Cours Electif ESGI3 :
SECURITE & INFRASTRUCTURE

La sécurité – Un des fondamentaux du Cloud Computing

Le Cloud : Des rappels

ESGI3 - 2022- 2023

C’est quoi le Cloud ?

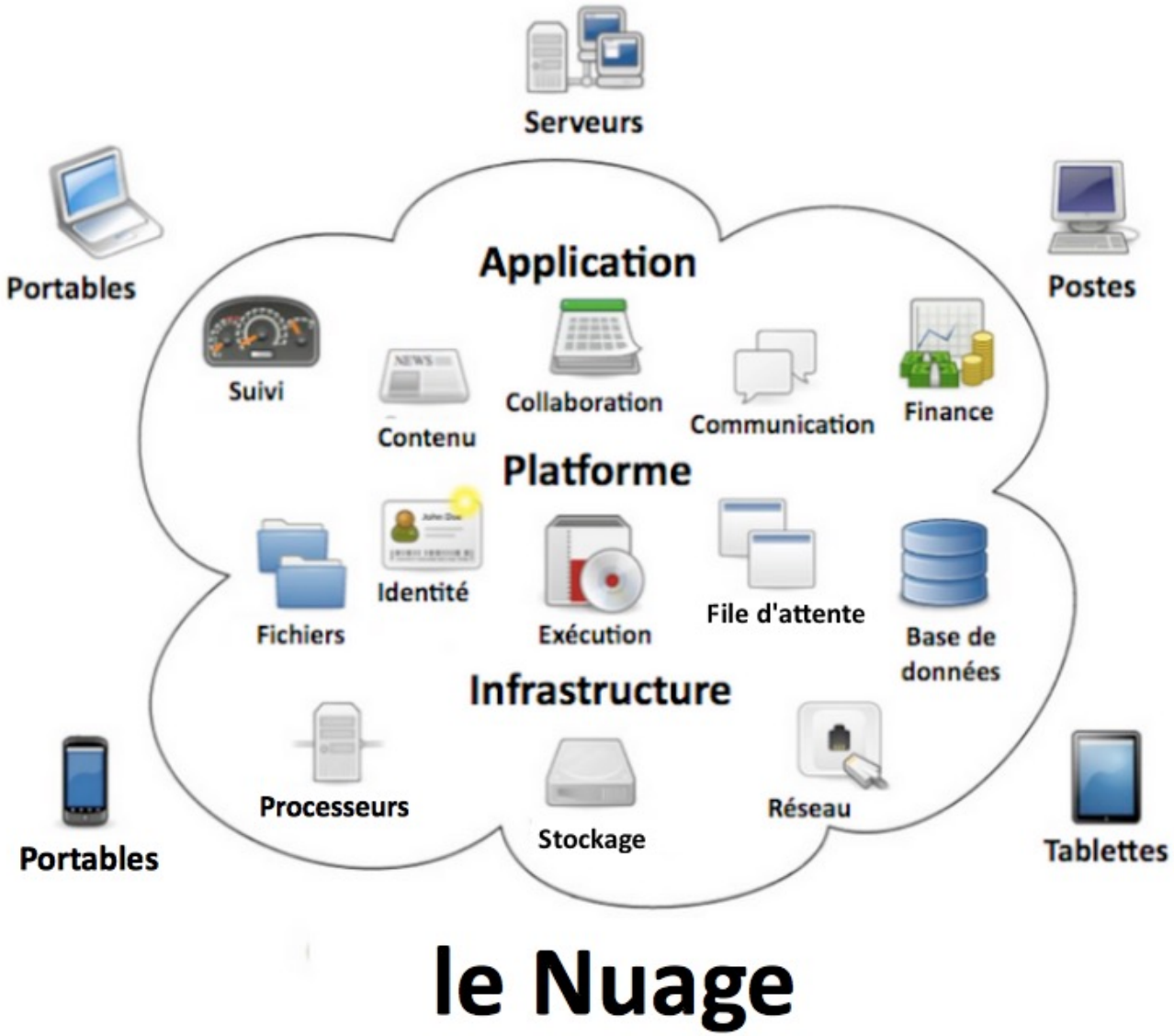
- La définition de la NIST (National Institute of Standards and Technology) a été approuvée et adoptée par plusieurs organisations et industries
  - **The International Standards Organisation (ISO)**
  - **The Cloud Industry Forum (CIF)**

- Ce modèle est composé de :
  - Cinq caractéristiques essentielles,
  - Trois modèles de service
  - Et de quatre modèles de déploiement.

Pourquoi le Cloud…

Time-to-Market	• Approvisionnement rapide des infrastructures
Flexibilité	• Ajustement du niveau des performances en fonction des besoins réels • Découplage entre le device d'accès aux applications et les infrastructures
Performances et Sécurité	• Bénéfices des dernières évolutions technologiques • Facilitation de la reprise après sinistre grâce à un approvisionnement plus rapide des infrastructures
Digital	• Facilitation de l'innovation et de la mise en place de technologies comme DevOps, Big Data, APIs • Favorisation de nouvelles méthodes de travail : mobilité et collaboration
Coûts	• Flexibilité sur les coûts grâce à un provisionnement à la demande et à une mise à disposition des ressources d'infrastructures limitée dans le temps • Optimisation de la consommation grâce à un paiement à l'usage et une prise en compte des pics de charge et du surbooking

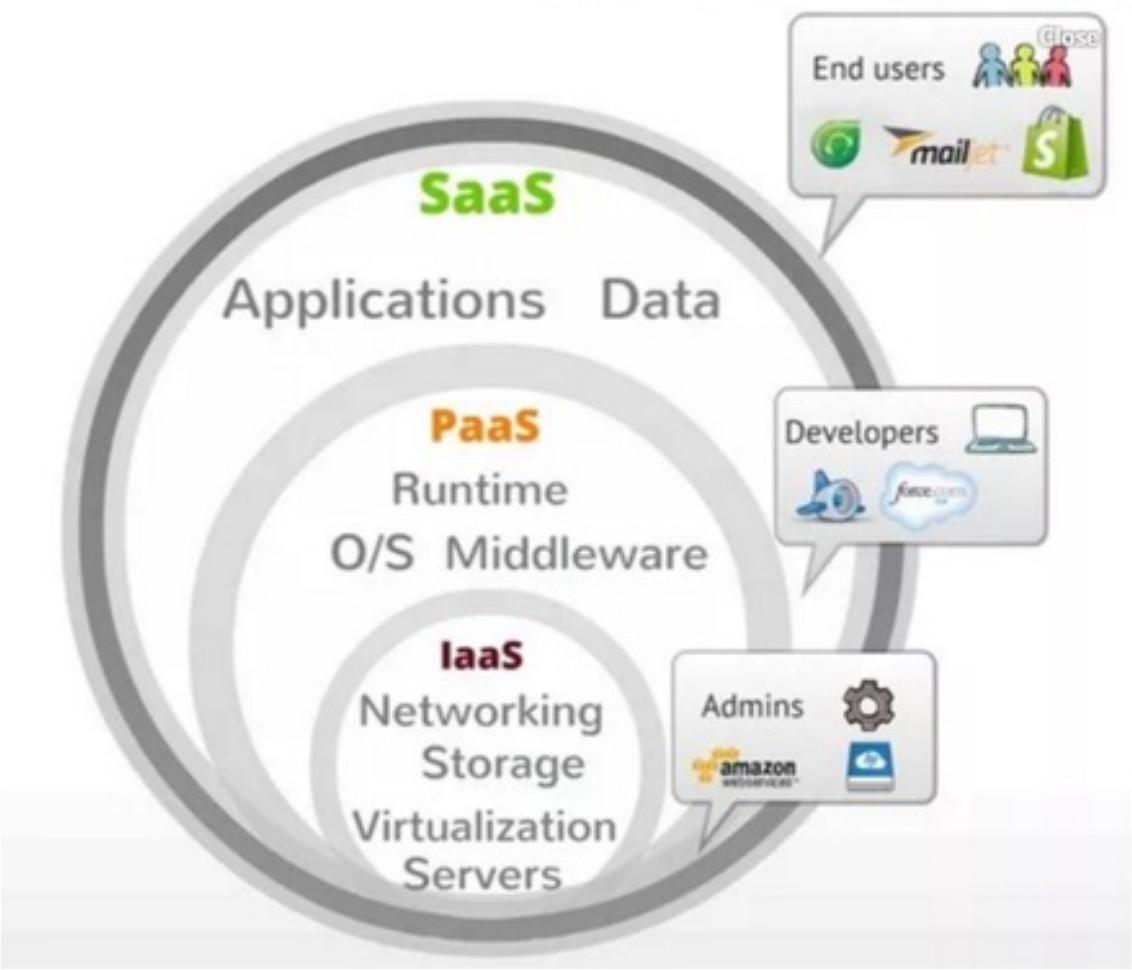
*… pour **augmenter la valeur ajoutée du SI** aux Métiers et aux clients, **avec plus d'innovation** et des solutions modernes et durables, **tout en apportant des leviers d'optimisation de coûts**.*



Cloud Computing

- Modèle informatique permettant un **accès réseau facile et à la demande à un ensemble partagé de ressources informatiques configurables** (réseaux, serveurs, stockage, applications et services) **qui peuvent être rapidement provisionnées et libérées avec un effort minimal de gestion ou d'interaction avec un fournisseur de service.**
- Ce modèle est composé de :
  - cinq caractéristiques essentielles,
  - trois modèles de service
  - et de quatre modèles de déploiement.

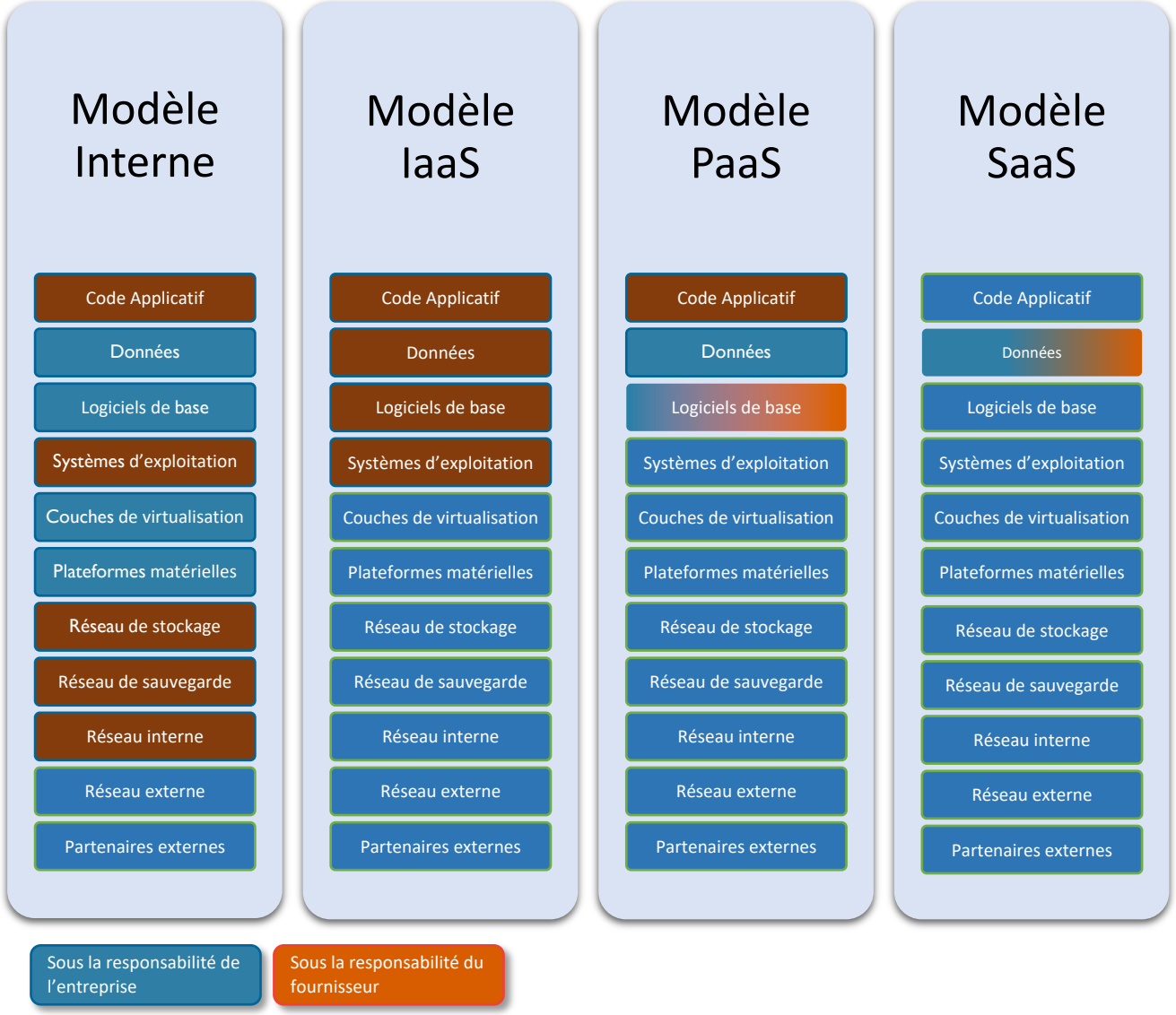
Les trois modèles de service SPI



- **SaaS :** *mise à disposition d'applications d'entreprise*
  - CRM, outils collaboratifs, messagerie, Business Intelligence, ERP, etc.
  - Le fournisseur offre une fonction opérationnelle et gère de façon transparente pour l'utilisateur l'ensemble des aspects techniques requérant des compétences informatiques.
- **PaaS :** *mise à disposition de plates-formes de middleware, de développement, de test, d'exécution d'applications…*
  - Le fournisseur gère et contrôle l'infrastructure technique (réseau, serveurs, OS, stockage…).
- **IaaS :** *mise à disposition de ressources informatiques*
  - Puissance CPU, mémoire, stockage…
  - Le modèle IaaS permet au client de disposer de ressources virtualisées et déportées.

Les responsabilités dans les modèles SPI

- **SaaS (*software as a service*)**
  - Seules des données sont sous la responsabilité du client (et encore…)
- **PaaS (*platform as a service*)**
  - Le client a la maîtrise des codes et des données exécutées,
  - Il doit les maintenir et les sauvegarder,
  - Le fournisseur maintient l'infrastructure et le système d'exploitation.
- **IaaS (*infrastructure as a service*)**
  - Seule l'infrastructure est à la charge du fournisseur.
  - Le client assure la maintenance et la sauvegarde de toutes les autres couches.
- Notons qu'il existe d'autres modèles de service Cloud, tous dérivés du SPI.



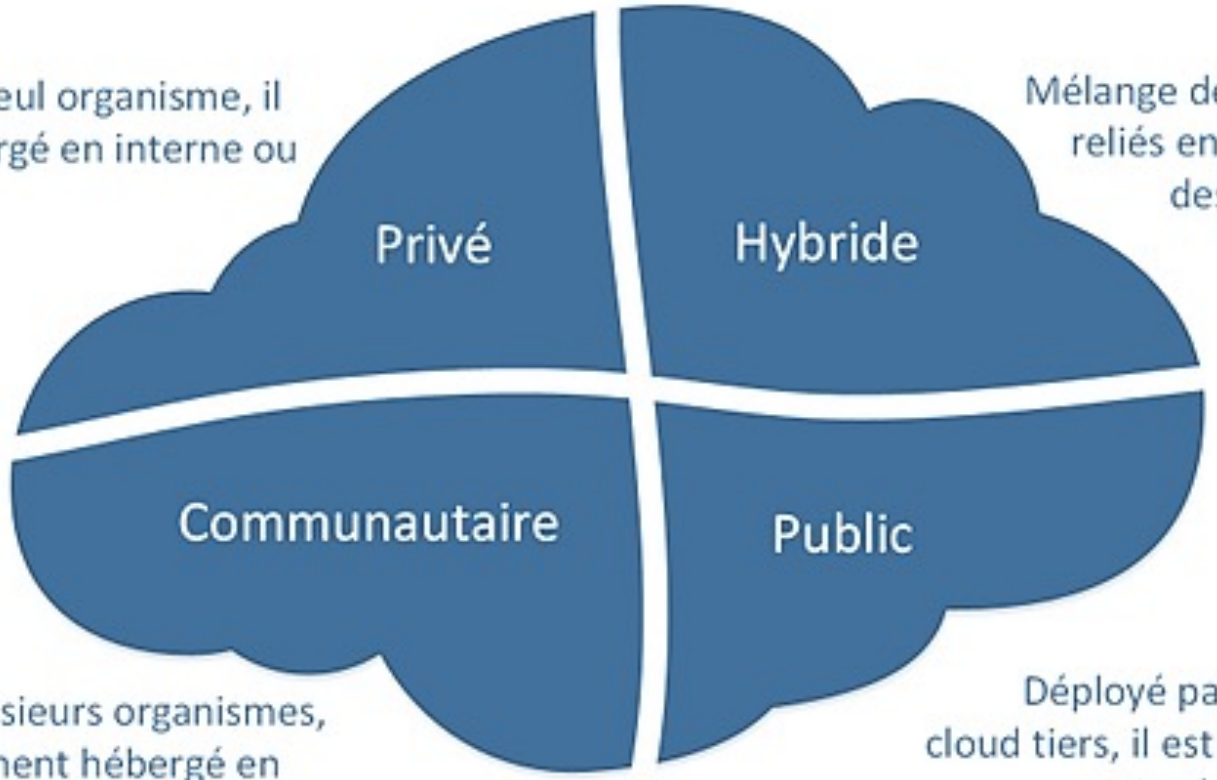
Cinq caractéristiques essentielles du Cloud

- **Libre-service à la demande**
  - Un consommateur peut provisionner arbitrairement des capacités informatiques (nombre de serveurs, stockage) selon les besoins et sans intervention du fournisseur de services.
- **Large accès au réseau - Ouverture**
  - Les services et moyens sont accessibles via le réseau par le biais de mécanismes standard qui favorisent l'utilisation de terminaux clients hétérogènes (mobiles, tablettes, ordinateurs portables et postes de travail,…).
- **Mutualisation des ressources**
  - Les ressources informatiques du fournisseur sont regroupées pour servir plusieurs consommateurs à l'aide d'un modèle mutualisé avec différentes ressources physiques et virtuelles affectées dynamiquement et réattribuées en fonction de la demande du consommateur.
  - Le client n'a généralement aucun contrôle ou connaissance sur l'emplacement exact des ressources fournies, mais peut être en mesure de spécifier l'emplacement à un niveau d'abstraction plus élevé (ex : pays, État ou centre de données).
- **Élasticité**
  - Les capacités peuvent être provisionnées de manière élastique et libérée, dans certains cas automatiquement, pour évoluer rapidement et être disponibles dans un délai réduit.
  - Pour le consommateur, les capacités disponibles pour l'approvisionnement semblent souvent illimitées et peuvent être affectées dans n'importe quelle quantité à tout moment.
- **Service mesuré - Paiement à l'usage**
  - La quantité de service consommée dans le Cloud est mesurée, à des fins de contrôle, d'adaptation des moyens techniques et de facturation.
  - L'utilisation des ressources peut être surveillée, contrôlée et signalée, ce qui assure la transparence tant pour le fournisseur que pour le consommateur du service utilisé.

