X-IAI WEBINAR

Sécurité dans les environnements Cloud

22 juin 2021

Panélistes

Delmat NOUMEDEM

Freelance/DB2N consulting

Modérateur

Guy Bertrand KAMGA

Principal Multi-Cloud Security Advisor / NOKIA

Animateur

Edmond FOTSO

Sr. IT Manager (APPSW/INFOSEC) / NMS Imaging
Adjunct Professor (Cybersecurity) / Montgomery Colle

Co-Animateur

Esther DZALE

Responsable Pôle Numérique/ INRAE

Contributeur

Sommaire

INTRODUCTION

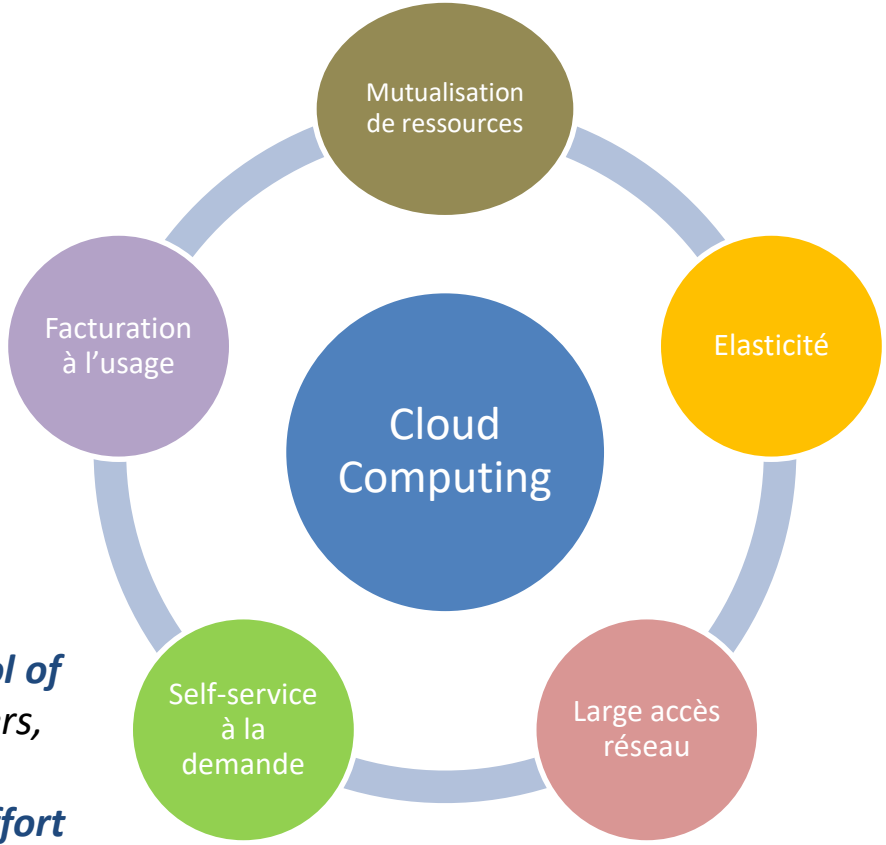
C’est quoi le Cloud ?

Informatique dans le nuage:
Services informatiques (serveurs, stockage, réseau, logiciels) accessibles via Internet (nuage)

Définition technique (NIST)

“*Cloud computing is a model for enabling* ***ubiquitous****,* ***convenient****,* ***on-demand network access*** *to a* ***shared pool of configurable computing resources*** *(e.g., networks, servers, storage, applications, and services) that can be* ***rapidly provisioned and released*** *with* ***minimal management effort*** *or service provider interaction*.”

