



# MOVE TO CLOUD

Promesses et défis

Janvier 2021

Ameur Kais



# Sommaire

## 1. Présentation du Cloud Computing

2. Pourquoi et comment migrer sur le Cloud ?

3. Les grands enjeux pour les acteurs des services financiers

4. Services du Cloud

5. Annexes

# Qu'est-ce que le Cloud Computing ?



## Une définition de l'ACPR (2013)



Définition basée sur celle du NIST



*Le Cloud computing consiste à déporter sur des serveurs distants des données et des traitements informatiques traditionnellement localisés sur des serveurs locaux, voire sur le poste de l'utilisateur. Il permet l'accès via un réseau, généralement entendu comme Internet, à la demande et en libre service, à des ressources informatiques virtualisées et mutualisées habituellement facturées à l'usage.*

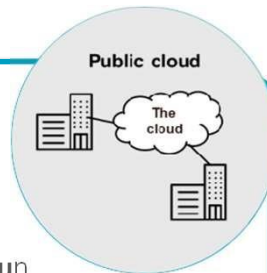
Le Cloud computing permet donc de passer à un modèle où les ressources informatiques (hardware, voire software) peuvent être louées au lieu d'être acquises.

- **Facilité d'accès** - Accès à du stockage, à de la puissance de calcul, à des applications
- **Scalabilité & Agilité** - Accès à ces ressources à la demande, accès à des outils d'intelligence artificielle
- **Modèle économique** - Paiement à l'utilisation: coûts variables plutôt que coûts fixes

## 1

### Public Cloud

Le Cloud public désigne une infrastructure gérée par un opérateur externe et présente uniquement dans les locaux du fournisseur de Cloud.



- Scalabilité
- SI plus flexible et agile/adaptation aux besoins immédiats
- Paiement à l'usage

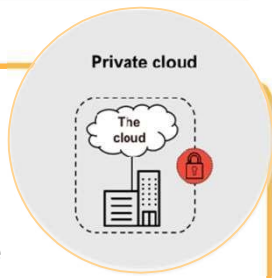


- Pas de maîtrise de l'infrastructure
- Sécurité des données

## 2

### Private Cloud

Le Cloud privé désigne une infrastructure qui est spécifique et gérée par la société elle-même, par un prestataire spécialisé ou une combinaison de ceux-ci. Ce sont les serveurs de la société – qui peuvent exister dans ou hors des locaux – qui vont gérer l'ensemble des données pour tous les utilisateurs de l'entreprise.

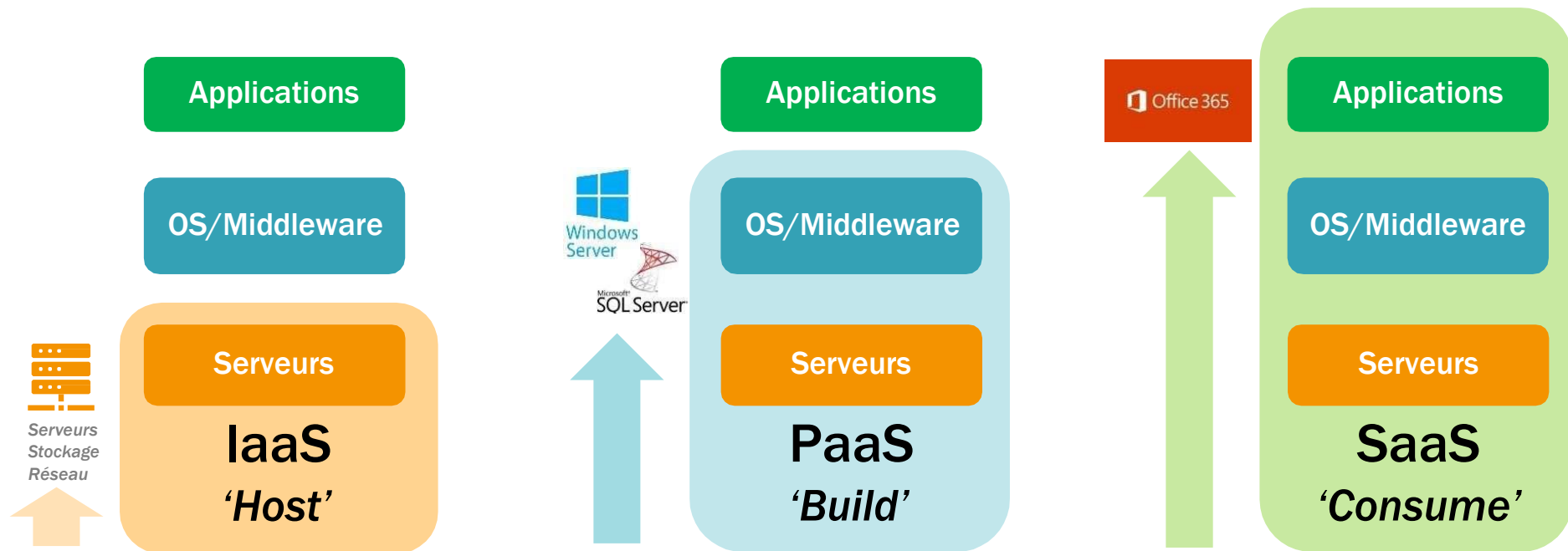


- Fait sur-mesure pour les besoins de la société
- Maîtrise de l'infrastructure
- Sécurité des données



- Investissement initial important (infrastructure et mises à jour)
- Peu flexible/scalable

# Les modèles de service du Cloud computing



## Infrastructure-as-a-service

L'IaaS (Infrastructure as a Service) offre une infrastructure informatique comme de la puissance de calcul, des machines virtuelles incluant un système d'exploitation, du stockage, des services de sauvegarde.



## Platform-as-a-service

Le PaaS (Platform as a Service) fournit une plateforme de développement et/ou d'exécution intégrée, reposant sur un catalogue de composants logiciels et techniques standardisés dont l'infrastructure sous-jacente est transparente pour l'utilisateur.



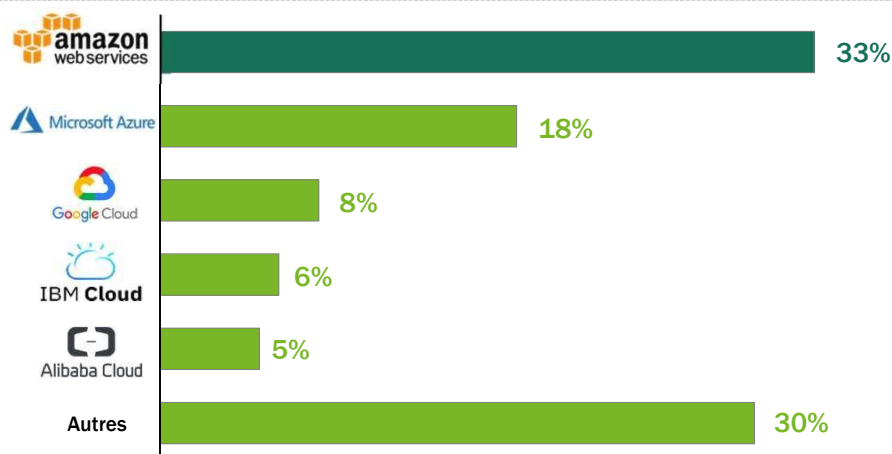
## Software-as-a-service

Le SaaS (Software as a Service) est une solution applicative répondant à un domaine d'utilisation précis supportant une fonction métier (gestion de la relation clientèle, gestion financière, ...) ou un service transverse (messagerie, outils collaboratifs, ...).

# Panorama du marché : principaux fournisseurs & chiffres clés



## Panorama des principaux fournisseurs de services d'infrastructure Cloud – Parts de marché IaaS/PaaS



Source : <https://www.statista.com/chart/18819/worldwide-market-share-of-leading-Cloud-infrastructure-service-providers/>

- **AWS**, en tête, maintient une part de marché supérieure à **30 %**, tandis que Microsoft, Google et Alibaba gagnent de plus en plus de parts de marché. Lancé en 2006, AWS bénéficie toujours d'une avance historique.
- Le reste du marché est composé de services de Cloud privé hébergés et gérés, où **IBM** est le leader du marché et où des sociétés comme Rackspace et **OVH** occupent une place plus importante.
- **Google Cloud Platform** (GCP) capitalise sur l'expertise de Google en IA (intelligence artificielle) et sur Kubernetes facilitant ainsi les déploiements multi-cloud. Le lancement de Google Anthos lancé en 2019 répond à cette stratégie.
- **Microsoft Azure** peut s'appuyer sur la forte présence de Microsoft dans les entreprises et l'intégration avec les autres services Microsoft.

Acteurs clés	Fournisseur Cloud					
	Développeur	Amazon	Microsoft	Alibaba Cloud	Google	IBM
	1 <sup>ère</sup> version	2006	2010	2009	2008	2009
	Chiffres clés	<ul style="list-style-type: none"> <li>CA Amazon : 280 mds \$ dont 27 mds \$ AWS</li> <li>Croissance* : +49%/an</li> </ul>	<ul style="list-style-type: none"> <li>CA Microsoft : 90 mds \$ dont 20 mds \$ Azure</li> <li>Croissance : +34%/an</li> </ul>	<ul style="list-style-type: none"> <li>CA Alibaba Cloud : 5,6 mds \$</li> <li>Croissance : +62%/an</li> </ul>	<ul style="list-style-type: none"> <li>CA google : 46 mds \$</li> <li>Dont 8,9 mds \$ Cloud</li> <li>Croissance : +53%/an</li> </ul>	<ul style="list-style-type: none"> <li>CA IBM : 77 mds \$ dont 5 mds \$ Cloud</li> <li>Croissance : +11%/an</li> </ul>
	Principaux clients en France (secteur financier)	 	    	<ul style="list-style-type: none"> <li>- N/A</li> </ul>	  	   

Ameur Kais



# Principaux fournisseurs en France









## Panorama des principaux fournisseurs de services d'infrastructure Cloud français – Parts de marché IaaS/PaaS

### Classement fournisseurs de Cloud en France



- En France, OVH Cloud et Orange Business Services arrivent en 3<sup>ème</sup> et 4<sup>ème</sup> position, respectivement, devant Google et IBM et derrière AWS et Microsoft. En France, Alibaba Cloud n'est pas présent dans le top 6.
- OVH Cloud, Online, Orange Business Services et Outscale sont 4 acteurs qui ont développé des offres Cloud à l'échelle internationale.