Cloud : Modèles de déploiement

Utilisé par un seul organisme, il peut être hébergé en interne ou en externe.

Mélange de plusieurs modèles de cloud reliés entre eux offrant les avantages des différents environnements.

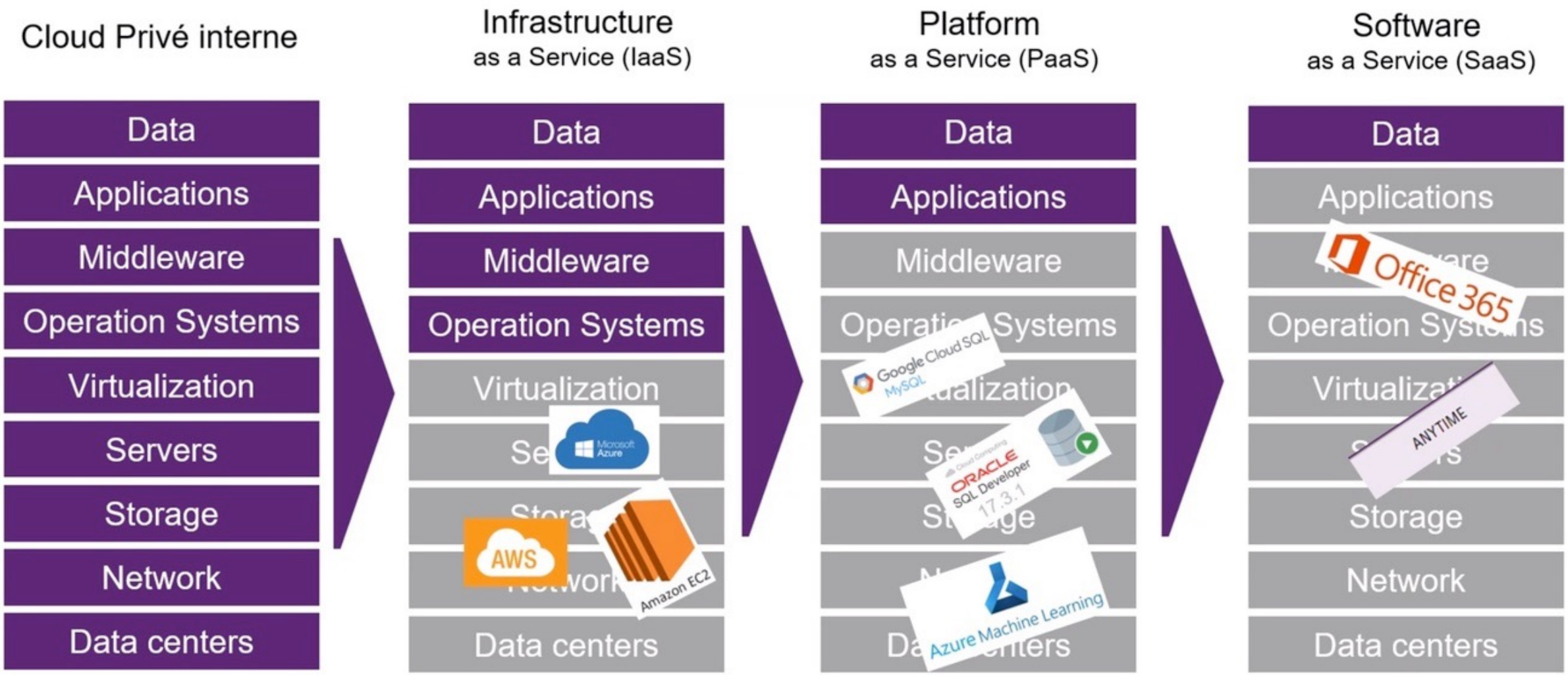


Partagé par plusieurs organismes, il est généralement hébergé en externe, mais peut être hébergé en interne par un des membres.

Déployé par un fournisseur de cloud tiers, il est ouvert au public et partagé par les utilisateurs.

Fournisseur de service = CSP (Cloud Service Provider)

Services traditionnels



Les piliers caractéristiques ?

Service à la demande

L'utilisateur/Client peut ajouter un nouveau service, espace de stockage ou traitement, sans une demande formelle de changement de contrat

Large accès au réseau

«n'importe quand, n'importe quel endroit et n'importe quel appareil» - Bill Gates 90

Nécessite suffisamment de bande passante

Le regroupement (Pool) des ressources

Multi-tenant - De nombreux utilisateurs/clients partagent un type et un niveau variés de ressources

Élasticité rapide

Adaptation dynamique ou manuel des services pour absorber la charge

Services mesurables

Des services surveillés, contrôlés et déclarés

Un modèle de service pay-per-use

Les services déployés en bureautique

- **Office 365**
  - Messagerie
    - Outlook Online (Cloud public)
    - Applications Web
  - Réseau social d'entreprise
    - Yammer (Cloud public)
  - Outil collaboratif
    - Teams (en remplacement de Skype)
- **Communication interne**
  - Skype/Jabber (Cloud privé)
  - Intranet (Cloud privé)

Qu’est ce qu’un Cloud Privé ?

- Environnement Cloud distinct et sécurisé dédié à une seule organisation
- Ressources et services accessibles par une seule organisation (non public)
- Ressources d’infrastructures (Serveurs, Equipements réseau, de stockage, etc) distinct
  - Hébergés dans les datacenter internes ou chez des hébergeurs
  - Accessible uniquement via des liaisons privées ou via VPN
- Possession complète de l’organisation (TCO à 100%)
- Responsabilité , maintenance et évolution à la charge de l’organisation

Qu’est ce qu’un Cloud Public ?

- Environnement virtualisés
- Ressources et services accessibles par le publique via Internet
- Capacité à la demande et grande évolutivité
- Coûts réduits grâce aux économies d’échelle
- De nombreux services disponible et prêt à être consommés
- Indépendant de la localisation
  - NB : AWS a des présences dans + de 100 pays au monde
- Contrôle de sécurité plus complexe
- Dépendance des services au fournisseur . Attention à la réversibilité parfois impossible

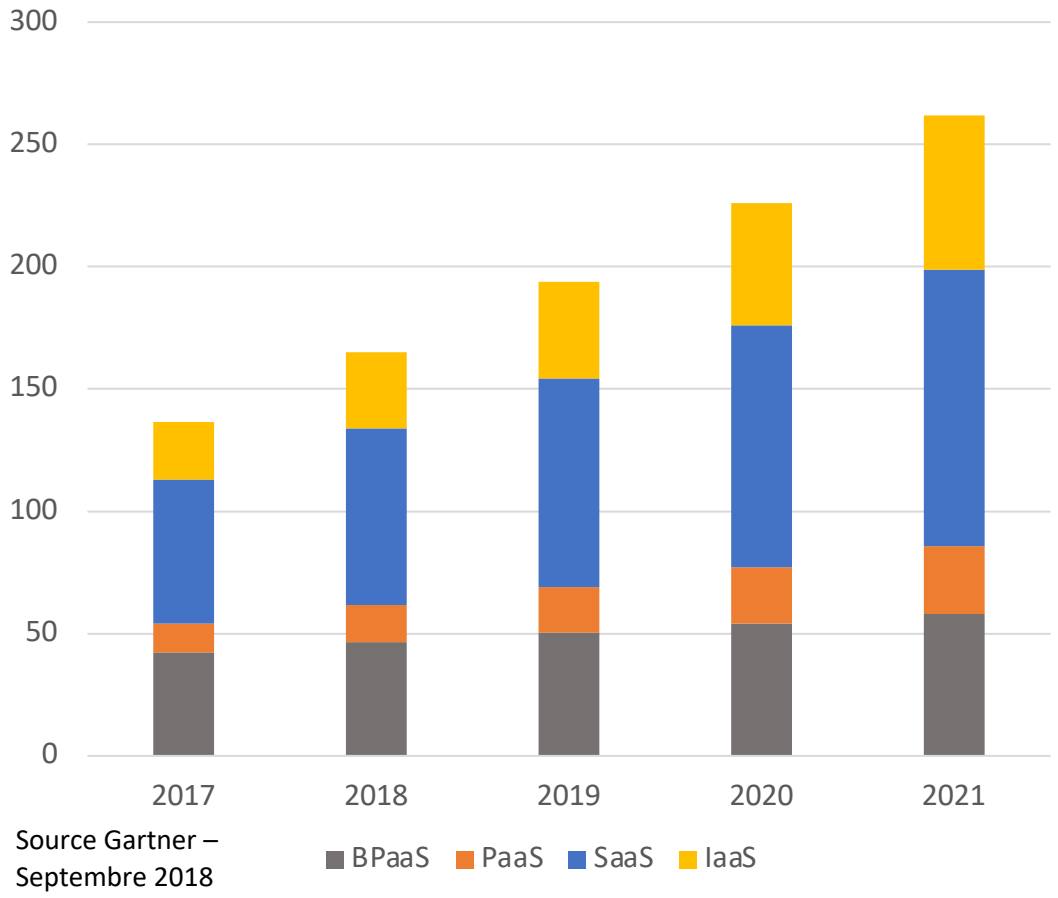
Qu’est ce qu’un Cloud Communautaire ?

- Utilisé par plusieurs organisations ayant des besoins et intérêts communs (StakeHolders)
- Permet d’héberger des applications génériques adaptés aux besoins et personnalisation de la communauté
- Permet de la mutualisation et donc :
  - Une réduction des coûts
  - Une amélioration des performances
  - Une amélioration de la sécurité des données
  - Une amélioration des SLAs

Qu’est ce qu’un Cloud Hybride ?

- Un ensemble de solutions de Cloud privées et publiques formant virtuellement un seul catalogue de services et de ressources
- Une souplesse de choix et fournitures de services en privé/public selon le besoin
- Extensibilité :
  - Possibilité de « déborder » d’un Cloud privé saturé vers un Cloud Public lors de période de charge exceptionnelle :
    - Exemple : vendredi 13 chez Française des jeux, Amazon en fin d’année, Séries populaires sur Netflix, etc…
- Pilotage fin des coûts en bénéficiant de coûts fixes limités complétés par des services en « Pay as You Go »

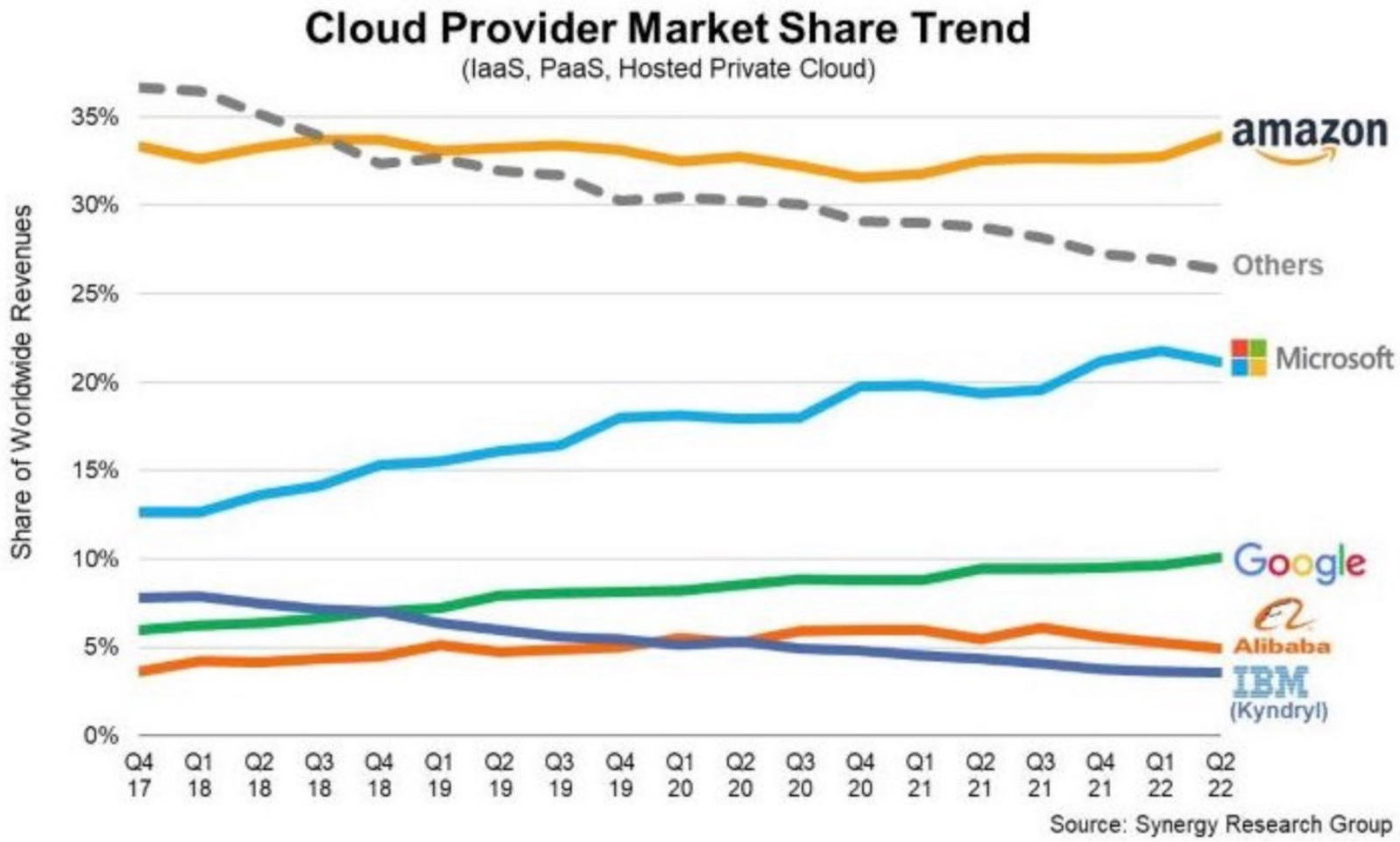
Marché mondial des services du Cloud public



Source Gartner – Septembre 2018

- La demande des entreprises s'oriente vers des **services intégrés IaaS et PaaS :**
  17% de croissance attendue en 2019 (Gartner).
- Toutefois, **le segment du logiciel en tant que service (SaaS) génère à nouveau le plus de revenus.**
- Amazon Web Services (AWS) reste de loin le fournisseur numéro 1 sur le marché IaaS, suivi de Microsoft (Azure), Alibaba, Google et IBM.
- Les entreprises doivent être prudentes quant à l'influence incontrôlée des fournisseurs IaaS sur les clients et le marché.
- **En réponse aux tendances de l'adoption multi cloud, les entreprises exigeront de plus en plus de moyens simples pour déplacer les charges de travail, les applications et les données dans le Cloud au travers d'offres IaaS sans pénalité.**

Marché mondial des services du Cloud public A Q2-2022



Adoption du Cloud en France en 2021

Clément DAVID · 2e
CEO chez Padok
3 j · Modifié ·

+ Suivre

🏆 Avec la sortie des chiffres pour 2021, c'est l'heure de faire le point sur les scores démentiels du marché du Cloud ☁️

Les géants du Cloud vont très bien, merci pour eux. Trafic fluide sur l'autoroute de la conquête du monde, aucun ralentissement à prévoir :

🇺🇸 **Amazon Web Services (AWS)** :
CA 2021 : 62 milliards (45Mds en 2020),
Croissance : 37%
PIB équivalent : Luxembourg 🇱🇺, Sénégal 🇸🇳