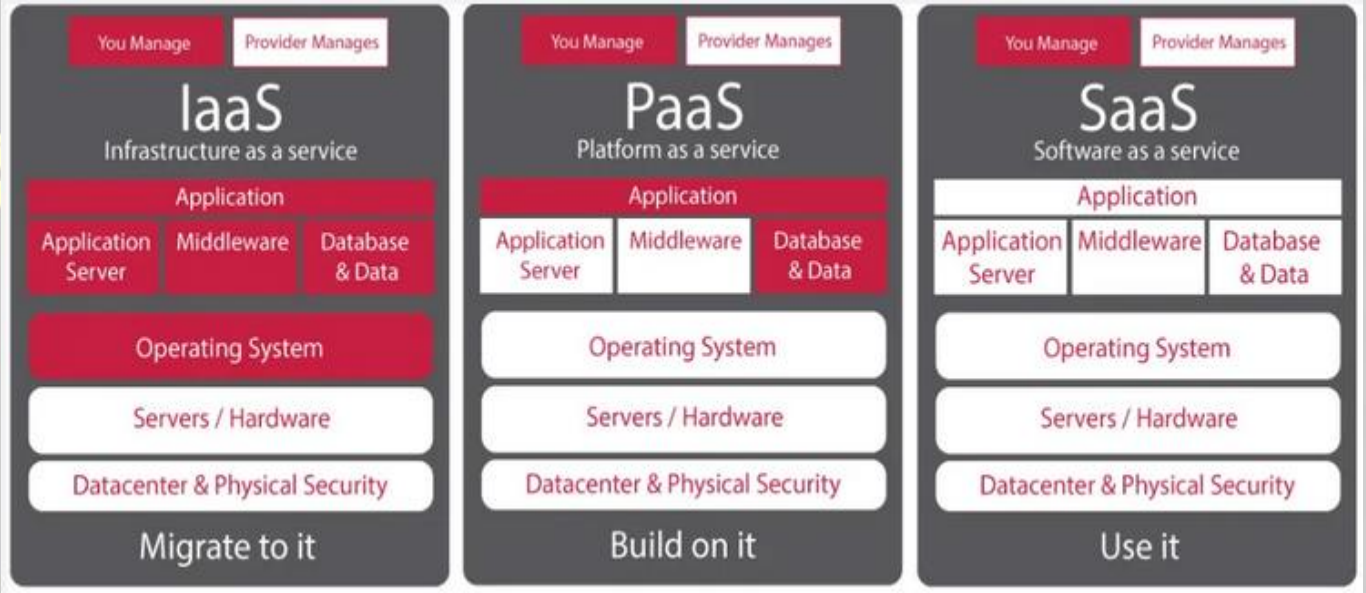
Principales caractéristiques



Cloud: typologie de solutions

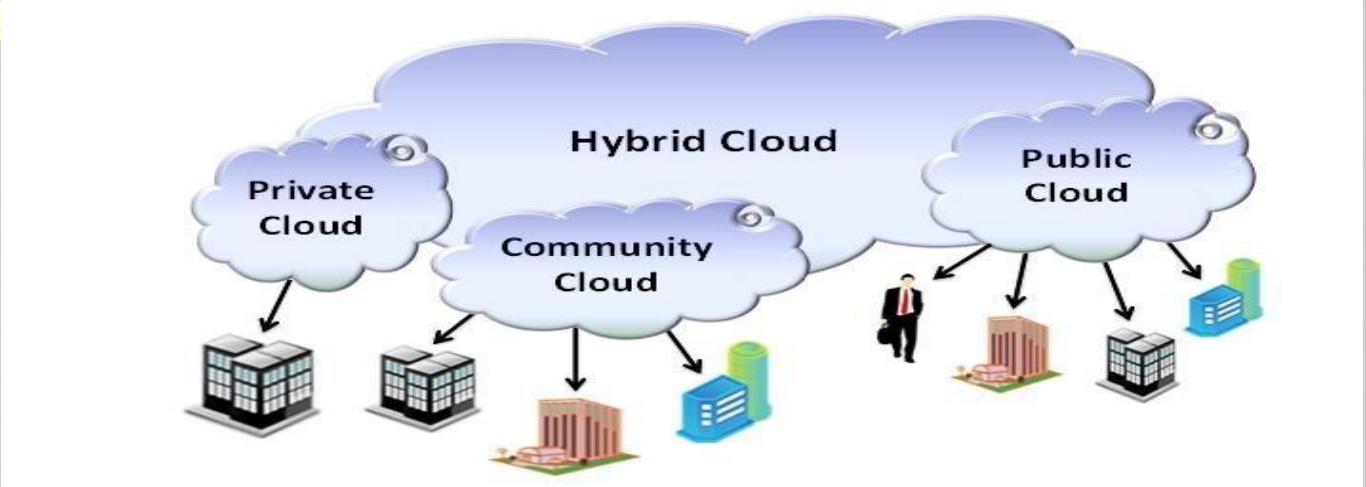
3 principaux modèles de service

- ✓ IaaS
- ✓ PaaS
- ✓ SaaS



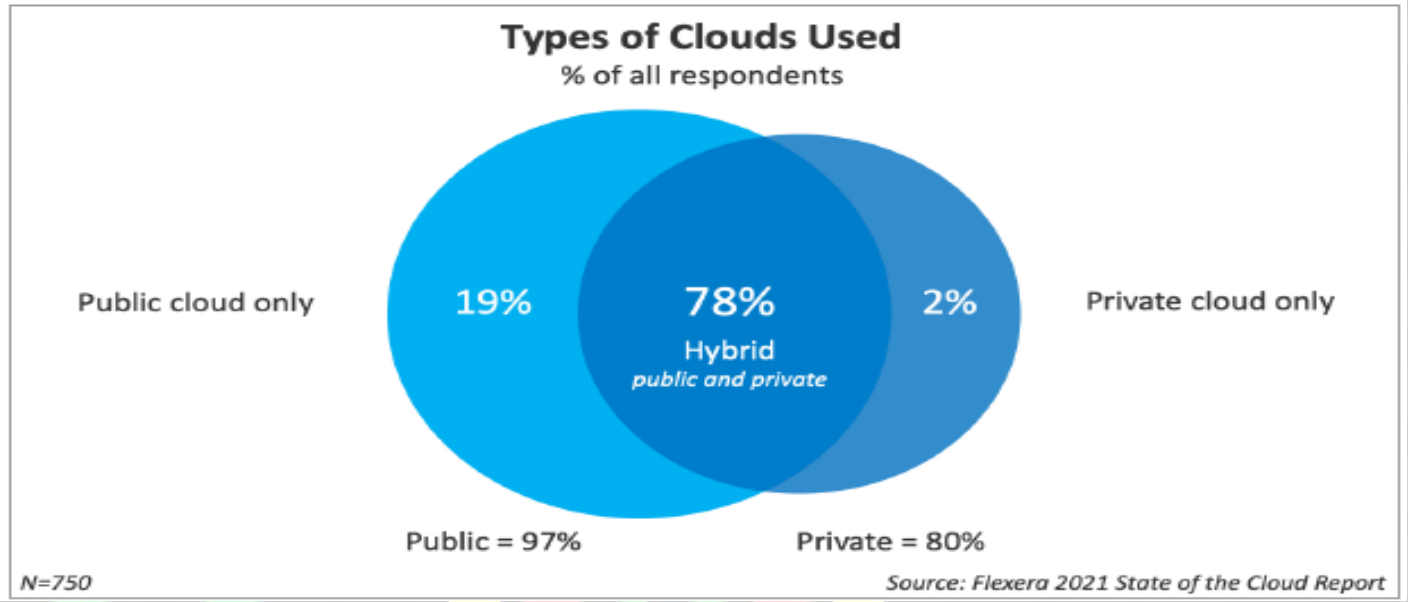
4 principaux modèles de déploiement

- Public
- Privé (Interne ou Externe)
- Communautaire
- Hybride

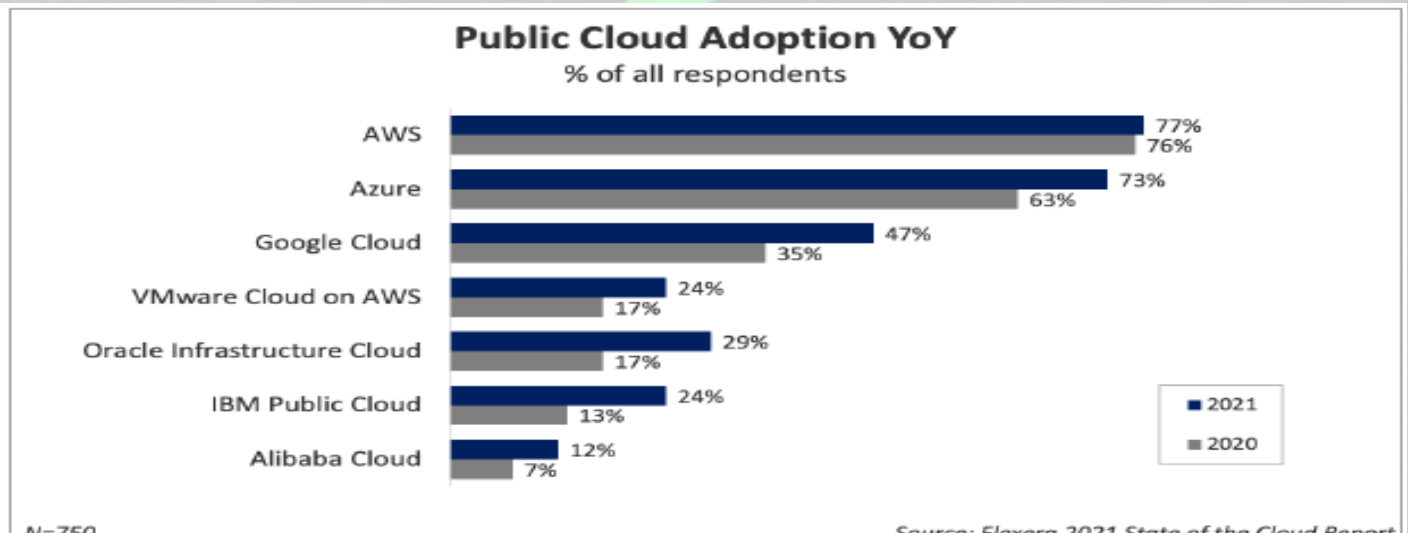


Cloud: typologie de solutions

- Le cloud public ne fait plus peur
- Le modèle hybride reste le standard



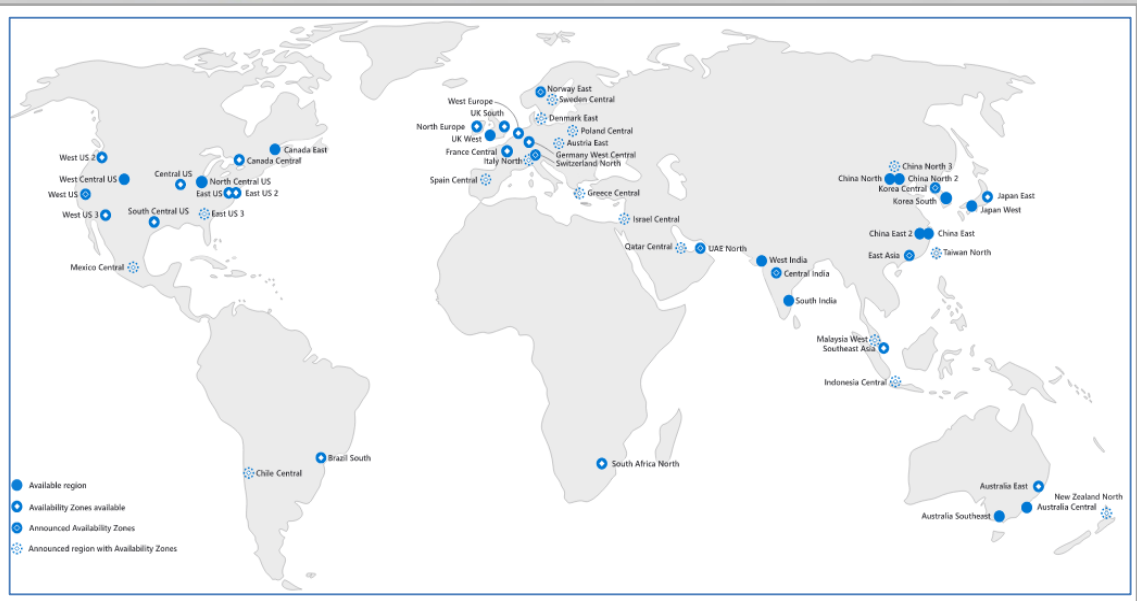
- AWS leader depuis 2006 mais challengé par Azure
- Forte domination des acteurs USA



Cloud: Les géants s'installent en Afrique

Microsoft Azure

- ✓ Disponible depuis 2019
- ✓ 1 région en Afrique du Sud (Johannesburg) + 1 autre en cours au Cap
- ✓ 3 zones de disponibilité



Amazon Web Services (AWS)

- ✓ Disponible depuis 2020
- ✓ 1 région en Afrique du Sud (Le Cap)
- ✓ 3 zones de disponibilité

Cloud: brique essentielle de la transformation numérique des entreprises

- **Types d'entreprise**: startup, PME, grandes entreprises, administrations publiques, etc.
- **Domaines d'activité**: Santé, Finance, Commerce, Distribution, Transport, Education, Télécommunication, etc.
- **Types de cas d'utilisation**: Applications métier, Big Data et analytique, Conteneurs & micro services, Développement et test, Hébergement web, IoT, Machine Learning, Migration de BDD/DC, Stockage, etc.