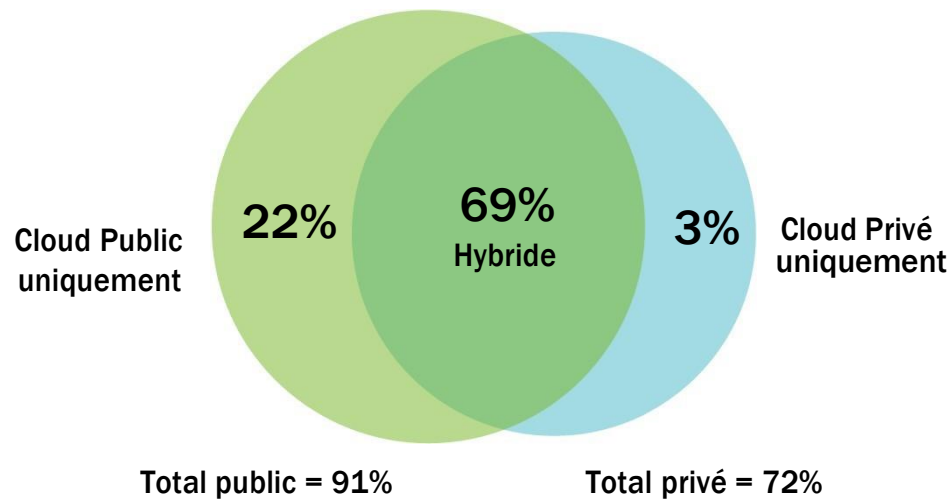
Acteurs clés	Fournisseur Cloud	 OVHcloud	 Orange Business Services	 3DS OUTSCALE	 NEURONES	 ikoula we host with care	 online by Scaleway
	Développeur	OVH	Orange Business Services	3DS Outscale (filiale Dassault Systèmes)	Neurones	Ikoula	Online by Scaleway (filiale Iliad)
	1 <sup>ère</sup> version	1999	2006	2010	2010	1998	1999
	Chiffres clés	<ul style="list-style-type: none"> <li>CA OVH Cloud : 530 m€</li> <li>Croissance : +20%/an</li> </ul>	<ul style="list-style-type: none"> <li>CA Orange : 41 mds€</li> <li>Dont 7.3 mds € OBS</li> <li>Croissance : +18% /an</li> </ul>	<ul style="list-style-type: none"> <li>CA 3DS Outscale : 25 m€</li> </ul>	<ul style="list-style-type: none"> <li>CA Neurones: 510 m€</li> <li>Croissance : +10%/an</li> </ul>	<ul style="list-style-type: none"> <li>CA Ikoula : 10 m€</li> </ul>	<ul style="list-style-type: none"> <li>CA Online Cloud : 71 m €</li> </ul>

Ameur Kais

# Panorama du marché : Cloud public ou privé ? Le marché répond « hybride »



Survey 2019 : Population de 786 Entreprises (456 GE (>1000 employés) et 330 PME)



- Le Cloud public a d'abord été perçu par les entreprises comme étant une solution adaptée à des données peu sensibles et non sujettes à la confidentialité.
- Pourtant aujourd'hui le Cloud public s'impose comme la solution la plus adoptée. Cela s'explique principalement par le fait qu'une infrastructure de Cloud privé est beaucoup plus coûteuse à mettre en place, et que les prestataires de Cloud public offrent un niveau de sécurité qui sera presque toujours supérieur à celui d'une infrastructure locale, chez une entreprise n'ayant pas migré vers le Cloud.
- Les services offerts par les prestataires de Cloud public constituent la véritable plus-value d'une migration à l'heure actuelle, et les prestataires de Cloud privé mettent progressivement en place des solutions hybrides afin d'attirer les clients qui ont choisi la solution Cloudpublic.

94%

Entreprises qui déclarent avoir recours au Cloud.  
24% de croissance dans l'utilisation du Cloud public  
8% de croissance dans l'utilisation du Cloud privé

38%

% moyen des données migrées sur un Cloud public  
33% chez les grandes entreprises  
43% chez les PME

41%

% moyen des données migrées sur un Cloud privé  
46% chez les grandes entreprises  
35% chez les PME

66%

Entreprises qui déclarent avoir une équipe Cloud centrale dédiée au sein de leur DSI  
+21% qui planifient d'en créer une prochainement

12M€

Parmi les grandes entreprises 13% présentent plus de 12M€ de dépenses Cloud par an  
50% des grandes entreprises dépenses plus de 1,2M€  
11% des PME dépenses plus de 1,2M€ dans le Cloud



Le stockage de nombreux aspects informatiques sur le Cloud est depuis longtemps devenu une réalité.

Dans le domaine privé ou professionnel, le stockage des données et les prestations informatiques sont de plus en plus délocalisés sur un lointain serveur sur Internet. Que ce soit pour sauvegarder d'anciennes photos de vacances ou pour des utilisations professionnelles, toujours plus d'utilisateurs optent pour des solutions basées sur le Cloud.

**Mais**, de nombreuses entreprises travaillent avec des données sensibles et ne sont pas disposées à les délocaliser sur un serveur Cloud même si elles éprouvent un intérêt pour ces nouvelles possibilités.

Autre argument pour un grand nombre d'entreprises : elles travaillent parfaitement sans Cloud depuis des années et ont établi un centre de calcul professionnel et parfaitement entretenu. **Pourquoi le remplacer ?**

Ce n'est **pas** forcément nécessaire. La solution s'appelle le **cloud hybride**, un mélange entre les solutions basées sur le Cloud et les solutions sur site. Ce modèle permet de réunir les avantages des deux approches.





Le terme « Cloud hybride » décrit généralement une forme croisée entre un centre de calcul local traditionnel ou un Cloud privé externe et un Cloud public. Par conséquent, une partie des données et des applications se trouve dans les locaux de l'entreprise et une autre sur les serveurs d'un prestataire dédié. Inutile pour autant de travailler avec deux systèmes différents. Cela nécessiterait la migration des données d'une solution à l'autre ainsi qu'un travail supplémentaire.

Idéalement, un Cloud hybride réunit les systèmes de façon symbiotique et transparente. L'entreprise décide seule de la répartition des différents domaines informatiques dans les solutions. On peut par exemple imaginer que tous les fichiers sensibles relevant de la protection des données soient conservés localement et que seules les données restantes soient stockées sur les serveurs Cloud. D'autres préféreront conserver le stockage complet dans leurs locaux et délocaliser uniquement le Cloud computing. Ou à l'inverse : il est possible d'utiliser la puissance de calcul localement alors que les données seront stockées dans un stockage Cloud afin de permettre une accessibilité depuis n'importe quel endroit.

## Mise en place technique : comment fonctionne le Cloud hybride ?



Afin de mettre en place un Cloud hybride, il ne suffit pas de commander un Cloud public et de l'utiliser en parallèle de votre propre centre de calcul. Les deux systèmes doivent parfaitement travailler ensemble. Pour y parvenir, les solutions sont toutefois multiples. Au final, tous les types de connexion individuels reposent sur l'utilisation d'un logiciel de gestion ou d'une API voire sur une combinaison des deux.

Dans ce cadre, la mise en œuvre effective dépend toujours des éléments devant être placés dans le Cloud et du prestataire de service. En effet, les solutions proposées par les différents prestataires sont généralement diverses.

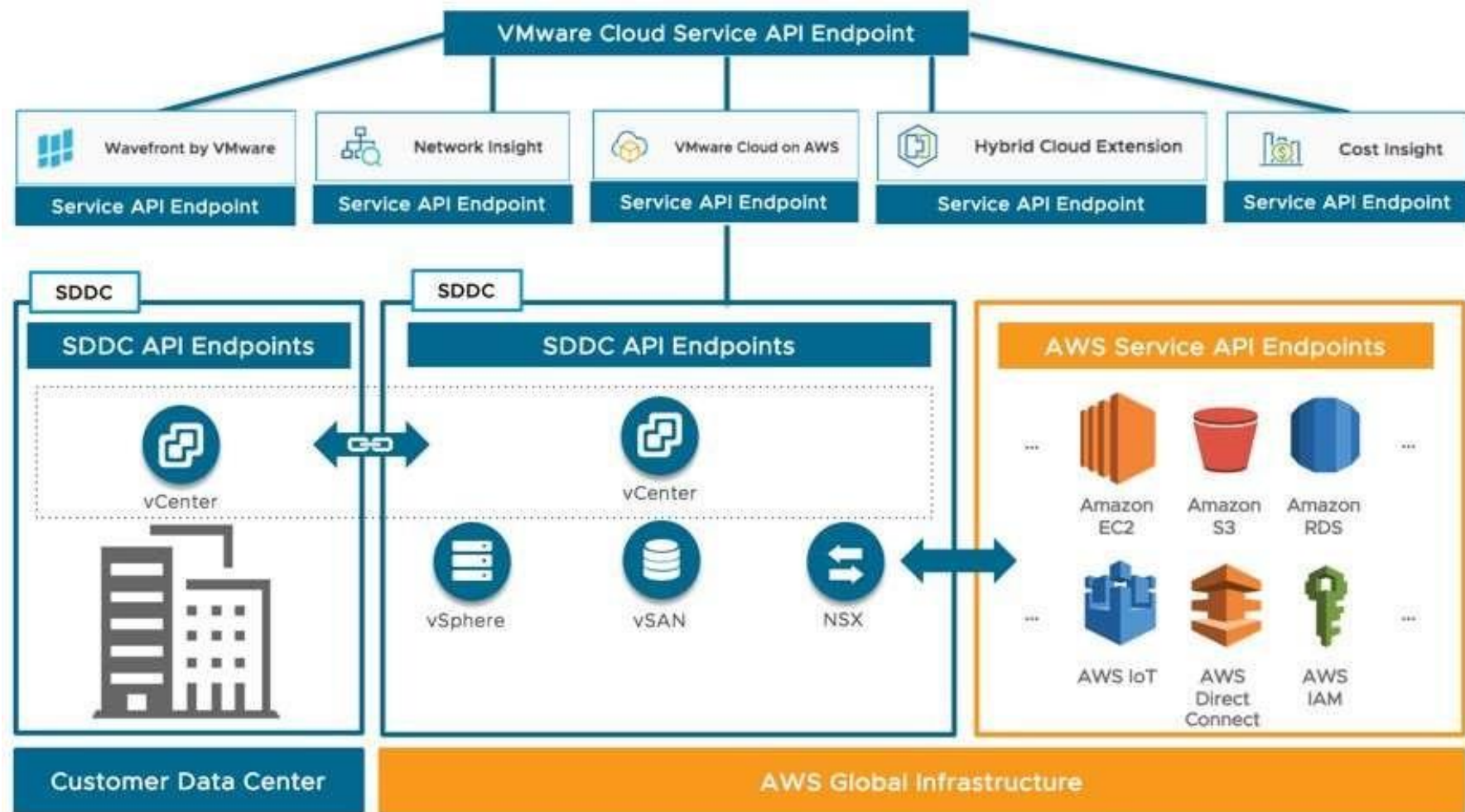
Le volume de données joue également un rôle. Pour les faibles exigences, une interface est souvent suffisante : par exemple lorsqu'une entreprise utilise des applications Office dans le Cloud, mais stocke toujours les données localement.