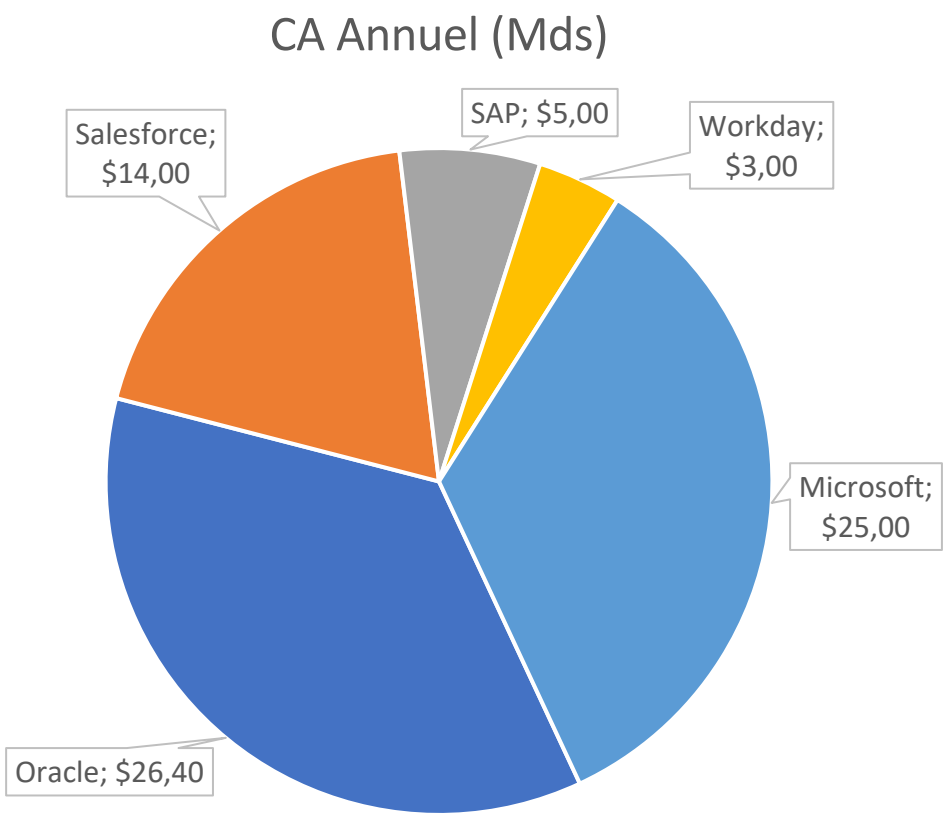
🇺🇸 **Microsoft Cloud** :
CA 2021 : 80 milliards (50Mds en 2020)
Croissance : 45%
PIB équivalent : Uruguay 🇺🇾, Slovénie 🇸🇮

🇺🇸 **Google Cloud** :
CA 2021 : 19 milliards (13Mds en 2020)
Croissance : 47%
PIB équivalent : Islande 🇮🇸, Mauritanie 🇲🇷

Précisions utiles :
🥈 Microsoft Azure n'est pas devenu leader du marché du cloud. Dans les 80 milliards, ils comptent d'autres activités comme Office 365, Dynamics 365 etc...
🥉 Google perd encore une blinde de cash cette année (3 milliards) mais moins qu'en 2020 (5 milliards). Quand tu vois cet investissement colossal pour devenir un compétiteur crédible, c'est marrant de se rappeler qu'en 2012 l'État français voulait un cloud souverain pour 150M...

Le Cloud est un OVNI de la croissance mondiale, 2022 prend la même direction. Et cette direction pointe toujours autant vers les US 🤦🏻‍♂️

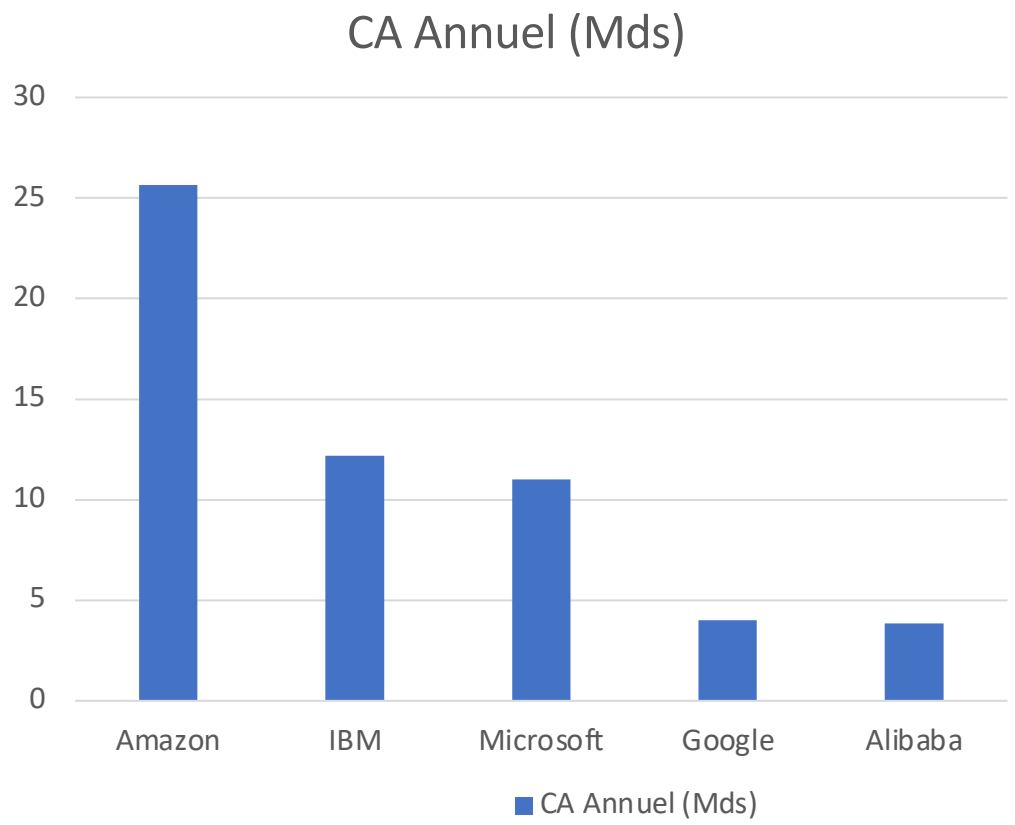
Maturité des acteurs majeurs du SaaS



- **Oracle** : fournisseur de bases de données en mode SaaS pour tout type d'entreprises qui migrent des logiciels sur site vers le cloud en passant par NetSuite.
  Dans ce domaine, la tendance va tout de même vers des solutions open source NoSQL.
- **Salesforce** : s'est développé dans tous les domaines, de l'intégration à l'analyse en passant par le marketing et le commerce.
- **SAP** : dispose d'une activité tentaculaire dans le domaine des logiciels en cloud qui va de l'ERP et des RH aux dépenses.
- **Workday** : s'est développé dans le domaine des finances et des ERP et désormais ajoute l'analyse par le biais d'une série d'acquisitions.

Maturité des acteurs majeurs du PaaS et de l'IaaS

- Selon Gartner, en 2018, il reste cinq grands CSP aptes à tenir la course mondiale dans le cloud d'infrastructure (IaaS et PaaS) :
  - Amazon, Microsoft, Google, IBM, Alibaba.
- Les autres acteurs sont condamnés à se replier sur des marchés de niche.
- A noter qu'IBM tient sa position de leader mondial sur les segments de cloud privé et hybride.
- Tous tendent à proposer des services vers l'IA et les environnements virtuels.



Objectifs des acteurs majeurs des Clouders depuis 2018

2018 : Consolider la présence des acteurs phares

- Par le rachat de sociétés

2019 : Gérer la complexité

- Avec l'IoT ou les nouvelles technologies (CaaS et FaaS), les déploiements deviennent parfois complexes

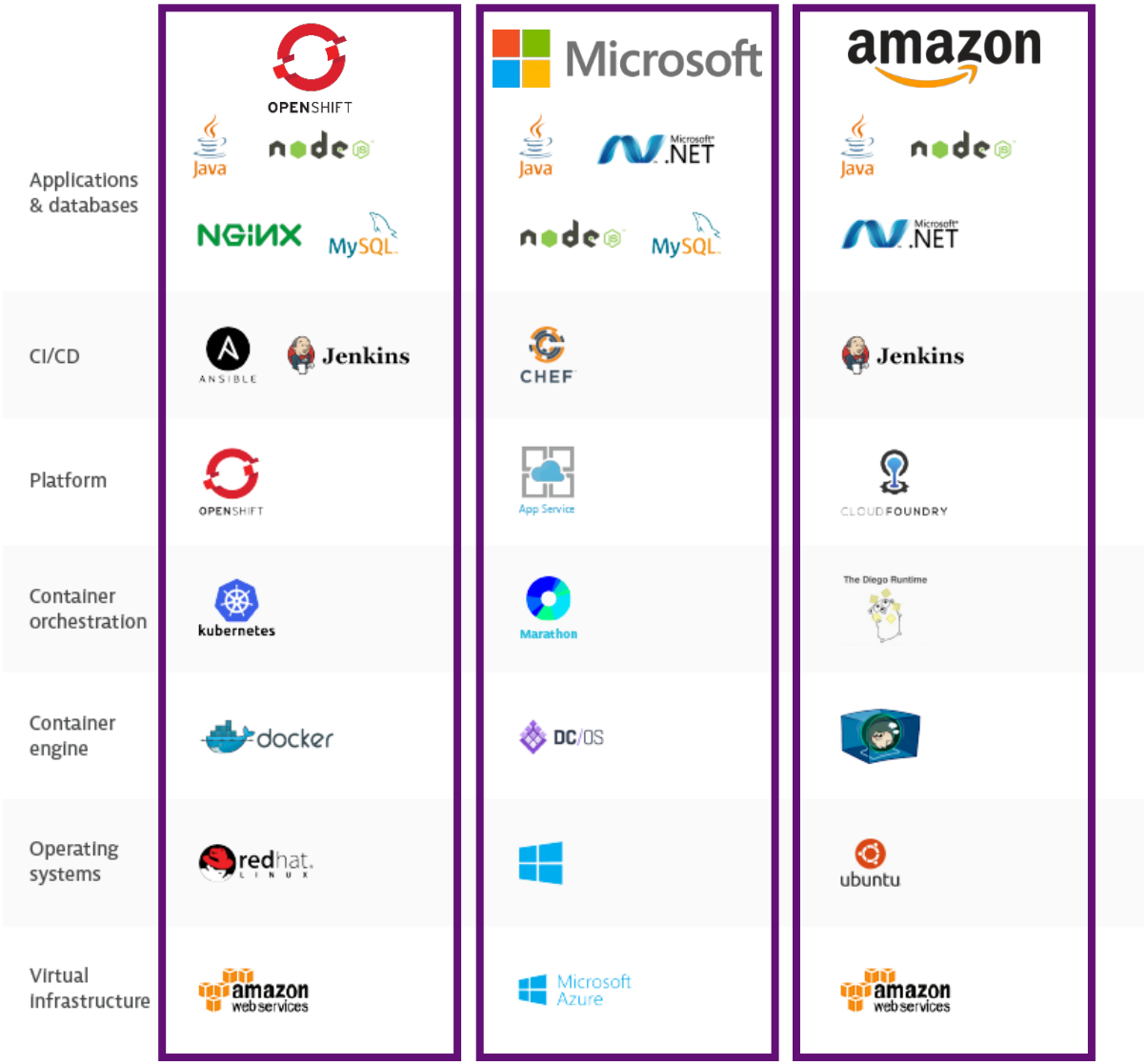
2020 : Automatiser les déploiements

- Pour réduire les temps de déploiement et assurer une haute disponibilité

2021-2022 : Proposer des services Numériques Responsables

- Sustainability Computing

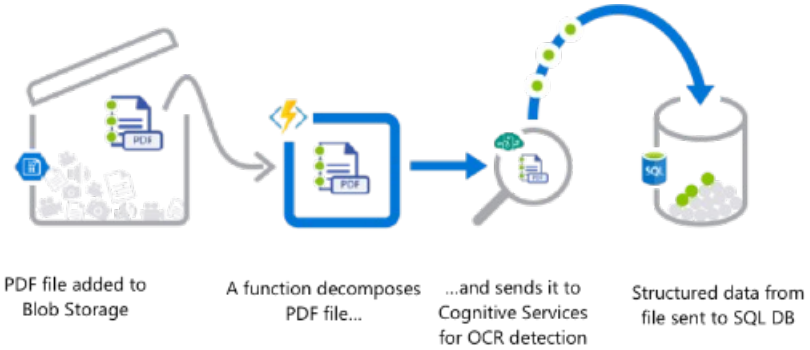
Les technologies Cloud les plus populaires