Cloud: Bénéfices vs Freins d'adoption

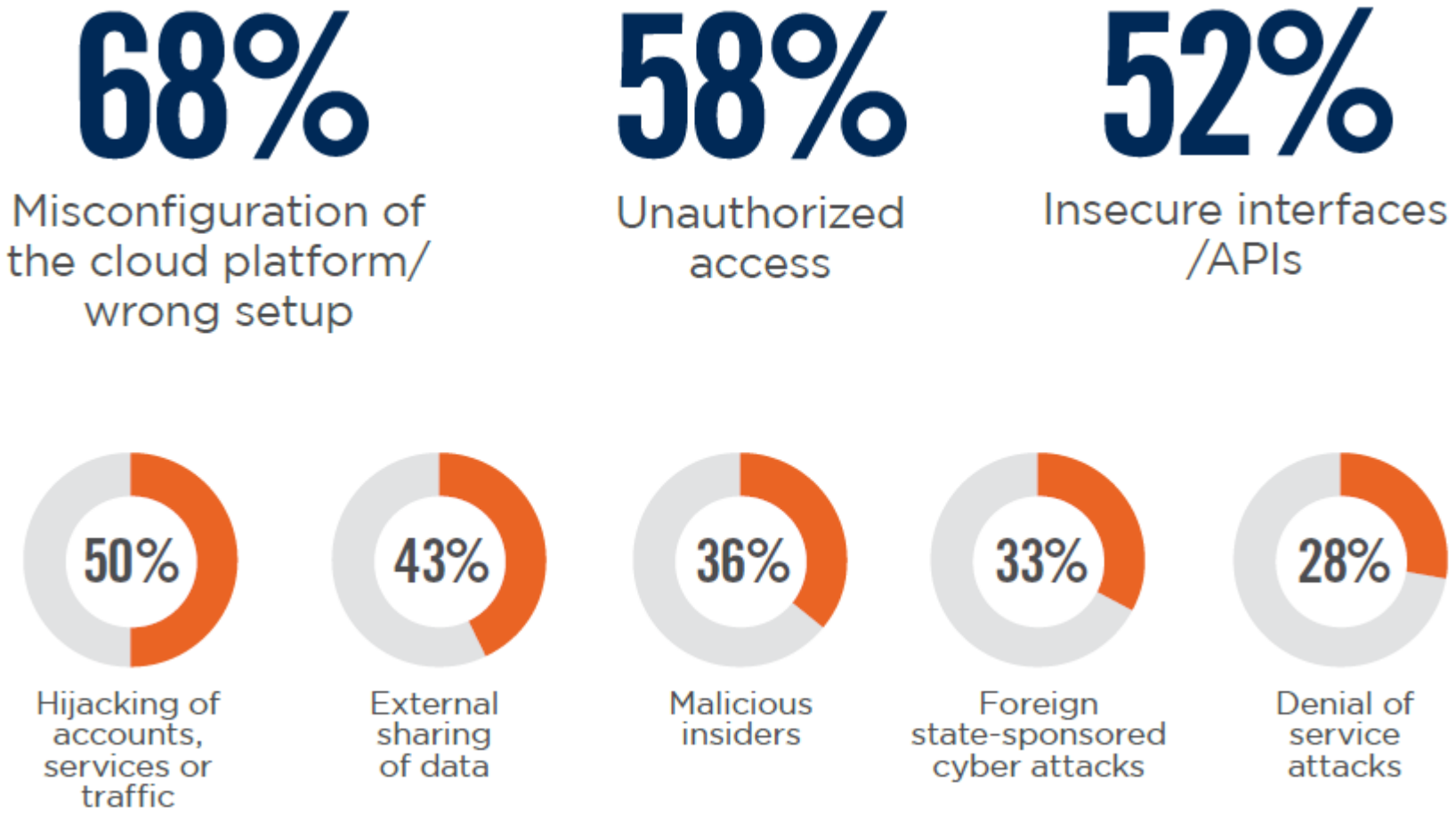
Bénéfices
Scalabilité/Flexibilité
Haute disponibilité
Agilité accrue
Rapidité de déploiement
OPEX vs CAPEX
Réduction des coûts
Large couverture géographique (collaboration, mobilité, etc.)

Freins
Sécurité
Gestion des coûts
Gouvernance
Conformité et souveraineté
Manque de personnels qualifiés
Réutilisation des licences
Migration des solutions existantes
Gestion du multicloud

Comment adresser les problèmes de **sécurité** et de **conformité** pour tirer le maximum de bénéfices des environnements cloud ?

SÉCURITÉ DANS LE CLOUD

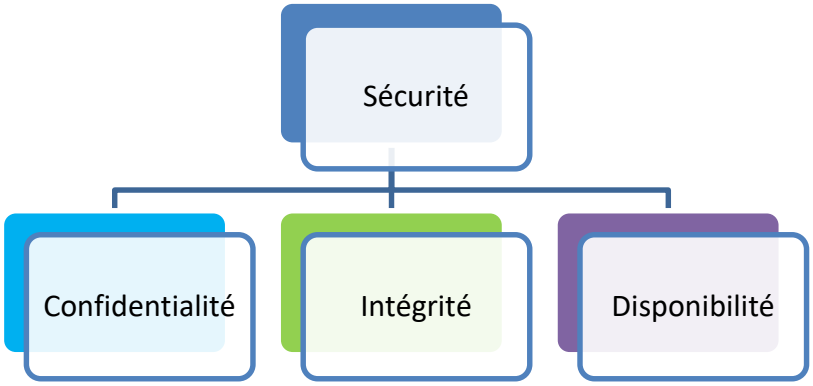
Sécurité dans le cloud
Principales menaces

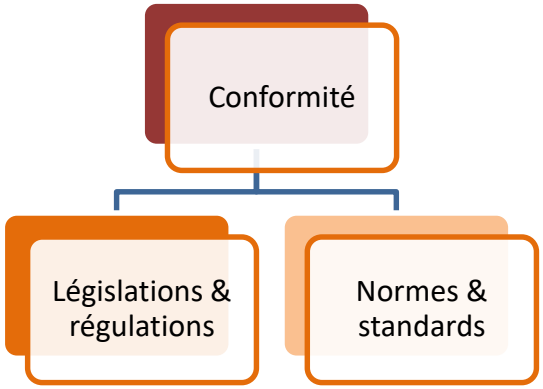


Source: Cybersecurity Insiders 2020 Cloud Security Report

Sécurité dans le cloud

Objectifs et délimitation des responsabilités





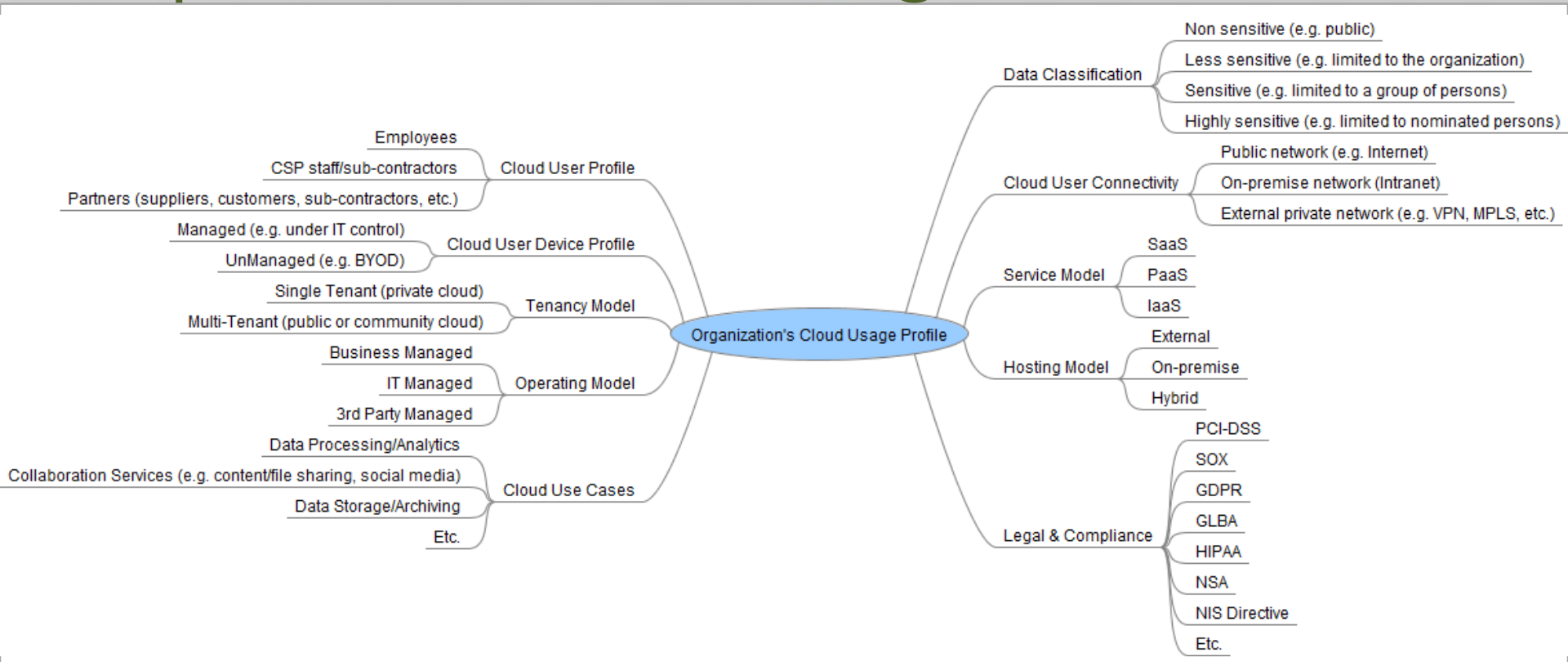
Responsabilité par modèle de service cloud	IaaS (Infrastructure as a Service)	PaaS (Platform as a Service)	SaaS (Software as a Service)
Gouvernance sécurité, Risque & conformité			
Sécurité des données			
Sécurité des applications			
Sécurité des plateformes			
Sécurité des infrastructures			
Sécurité physique			