Dans les cas plus complexes, il est toutefois possible de s'appuyer sur un **logiciel de gestion de Cloud hybride**. S'il est par exemple nécessaire que des solutions systèmes complètes fonctionnent sans difficulté, un répartiteur de charge constituera alors un élément particulièrement utile dans la gestion du Cloud. Une répartition des charges efficace et automatisée permettra de garantir une disponibilité illimitée des services et des données.

# Cloud Hybride vCloud



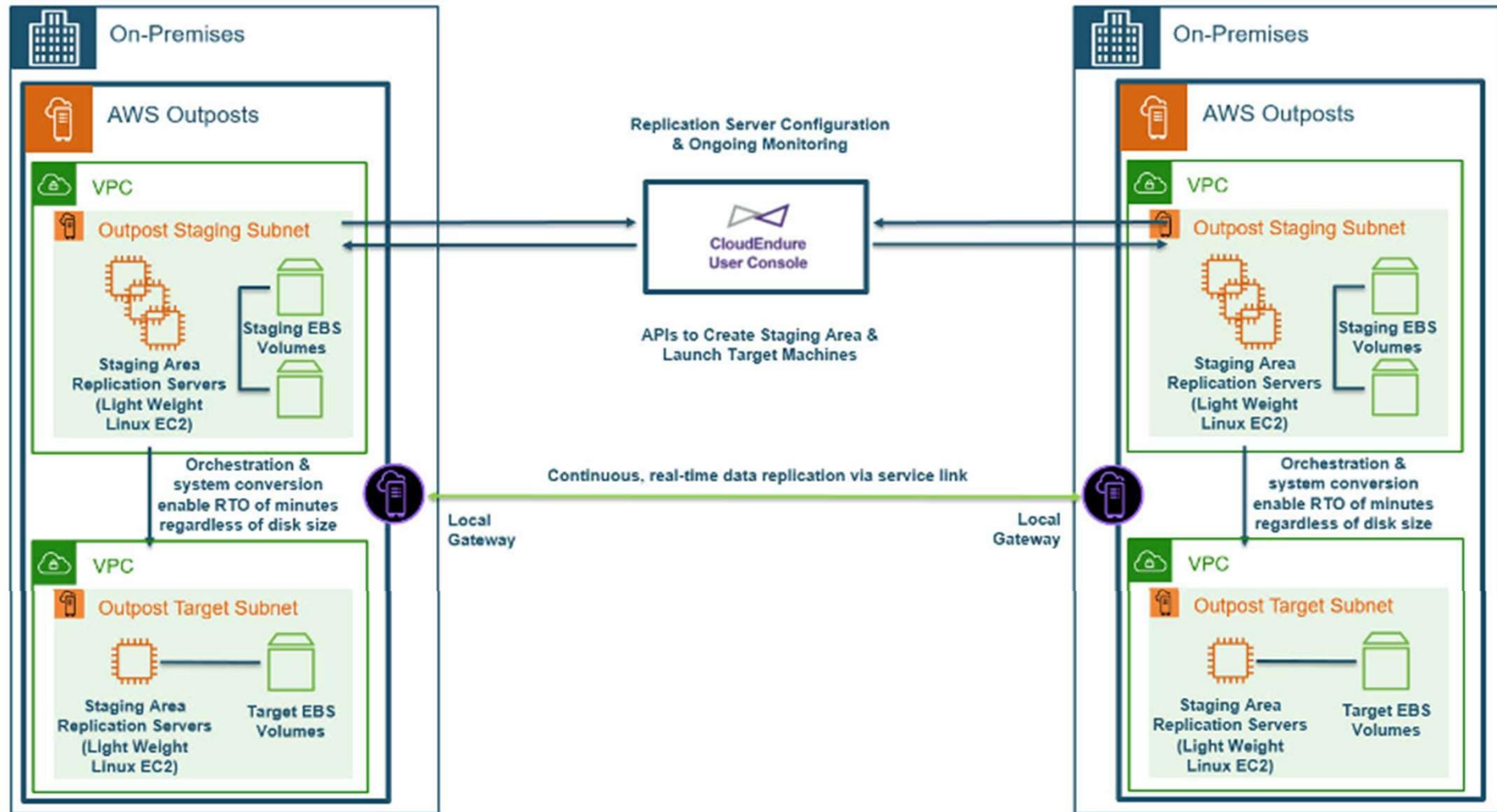
## VMware Cloud on AWS



# AWS Outposts



## AWS On prem

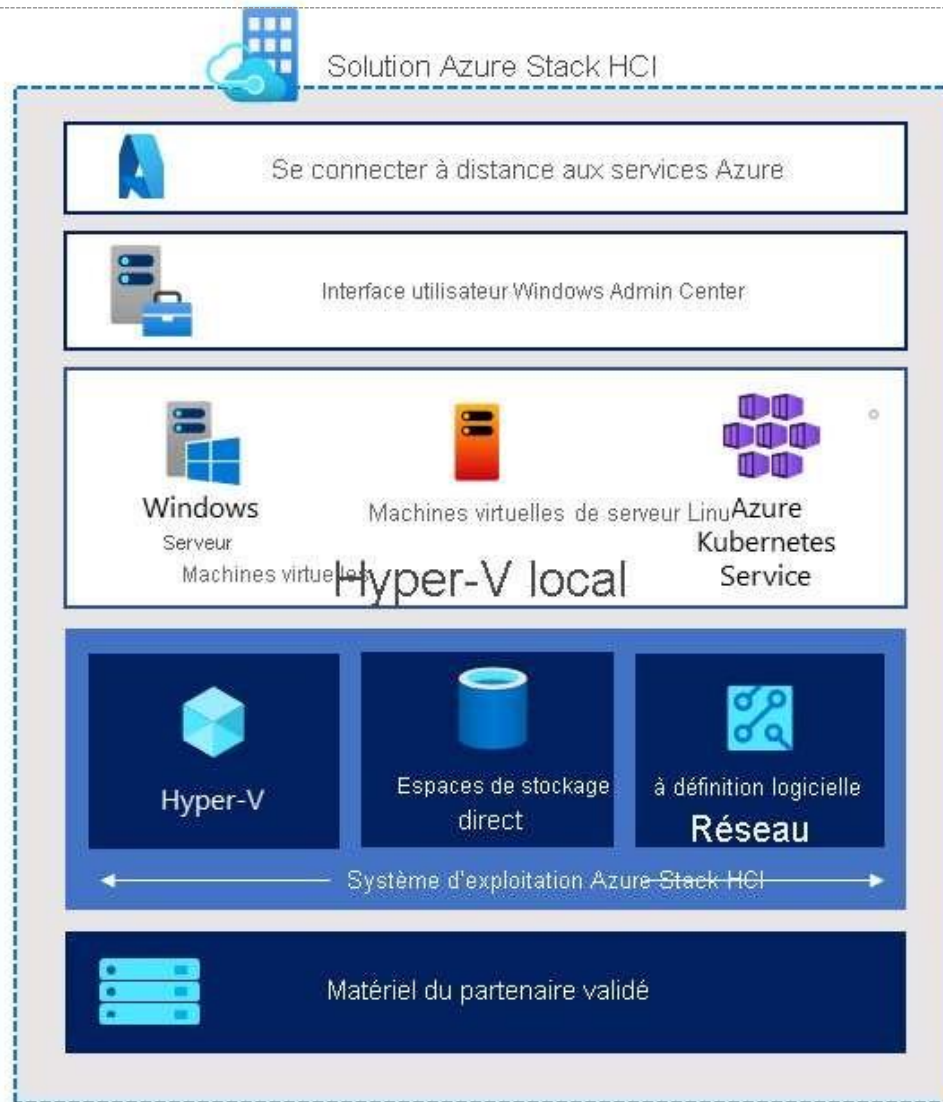


© 2021, Amazon Web Services, Inc. or its Affiliates. All rights reserved.





## Azure On prem





## Avantages et inconvénients du Cloud hybride



De prime abord, le Cloud hybride semble combiner le meilleur des deux solutions. Mais, à l'instar de chaque technologie, ce concept présente également certains inconvénients. L'impact de ces inconvénients va dépendre des circonstances individuelles.

### Avantages

Flexible et évolutif

Économie de ressources

Peu coûteux par comparaison

Sécurité des données sensibles et des applications critiques

### Inconvénients

Effort supplémentaire

La sécurité peut uniquement être garantie par des règles claires

# Avantages et inconvénients du Cloud hybride



## Avantages

L'avantage d'un Cloud privé – notamment lorsque ce dernier est réalisé sous la forme d'un centre de calcul local – réside dans le fait que l'on garde la main sur l'essentiel. L'entreprise est personnellement responsable de la sécurité des données et de la mise à disposition des services et peut réagir rapidement si nécessaire. Il est ainsi possible de conserver à porter de main tout ce qui est impérativement nécessaire au succès de l'entreprise.

Un Cloud public en revanche peut être adapté aux besoins. La plupart des prestataires de telles solutions basées sur le Cloud permettent à leurs clients d'ajouter ou de supprimer rapidement et simplement des ressources. Vous payez donc uniquement pour ce dont vous avez réellement besoin. Il en va de même pour une solution de Cloud hybride : une solution Cloud vous permet de revoir à la hausse ou à la baisse tous les domaines que vous ne souhaitez pas garder en sécurité chez vous. Cela permet de faire l'économie des coûts d'entretien pour la part qui n'est pas hébergée dans l'entreprise : en effet, en optant pour l'offre d'un prestataire tiers, celui-ci prendra en charge la maintenance et l'entretien du matériel et des logiciels.