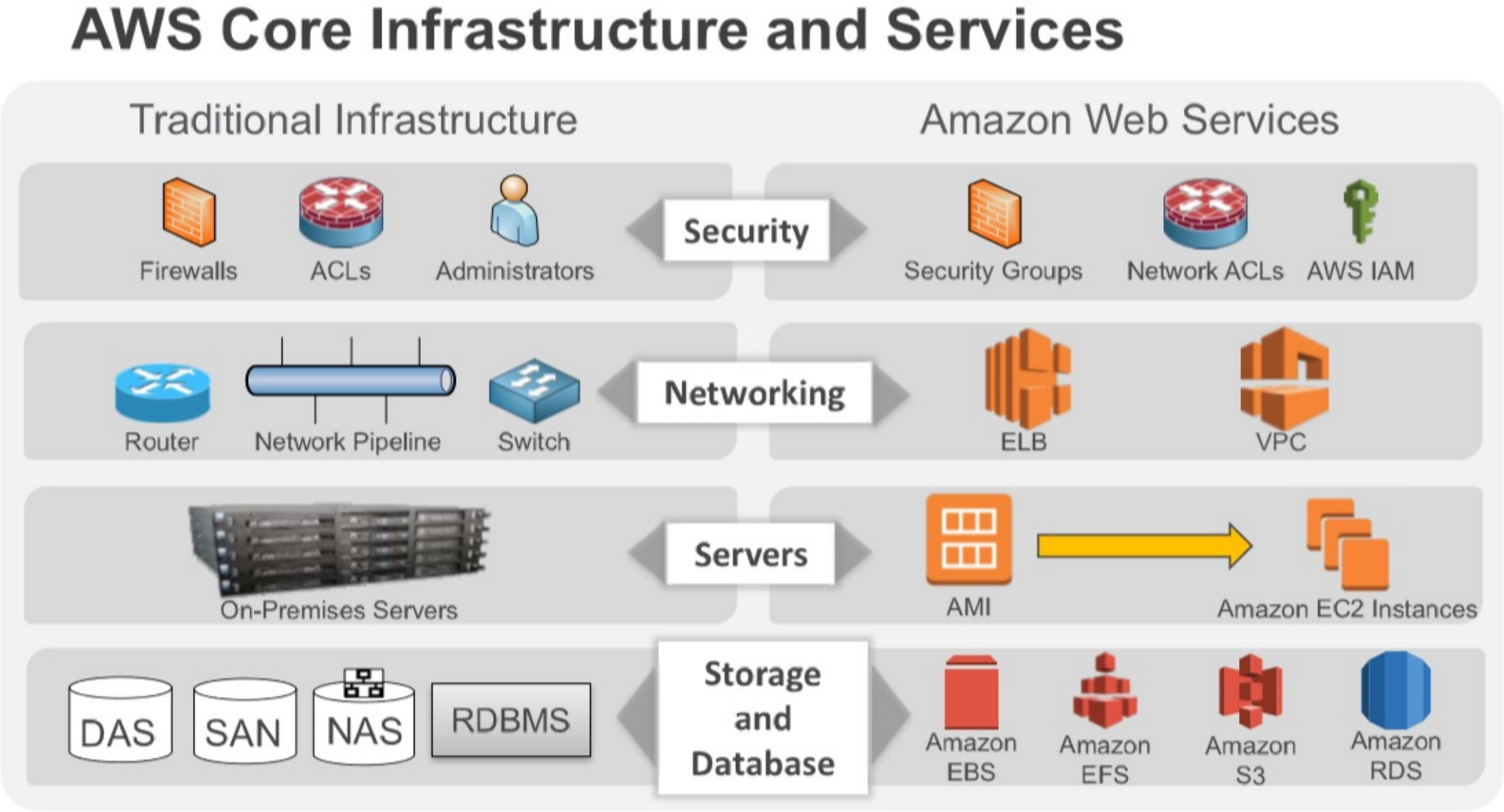
Source : DynaTrace - 2019

FaaS : Function as a Service

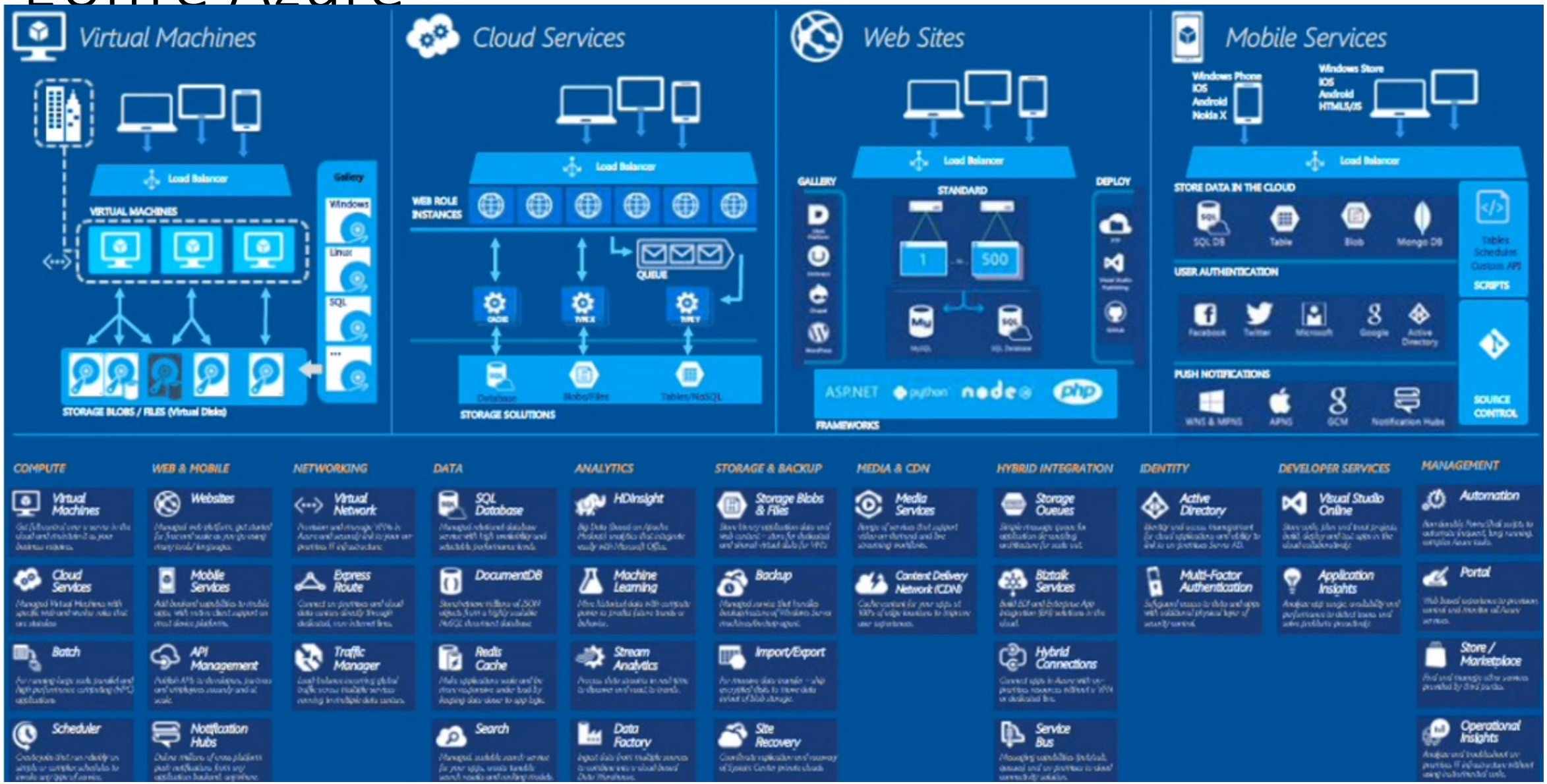
- Catégorie de services qui fournit une plate-forme permettant aux clients de développer, d'exécuter et de gérer les fonctionnalités de l'application sans la complexité de la construction et de la maintenance de l'infrastructure généralement associée au développement et au lancement d'une application.
- La création d'une application est une façon d'obtenir une architecture «sans serveur» et est **généralement utilisée lors de la création d'applications de micro services**.
- Pas adapté à toutes les applications mais convient pour **les transactions à volume extrêmement élevé**, car il est possible de les **isoler** et de les « **scaler ».**
- **Cas d'usage :**
  - Généralement associés à une fonctionnalité « à la demande » qui permet à l'infrastructure prise en charge d'être mise hors tension et de ne pas engager de frais lorsqu'elle n'est pas utilisée.
  - Exemples : le traitement des données (traitement par lots, traitement des flux, ETL), les services Internet des objets (IoT), les applications mobiles et les applications Web.



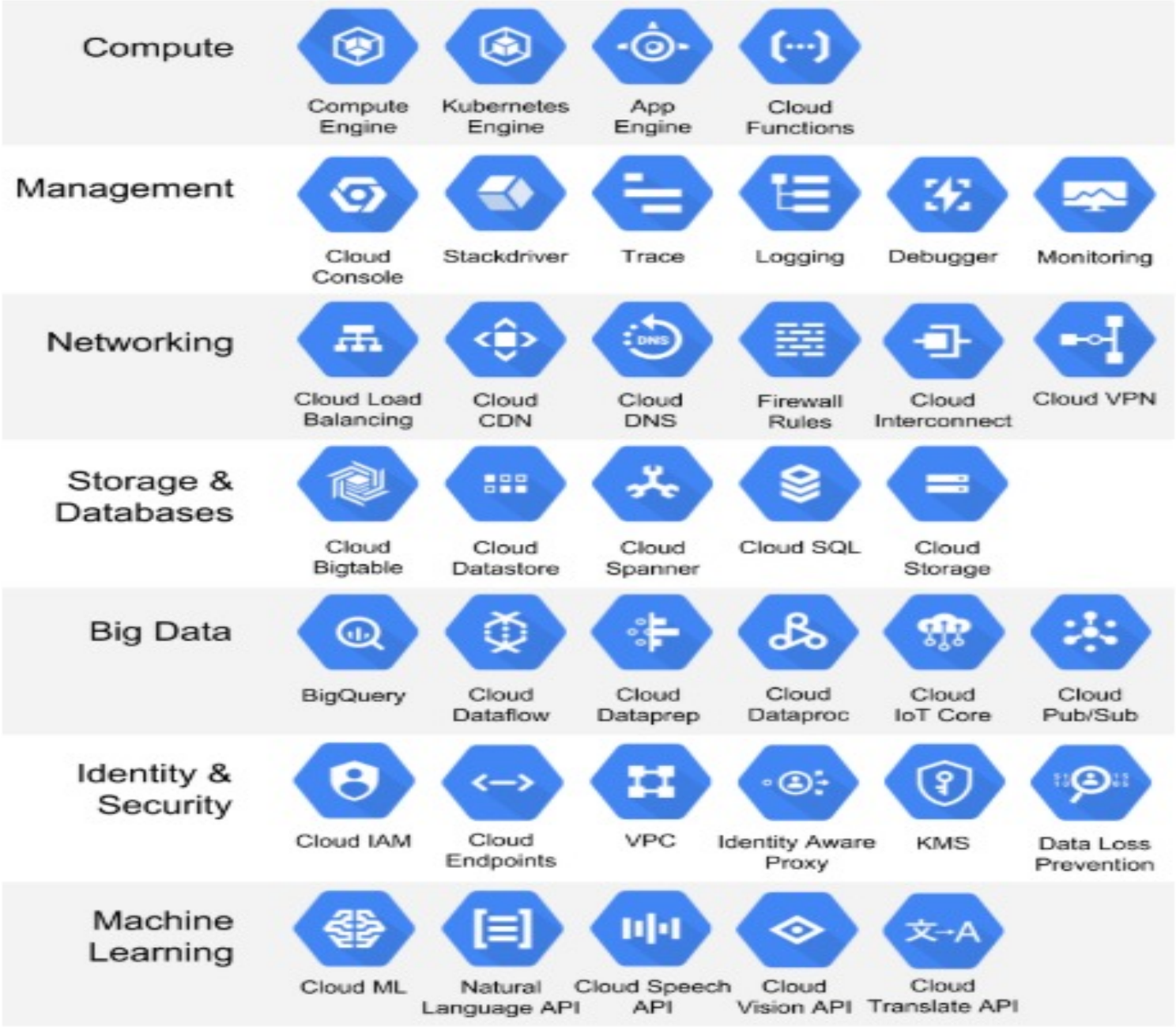
L’offre d’AWS


AWS Core Infrastructure and Services
Traditional Infrastructure
Amazon Web Services
Firewalls
ACLs
Administrators
Security
Security Groups
Network ACLs
AWS IAM
Router
Network Pipeline
Switch
Networking
ELB
VPC
On-Premises Servers
Servers
AMI
Amazon EC2 Instances
DAS
SAN
NAS
RDBMS
Storage and Database
Amazon EBS
Amazon EFS
Amazon S3
Amazon RDS

L’offre Azure



L’offre Googl



Cloud Comparison

	OVHcloud	aws	Azure	Google Cloud
Available Regions	OVHcloud OpenStack Regions	AWS Regions and Zones	Azure Regions	Google Compute Regions & Zones
Compute Services	✓ Public Cloud Instances	✓ EC2 (Elastic Compute Cloud)	✓ Virtual machines	✓ Compute Engine
Bare Metal Servers	✓ Bare Metal	✗ -	✗ -	✗ -
App Hosting	✓ WebPaaS	✓ Amazon Elastic Beanstalk	✓ Azure App Services	✓ Google App Engine
Kubernetes platform	✓ Managed Kubernetes Service	✓ EKS (Elastic Kubernetes Service)	✓ AKS (Azure Kubernetes Service)	✓ GKE (Google Kubernetes Engine)
Scaling Options	✓ Cluster autoscaler	✓ Autoscaling	✓ Azure Autoscale	✓ Autoscaler
Serverless Computing	✗ -	✓ AWS Lambda	✓ Azure Functions	✓ Google Cloud Functions
Object Storage	✓ Object storage	✓ S3 (Simple Storage Service)	✓ Blob storage	✓ Cloud Storage
Block Storage	✓ Block storage	✓ EBS (Elastic Block Store)	✓ Azure Managed Storage	✓ Persistent Disks
Archive	✓ Cloud archive	✓ AWS Glacier	✓ Azure Archive Blob Storage	✓ Google Cloud Storage Nearline
Content Delivery Network (CDN)	✓ OVHcloud CDN	✓ Amazon CloudFront	✓ Azure CDN	✓ Cloud CDN
Relational database	✓ PostGreSQL / MySQL Database	✓ Amazon RDS	✓ Azure SQL Database	✓ Google Cloud SQL
In Memory Database	✓ Redis Database	✓ Amazon ElastiCache	✓ Azure RedisCache	✓ Cloud MemoryStore
No SQL Database	✓ MongoDB Databse	✓ Amazon DynamoDB	✓ Azure Cosmos DB	✓ MongoDB Atlas

Virtual Network	✓	Private Network (vRack)	✓	VPC (Virtual Private Cloud)	✓	Virtual Network (Vnet)	✓	VPC (Virtual Private Cloud)
Private connectivity	✓	OVHcloud Connect	✓	Direct Connect	✓	ExpressRoute	✓	Google Cloud Interconnect
DNS Services	⟳	DNS and Domain name	✓	Amazon Root 53	✓	Azure Traffic Manager	✓	Cloud DNS
Log Monitoring	✓	Logs Data Platform	✓	Amazon CloudTrail	✓	Azure Operation Insights	✓	Cloud Logging
Performance Monitoring	✗	-	✓	Amazon CloudWatch	✓	Azure Application Insights	✓	StackDriver Monitoring
Administration and Security	⟳	-	✓	AWS Identity and Access Management (IAM)	✓	Azure Active Directory	✓	Cloud Identity and Access Management (IAM)
Compliance	✗	-	✓	AWS CloudHSM	✓	Azure Trust Center	✓	Google Cloud Platform Security
Analytics	✓	Grafana and Data Processing	✓	Amazon Kinesis	✓	Azure Stream Analytics	✓	Cloud Dataflow
Automation	✗	-	✓	AWS Opsworks	✓	Azure Automation	✓	Compute Engine Management
Develop AI Models	✓	AI Notebooks	✓	Amazon SageMaker Notebook Instances	✓	Azure Machine Learning Jupyter Notebooks	✓	GPC - Vertex AI Workbench
Train AI Models	✓	AI Training	✓	Amazon SageMaker	✓	Azure Machine Learning	✓	GPC – Vertex AI
Load Balancing	✓	Load Balancer	✓	Elastic Load Balancing	✓	Load Balancing for Azure	✓	Cloud Load Balancing
Ddos protection	✓	AntiDDoS	✓	AWS Shield	✓	Ddos protection	✓	Ddos protection

L’évolution de projets Cloud

- Le développement de projets « Cloud » implique des évolutions dans :
  - **Le mode de gestion des projets**
    - Qui dit « Time to Market » dit rapidité, voire agilité… dans le développement
  - **Les relations avec les partenaires**
    - Dans le cadre de projets innovants, nous avons souvent affaire à des startup.
      Leur taille, organisation et mode de fonctionnement sont différents de ceux d’un grand groupe.
  - **La relation avec les clients (et donc leur satisfaction)**
    - Elle va augmenter les interactions avec les clients et inciter à une analyse plus profonde des données collectées.
- Conséquences :
  - Changements dans l’organisation et les processus
  - Changements dans les métiers

Améliorer l’agilité

- S’appuyer sur des méthodes de développement informatique permettant de concevoir des logiciels en impliquant au maximum le demandeur (client)

  ➔ meilleure réactivité à ses demandes

- Les méthodes Agiles se veulent plus pragmatiques que les méthodes traditionnelles.
- **Elles visent la satisfaction réelle du besoin du client, et non celle d'un contrat établi préalablement.**

Les individus et leurs interactions plutôt que processus et outils.
La communication est une notion fondamentale.

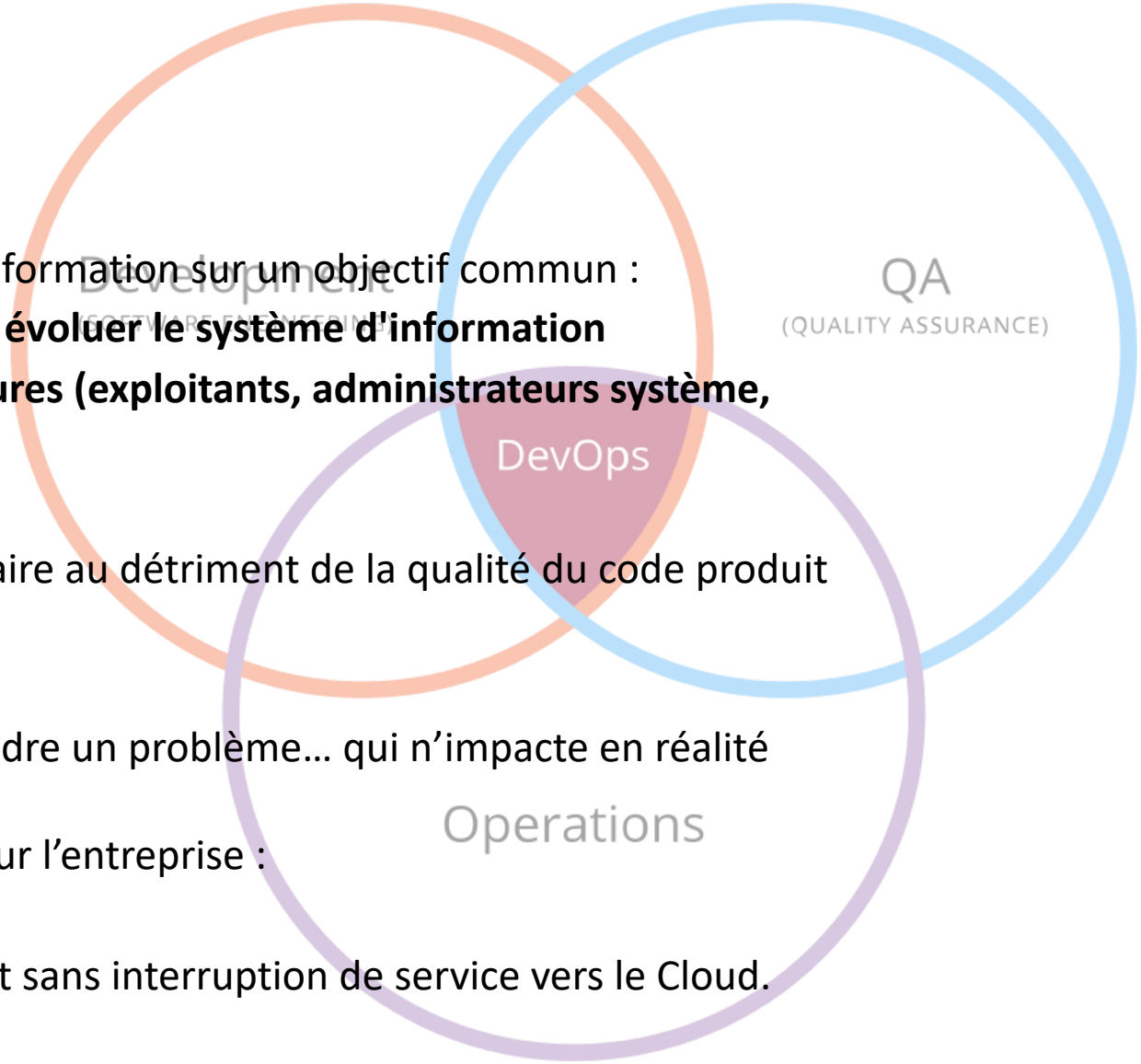
Fonctionnalités opérationnelles plutôt que documentation exhaustive :
il est vital que l'application fonctionne.
Le reste, et notamment la documentation technique, est secondaire.
Il est préférable de transférer les compétences au sein de l'équipe (on en revient à l'importance de la communication).