Responsabilité du client

Responsabilité partagée

Responsabilité du fournisseur

Sécurité dans le cloud
Quel contexte d'usage?



Comprendre la stratégie cloud de l'entreprise

Définir la stratégie de sécurité adaptée

Implémenter la stratégie de sécurité

Amélioration continue de la stratégie de sécurité

Sécurité dans le cloud

Définir & implémenter une stratégie adaptée

Processus	Technologique	Humain
Gouvernance des données, de la sécurité et de la conformité	Gestion des identités et des accès	Clarification des rôles et responsabilités
Élaboration et maintenance des bonnes pratiques	Protection des données au repos, à l'usage et lors des transmissions	Mix des compétences internes et externes
Gestion des risques et des incidents	Gestion des clés de chiffrement	Sensibilisation et formation en fonction des rôles
Evaluation & choix des fournisseurs et partenaires	Protection des applications, des postes clients, des serveurs et du réseau	Centre d'excellence cloud multidisciplinaire (architecture, sécurité, réseau, système, etc.)
Culture DevSecOps	Supervision et gestion de la posture sécurité en continue	Attraction et rétention des talents (hauts potentiels)
	Continuité de service et reprise après panne ou sinistre	
	Gestion des incidents	
	Gestion des vulnérabilités et des patches	
	Gestion des configurations et des changements	
	Prévention et détection des intrusions	

Principes fondamentaux:

- ☑ Fédération d'identité
- ☑ Sécurité en profondeur
- ☑ Sécurité et conformité by design
- ☑ Zéro Trust
- ☑ Automatisation des bonnes pratiques

Cloud Security

Cloud-Augmented Security Services

SECaaS
Security as a Service
Clients may wish to outsource security for various reasons: • In-house security may be too expensive. • In-house security may be too difficult to maintain.
Enterprise can function optimally while remaining protected
Some providers give clients tools to actively improve their security
Security tools can come in several forms
SECaaS providers - Services: • Hash Matching. • Cloud Sandboxing. • Content Filtering.
In SECaaS, you don't have complete control over your own security.

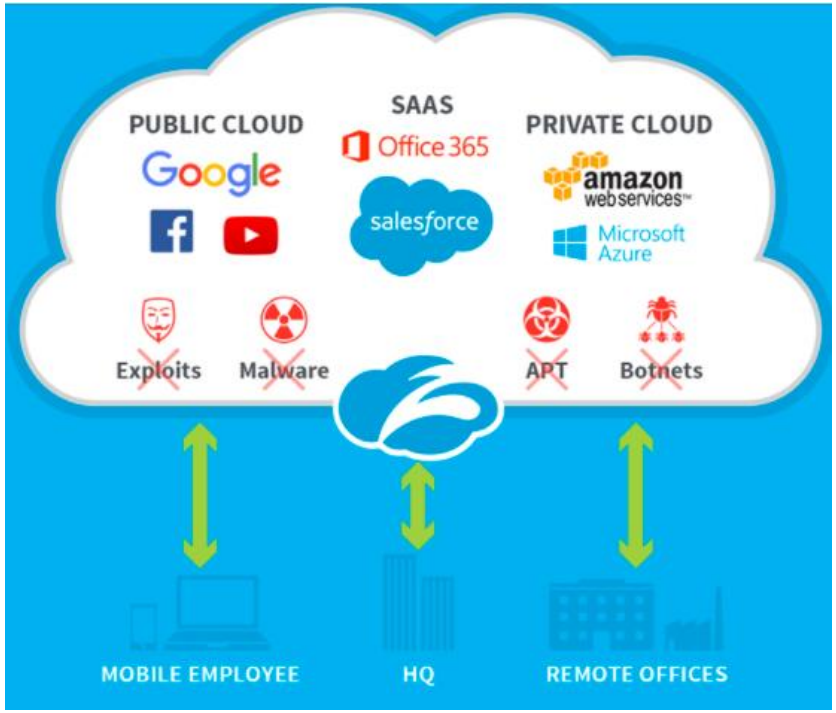


Image Source: airloom.com

<u>Examples of SECaaS/MSS Providers:</u>

- Cloudflare, Imperva,
- SecureWorks, IBM,
- HP, Trustwave, and many more.