Par ailleurs, chaque entreprise doit considérer avec attention si elle a véritablement besoin d'un Cloud hybride. Si l'entreprise dispose d'ores et déjà d'un centre de calcul propre et que celui-ci suffit selon toutes prévisions pour répondre aux besoins des années à venir, dans ce cas, une délocalisation sur un Cloud hybride n'est pas nécessaire et représentera uniquement une charge supplémentaire. Autre cas : une entreprise ayant la possibilité de confier ses données à un prestataire d'hébergement digne de confiance et avec un haut niveau de protection des données n'aura pas besoin de centre de calcul supplémentaire ou de Cloud privé propre et pourra alors pleinement se satisfaire d'un Cloud public.

## Inconvénients

Même si des logiciels permettent de faciliter la gestion d'un Cloud hybride, l'effort de gestion est toujours plus important que pour les deux autres alternatives. Cet effort inclut également le fait de devoir définir clairement quels domaines de l'entreprise doivent être enregistrés dans quelle partie du Cloud. Seul un plan concret peut permettre d'éviter durablement les problèmes dans l'exploitation d'un Cloud hybride.

Un second grand inconvénient des Clouds hybrides : une sécurité comparativement plus faible. La forme hybride est forcément moins sûre qu'une solution locale fermée. Mais afin de garantir la meilleure protection des données possible, il convient également d'établir un système clair en matière de sécurité. S'il existe un risque que des données sensibles se retrouvent dans le mauvais secteur, il est impossible de garantir la sécurité des données. C'est la raison pour laquelle il est impératif de développer et mettre en œuvre des stratégies empêchant une utilisation erronée du Cloud hybride ou réduisant le risque d'une telle utilisation.

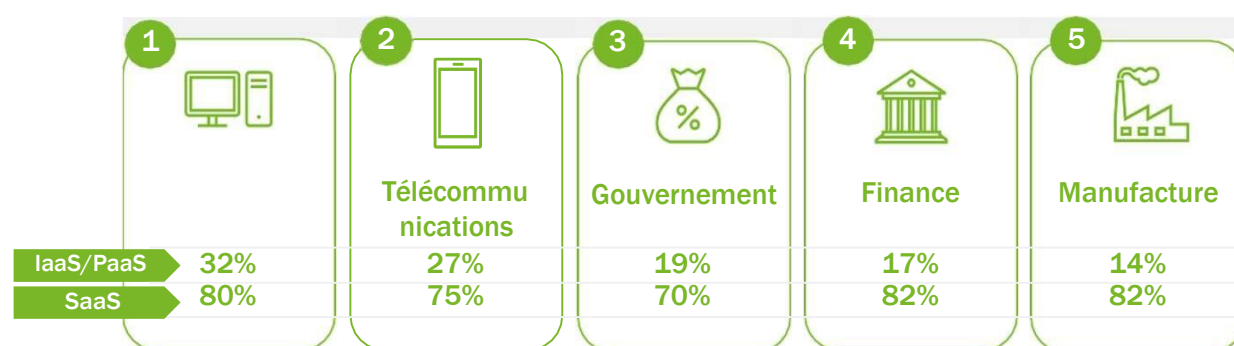
# Panorama du marché : la finance en retard



# 1

Le panorama des secteurs ayant le plus adopté le Cloud met en évidence le retard des grandes institutions financières qui ont, dans un premier temps, rejeté l'idée de transférer leur données sur le Cloud, pour des raisons de sécurité, de fiabilité et de conformité à la réglementation.

Une différence notable se remarque entre le taux d'adoption du Cloud IaaS/PaaS (migration des activités « core » sur le Cloud) et celui de l'adoption du Cloud SaaS (utilisation de messageries/bureautique).



Dans ce cas spécifique, les chiffres IaaS/PaaS correspondent aux taux de migration vers AWS et les chiffres SaaS correspondent aux taux d'utilisation de Office 365.

En ce qui concerne l'adoption de services Cloud IaaS/PaaS, les institutions financières se montrent réticentes à migrer leurs activités de « core banking » sur le Cloud, principalement pour des raisons de sécurité et de gouvernance des données.

Dans un sondage de l'*American Bankers Association* de 2018, 50% des acteurs bancaires interrogés ont déclaré ne pas être sûr de migrer leurs activités principales sur le Cloud et 21% ont même déclaré qu'ils étaient contre.

Les chiffres vu ci-dessus démontrent donc que les acteurs financiers prennent du retard par rapport aux autres secteurs dans la course au Cloud (seulement 17%)

# 2

La réticence initiale des institutions financières est aujourd'hui remise en cause par l'émergence de nouveaux acteurs. Les Fintech ne sont en effet pas freinés par des systèmes « legacy » entravant leur agilité, et s'appuient largement sur le Cloud pour développer de nouveaux services plus rapidement et à des coûts inférieurs. Elles bénéficient aussi parfois d'un environnement réglementaire favorable, DSP2 par exemple. D'une manière générale, le recours au Cloud leur permet de s'inscrire parfaitement dans le mouvement d'ouverture du secteur financier (open banking notamment) et de bénéficier des dernières technologies comme l'IA (intelligence artificielle). Les acteurs traditionnels recourent donc de plus en plus au Cloud pour pouvoir faire face à cette nouvelle concurrence.

# 3

La crise du COVID-19 va sans aucun doute développer plus encore le recours au Cloud. Le CTO de Goldman Sachs, Atte Lahtiranta, explique ainsi que l'adoption récente du Cloud public a donné aux entreprises une « base technologique très polyvalente » qui leur permettra de mettre en œuvre des changements rapides et importants dans la façon de fonctionner des entreprises dans les années à venir.

Plus de 95% des équipes de Goldman Sachs ont pu télétravailler pendant la crise et absorber des volumes exceptionnels de transactions sur les marchés financiers.



# Sommaire

1. Présentation du Cloud Computing
2. Pourquoi et comment migrer sur le Cloud ?
3. Les grands enjeux pour les acteurs des services financiers
4. Services du Cloud
5. Annexes

# Quels sont les principaux avantages du Cloud Computing ?



**Coût** : Passer dans le Cloud élimine la nécessité d'investir dans une infrastructure propre (matériel et logiciels) de même que les coûts liés à la maintenance (alimentation, entretien matériel). Le Cloud offre une structure de coûts essentiellement variable. *Réduction du coûts opérationnels IT estimée entre 15% et 40%. Attention toutefois, le passage dans le Cloud n'est pas une garantie systématique de baisse des coûts, et demande de nouvelles compétences pour suivre au plus près les coûts variables facturés par les fournisseurs.*



**Sécurité et fiabilité** : Les fournisseurs de services Cloud se portent garants de la sauvegarde et de la sécurité des données et des infrastructures contre les menaces externes. Ils assurent la mise à jour systématique de leurs systèmes et investissent massivement pour sécuriser au mieux leurs infrastructures. *Les institutions financières doivent évidemment rester attentives aux services et garanties apportées par leurs fournisseurs notamment dans le cadre de PSEE. Si le niveau de sécurité offert par les fournisseurs est bien souvent supérieur à celui possible dans des institutions financières, des fuites de données sont toujours possibles, même pour celles hébergées dans le Cloud.*



**Performance et vitesse** : Les capacités peuvent être rapidement mises à l'échelle («scalability»), parfois automatiquement, pour évoluer rapidement et être disponible dans un temps réduit. Pour le client de services Cloud, les capacités disponibles pour l'approvisionnement semblent souvent illimitées et peuvent être achetées en n'importe quelle quantité et à tout moment.



**Service mesuré** : Les systèmes de Cloud contrôlent et optimisent automatiquement l'utilisation des ressources en exploitant une capacité de mesure à un niveau d'abstraction approprié au type de service (par exemple stockage, traitement, bande passante et comptes d'utilisateurs actifs).



**Productivité** : Les tâches liées à la maintenance du matériel et à la mises à jour des logiciels sont totalement supprimées, ce qui permet un gain important en temps et en productivité. Les équipes IT peuvent ainsi passer plus de temps sur des tâches à plus forte valeur ajoutée et travailler plus étroitement avec le business.



**Evolutivité** : Les fournisseurs de Cloud mettent à disposition de larges catalogues de services permettant de mettre en œuvre simplement de nouvelles fonctionnalités. Le fait d'avoir son infrastructure et ses données sur le Cloud permettra par exemple un recours facilité aux outils d'intelligence artificielle mis à disposition par ces fournisseurs.

Ameur Kais



# Focus sur les coûts



## Le Cloud modifie en profondeur la structure des coûts de l'IT

### Les centres de coûts en capital pour l'installation et l'entretien d'une infrastructure locale

Serveurs	▪ Coûts liés à l'acquisition, l'alimentation, à la réparation et au remplacement de serveurs physiques situés sur site.
Stockage	▪ Coûts liés à l'achat et à l'entretien du matériel de stockage. Ils peuvent être optimisés en fonction de l'importance des données stockées, avec des charges plus élevées pour les données plus sensibles.
Réseau	▪ Ces coûts incluent tous les composants matériels locaux comme les câbles, commutateurs, points d'accès et routeurs. Ils englobent également le réseau étendu (WAN) et les connexions Internet.
Sauvegarde et archivage	▪ Cette catégorie englobe également le coût de la maintenance des données sauvegardées.
Continuité et reprise d'activité	▪ Coûts liés à la tolérance de panne, la reprise d'activité après sinistre, la récupération des données, ce qui peut comprendre notamment des générateurs de secours.
Infrastructure du centre de données	▪ Il s'agit de l'alimentation, de l'occupation d'espace, du refroidissement, de la maintenance des bâtiments, etc...

- La mise en place d'une **infrastructure réseau locale** est **très coûteuse** et représente un **investissement important** pour toute entreprise, quelle que soit sa taille. En plus de cet investissement viennent s'ajouter **les charges de maintenance du matériel**. Les coûts fixes, dans le cas d'une structure *on-premise*, sont importants et les coûts variables négligeables.
- Migrer sur le Cloud consiste à remplacer un investissement en capital lourd par **une charge variable maîtrisée**. En effet le modèle économique des fournisseurs de services Cloud consiste à fournir une infrastructure virtuelle via Internet, qui remplacera totalement l'infrastructure locale des entreprises clientes, pour une performance, une sécurité et une flexibilité accrue. Dans le cas d'une migration dans le Cloud, les coûts fixes deviennent minimes.
- Les **coûts d'investissement (CapEx)** sont donc remplacés par des **coûts opérationnels (OpEx)**. Ce changement a un impact important d'un point de vue du **résultat comptable** : contrairement aux charges CapEx, les charges OpEx ne sont pas amortissables
- Le déploiement d'une offre Cloud vient s'accompagner d'une **formule de paiement à l'utilisation** (IaaS et PaaS) ou **formule d'abonnement** (SaaS), qui, lorsqu'elle est adaptée à l'organisation, peut réduire fortement les coûts opérationnels IT.