Collaboration avec le client plutôt que contractualisation des relations : le client doit être impliqué dans le développement, collaborer avec l'équipe et fournir un feed-back continu sur l'adaptation du logiciel à ses attentes.

Acceptation du changement plutôt que conformité aux plans :
la planification initiale et la structure du logiciel doivent être flexibles afin de permettre l'évolution de la demande du client tout au long du projet.
Les premiers livrables vont souvent provoquer des demandes d'évolution.

La gestion en mode DevOps

- Vise à l'alignement de l'ensemble des équipes du système d'information sur un objectif commun :
  - **Les équipes de Dev (ou dev engineers) chargées de faire évoluer le système d'information**
  - **Les Ops (ou ops engineers) responsables des infrastructures (exploitants, administrateurs système, réseau, bases de données,...)**
- **Enrichir les environnements de développement**
  - Réduire les cycles de mise en production ne doit pas se faire au détriment de la qualité du code produit
    ➔ **besoin d'anticiper les risques**
- **Prioriser les tâches**
  - Il n'est pas rare de voir un développeur s'obstiner à résoudre un problème… qui n'impacte en réalité qu'une infime partie des utilisateurs !
  - Se concentrer sur un facteur clé de création de valeur pour l'entreprise :
    ➔ **la satisfaction des utilisateurs**
- Cette méthode devrait favoriser la transition et le déploiement sans interruption de service vers le Cloud.
- **Noter que DevOps s'appuie sur une méthode Agile (Scrum)**



Le projet et DevOps

- **Encourager la transparence et la communication de l'ensemble des équipes de la chaîne applicative**
  - **Mettre en œuvre des processus de communication et des outils partagés**, permettant à chacun d'avoir une visibilité totale et de suivre l'état d'avancement de chaque phase d'un déploiement.
  - **Partager des tableaux de bord et des indicateurs de performance**, mettre en place des systèmes d'alertes ciblés en fonction de la nature du problème identifié, systématiser les feedbacks entre les équipes.
- **Automatiser les tests et les configurations**
  - L'automatisation permet de **sécuriser, de fiabiliser et d'accélérer le traitement de l'énorme volume de données** qui afflue quotidiennement dans une entreprise.
- **Surveiller les performances en continu**
  - Le DevOps, à l'instar des méthodes Agiles, doit permettre d'être **plus efficace dans l'identification des incidents et de réduire les temps moyens de résolution**.
  - **Mettre en œuvre des processus de surveillance de la performance applicative est indispensable**, pour disposer d'une visibilité totale et continue sur l'ensemble de la chaîne applicative, et identifier instantanément la cause et l'impact potentiel d'un dysfonctionnement.

Évoluer vers de nouveaux rôles

- Liés à l'évolution des technologies d'intégration et d'architecture :
  - ***Cloud Broker***, *Cloud Coach*, ***Cloud Architect***, ***Cloud Admin***, ***DataCenter Urbanist***, *Cloud Mobile Architect, Consultant Green IT, etc.*
- Liés à la prise en compte des impacts juridiques relatifs à la protection des données et aux contrats avec les opérateurs Cloud
  - ***SecOps***, *Open Data manager, etc.*
- Liés au besoin de gérer les données
  - *Data Protection Officer, Data Architect, etc.*
- Liés à la prise en compte des besoins
  - *FinOps, Data Scientist,* ***DevOps***, *Machine Learning Ops, etc.*
- Certains rôles existants vont aussi évoluer
  - *Technicien PC, Community manager,* ***Cloud Ops***, ***Développeur*** *…*

Une sécurité accrue

La migration vers le cloud est une opportunité de remettre complètement à plat la gestion de la sécurité en privilégiant une démarche proactive et analytique s'appuyant sur l'automatisation des processus, la collecte et l'analyse de données favorisée par les plateformes cloud.

Cela nécessite l'implication des départements sécurité dès les premières phases de spécification pour définir les principes de sécurité des *landing zone*, des processus de *provisioning* et des opérations récurrentes.

En prenant l'opportunité de redéfinir l'ensemble de ses éléments dès la création des plateformes, cela garantit et facilite leur application puisqu'elles sont appliquées de manière systématique lors de la migration. Cela permet d'appliquer les principes de *security by design* sur les socles d'hébergement :

- **Minimiser la surface d'attaque** : en contraignant les modes d'accès lors du déploiement.
- **Le moindre privilège** : en appliquant de manière systématique les politiques de droits et d'accès.
- **La défense en profondeur** : en cumulant les différents outils à disposition en appliquant des patterns validés.

L'ensemble de ces principes doit évidemment s'étendre aux méthodes et pratiques de développement dans le cadre de modernisations applicatives.

Le modèle Cloud Privé d’un point de vue sécurité générale

- Environnement Cloud distinct et sécurisé dédié à une seule organisation
- Pool de ressources accessible par une seule organisation
  - Offre davantage de contrôle, de protection et de confidentialité
- Pool distinct de serveurs physiques
  - hébergés en interne ou hors de l'entreprise
  - accessible par des liaisons privées ou chiffrées via les réseaux publics
- Existe encore un degré élevé de coût total de possession (TCO)
- Grand degré de responsabilité
  - Prise en charge de la maintenance et des évolutions

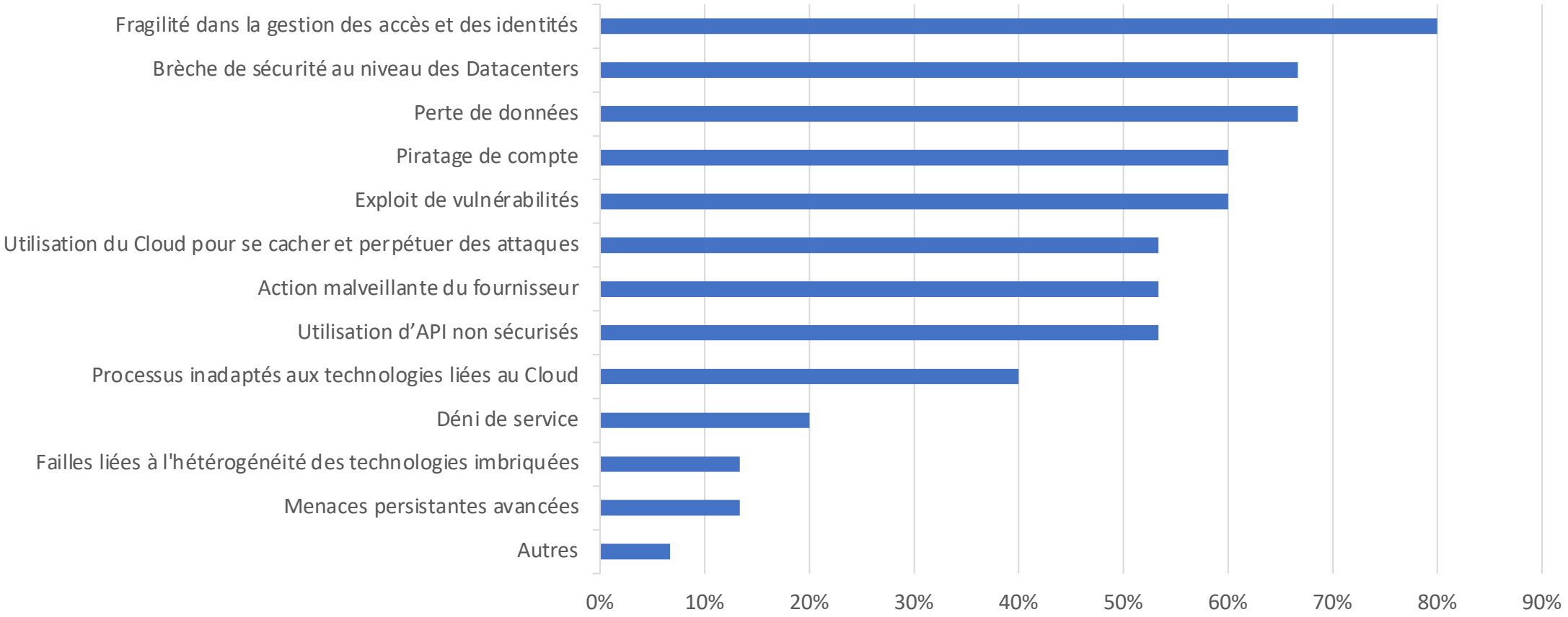
Le modèle Cloud Public d’un point de vue sécurité générale

- Environnement virtualisé
  - Ressources physiques partagées et accessibles via Internet
- Grande évolutivité
  - Disponible à la demande depuis un pool de ressources
- Coûts réduit
  - Bénéficie de vastes économies d'échelle
- Flexibilité
  - Multitude de services disponibles prêts à être utilisés
- Indépendance de l'emplacement
  - Disponibilité par connexion Internet donc partout
- Contrôle de sécurité plus complexe
  - Difficile de respecter différents types de législation internationale
- Grande dépendance au fournisseur
  - Services parfois spécifiques / propriétaires

Les dangers du Cloud Public d'un point de vue sécurité générale

- Il existe de nombreux problèmes si vous souhaitez utiliser les services de Cloud en toute sécurité
  - Perte de données (par exemple en raison de l'insolvabilité d'un fournisseur, de pannes techniques ou d'un blocage inattendu du compte)
  - L'accès non autorisé ou non désiré par des tiers

Risques de sécurité du Cloud selon les utilisateurs



Les dangers du Cloud Public d'un point de vue « Stratégie »

- L'élaboration d'une feuille de route et d'une liste de contrôle pour optimiser la rapidité d'exécution des actions est essentiel pour une plus grande chance de succès

- Une organisation qui se précipite à adopter des technologies de cloud computing en choisissant les CSPs sans une réflexion raisonnable s'expose à une myriade de soucis
  - Commerciaux
  - Financiers
  - Techniques
  - juridiques
  - et de conformité
- qui mettent en péril son succès.

CSA SECURITY GUIDANCE REFERENCE

Domain 1: Cloud Computing Architectural Framework
Domain 2: Governance and Enterprise Risk Management
Domain 3: Legal Issues: Contracts and Electronic Discovery
Domain 4: Compliance and Audit Management
Domain 5: Information Management and Data Security
Domain 6: Interoperability and Portability
Domain 7: Traditional Security, Business Continuity, and Disaster Recovery
Domain 8: Data Center Operations
Domain 9: Incident Response
Domain 10: Application Security
Domain 11: Encryption and Key Management
Domain 12: Identity, Entitlement, and Access Management
Domain 13: Virtualization
Domain 14: Security as a Service

Les dangers du Cloud Public d’un point de vue « Stratégie » - Exemples

- En 2012, le service Amazon Web (AWS) sur lequel s’appuie Netflix pour diffuser du contenu aux clients a connu une interruption dans sa région des États-Unis-Est (couvrant plusieurs zones dans AWS), en raison de la suppression accidentelle d'informations d'équilibrage de charge des contrôles.

- En 2013, Nirvanix, spécialiste du stockage cloud qui héberge des données pour IBM, Dell et ses propres clients, a fait faillite et fermé ses activités. Les clients ont reçu moins de deux semaines pour déplacer leurs données sur un autre service.

Les dangers du Cloud Public d'un point de vue « Migration »

- Déploiements de services cloud mal sécurisés, essais de services cloud gratuits et inscriptions de compte frauduleux pemettent d'utiliser ses catalogues de services pour des attaques malveillantes.

- Les acteurs peuvent tirer parti des ressources cloud computing pour cibler les utilisateurs, les organisations ou d'autres fournisseurs de cloud.

CSA SECURITY GUIDANCE REFERENCE

Domain 3: Legal Issues: Contracts and Electronic Discovery
Domain 7: Traditional Security, Business Continuity and Disaster Recovery
Domain 9: Incident Response

Les dangers du Cloud Public d'un point de vue « Migration » - Ex

- Les DDoS brisaient Internet
- Les attaquants ont pu générer plus de 300 Gbps de trafic probablement avec un réseau propre qui n'avait accès qu'à 1 / 100e de ce volume de trafic

- Sneak Back Into AWS for DDoS Launch Hub
- Le Cloud Computing Amazon Elastic souffrait d'une attaque très sophistiquée par un groupe de pirates informatiques inconnus, qui avait trouvé un moyen de créer une porte dérobée facilement accessible pour eux-mêmes et utiliser la puissance de traitement disponible d'Amazon
- https://www.cpomagazine.com/cyber-security/ddos-attack-on-amazon-web-services-raises-cloud-safety-concerns/

Les dangers du Cloud Public d'un point de vue « Data »

- « Voleurs de données »
  - Personnes qui souhaitent gagner de l'argent avec des données volées
- Hackers
  - Testent leurs compétences en essayant de pénétrer et de forcer les barrières de sécurité d'institutions ou d'entreprises
- Organismes d'État
  - L'affaire de la NSA a attiré l'attention du grand public sur le fait que les services secrets peuvent avoir accès aux données personnelles des citoyens
- Fournisseurs de Cloud
  - Nombreuses grandes entreprises dans de le domaine de l'informatique et du Web comme Google ou Facebook tirent aussi profit du traitement ultérieur des données des utilisateurs
- Personnes internes
  - Les employés actifs ou au repos d'une entreprise posent aussi un risque pour la sécurité

Les dangers du Cloud Public d'un point de vue « Data »

- Les données stockées dans le cloud peuvent être perdues pour des raisons autres que les attaques malveillantes
- Suppression accidentelle par le fournisseur de services cloud
- Catastrophe physique comme un incendie ou tremblement de terre
- Nécessite de prendre des mesures adéquates pour sauvegarder les données de manière adaptée
  - PRA, PCI, RTO/RPO, …

CSA SECURITY GUIDANCE REFERENCE

Domain 5: Information Management and Data Security
Domain 10: Application Security
Domain 12: Identity, Entitlement and Access Management
Domain 13: Virtualization

Les dangers du Cloud Public d'un point de vue « Data » - Exemples

- En Novembre 2014, les attaquants ont fait irruption dans Sony et engendré une pertes d'informations confidentielles telles que des échanges de PII et de courrier électronique. Au premier trimestre 2015, Sony a mis de côté 15 millions $ USD pour répondre dommages-intérêts permanents du hack.

- En Juin 2014, Code-Space, un hébergement en ligne et fournisseur d'édition de code, a été piraté, ce qui a conduit à la destruction complète de la plupart des données des clients. La société a finalement été incapable de se remettre de cette attaque et a cessé ses activités.

Les dangers du Cloud Public d'un point de vue « Accès réseau »

- Le passage par la connexion Internet impose des considérations de sécurité fortes
  - Pour l'administration
  - Pour la consommation des services par le cloud privé
  - Pour l'utilisation des applications par les utilisateurs
- Plusieurs solutions réseaux sont disponibles

Les dangers du Cloud Public d'un point de vue « Accès réseau »

Cloud		Client	Segment et charge de travail
	Connexion sécurisée Point to Site		• Développeurs • POC • Small scale deployments • Connecter depuis partout
	Connexion VPN sécurisée Site-to-Site		• SMB, Enterprises • Connexion aux machines Azure
	Connexion privée ExpressRoute / DirectConnect		• SMB & Enterprises • Charge de travail critique • Backup/DR, media, HPC • Connexion à tous les services Azure

Les dangers du Cloud Public d'un point de vue « Code »

- Des hackers s'attaquent régulièrement aux comptes GitHub afin de faire miner de la monnaie virtuelle aux utilisateurs des logiciels hébergés
  - https://journalducoin.com/altcoins/le-compte-github-de-syscoin-compromis/

- Praetorian lance un service gratuit de piratage de mot de passe basé sur le cloud AWS
  - https://www.praetorian.com/newsroom/free-access-to-new-cloud-based-password-cracking-service-gpu-support

Les dangers du Cloud Public d'un point de vue « Code »

- Les API doivent être présent dans le périmètre de sécurisation

- Les services sont fortement exposés sans bénéficier d'une bonne visibilité des clients qui ne les utilisent pas

CSA SECURITY GUIDANCE REFERENCE

Domain 5: Information Management and Data Security
Domain 10: Application Security
Domain 11: Encryption and Key Management
Domain 12: Identity, Entitlement and Access Management
Domain 13: Virtualization

Les dangers du Cloud Public d'un point de vue « Code » : Exemples

- À la mi-2015, l'Internal Revenue Service (IRS) ont exposé plus de 300.000 enregistrements via une API vulnérable (« Get Transcript »)
- Dans le cas des API exposées, les données sensibles sont une cause de préoccupation
- Implique plus que la sécurisation de l'API elle-même:
  - protection des clés de l'API
  - informations d'identification et d'autres données sensibles
  - parfois négligés par les développeurs.