Cloud Security
Cloud-Augmented Security Services

CASB

Cloud Access Security Brokers

Four pillars of CASB:

1. Visibility
2. Compliance
3. Data Security
4. Threat Protection

Many CASB security features may include:

- Cloud governance and risk assessment
- Data loss prevention
- Threat prevention
- Configuration auditing
- Malware detection
- Data encryption and key management
- SSO and IAM integration
- Contextual access control

How does a CASB work?:

1. Discovery
2. Classification
3. Remediation

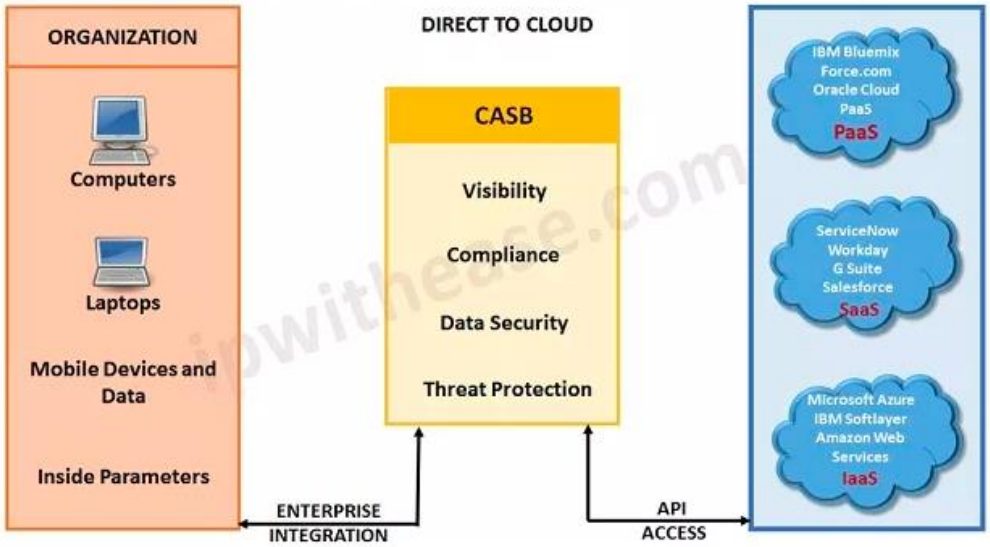
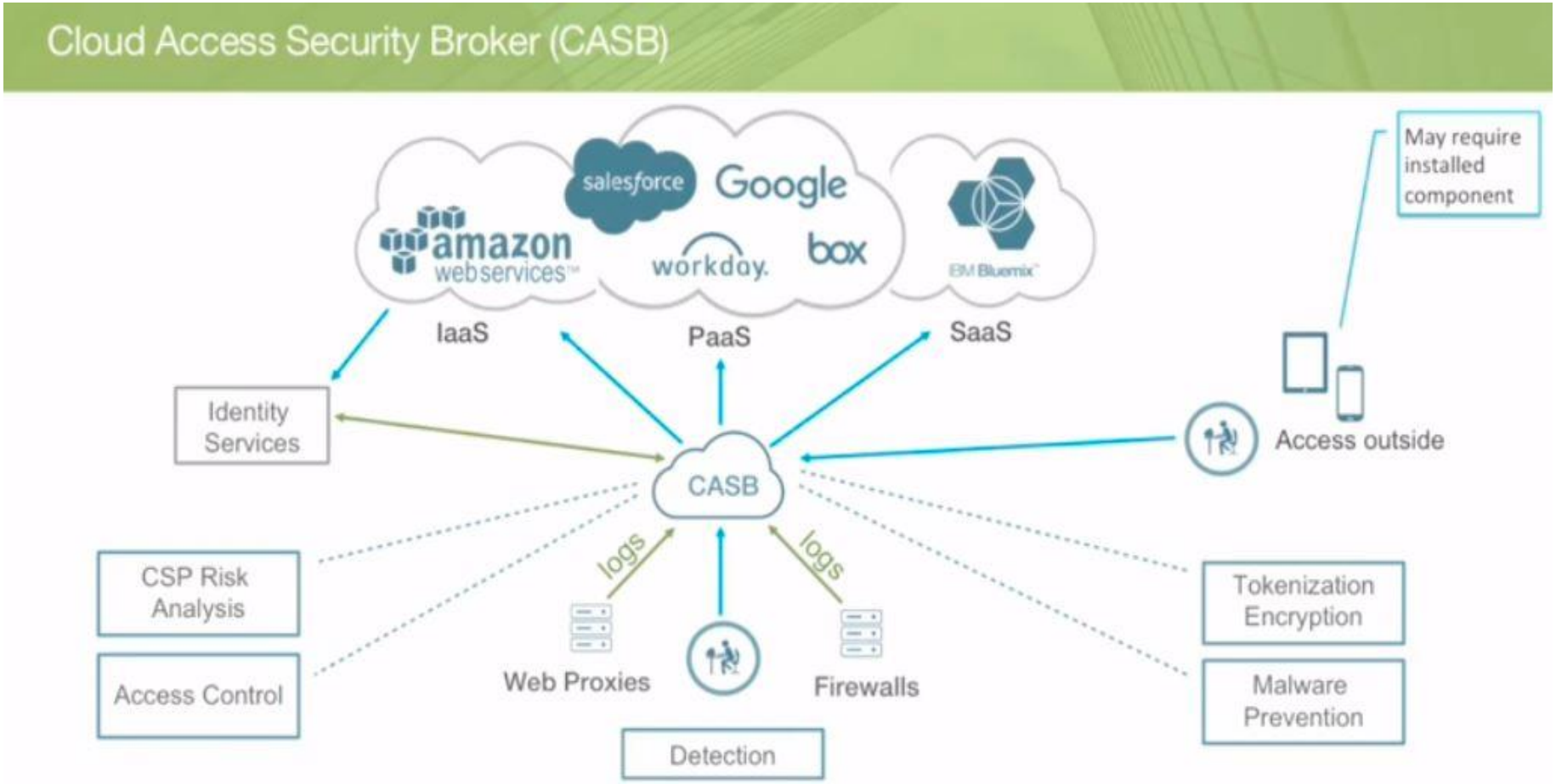


Image Source: ipwithease.com

Cloud Security

Cloud-Augmented Security Services



Cloud Security

Cloud-Augmented Security Services

CASB

Cloud Access Security Brokers

Provide organization with greater visibility into cloud-based usage.

Enable the organization to apply access control, DLP, etc., to cloud traffic.

Forward proxy mode sites near client network:

- Requires device configuration.
- Inspects traffic in real-time, even unsanctioned traffic.

Reverse proxy mode sites near cloud network

- Doesn't require device configuration.
- Inspects only sanctioned traffic.

API mode:

- Operates out-of-band.
- Uses specific app's API when applying security policies to traffic.