### Les coûts liés au Cloud sont les suivants :



#### Coûts du fournisseur

- Paiement à l'utilisation : Payer à l'utilisation permet de s'adapter plus facilement à l'évolution des besoins du clients et ainsi minimiser les risques de sur ou sous-capacités.
- Réserver des ressources pour économiser : Certains fournisseurs proposent des remises sur des engagements d'utilisation.
- Tarifs dégressifs sur l'utilisation



#### Coûts du réseau

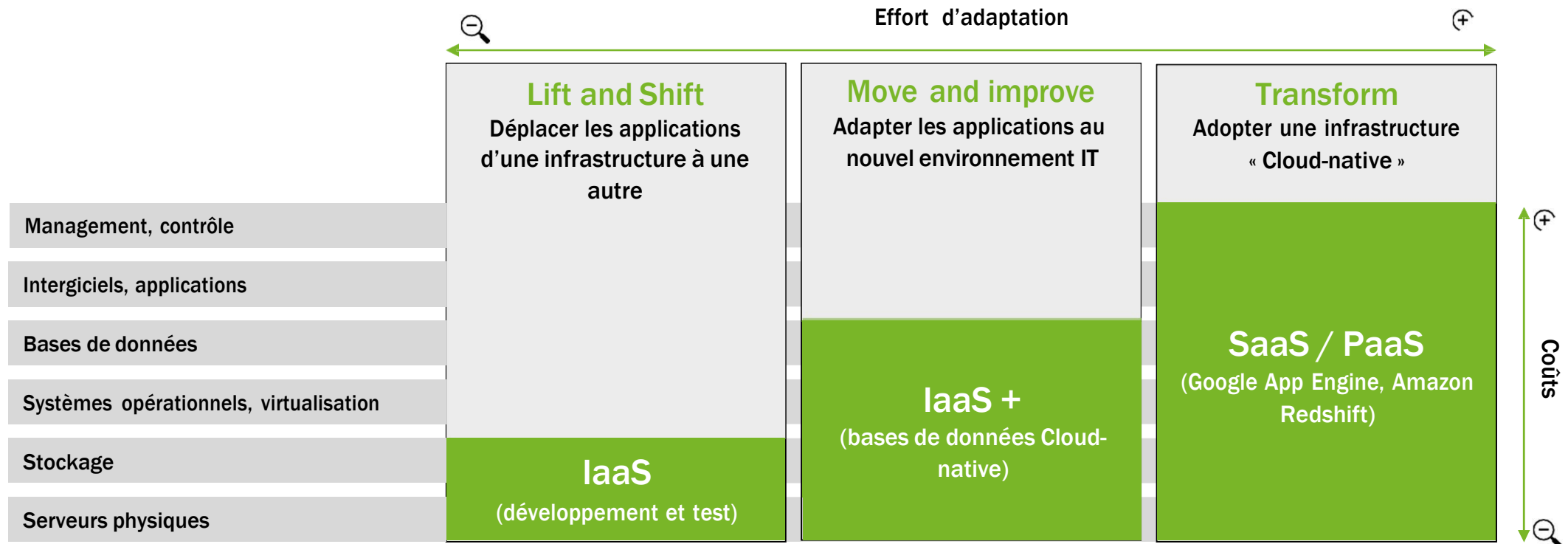
Lien télécom vers le fournisseur de Cloud



#### Continuité et reprise d'activité

Simplification des PCA grâce à la redondance et résilience offerte nativement par le Cloud

# Comment mener à bien un projet de migration vers le Cloud ? (1/2)



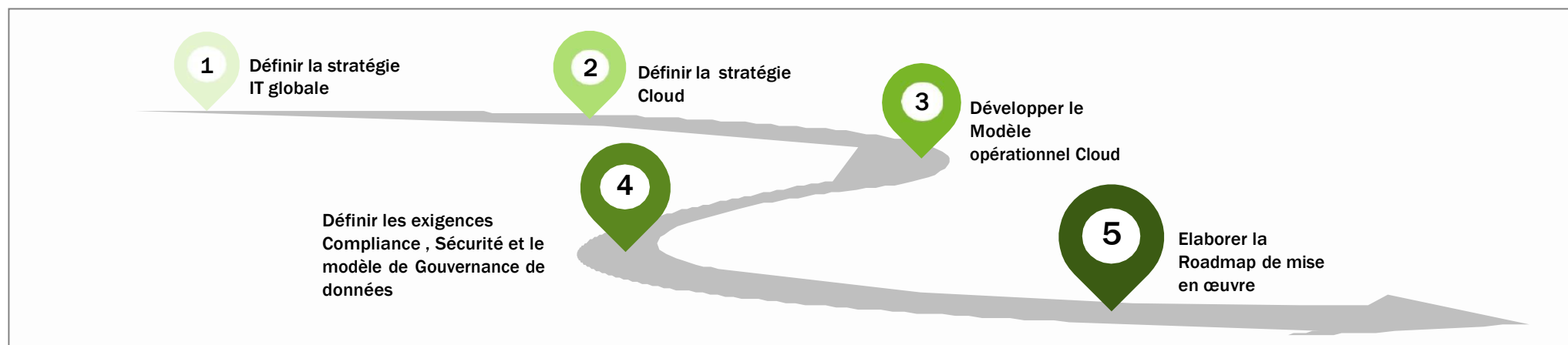
## Trois approches pour migrer vers le Cloud :






- L'approche « **Lift and shift** » consiste à simplement déplacer l'ensemble des données telles quelles depuis un serveur physique, vers un serveur Cloud. Cette approche est la moins couteuse en termes de frais de migration, mais entraîne généralement des coûts supplémentaires post-migration.
- L'approche « **Move and improve** » consiste à effectuer un travail d'adaptation avant de faire migrer des applications qui ne sont pas totalement aptes à fonctionner sur le Cloud. Les centres de coûts peuvent englober, en plus du stockage et de la location des serveurs, la mise en place de bases de données, ou encore la virtualisation de certains logiciels et systèmes opérationnels.
- L'approche « **Transform** » est une refonte globale des outils pour un fonctionnement optimal sur le Cloud, et nécessite non seulement une prestation technique, mais aussi un accompagnement spécialisé (monitoring, advisory). Il s'agit de la solution la plus coûteuse mais qui maximisera par la suite l'efficacité opérationnelle.

# Comment mener à bien un projet de migration vers le Cloud ? (2/2)



Une migration réussie vers le Cloud doit être accompagnée d'une stratégie de transformation organisationnelle, et d'optimisation de l'infrastructure IT



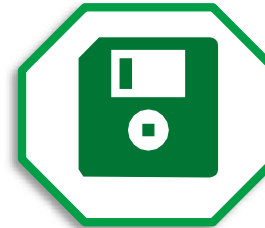
 Définition de la stratégie IT globale	 Définition de la stratégie de migration vers le Cloud	 Modèle opérationnel Cloud	 Compliance, Sécurité et Gouvernance de données	 Roadmap de mise en œuvre
<ul style="list-style-type: none"> <li>Établir une vision et une stratégie globale orientée métier intégrant les différents aspects : business, processus et IT</li> <li>Evaluer l'environnement SI afin de déterminer la maturité des applications, pour une migration vers le Cloud</li> <li>Fournir un Business Case approprié afin d'illustrer et de justifier la nécessité de l'investissement</li> <li>Identifier les fournisseurs clés à solliciter</li> <li>Fournir une estimation des coûts (analyse du TCO, ROI,...)</li> <li>Pour le TCO, fournir un modèle pour une vue du coût total de possession dans le Cloud</li> </ul>	<ul style="list-style-type: none"> <li>Fournir une stratégie approfondie pour la migration vers le Cloud en tenant compte de la préparation des applications, des directives réglementaires et de sécurité et des principes d'architecture</li> <li>Mettre en place une méthodologie standardisée et structurée pour servir l'organisation cible</li> <li>Identifier les outils et applications adaptés à l'environnement actuel mais aussi aux changements que va connaître cet environnement</li> <li>Identifier les fournisseurs et les services adaptés aux besoins de l'entreprise</li> </ul>	<ul style="list-style-type: none"> <li>Développer une vision Cloud ainsi qu'un modèle opérationnel adapté à la stratégie de l'entreprise cible</li> <li>Définir les impacts organisationnels et principalement la transformation de la DSI : nouveau rôle, compétences à développer, profils à recruter..</li> <li>Mettre en place des procédures adaptées à l'évolution du rôle des collaborateurs, et visant à une utilisation plus efficace des ressources.</li> <li>Définir les rôles et les responsabilités</li> <li>Établir un alignement clair entre l'architecture d'entreprise, l'informatique et le fournisseur de services Cloud</li> </ul>	<ul style="list-style-type: none"> <li>Définir les principes et les considérations clés pour la définition de l'architecture et la stratégie de migration</li> <li>Respecter les différentes exigences réglementaires, de sécurité et de gouvernance des données</li> <li>Mettre en place des mesures tangibles ainsi que des instruments gravitants autour de l'organisation suite à la migration, et permettant de remonter rapidement les succès et échecs.</li> <li>Développer des chemins d'escalade et de remontée de l'information afin de minimiser les impacts envers le business</li> </ul>	<ul style="list-style-type: none"> <li>Faire une sélection des premiers éléments et applications à migrer vers le Cloud</li> <li>Mettre en place un plan de transformation et entamer une migration en plusieurs phases</li> <li>Décliner les différents chantiers de la stratégie de migration vers le Cloud en tenant compte de la préparation des applications, des directives réglementaires et de sécurité et des principes d'architecture</li> </ul>

# Les points d'attention à prendre en compte



## Projet complexe

La transition vers le cloud représente un grand changement dans l'organisation d'une entreprise. Cela implique un grand investissement mais aussi un travail en profondeur pour définir de nouvelles méthodes de travail. Cette transition requiert donc une mobilisation de ressources importante.