Les dangers du Cloud Public d'un point de vue « Système »

- Manque de mise à jour sur les composants systèmes bas niveau
- Nécessite des architectures et des stratégies de mises à jour adaptées
  - Template
  - Déploiement vertical
  - Déploiement horizontal

CSA SECURITY GUIDANCE REFERENCE

Domain 5: Information Management and Data Security
Domain 10: Application Security
Domain 11: Encryption and Key Management
Domain 12: Identity, Entitlement and Access Management
Domain 13: Virtualization

Les dangers du Cloud Public d'un point de vue « Système » - Exemples

- Même les applications open source, que l'on croyait plus sûrs que leurs homologues commerciaux …, sont vulnérables aux menaces
  - Systèmes particulièrement affectés sous Linux, qui est préoccupante étant donné que 67,7% des sites Web utilisent UNIX / Linux)
- Le bug Shellshock dans Bash était la deuxième vulnérabilité la plus exploitée, éclipsant rapidement heartbleed en raison de nombreuses attaques et du taux de succès
- 2014 cybermenaces Defense Report
  - 75% des attaques exploitant des vulnérabilités connues dans les logiciels commerciaux pourraient être évités par l'application des mises à jour

Les dangers du Cloud Public d'un point de vue « Technologies »

- Les fournisseurs de services Cloud offrent leurs services scalable en partageant l'infrastructure, les plates-formes ou des applications.
- La technologie Cloud divise le « en tant que service » offre, sans modifier substantiellement le matériel / logiciel offthe-étagère parfois au détriment de la sécurité.

CSA SECURITY GUIDANCE REFERENCE

Domain 1: Cloud Computing Architectural Framework
Domain 5: Information Management and Data Security
Domain 11: Encryption and Key Management
Domain 12: Identity, Entitlement, and Access Management
Domain 13: Virtualization

Les dangers du Cloud Public d’un point de vue « Technologies » - Ex

- Canaux latéraux Cross-VM et leur utilisation pour extraire les clés privées - « … construction d'une attaque à canal du côté entraîné accès par lequel une machine virtuelle malveillant (VM) extrait des informations à grains fins à partir d'une victime VM en cours d'exécution sur le même ordinateur physique. »

- Comprendre la vulnérabilité VENOM - « La vulnérabilité de tampon non contrôlé (CVE-2015-3456) a lieu dans le code de contrôleur de disquette virtuelle QEMU. Une attaque de débordement de tampon avec succès l'exploitation de cette vulnérabilité peut permettre à un attaquant d'exécuter son code dans le contexte de sécurité de l'hyperviseur et échapper au système d'exploitation invité à prendre le contrôle de toute l'armée « .

Les dangers du Cloud Public d'un point de vue « Comptes »

- Les détournement de service ou de compte ne sont pas nouveaux
  - Phishing, la fraude et exploitation des vulnérabilités logicielles offrent de bons résultats
- Si des attaquants parviennent à accéder aux informations d'identification
  - espionnage des activités et transactions
  - manipulation des données
  - redirection des clients vers des sites illégitimes

CSA SECURITY GUIDANCE REFERENCE

Domain 2: Governance and Enterprise Risk Management
Domain 5: Information Management and Data Security
Domain 7: Traditional Security, Business Continuity and Disaster Recovery
Domain 9: Incident Response
Domain 11: Encryption and Key Management
Domain 12: Identity, Entitlement, and Access Management

Les dangers du Cloud Public d'un point de vue « Comptes » - Exemples

- En Avril 2010, Amazon a connu un bug sur des scripts inter-sites (XSS) qui permettait aux attaquants de détourner des informations d'identification du site
- En 2009, ont été détournés de nombreux systèmes Amazon pour exécuter des nœuds botnet Zeus
- En Juin 2014, le compte Amazon AWS de Code Spaces a été compromis
  - Tous les actifs de l'entreprise ont été détruits…
  - https://www.infoworld.com/article/2608076/murder-in-the-amazon-cloud.html

Les dangers du Cloud Public d'un point de vue « Malveillance »

- Les risques de malveillance interne existent aussi bien pour les systèmes d'information traditionnels que pour les environnements de type Cloud Computing.

- Quelques exemples illustrant ce type de risques :
  - L'ingénieur commercial licencié qui quitte son entreprise avec une **copie des fichiers clients**.
  - L'informaticien administrant le serveur de messagerie qui **accède aux boîtes des membres du comité de direction**.
  - Les fraudes financières impliquant des **modifications de données sur les applications comptables** de l'entreprise.
  - Un développeur **cache un morceau de code** (backdoor) dans les sources d'un programme pour réaliser des accès ultérieurs sans authentification.

CSA SECURITY GUIDANCE REFERENCE

Domain 2: Governance and Enterprise Risk Management
Domain 5: Information Management and Data Security
Domain 11: Encryption and Key Management
Domain 12: Identity, Entitlement, and Access Management

Petit jeu….

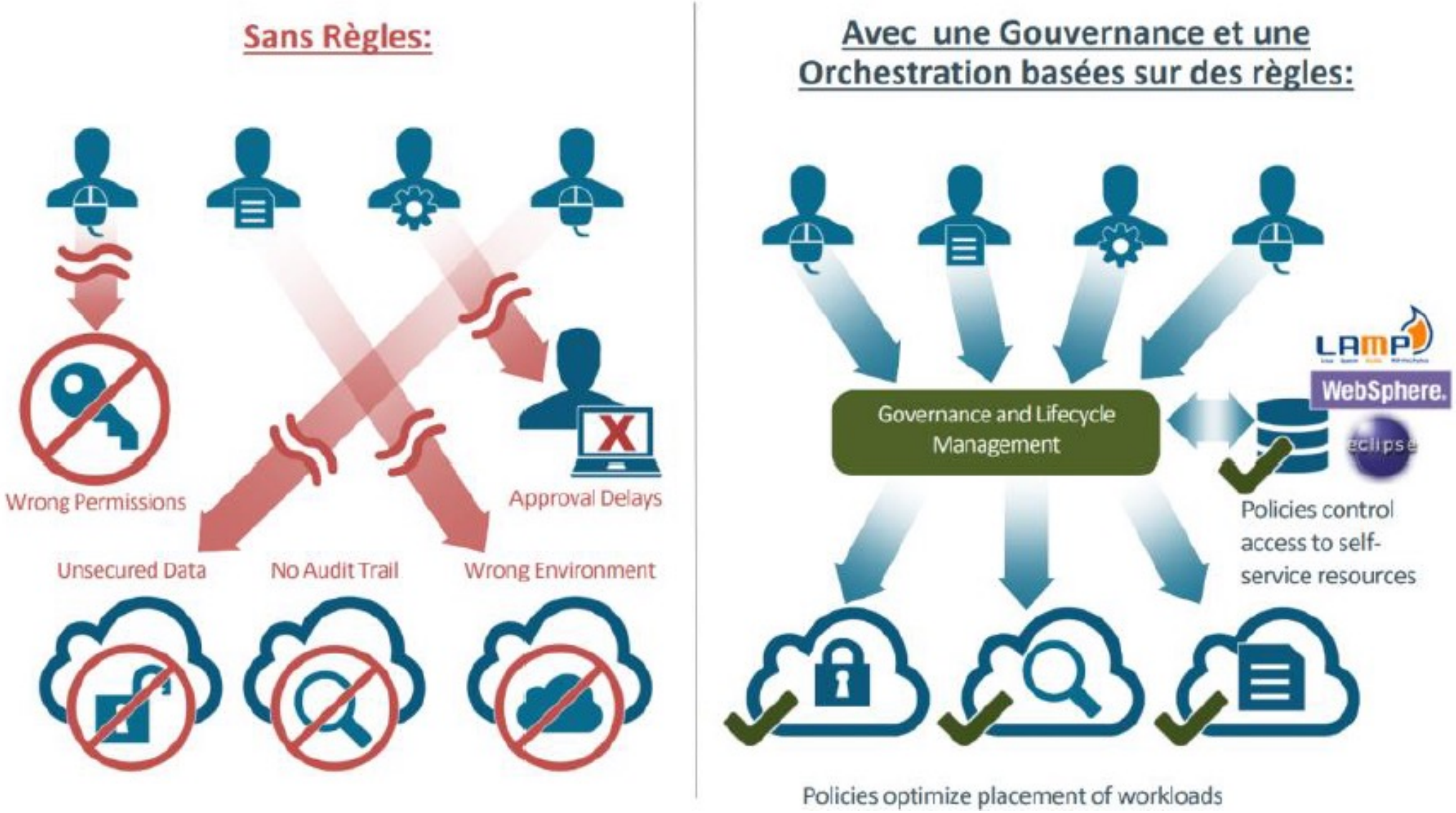
/etc/hosts ; /etc/passwd , /etc/shadow Yellow pages Nis et NIS+
PAM (Pluggable Authentification Manager) LDAP
IAM et CIAM
Aws Directory, Azure AD et Google Cloud identity
IDP ou Identity Provider ?
Open IOD Connect
Oauth 2
AWS Cognito

Travail en 8 groupes . 30 mn + 5 mn de presentation

Les dangers du Cloud Public d’un point de vue « identités IAM »

- Permet d'administrer et de gérer les comptes utilisateurs et les ressources de l'entreprise, y compris les droits d'accès
- La gestion des identités et des accès inclut les fonctionnalités permettant de gérer l'identité d'un utilisateur dans le réseau
- Permet d'authentifier les utilisateurs sur le réseau et de pouvoir assurer la traçabilité des droits demandés par l'utilisateur sur le réseau

Les dangers du Cloud Public d'un point de vue « identités IAM »



Les dangers du Cloud Public d'un point de vue « identités IAM »

- L'utilisateur final prouve son identité sur le réseau
- Méthode traditionnelle :
  - nom d'utilisateur et mot de passe.
- L'autre méthode
  - Combiner mémorisation et support physique.
  - Badge, téléphone portable, jeton, empreintes digitales, etc.
  - Ces dernières étant considérées comme des authentifications fortes ou méthode d'authentification à facteurs multiples

Les dangers du Cloud Public d’un point de vue « identités IAM »

- En plus de l'authentification, la partie autorisation/droits d'accès joue un rôle primordial au niveau de la Gestion des Identités et des Accès.
- L'autorisation détermine à quels éléments (ressources) un utilisateur peut accéder dans le réseau.
- Ces ressources regroupent : les systèmes, les applications, les imprimantes, les partages, etc..
- Fait appel à un ensemble de règles souvent complexes. Les droits d'accès sur le réseau de l'entreprise sont en effet attribués en fonction du poste/fonction occupé par chaque utilisateur.

Les logiciels « identités IAM »

- Permet à l'utilisateur de rationaliser l'ensemble des procédures touchant à la gestion de l'authentification et des autorisations.

- Ces fonctionnalités permettent notamment :
  - Le Provisioning automatique des comptes utilisateurs
  - La Gestion des workflows et le Self-Service
  - La Gestion des mots de passe
  - Le Single Sign-On (SSO)
  - Le RBAC (Role Based Acces Control) /Gouvernance des accès
  - Audit & Conformité

L’authentification multi facteurs

- Système de sécurité qui fait appel à plusieurs méthodes d'authentification
- A partir de différentes catégories d'informations d'identification (des preuves), on vérifie l'identité de l'utilisateur
- Chaque facteur d'authentification supplémentaire augmente l'assurance qu'une entité se livrant à une quelconque communication ou demandant l'accès à un système est bien la personne ou l'organisme qu'elle prétend être

L’authentification multi facteurs

- Facteurs mémoriels
  - informations qu'un utilisateur doit pouvoir fournir pour se connecter. Comprend les noms d'utilisateur ou identifiants, les mots de passe, les codes PIN et les réponses aux questions secrètes.
- Facteurs matériels
  - désignent les éléments qu'un utilisateur doit avoir en sa possession. un Token, un jeton de mot de passe à usage unique (OTP), un porte-clé, un badge d'employé ou un smartphone avec une application OTP.
- Facteurs corporels
  - caractéristiques biologiques de l'utilisateur. Méthodes d'authentification biométrique (balayage de la rétine, de l'iris, l'analyse de l'empreinte digitale, l'identification des veines du doigt, le lobe de l'oreille)
- Facteurs de lieu
  - la localisation de l'utilisateur à l’aide des smartphones facilite l'authentification dans ce cas : en effet, la plupart des smartphones sont équipés d'un GPS, qui permet de confirmer le lieu de la connexion
- Facteurs temporels
  - l'heure permet la vérification des identifiants par rapport à des emplois du temps. Exemple: on ne peut pas utiliser sa carte en France puis en Russie 15 minutes plus tard

Le modèle Cloud Public : Les failles et menaces

- Le Cloud Computing représente le sommet de l'externalisation informatique
- Craintes d'une perte de contrôle sur les systèmes d'informations
  - Ex: Yahoo et Orange se sont vues pirater les informations de millions d'utilisateurs
- Avec le Cloud public, les données et/ou applications sont confiées à un tiers
  - Sur lequel l'on exerce un faible contrôle
  - Les données sont protégées par la loi de la zone où elles sont hébergées.
- On ignore
  - leur lieu d'hébergement
  - la loi qui les protèges
- Initiatives de la France et l'Allemagne
  - Etablir un Cloud européen pour sécuriser leurs données stratégiques et celles de leurs entreprises
  - Réflexion sur les frontières, même dans le Cloud Computing
  - Conformité aux juridictions du pays

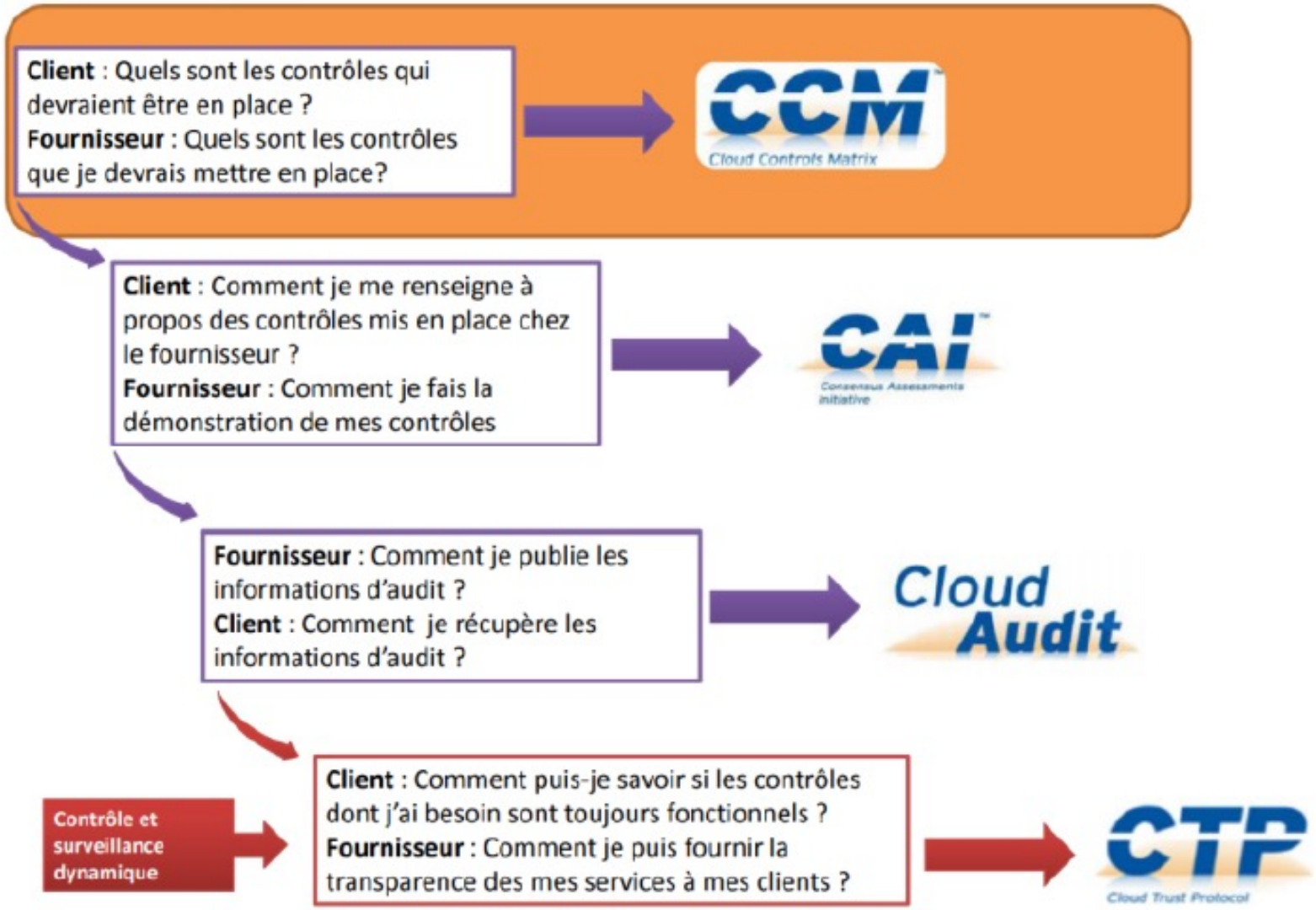
Le modèle Cloud Public : Les exemples de failles

- Des données critiques d'Accenture stockées sans sécurité dans AWS
  - https://www.lemondeinformatique.fr/actualites/lire-des-donnees-critiques-d-accenture-stockees-sans-securite-dans-aws-69671.html
- AWS est tombé : pourquoi le web vous semble cassé
  - https://www.numerama.com/tech/237047-aws-est-tombe-pourquoi-le-web-vous-semble-casse.html
- Des données du Pentagone stockées sur AWS accessibles publiquement
  - https://www.silicon.fr/donnees-pentagone-stockees-aws-190971.html
- Meltdown et Spectre : quels impacts sur Amazon Web Services ?
  - https://blog.alterway.fr/meltdown-et-spectre-quels-impacts-sur-amazon-web-services.html