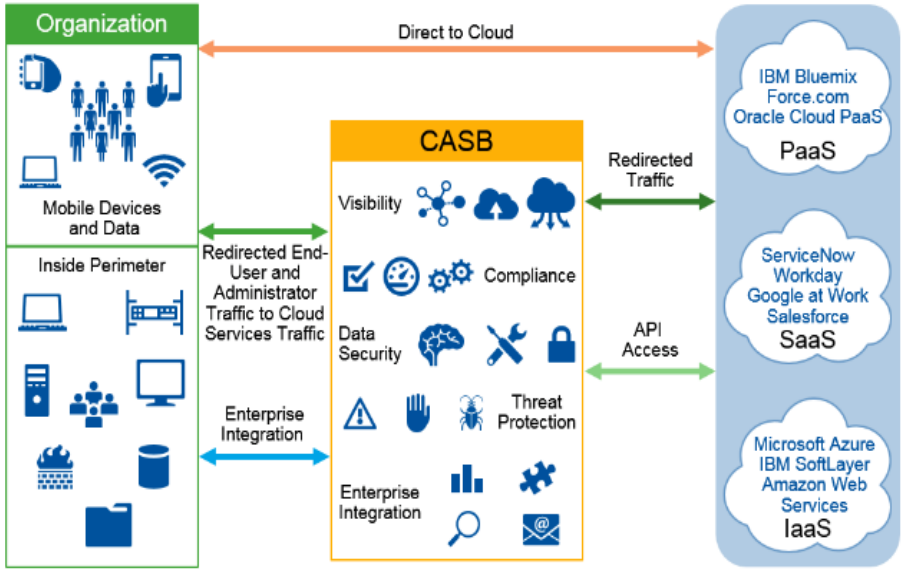


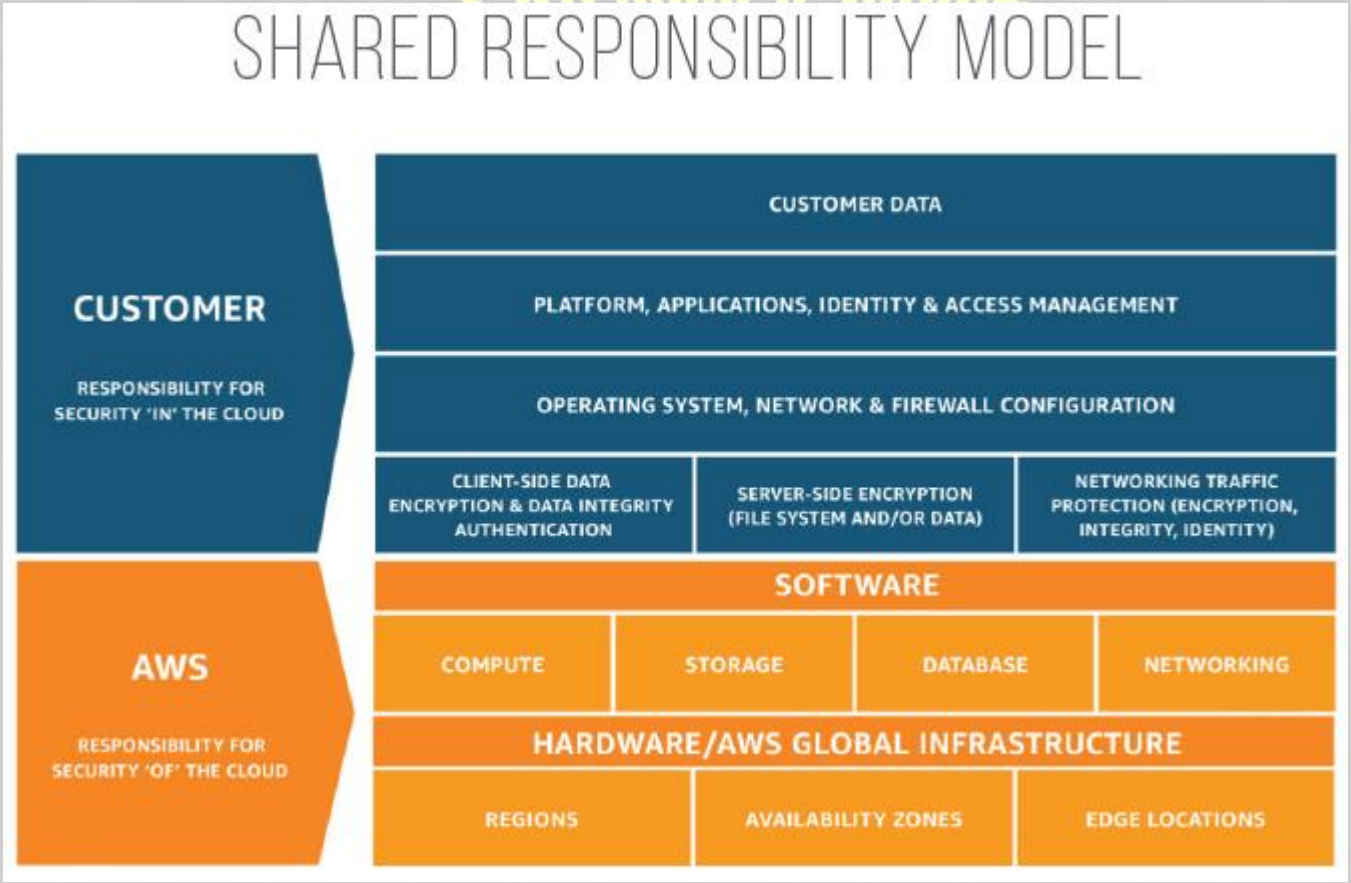
Image Source: managedmethods.com

Examples of CASB solutions:

- Blue Coat (Symantec)
- SkyHigh Networks (MacAfee)
- Forcepoint
- Microsoft Cloud App Security
- Cisco Cloudlock

Sécurité dans le cloud

Cas d'AWS



Sécurité dans le cloud

Services sécurité dans AWS

Catégorie	Cas d'utilisation	Service AWS
Identity & Access Management	Gérer de manière sécurisée l'accès aux services et aux ressources	**AWS Identity & Access Management (IAM)**
	Service d'authentification unique (SSO) cloud	**AWS Single Sign-On**
	Gérer des identités pour vos applications	**Amazon Cognito**
	Version gérée de Microsoft Active Directory	**AWS Directory Service**
	Service simple et sécurisé pour le partage de ressources AWS	**AWS Resource Access Manager**
	Gouvernance et gestion centralisées dans les comptes AWS	**AWS Organizations**
Détection	Centre de sécurité et de conformité unifié	**AWS Security Hub**
	Service de détection de menaces gérées	**Amazon GuardDuty**
	Analyse de la sécurité des applications	**Amazon Inspector**
	Enregistrer et évaluer les configurations de vos ressources AWS	**AWS Config**
	Suivre l'activité des utilisateurs et l'utilisation des API	**AWS CloudTrail**
	Gestion de la sécurité des appareils IoT	**AWS IoT Device Defender**