## Gouvernance des données

Les données les plus sensibles ne peuvent être migrées sur le Cloud et certains acteurs, par précaution, préfèrent voir leur données hébergées en France ou en Europe. En effet, l'inquiétude quant à la sécurité reste vive en raison fuites de données toujours possibles.



## Projet long

Pour tirer tout le profit du Cloud, il est préférable de modifier la conception et l'architecture des applications migrées. Une migration d'envergure implique le décommissionnement d'infrastructures existantes (cf l'exemple plus bas d'un projet ambitieux pour décommissionner un data center ayant pris trois ans au total).



## Dépendance au fournisseur

La réversibilité (c'est-à-dire la capacité à changer de fournisseur de Cloud) paraît très difficile. La migration dans le Cloud est une décision stratégique qui engage fortement.



## Législation de certains pays

Dans certains pays, la loi interdit ou restreint fortement la possibilité de stocker des données bancaires en dehors des frontières. C'est le cas notamment de la Suisse, du Luxembourg et de la Russie en Europe, de l'Algérie, de la Tunisie et de quelques pays de l'Afrique subsaharienne en Afrique.



## Mise en place de liens réseau performants

Le recours au Cloud implique des échanges de données importants avec les data centers des fournisseurs. La migration de certains services doit donc bien prendre en compte cette dimension et son coût.



# Sommaire

1. Présentation du Cloud Computing
2. Pourquoi et comment migrer sur le Cloud ?
- 3. Les grands enjeux pour les acteurs des services financiers**
4. Services du Cloud
5. Annexes

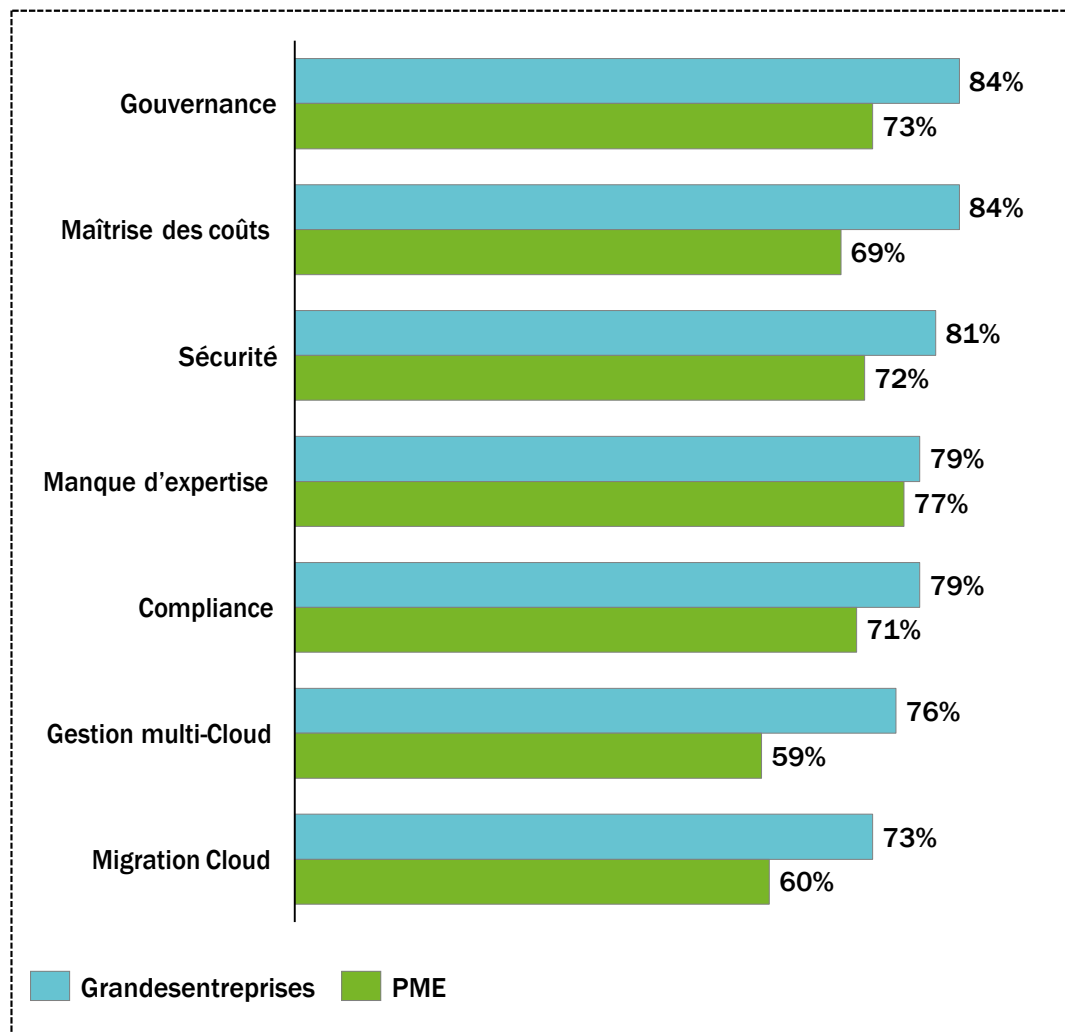
Ameur Kais



# Quels sont les enjeux actuels pour les entreprises?



Défis majeurs par taille d'entreprise (Enquête réalisée par FLEXERA en 2019)



Source : <https://resources.flexera.com/web/media/documents/rightscale-2019-state-of-the-cloud-report-from-flexera.pdf>

## 1 La gouvernance des données

84% des entreprises ont identifiés la sécurité et la gouvernance de données comme leur 1<sup>ère</sup> préoccupation (84% des Grandes entreprises vs 73% des PME)

## 2 Maîtrise des coûts Cloud

L'optimisation de l'infrastructure Cloud afin de réduire les coûts est la priorité pour 84% des grandes entreprises (69% pour les PME)

## 3 Transformation de la DSI

79% des entreprises estiment un manque d'expertise des technologies Cloud au niveau de leur équipes IT et ont identifié de nouveaux rôles pour la DSI

## 4 Le multi-Cloud

84% des entreprises ont une stratégie multi-Cloud.

Une enquête sur l'état du Cloud en 2019 montre que le multi-Cloud reste la stratégie privilégiée

Ameur  
Kais

# Gouvernance des données : est-il possible de mettre des données personnelles sur le Cloud ?



## Les institutions financières restent prudentes mais les mentalités évoluent rapidement



**L'EBA – European Banking Authority** – n'interdit pas aux sociétés européennes de migrer sur le Cloud et, par conséquent, d'y mettre des données personnelles. Cependant elle formule des recommandations\* quant à l'externalisation vers des fournisseurs de services Cloud hors Union Européenne (et donc vers les fournisseurs américains).

Avec le **Cloud Act** toute la réglementation européenne, notamment le **RGPD**, ne permet pas d'assurer la confidentialité des données stockées sur des serveurs américains, qu'ils soient situés aux Etats-Unis ou pas.



### RGPD

- Règlement général sur la protection des données
- Règlement de l'Union Européenne relatif à la protection des données à caractère personnel
- Entrée en application en mai 2018



### Cloud Act

- Clarifying Lawful Overseas Use of Data Act
- Loi fédérale des États-Unis sur la surveillance des données personnelles, notamment dans le Cloud.
- Adoptée en 2018

Le **chiffrement des données** migrées constitue une réponse à cet écueil. Elle doit cependant, être mise en place en respectant certaines règles.

En effet, si les clés sont laissées à l'opérateur, le risque d'accès aux données confidentielles persiste. Néanmoins, si les clés restent chez le client, ce dernier risque de ne pouvoir accéder à certaines fonctionnalités du fournisseur.

Voir Annexe pour plus de détails – Gouvernance des données – Technique



\* Voir Annexe – *EBA – Recommandations sur l'externalisation vers des fournisseurs de service Cloud*

# Maîtrise des coûts: comment le *FinOps* aide à les surveiller et les contenir



Le métier du *Cloud FinOps* est un nouveau métier, absolument clé dans le processus d'adoption du Cloud dans les entreprises car il gère l'optimisation financière de l'usage du Cloud. Il sert de lien entre Finance et IT.

A l'image de la montée en puissance du *DevOps* abolissant la frontière entre les fonctions de développement et d'administration, le Cloud a favorisé l'émergence d'une nouvelle fonction *Finops* qui a pour but d'optimiser les coûts liés à l'utilisation du Cloud.

Le **profil hybride** du FinOps lui permet d'assumer différentes missions :



INFORMER

Informer sur les différentes possibilités du Cloud. Pour faire cela, il doit connaître le catalogue complet de services proposés par les fournisseurs.



OPTIMISER

Optimisation financière en fonction de la tarification du fournisseur.  
Par exemple, par l'utilisation de calculateurs spécifiques, fournir une estimation des futurs coûts; selon les usages envisagés, il peut conseiller un fournisseur plutôt qu'un autre, etc.



SURVEILLER

Évaluer continuellement les usages afin de les adapter si les volumes ou les utilisations venaient à varier. Cette mission se base sur une étude de l'historique, le monitoring et des projections d'activité.

Les trois principales activités du FinOps sont donc: **l'allocation des coûts**, **l'optimisation des coûts** et **le pilotage budgétaire**..

Le travail de Cloud Finops ne s'arrête pas aux optimisations financières à court terme. Il s'agit aussi d'**accompagner** les entreprises dans leur passage à une culture Finops. Le représentant FinOps a également une mission de **conduite du changement** : former les équipes aux bonnes pratiques Cloud, de l'architecte au financier, du développeur à l'acheteur.

Ameur Kais

## Driver économique ou stratégique?

En règle générale, les fournisseurs de Cloud estiment qu'une migration sur le Cloud permet une réduction d'environ 30% des coûts IT. Mais le driver économique n'est pas toujours la raison principale de la migration.

## DRIVER ECONOMIQUE



- Le paiement à l'usage peut se révéler plus économique, notamment si une approche FinOps est adoptée. Cette approche est indispensable étant donné les approches radicalement différentes induites par le Cloud. Des serveurs existants inutilisés on-premise ont un coût marginal ce qui n'est pas le cas de ressources facturées mais inutilisées ou sous-utilisées.
- La répartition CapEx / OpEx permet une plus grande agilité et flexibilité pour maîtriser les coûts IT.
- OakNorth (voir use cases *Banque de Détail*) a réalisé des **économies de 60%** suite au déploiement dans le Cloud de son core banking Mambu.

Mais le driver principal qui mène à migrer vers le Cloud est bien plus souvent **stratégique**.