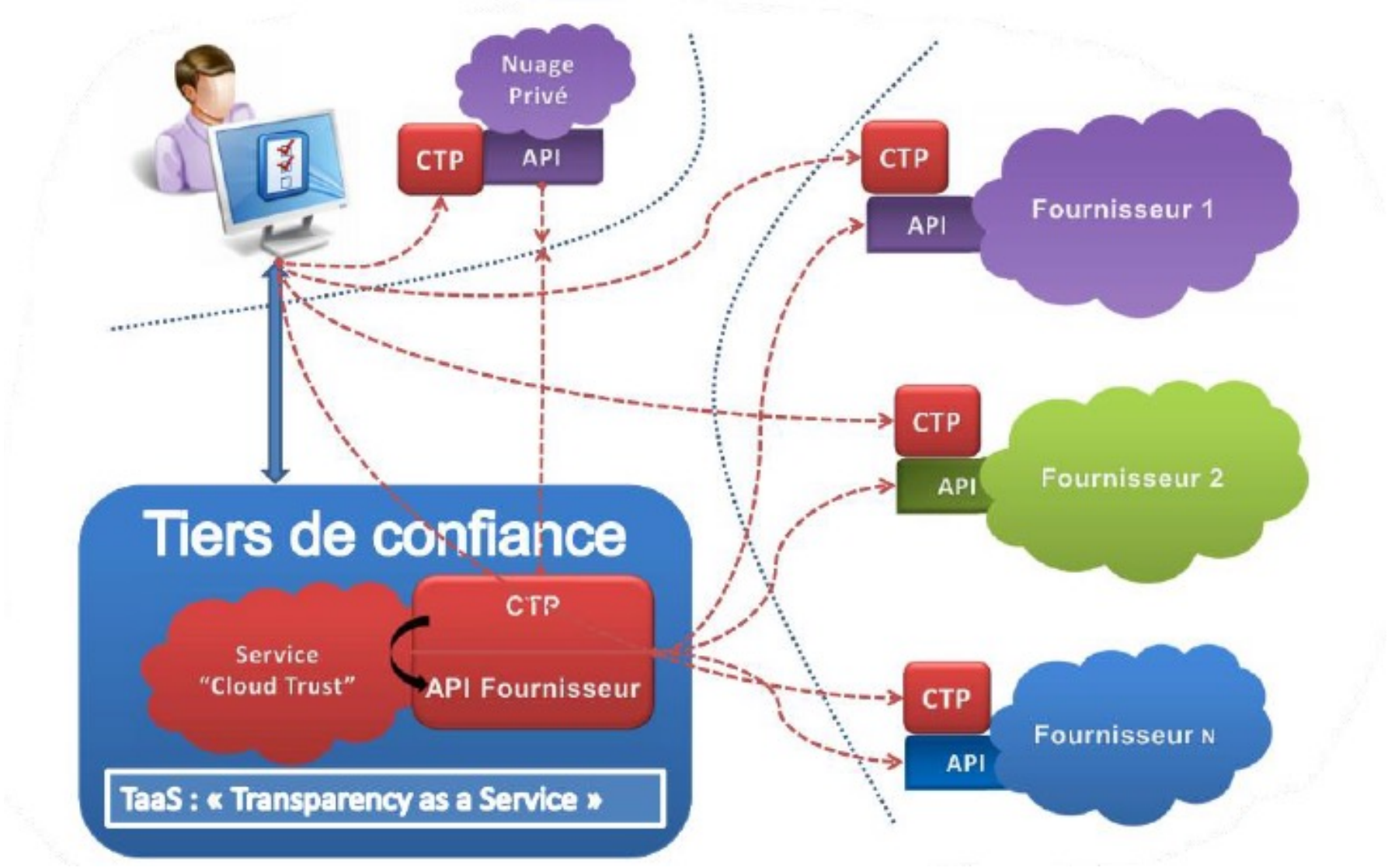
Le modèle Cloud Public : Gouvernance, Risques et Compliance (GRC) – Les outils

- Famille de 4 projets de recherche donnant 4 outils
  - CCM : Cloud Control Matrix
  - CAIQ : Consensus Assessment Initiative Questionnaire
  - Cloud Audit
  - Cloud Trust Protocol

Le modèle Cloud Public : Gouvernance, Risques et Compliance (GRC) – Les outils



Le modèle Cloud Public : Gouvernance, Risques et Compliance (GRC) – Le CTP



Le modèle Cloud Public : GRC – Synthèse

Fournit	Outils	Description
Éléments de contrôle fondamentaux	CCM	Guide les fournisseurs et assiste les clients pour l'évaluation « sécurité » d'un fournisseur de Cloud Computing
Questionnaire de préaudit permettant d'inventorier les contrôles	CAI	Documente quels contrôles de sécurité sont implantés
Délivre les résultats d'audits	Cloud Audit	Interface pour automatiser la collecte des informations d'audit du fournisseur
Surveillance en continue des éléments de transparence	CTP	Mécanismes pour demander et recevoir les affirmations et preuves de l'état courant des services chez le fournisseur

Le modèle SECaaS : Les grands principes

- Le fournisseur en charge de sécuriser l'infrastructure en mode SECaaS fournira tous les services clefs en mains
- Les logiciels de protection tourneront dans le Cloud
- La puissance du Cloud permet de lutter de manière efficace et compétitive contre la cybercriminalité :
  - Ressources et puissances de calcul scalables
  - Rapidité et élasticité des infrastructures
  - Facturation à l'usage…
- De fait, les entreprises bénéficient avec une telle solution, d'une expertise et d'une technologie qui leur permettent de se protéger contre la plupart des attaques.

Le modèle SECaaS : Les grands principes

- La SECaaS peut-elle être la réponse à ce besoin de sérénité ? Peut-on s'abonner à la sécurité comme on s'abonne à NetFlix ?
- La SECaaS est une solution qui permet d'externaliser la gestion d'un panel de services:
  - Antivirus
  - Scans périodiques
  - Rapports de préconisations
  - Audit
  - …
- Ceci afin de répondre à l'ensemble des défis que posent la cyber sécurité moderne

Le modèle SECaaS : Les avantages

- Permet de filtrer les flux dynamiquement, et de ne rediriger vers l'entreprise que les flux sains.
- Exemple : Le filtre antispam et antivirus
  - La base virale est dans le cloud, constamment mise à jour, les flux sont orientées vers le prestataire qui ne redirige que les messages "propres"
- L'entreprise ne gère plus les questions de dimensionnement, d'approvisionnement, de mise à niveau du matériel et des logiciels, et du maintien en condition opérationnelle
- Via un abonnement mensuel, elle bénéficie d'une meilleure fiabilité quant à la protection de ses données, libérant des ressources internes pour gagner du temps et donc de la productivité sur des projets plus structurants, ou davantage orientés "métiers"

Le modèle SECaaS : La démarche

- Identifier le lieu physique où elles sont stockées et l'entreprise qui les stockes
- C'est l'emplacement des données et l'implantation du siège de l'entreprise qui vont déterminer les règlementations et lois auxquelles ces données sont soumises.
  - Sans prendre peur à la moindre notion de Patriot Act

Le modèle SECaaS : La démarche – Ne pas faire confiance aux normes

- Par exemple, l'infrastructure AWS est certifiée PCI-DSS, mais pas que toutes les entreprises hébergées sur AWS en bénéficient par défaut
- Cela montre simplement qu'il est possible d'obtenir la certification puisque AWS est conforme
- Seuls certains clients ont demandé à être certifiés et respectent les procédures imposées par la norme

Le modèle SECaaS : Les mythes

- On s'imagine des serveurs partagés sur les clouds publics et des serveurs dédiés sur les clouds privés
- Toutefois:
  - Il est recommandé de créer son propre espace privé virtuel au sein d'un cloud public
  - Les cloud public bénéficient d'équipes sécurité particulièrement bien dimensionnées
- Plus que « quel cloud choisir ? », la question est réellement « comment sécuriser mon environnement, quel que soit le cloud ? ».

Le modèle SECaaS : Les bonnes pratiques – Tools & Data

- Les fournisseurs de cloud s'occupent de la sécurité de leurs infrastructures
  - Publication d'outils permettant la protection de l'architecture
- Les clients sont garants de la protection des données
  - Nécessite de bien évaluer les risques, et de choisir les solutions adaptées pour se protéger

Le modèle SECaaS : Les bonnes pratiques – Le code

- Ne laisser aucune vulnérabilité dans le code source
- Avant la mise en production, réaliser un audit et des tests d'intrusion pour découvrir les failles et les corriger avant qu'elles ne soient exploitées
- Répéter ces tests régulièrement afin de vérifier qu'aucune vulnérabilité n'a été oubliée ou exposée par une montée en version, un module supplémentaire, un nouveau développement…

Le modèle SECaaS : Les bonnes pratiques – Le Code

- Au-dessus du code source, il y a souvent une application web.
  - WordPress, Magento, Drupal, Typo3…
- Des failles informatiques sont régulièrement publiées sur ces technologies : leur mise à jour régulière est nécessaire pour rester protégé

Le modèle SECaaS : Les bonnes pratiques – L'architecture

- Le type de cloud importe peu, c'est la manière dont la plateforme et construite qui fait la différence
- De nombreuses solutions existent pour contrer tout type d'attaques malveillantes
  - anti-DDoS, pare-feu applicatif, système de détection d'intrusion…
- Il faut choisir selon les risques auxquels sont confrontés l'entreprise

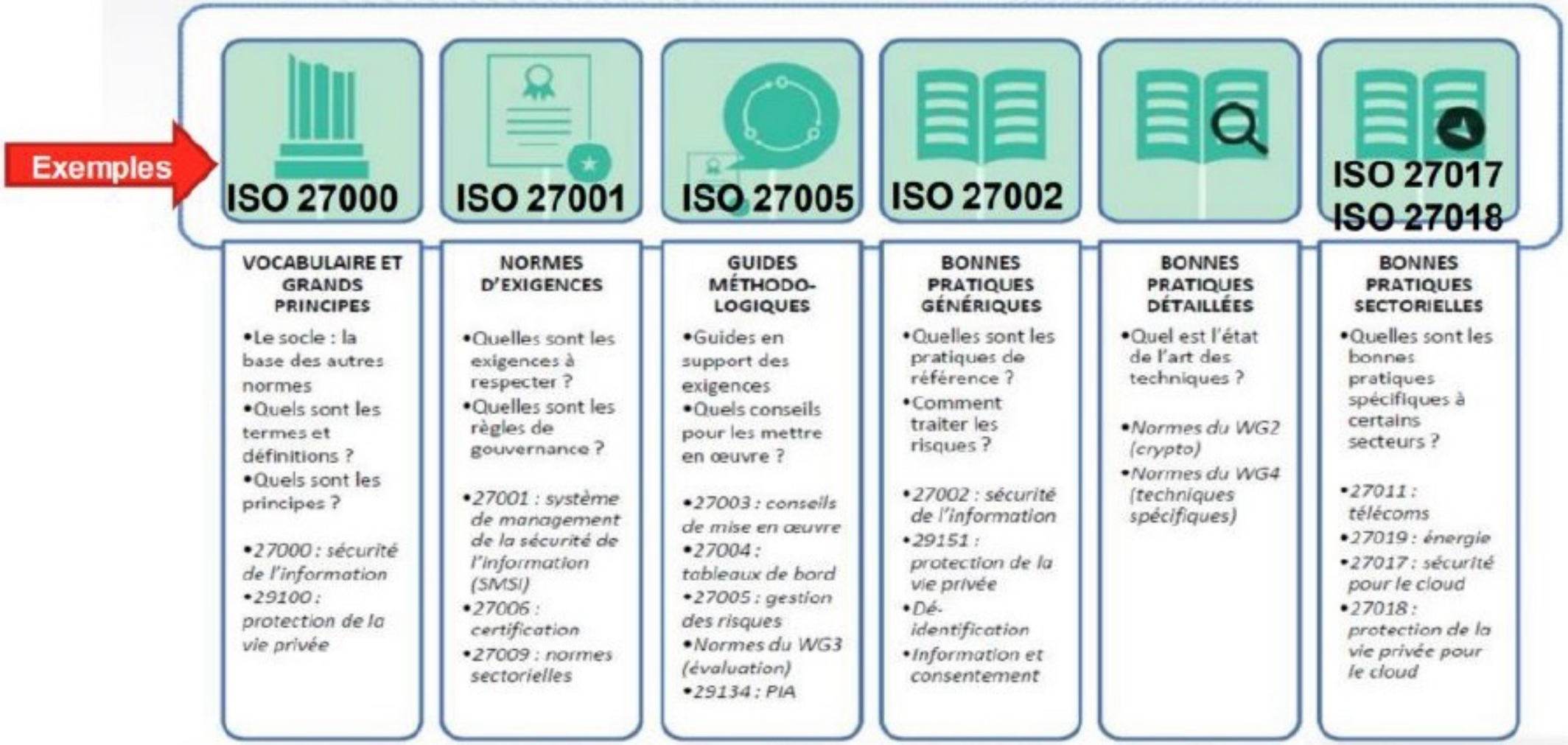
Le modèle SECaaS : Les bonnes pratiques – L'humain

- Ne pas oublier la dimension humaine, encore impliquée dans la majorité des vols ou pertes de données de grande ampleur
- Les pertes sont souvent liées à des négligences ou erreurs humaines
- Des formations ou sessions de sensibilisation sur les bonnes pratiques de sécurité en entreprise peuvent préparées les équipes
- Adopter une gestion des accès restrictive à votre SI, que ce soit en interne ou avec vos prestataires : la confiance n'exclut pas le contrôle

Le modèle SECaaS : Les bonnes pratiques – Les normes

- ISO/IEC 17788:2014
  - Technologies de l'information — Informatique en nuage — Vue d'ensemble et vocabulaire
- ISO/IEC 17789:2014
  - Technologies de l'information — Informatique en nuage — Architecture de référence
- ISO/IEC 27017:2015
  - Technologies de l'information — Techniques de sécurité — Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage
- ISO/IEC 27018:2019
  - Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII

Le modèle SECaaS : Les bonnes pratiques – Les normes



Les 7 conseils de la CNIL sur la confidentialité des données

- Des recommandations pratiques permettant de définir le partage des responsabilités

- Avant tout engagement commercial, l'organisme souhaitant recourir à une prestation d'externalisation devra mener une réflexion spécifique afin :
  - D'identifier clairement les données et les traitements qui passeront dans le cloud ;
  - De définir ses propres exigences de sécurité technique et juridique ;
  - De conduire une analyse de risques afin d'identifier les mesures de sécurité essentielles pour l'entreprise ;
  - D'identifier le type de cloud pertinent pour le traitement envisagé ;
  - De choisir un prestataire présentant des garanties suffisantes ;
  - De revoir la politique de sécurité interne ;
  - De surveiller les évolutions dans le temps.

Les 7 conseils de la CNIL permettent :

- De déterminer la qualification juridique du prestataire : s'agit-il d'un simple sous-traitant au sens de l'article 35 de la loi Informatique et libertés ou bien d'un responsable conjoint de traitement au sens de l'article 2 de la Directive 95/46/CE ?

- La CNIL recommande que les obligations et le périmètre des responsabilités de chacun, notamment en matière de sécurité, soient clairement établis. Cette distribution des responsabilités doit être actée en amont, par exemple dans le contrat de prestation de services, et cela de la manière la plus précise possible.

- La CNIL retient la responsabilité conjointe du client et du prestataire lorsque le client ne peut pas réellement donner d'instructions à son prestataire et ne peut pas contrôler l'effectivité des garanties de sécurité apportées par ce dernier. Ceci peut être dû notamment à des offres standardisées, non modifiables par les clients, et à des contrats d'adhésion qui ne laissent aucune possibilité de négociation. Cette absence d'instruction et de moyens de contrôle étant constatée pour certains services de PaaS et de SaaS publics, le prestataire pourrait donc dans ces cas être a priori considéré comme responsable conjoint de traitement.

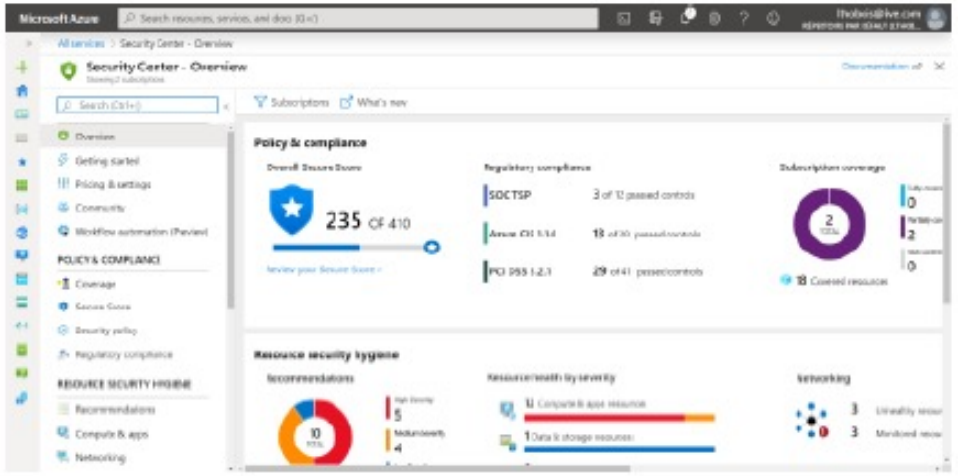
- D'évaluer le niveau de protection assuré par le prestataire aux données traitées : le niveau de sécurité offert par le prestataire est-il supérieur ou égal à celui qui était préalablement assuré ?

