispositif, encore loin d'être finalisé, traduit aussi un pan de la stratégie de Google Cloud de « territorialisation » de sa GCP (Google Cloud Platform).

Ils y voient une confiance dans l'alliance : Thalès et Google Cloud ont présenté cette semaine leur propre vision du « cloud de confiance » en annonçant une association stratégique. Après les certifications SecNumCloud de 3DS Outscale et d'OVHcloud d'un côté et le partenariat Capgemini, Orange et Microsoft au sein de la société Bleu d'un autre côté, Thalès et Google forment la 3e pièce du puzzle français du cloud dit souverain.

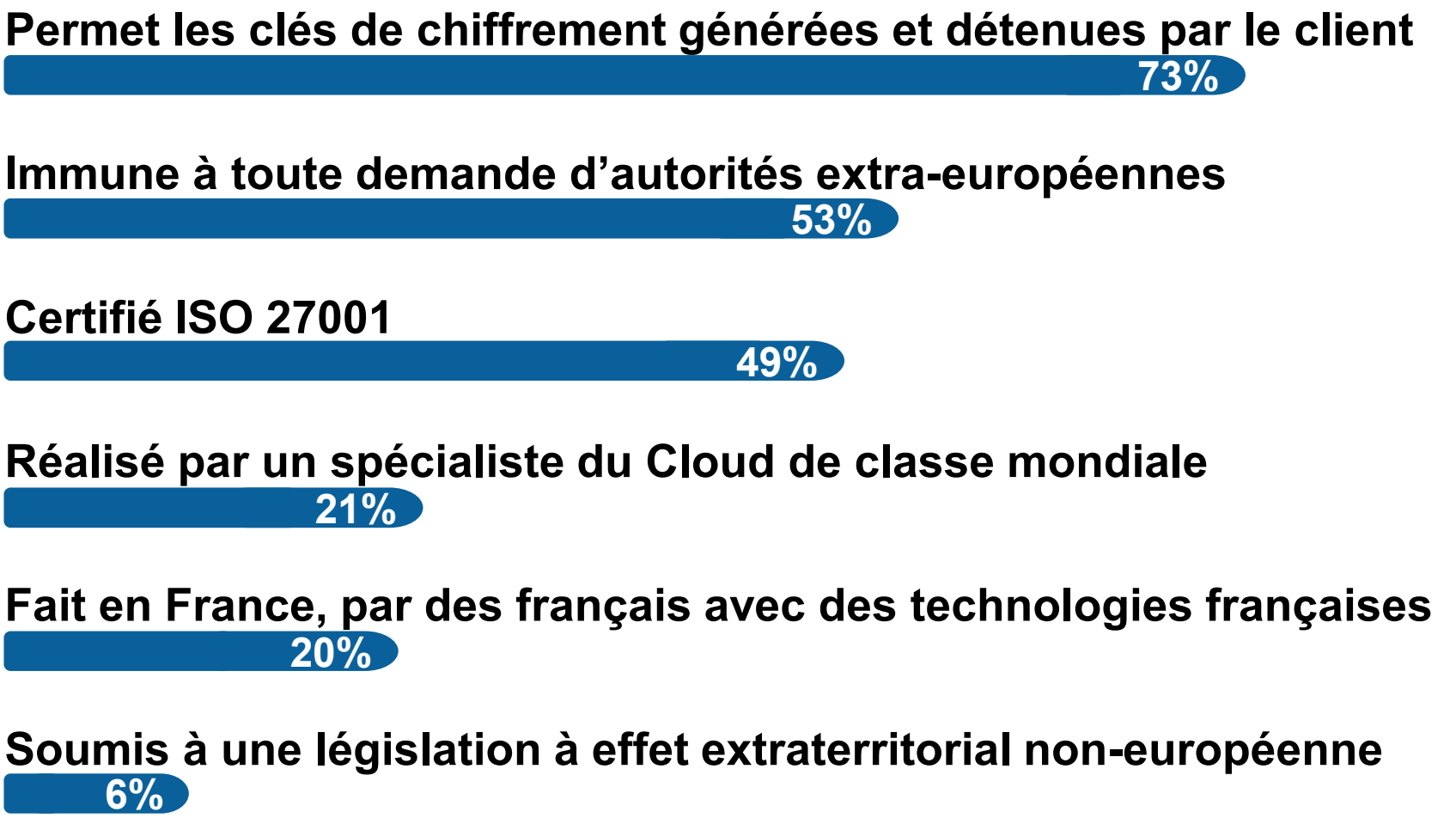
La labellisation « Cloud de Confiance » fait partie de la très récente doctrine « Cloud au Centre » du gouvernement français, qui entend privilégier le recours systématique au cloud pour ses usages internes et de se reposer sur des offres dites de confiance. Ce label s'appuie sur la certification SecNumCloud délivrée par l'ANSSI, à laquelle s'ajoute des critères juridiques dont l'ambition est d'immuniser les entreprises et les administrations des notions d'extra-territorialité imposées par certaines régulations étrangères, comme le Cloud Act. La réversibilité constitue également un critère essentiel.

Ainsi, le cloud de confiance de Thalès et de Google Cloud sera opéré par une entité tierce, détenue et contrôlée majoritairement par Thalès, ont expliqué Anthony Cirot et Marc Darmon, respectivement directeur général de Google Cloud France et directeur général adjoint, Systèmes d'information et de communication sécurisés, de Thalès. Cette société, de droit français, est encore en construction et n'a pas de nom. A vrai dire, la certification SecNumCloud est aussi en cours. Mais « *l'architecture a été présentée à l'Anssi et nous nous sommes arrangés pour qu'elle soit éligible* » avance Marc Darmon.

Email
Print
Facebook
Twitter
Linkedin

C’est quoi un Cloud de confiance ?

Quelles sont les caractéristiques réalistes indispensables d’un Cloud de confiance ?



Les principaux acteurs du IaaS/PaaS

Magic Quadrant pour l'infrastructure cloud et les services de plateforme

Worldwide IaaS Public Cloud Services Market Share 2020-2021 (Millions of U.S. Dollars)

Company	2021 Revenue	2021 Market Share (%)	2020 Revenue	2020 Market Share (%)	2020-2021 Growth (%)
Amazon	35,380	38.9	26,201	40.8	35.0
Microsoft	19,153	21.1	12,659	19.7	51.3
Alibaba	8,679	9.5	6,117	9.5	41.9
Google	6,436	7.1	3,932	6.1	63.7
Huawei	4,190	4.6	2,681	4.2	56.3
Others	17,056	18.8	12,697	19.8	34.3
Total	**90,894**	**100.0**	**64,286**	**100.0**	**41.4**

Source: Gartner (June 2022)

Source : Gartner

Que peut faire OVH face à AWS ?

CA 2022 d'OVH
788 millions d'euros (source OVH)

Dépense en R&D d'AWS en 2020 :
47,2 milliards de dollars (source : Bloomberg)

Comment lutter contre un concurrent qui investi 60 fois votre chiffre d'affaire en R&D ?

Qu’en pense l’ANSSI ?

Audition en commission des Affaires étrangères au Sénat

(5 octobre 2022)

Guillaume Poupard

« Nous ne sommes pas capables de faire du cloud de haut niveau en France aujourd'hui avec des technologies exclusivement françaises développées en France ».

"Sur le cloud de confiance, on ne parle pas de souveraineté absolue."

Merci de votre attention !

Rejoignez-moi sur LinkedIn

https://www.linkedin.com/in/boris-motylewski

Replay & slides du Webinaire

https://www.securitecloud.com/actualites/webinaire-securite-dans-le-cloud