## DRIVER STRATEGIQUE



Un des **avantages** mis en avant lors de la migration vers le Cloud est **l'agilité** qui est acquise. Une fois la migration réalisée, le déploiement d'un nouveau service ou la mise à niveau d'une application existante se fait **beaucoup plus rapidement et facilement**.

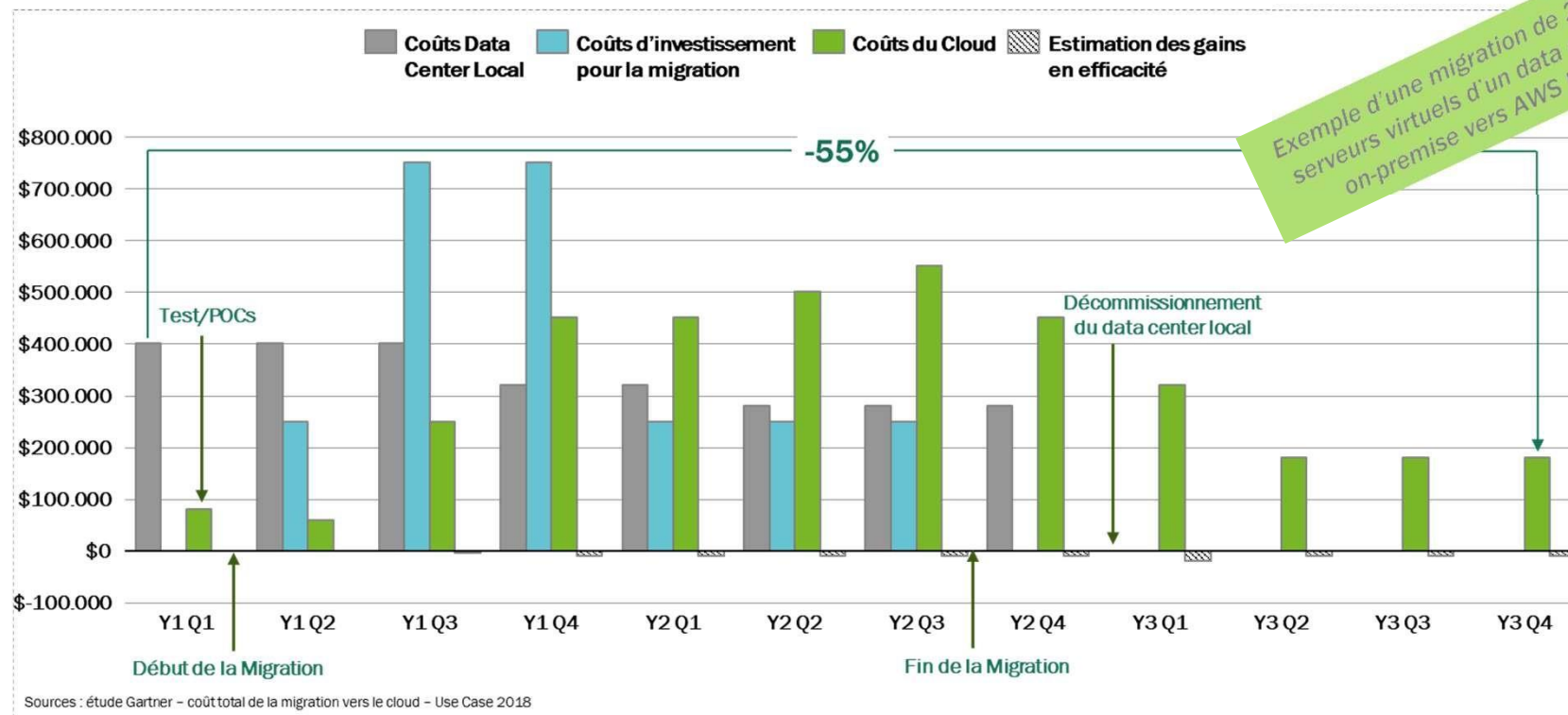
## Examples Use Cases

- GEICO : les nouvelles fonctionnalités majeures sont dispo en 3 semaines au lieu de 6 et les mises à jour mineures peuvent être effectués sans interruption de service.
- AON : le recalcul des polices prend quelques minutes plutôt que des heures voire des jours et la génération d'un reporting financier trimestriel prend quelques heures et non plus deux semaines.
- Capital One : déploiement de nouvelles fonctionnalités et nouveaux services en quelques semaines au lieu de plusieurs mois.
- Banque Nationale du Canada : optimisation de ses opérations de trading grâce à une puissance de calcul qui permet de réaliser en quelques heures des analyses post-trade qui pouvaient prendre auparavant plusieurs semaines.

Cependant, pour pouvoir bénéficier totalement d'une migration vers le Cloud, un **effort d'adaptation est indispensable**. En effet, l'approche lift & shift ne permet pas les mêmes économies et la même agilité qui s'acquière avec une approche de **transformation complète**. Par exemple, Capital One a décidé de réécrire toutes ses anciennes applications lors de la migration sur le Cloud pour qu'elles soient optimisées.



# Use Case : évaluation des impacts financiers d'une migration Cloud



Cet exemple illustre les challenges associés à une migration

- Des coûts de **run du Cloud**, largement inférieurs (**55%**) aux coûts du data center avant la migration
- Le délai pour une migration d'ampleur : deux ans pour décommissionner le data center, près de trois ans en tout pour arriver à la cible
- Des coûts d'**investissement pour la migration** très importants impactant le ROI
  - Economies de \$880 000 / an suite à un investissement total d'environ \$5 400 000 (coûts d'investissement et overlap Cloud / data center)

# Transformation de la DSI avec l'arrivée du Cloud



Avec l'arrivée du Cloud, la DSI subit une mutation afin d'accompagner les directions métier et leur proposer des solutions à forte valeur ajoutée. Il est désormais au cœur de l'innovation.



## Une remise en question du rôle de la DSI

- Face au manque d'efficacité des systèmes d'information quant à leur alignement sur les besoins stratégiques des entreprises, les dirigeants passent outre les DSI par le biais de services Cloud. Selon une enquête, réalisée auprès de 650 dirigeants et DSI (dont 31% en France), 65% des dirigeants interrogés confirment que « l'informatique ne les aide pas à faire évoluer les choses comme ils le voudraient ».
- Selon cette étude, « cet échec des systèmes IT » est lié au non-respect des délais des projets, au manque de souplesse et à l'isolement des systèmes de l'entreprise.
- Ainsi, il n'est pas rare qu'une direction métier, au sein d'une grande entreprise, souscrive une offre SaaS externe pour satisfaire ses propres besoins, sans même solliciter ni notifier la DSI.

Source : Etude réalisée par l'éditeur d'outils de BPM Cordys ([lien](#))



## Un nécessaire repositionnement de la DSI

- La DSI doit se replacer comme l'interlocuteur privilégié des directions métier au sein de l'entreprise, ce qui sous-entend que la DSI assure le pilotage des prestations et fonctions externalisées, sous tous les angles : opérationnel projet, financier/administratif, contrôle du respect des engagements de service des prestataires, ... Sa structure devient ainsi plus transverse et plus agile.
- Rôle de garant : la DSI se porte garante du bon fonctionnement du système via la mise en place d'une gouvernance, des contrôles en lien avec les fournisseurs / prestataires.
- Rôle de sachant : La DSI doit développer de nouvelles compétences et transformer son savoir-faire : sécurité, technologie, maîtrise de données...
- Rôle d'accompagnement et de formateur : un partenaire technologique pour le métier dans la mise en œuvre des projets.

En outre, en termes de capital humain, le passage au Cloud permet d'attirer les meilleurs profils très motivés pour travailler sur ces environnements et évoluer vers des technologies plus valorisées (voir les use cases GEICO et CAPITAL ONE).

En conclusion, il ressort de ces constats que la DSI, loin d'être menacée par le développement du Cloud, peut au contraire tirer profit de sa maîtrise technologique pour accompagner les directions métier et leur proposer des solutions à forte valeur ajoutée. Elle retrouve ainsi toute sa place dans la stratégie de l'entreprise.

# Le multi-Cloud



Le recours à plusieurs fournisseurs de services de Cloud – le multi-Cloud – est une stratégie qui présente des avantages mais peut être difficile à mettre en œuvre.

## AVANTAGES\*

- Agilité et flexibilité nécessaire pour innover rapidement
- Sélection des services spécialisés nécessaires chez les différents fournisseurs
- Gouvernance des données et compliance. Avec la mise en place de réglementations conflictuelles, notamment le Cloud Act et le RGPD, certaines entreprises sont très sensibles à l'emplacement de stockage de leurs données et préfèrent garder la donnée dans leur pays
- Pouvoir de négociation en exploitant les différences de prix entre les fournisseurs
- Compatibilité permanente avec ses logiciels c'est-à-dire pouvoir s'assurer la perpétuité de ses logiciels avec son service Cloud et donc, ne pas être dépendant de l'alignement de la stratégie commerciale des éditeurs de licence avec celle des fournisseurs de Cloud

## INCONVENIENTS\*

- Réduction de possible économies d'échelle et redondance de certains coûts et services: étant donné que chaque Cloud dispose de coûts fixes mensuels, une migration sur plusieurs providers correspond à multiplier ces coûts par autant de fois que l'on a de Clouds (par exemple, les coûts mensuels de support pour les entreprises s'élèvent à une dizaine de milliers d'euros.)
- Multitude de factures
- Augmentation de la complexité de la gestion, des structures, de la sécurité et réduction de l'agilité. Il faut réussir à créer des connexions entre les Clouds.
- Besoin d'expertise plus large. Une connaissance approfondie de chaque Cloud utilisé est nécessaire.

## Qui et comment ?



Pour les **grosses structures**, la migration vers deux fournisseurs peut apparaître sécurisante, afin de diversifier et ainsi minimiser les risques. Dans ce cas, un suivi FinOps poussé est nécessaire.

Pour une entreprise en dessous d'une taille critique, l'intérêt de la mise en place d'une stratégie multi-Cloud est limité.