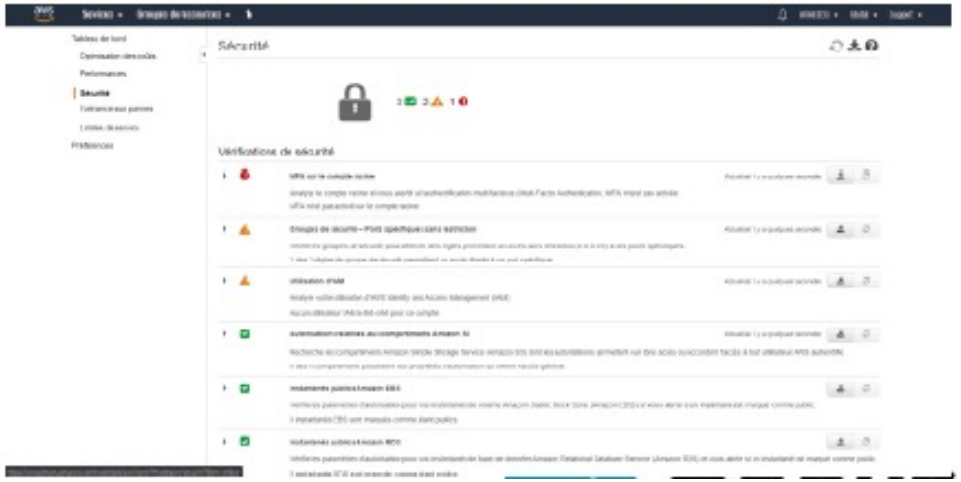
Les 7 conseils de la CNIL permettent les considérations :

- Le cloud ne doit pas aboutir à une diminution du niveau de protection des données, particulièrement s'agissant de donnés sensibles, au sens de l'article 8 de la loi Informatique et libertés.
- Des modèles de clauses pour définir clairement les responsabilités dans un contrat
- Que la responsabilité du traitement soit conjointe ou bien à la charge unique du client, les responsabilités du client et du prestataire doivent être expressément définies

Le modèle SECaaS : Les outils intégrés

- Azure
  - Security Center
  - Advisory Board
  - Logs analytics
  - …
- AWS
  - Trusted Advisor
  - CloudTrail
  - CloudWatch
  - …





Le modèle SECaaS : Les CASB – Cloud Access Security Broker pour la maîtrise du SaaS

Principales Fonctions :

- Les solutions CASB - une technologie incontournable pour l'adoption du SaaS - ont évolué rapidement ces dernières années.
- Les principaux fournisseurs prennent en charge un large éventail de modes de déploiement, de sécurité des données, de protection contre les menaces et de fonctionnalités de visibilité et de conformité.
- Les fonctionnalités de visibilité et d'application des règles pour les applications cloud «shadow IT» non approuvées sont très matures
- Toutes les solutions s'intègrent aux pare-feu d'entreprise ou aux passerelles Web sécurisées. La plupart offrent leur propre option de déploiement de proxy direct.
- Les fonctionnalités d'application des politiques et de gouvernance pour les applications cloud approuvées montrent une plus grande différenciation entre les solutions. Cela inclut les modes de déploiement (modes disponibles et préférés), la possibilité d'intégrer de nouvelles applications cloud et l'étendue des fonctionnalités de sécurité des données et de protection contre les menaces.
- Les CASB étant des plates-formes de cas multifonctions et multi-usages, les interfaces utilisateur de gestion et de surveillance ont tendance à être complexes. Les fonctionnalités de gestion de l'interface utilisateur et la personnalisation varient.

Le modèle SECaaS : Les CASB – Cloud Access Security Broker pour la maîtrise du SaaS

Recommandations et bonnes pratiques :

- Évaluez les solutions en fonction des cas d'utilisation actuels et des cas d'utilisation qui devraient émerger à court et moyen terme. Cela façonne des exigences précises concernant les modes de déploiement et l'application des stratégies, et peut aider à créer une liste restreinte.
- Concentrez la sélection et les preuves de concept sur la différenciation des fonctionnalités de sécurité des données et de protection contre les menaces.
- Effectuez des tests par rapport aux principales applications cloud, telles que Microsoft O365 et AWS, et évaluez la prise en charge des applications et des fonctionnalités plus petites et stratégiques pour l'intégration de nouvelles applications.
- Privilégiez les contrats à plus court terme lors du choix d'une solution CASB. Le marché est toujours en évolution, notamment en termes de prise en charge de tous les modes de déploiement ou de fonctionnalités avancées.

Le modèle SECaaS : Les CASB – Le marché

Le marché des (CASB) a été l'un des marchés de la sécurité de l'information à la croissance la plus rapide ces dernières années. Depuis 2017
Les CASB fournissent des fonctionnalités de sécurité essentielles pour protéger votre cloud SaaS, ainsi qu'une administration d'infrastructure en tant que service (IaaS), un stockage cloud et une plateforme en tant que service (PaaS) limitée.

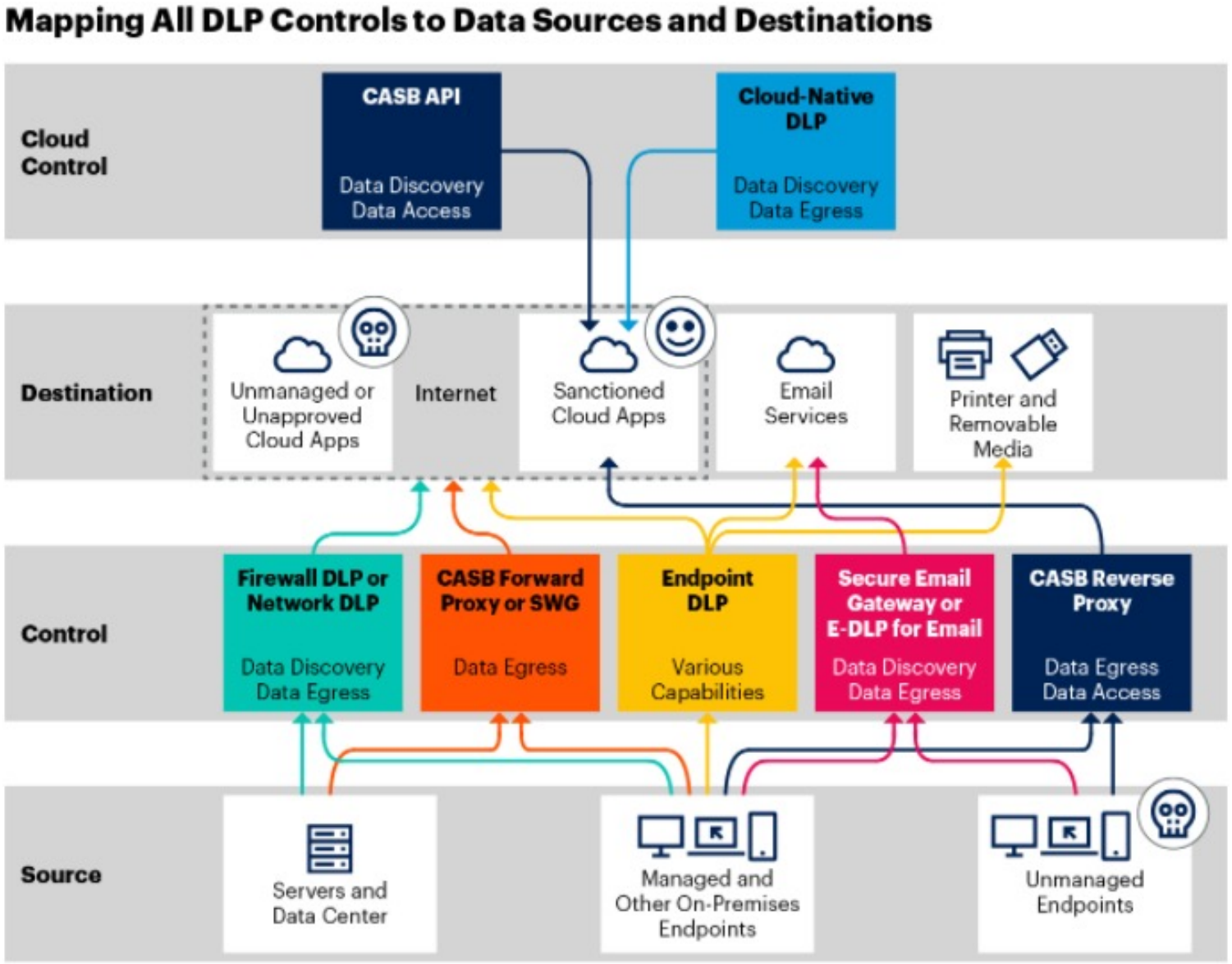
Le modèle SECaaS : Les CASB – Les principales fonctions

1) Architecture et déploiement: y compris les options de déploiement, les agents et la prise en charge de la redirection, les centres de données, la prise en charge géographique, la bande passante et la protection contre les dénis de service distribués (DDoS).
2) La Sécurité des données: y compris la prévention des pertes de données (DLP), la classification et le cryptage des données.
3) Protection contre les menaces: y compris le contrôle d'accès adaptatif, l'anti-malware, la protection avancée contre les menaces et l'intelligence des menaces.
4) Visibilité et risque: y compris l'audit, la création de rapports et les risques liés aux applications cloud, ainsi que l'analyse du comportement des entités utilisateur (UEBA).
5) Gestion et opérations: y compris la configuration, l'interface utilisateur, la journalisation, la réponse aux incidents et d'autres capacités opérationnelles.
6) L'intégration d'entreprise est couverte par des critères individuels. Cela comprend des capacités d'intégration avec des passerelles Web sécurisées (SWG), des pare-feu (FW), la gestion des identités et des accès (IAM), la gestion des identités et des accès (IAM) dans le cloud, la prévention de la perte de données d'entreprise (EDLP), la gestion de la mobilité d'entreprise (EMM) et la gestion des informations et des événements de sécurité. (SIEM).

Les CASB – Exemple Microsoft Cloud App Security (MCAS)

Architecture and Deployment		
Deployment modes	Medium	▪ Offers API and reverse proxy deployment modes but lacks a virtual appliance reverse proxy. ▪ Supports API integration via app connectors. ▪ No dedicated forward proxy support. ▪ Integrates with SWGs and enterprise network firewalls for traffic log ingestion, access control to unapproved apps, and reporting. Source: Connect Apps
Geographic coverage	Low	Dedicated data centers maintained by MCAS are: ▪ North America: Three Azure data centers ▪ Europe: Two Azure data centers
DDoS protection	High	▪ MCAS leverages Azure DDoS Protection. It provides a scrub feature at the network edge.

Les CASB – Cas d'usage DLP (Data Lost Prevention)



L'accélération de la crise du COVID et le télétravail

Un marché de services très dynamique

17.5 %

Forecast YoY growth du marché de services Cloud entre 2020 to 2025 (avant COVID)*

Une acceleration en 2020 (+30% ytd)

Des investissements massifs des Hyperscalers pour assurer la résilience de leurs capacités

Une consolidation du marché autour des deux acteurs majoritaires : MS et AWS c (48% growth ytd)

Les services **PaaS connaissent la croissance la plus importante (Gartner)**

L'enjeu énergétique devient central

Les Hyperscalers mettent en œuvre des stratégies "lock-in"

Egress fees – *s'applique en cas de Mobilité des données vers un autre CSP.*

Contract terms – *en moyenne, les consommateurs sont liés pour 3 à 5 ans avec les CSP*

Free tier offerings – *prix initiaux attractifs à l'entrée, mais bundle avec d'autres services*

Complex technical frameworks – *les SLA exigent une expertise propre et ne sont pas transparents*

Ces stratégies ont fait l'objet d'un rapport récent du congrès américain et d'initiatives de la Commission européenne.

Pour répondre à ces tendances, nos clients demandent des solutions pour accroître la portabilité et l'interopérabilité des services et disposer de **solutions multicloud.**

La 'containerisation' et le multiCloud sont au cœur des stratégies gagnantes***

93% *Des entreprises privilégient une stratégie multi-cloud*

78% *Ont une stratégie de cloud hybride*

2 standards émergent:
- ***Kubernetes*** pour l'orchestration
- ***Docker*** pour la containerisation

Le Multi-cloud réduit le poids des effets lock-en permettant aux clients de basculer les ***computing workloads***

La gestion des identités devient un enjeu stratégique

Les solutions hybrides permettant **d'envisager différents niveaux de sécurité**

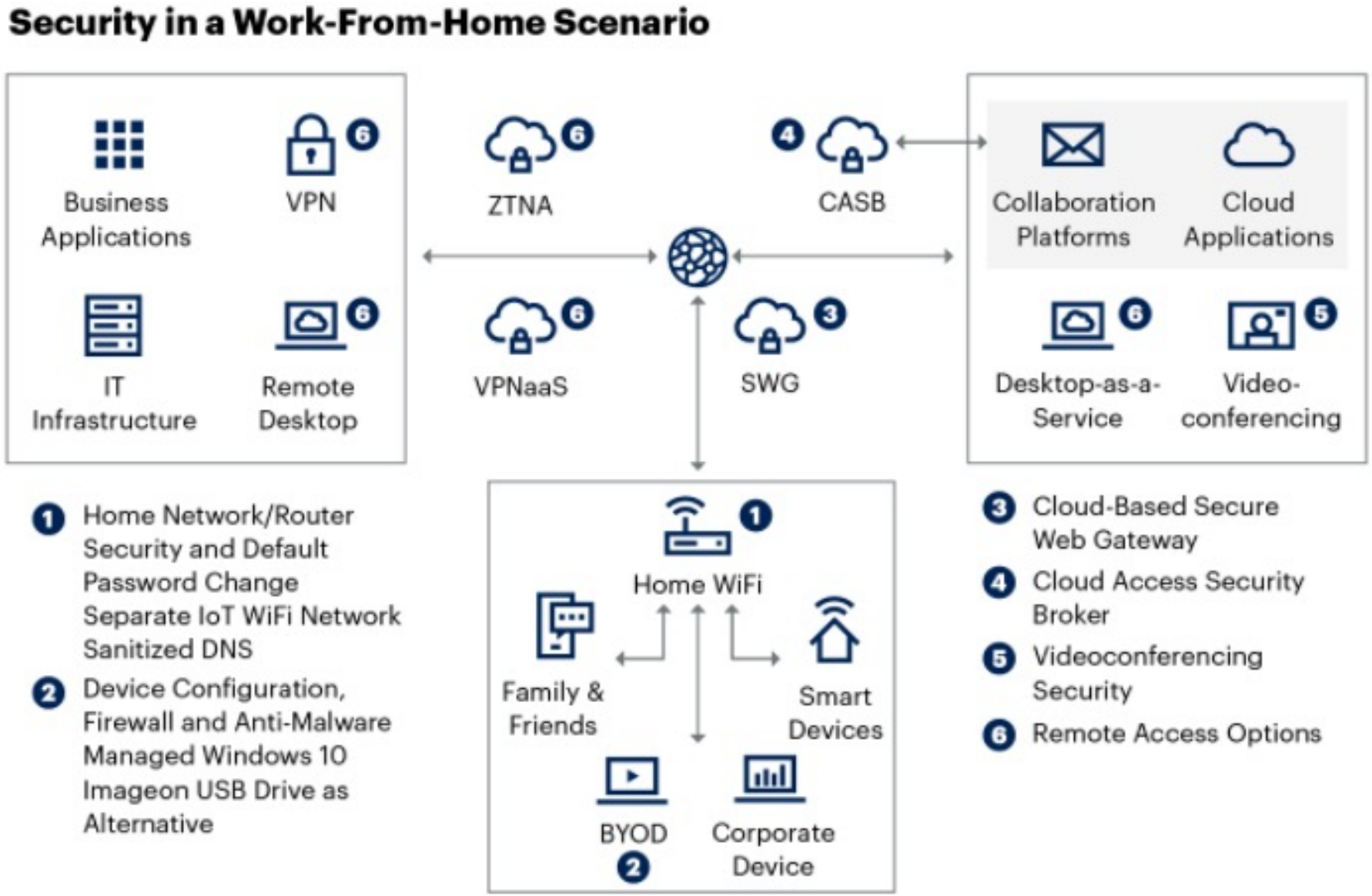
Le Edge computing va redistribuer les cartes et favoriser les reseaux décentralisés

2018 20 % → **2025** 80 %

*du data processing devra basculer sur des plateformes 'edge' d'ici 2025**

> Le Edge computing va améliorer l'expérience utilisateur en permettant de réduire la **latence**, de faciliter la **décision en temps réel** et de réduire les coûts d'infrastructure

> Les entreprises font face à des challenges d'**infrastructure**, de **cybersecurité**

> **Les Hyperscalers ont lance des offres de services Edge** en lien avec leurs services cloud centraux

L’accélération de la crise du COVID et le télétravail