Sécurité dans le cloud

Services sécurité dans AWS

Protection des infrastructures	Sécurité du réseau	AWS Network Firewall
	Protection contre les DDoS	AWS Shield
	Filtrage du trafic web malveillant	AWS Web Application Firewall (WAF)
	Gestion centrale des règles de pare-feu	AWS Firewall Manager
Protection des données	Identification et protection de vos données sensibles quelle que soit l'échelle	Amazon Macie
	Gestion et stockage des clés	AWS Key Management Service (KMS)
	Stockage matériel de clés à des fins de conformité réglementaire	AWS CloudHSM
	Allocation, gestion et déploiement de certificats SSL/TLS publics et privés	AWS Certificate Manager
	Rotation, gestion et extraction de secrets	AWS Secrets Manager
Réponse aux incidents	Enquêter sur d'éventuels problèmes de sécurité	Amazon Detective
	Reprise après sinistre rapide, automatisée et rentable	CloudEndure Disaster Recovery
Conformité	Portail gratuit et en libre service pour un accès à la demande aux rapports de conformité d'AWS	AWS Artifact
	Auditez en continu votre utilisation d'AWS pour simplifier vos évaluations de risques et de conformité	AWS Audit Manager

CADRES DE RÉFÉRENCE DE LA CONFORMITÉ DANS LE CLOUD

Cadres de référence de la conformité dans le cloud

Global
- Conformité réglementaire dans Azure Policy (préversion)
- Référence CIS
- Attestation CSA STAR
- Certification CSA STAR
- Auto-évaluation CSA STAR
- SOC 1
- SOC 2
- SOC 3

Services financiers
- 23 NYCRR Part 500 (États-Unis)
- AFM et DNB (Pays-Bas)
- AMF et ACPR (France)
- APRA (Australie)
- CFTC 1.31 (États-Unis)
- EBA (UE)
- FCA et PRA (Royaume-Uni)

Automobile, énergie, multimédia et télécommunications
- CDSA
- DPP (Royaume-Uni)
- FACT (Royaume-Uni)
- MPA
- GSMA
- NERC (États-Unis)
- TISAX

Global
- ISO 20000-1
- ISO 22301
- ISO 27001
- ISO 27017
- ISO 27018
- ISO 27701
- ISO 9001
- WCAG

Services financiers
- FINRA 4511 (États-Unis)
- FISC (Japon)
- FSA (Danemark)
- GLBA (États-Unis)
- KNF (Pologne)
- MAS et ABS (Singapour)
- NBB et FSMA (Belgique)

Régional - Amériques
- PDPA (Argentine)
- Législation canadienne relative à la protection des données personnelles
- US CCPA

Gouvernement américain
- CJIS
- CNSSI 1253
- DFARS
- DoD IL2
- DoD IL4
- DoD IL5
- DoD IL6
- DoE 10 CFR Part 810

Services financiers
- OSPAR (Singapour)
- PCI 3DS
- PCI DSS
- RBI et IRDAI (Inde)
- SEC 17a-4 (États-Unis)
- SEC Regulation SCI (États-Unis)
- SOX (États-Unis)

Régional - Asie/Pacifique
- IRAP (Australie)
- China GB 18030
- China DJCP (MLPS)
- China TCS
- India MeitY
- Japan CS Gold Mark
- My Number Act (Japon)
- Korea K-ISMS
- New Zealand ISPC
- Singapore MTCS

Gouvernement américain
- FedRAMP
- FERPA
- FIPS 140-2
- IRS 1075
- ITAR
- NIST 800-171
- NIST 800-53
- NIST CSF

Santé et sciences de la vie
- ASIP HDS (France)
- GxP (FDA 21 CFR Partie 11)
- HIPAA (États-Unis)
- HITRUST
- MARS-E (États-Unis)
- NEN 7510 (Pays-Bas)

Régional - EMEA
- EU EN 301 549
- ENISA IAF
- EU GDPR
- Clauses de modèle (UE)
- Allemagne C5
- BIR 2012 (Pays-Bas)
- Espagne ENS Niveau élevé
- UAE DESC
- UK Cyber Essentials Plus
- UK G-Cloud
- UK PASF

BIBLIOGRAPHIE :
Pour aller plus loin…

… Pour poursuivre le sujet, vous pouvez vous référer aux liens ci-après:

1. Cybersecurity Insiders 2020 Cloud Security Report
2. Flexera 2021 State of the Cloud Report
3. Agile & Effective Cloud Security Strategy: A Cloud Usage Profile based approach
4. AWS Cloud Adoption Framework
5. Azure Cloud Adoption Framework
6. Google Cloud Adoption Framework
7. Opportunities in Security as a Service
8. What Is a CASB?
9. 2020 Gartner Magic Quadrant for Cloud Access Security Brokers
10. ISO/IEC 27018:2019 - Information technology — Security techniques
11. Expansion des clouds: les nuages arrivent en Afrique

X-IAI WEBINAR

Institut Africain d'Informatique

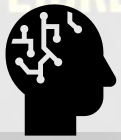
ASSOCIATION DES ANCIENS ETUDIANTS CAMEROUNAIS
DE L'IAI LIBREVILLE

X-IAI WEBINAR

Une pause de 45mn sur un sujet d'actualité

Prochaines dates…

Date	Horaire Pari	Theme	Intervenant(s)
Mardi 22 Juin	21H	Sécurité dans des environnements cloud	Guy Bertrand Kamga
Jeudi 22 juillet	21H	(Open) data	Esther Dzale
Jeudi 12 Aout	21H	Knowledge with an Entrepreneur : "Lead and Inspire each Other"	Guy Roger Gatcha
mardi 9 Septembre	12H30	Developpement Personnel	Christelle Rentch
Jeudi 23 Septembre	21H	Modéles d'évaluation des AO au Cameroun (Administratifs, Technique et Financier)	Oumarou / Mamoudou
Samedi 09 Octobre	21H	Capital-Risque et financement des startups	Gaston Feulifack
Jeudi 21 Octobre	21H	Cybersecurité dans les SI Bancaires	Francois Roger Tiomena
Samedi 06 Novembr	21H	management des activités et évaluation de performances de la DSI	Gaston Feulifack
Jeudi 18 Novembre	21H	SAP	Marie Paule Aboudi



Merci pour votre participation!