Cette stratégie présente des **avantages** comme des **inconvénients**\*. Afin de minimiser les impacts négatifs du multi-Cloud, certains **outils** sont disponibles:

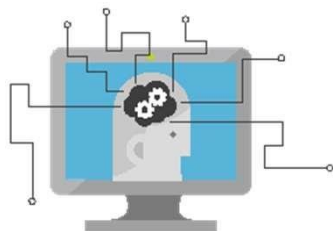
- **Terraform** permet de masquer les différences entre Cloud en ajoutant une surcouche (langage commun mais bibliothèques différentes pour chaque Cloud).
- Déploiement des **clusters Kubernetes** (logiciel d'orchestration open source conçu pour déployer, gérer et mettre à l'échelle des conteneurs) permettant en partie de s'affranchir du fournisseur de Cloud.



# Sommaire

1. Présentation du Cloud Computing
2. Pourquoi et comment migrer sur le Cloud ?
3. Les grands enjeux pour les acteurs des services financiers
- 4. Services du Cloud**
5. Annexes

# Comment les entreprises utilisent le cloud



## Communication

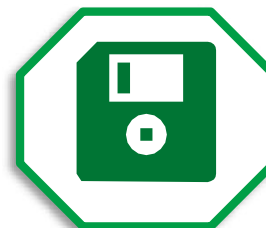
Le cloud offre aux utilisateurs un accès aisé, via le web, à des outils de communication et de collaboration tels que le courrier électronique et la gestion de calendrier. Les applications de messagerie et d'appel audio et vidéo telles que Skype tirent également parti du cloud. Vos messages et informations sont conservés sur le réseau du fournisseur de service plutôt que sur votre appareil personnel.

## Productivité

Des outils Office (tels que Microsoft Office 365) peuvent être basés sur le cloud, ce qui vous permet de vous connecter à vos applications les plus utilisées via Internet. Vous pouvez utiliser vos logiciels de traitement de texte, de présentation ou de tableur pratiquement en tout lieu. Vos informations étant stockées dans le cloud, vous n'avez pas à vous soucier de perdre des données en cas de panne de votre appareil. Vous pouvez exécuter de nombreuses applications directement à partir de votre navigateur web.

## Processus métier

De nombreuses applications commerciales sophistiquées, par exemple, de gestion de la relation client, de planification des ressources d'entreprise et de gestion des documents, peuvent également être louées auprès d'un fournisseur de service cloud. Cela garantit la disponibilité et la sécurité des ressources métier stratégiques de votre organisation.



## Stockage Fichier

Le cloud peut être utilisé pour le stockage de fichiers. L'avantage pour vous est la facilité de sauvegarde, car de nombreux services cloud synchronisent automatiquement vos fichiers à partir de votre bureau. De plus, si vous passez à un autre ordinateur ou appareil mobile, vous pouvez toujours récupérer vos fichiers. Les organisations ne paient que pour le stockage utilisé, et ne doivent pas maintenir d'infrastructure. Le fournisseur de service cloud s'en charge.

## Sauvegarde et récupération

Lorsque votre organisation s'appuie sur des services cloud pour la sauvegarde et la récupération de données, elle peut éviter de consacrer des dépenses de capital à l'infrastructure et à la gestion. Au lieu de cela, le fournisseur de service cloud se charge de la gestion des données et du respect des exigences légales et de conformité. Le cloud offre également davantage de flexibilité dans la mesure où il peut répondre à des besoins imprévisibles de stockage et de sauvegarde. Votre fournisseur de service cloud peut également effectuer une récupération plus rapide, car les ressources de votre organisation sont situées sur un réseau d'emplacements physiques plutôt que dans un centre de données local..





# Comment les entreprises utilisent le cloud



## Développement d'applications

Si vous développez des applications web, mobiles ou de jeu, le cloud peut vous aider à créer rapidement des expériences multiplateformes dont l'échelle s'adapte à mesure qu'augmente votre base d'utilisateurs. De nombreux services cloud incluent des outils déjà codés, tels que des services d'annuaire, de recherche et de sécurité, qui peuvent accélérer et simplifier le développement.

Kais

## Test et développement

Le cloud peut vous fournir un environnement vous permettant d'économiser des coûts et de commercialiser vos applications plus rapidement. Au lieu de dégager des budgets et de consacrer des ressources et un temps précieux à mise en place d'un environnement physique, vos équipes peuvent rapidement configurer et démanteler des environnements de test et de développement dans le cloud. Vous pouvez adapter l'échelle de ces environnements de développement et de test en fonction des besoins.

Ameur

# Comment les entreprises utilisent le cloud



A  
n  
a  
l  
y  
t  
i  
q  
u  
e  
  
d  
u  
  
B  
i  
g  
  
D  
a  
t  
a  
L  
e  
  
c  
l  
o  
u  
d

vous permet de puiser dans les données de votre organisation pour les analyser afin d'en extraire des tendances et perspectives, de faire des prédictions, d'améliorer les prévisions et de prendre diverses décisions. Les services cloud peuvent fournir à votre organisation une puissance de traitement supérieure, des outils sophistiqués pour exploiter des quantités massives de données, ainsi quela capacité de mettre à l'échelle rapidement votre environnement à mesureque croît le volume de vos données.





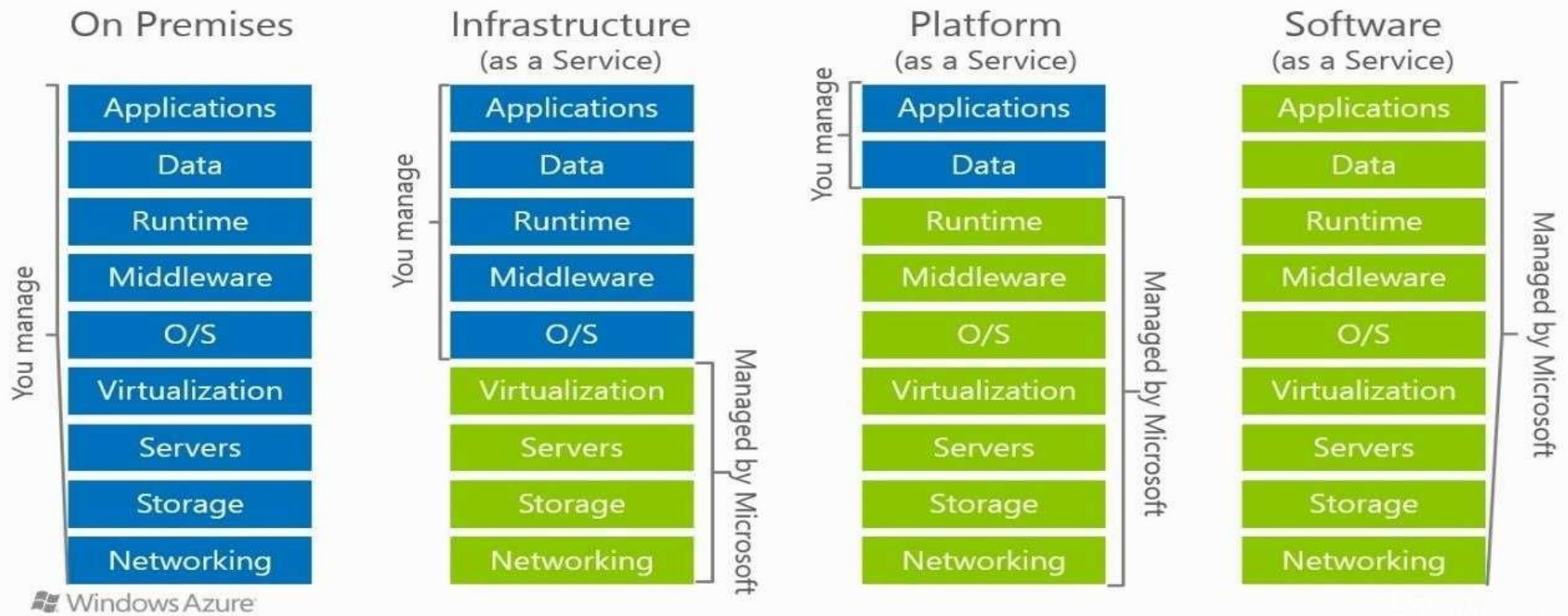
# Sommaire

1. Présentation du Cloud Computing
2. Pourquoi et comment migrer sur le Cloud ?
3. Les grands enjeux pour les acteurs des services financiers
4. Services du Cloud
5. Annexes

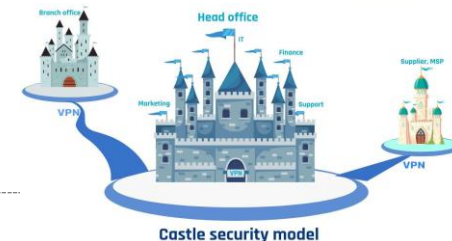
# Les modèles de services Cloud et la responsabilité partagée



## Cloud Models



## Sécurité : Accès Zero Trust



L'accès Zero Trust est un modèle stratégique de cybersécurité conçu pour protéger l'environnement numérique des entreprises modernes, incluant de plus en plus les clouds publics et privés, les applications SaaS, les environnements DevOps, l'automatisation des processus par la robotique (APR), etc. L'accès Zero Trust est centré sur la conviction que les entreprises devraient systématiquement **ne jamais faire confiance à quoi que ce soit**, ni à l'intérieur et ni à l'extérieur de leur périmètre réseau. Selon les modèles Zero Trust, tous les éléments et toutes les personnes qui tentent de se connecter aux systèmes d'une organisation doivent d'abord être vérifiés avant qu'un accès leur soit accordé. L'objectif principal du modèle Zero Trust consiste à réduire le risque de cyberattaque dans l'environnement moderne utilisé par la plupart des organisations.

Le modèle Zero Trust rejette en grande partie l'approche traditionnelle de la cybersécurité, de type « château entouré de douves », qui cherche à défendre le périmètre, empêcher les attaquants d'entrer, tout en supposant que toutes les personnes et tous les éléments présents à l'intérieur du périmètre disposent d'un accès valide et ne posent ainsi aucun risque pour l'organisation. Cette approche s'appuie largement sur des pare-feu et autres mesures de sécurité similaires, mais elle s'est avérée impuissante face à la menace posée par des acteurs malveillants situés à l'intérieur des organisations et qui ont obtenu (ou à qui l'on a donné) l'accès à des comptes à privilèges.

La transformation digitale a accru la complexité de l'écosystème technologique actuel. Il est donc nécessaire d'ajuster les stratégies de sécurité traditionnelles. Plus la surface d'attaque augmente, plus les méthodes de protection du périmètre se montrent inefficaces. En outre, les fournisseurs distants requièrent souvent un accès à privilèges aux systèmes internes critiques et il peut s'avérer difficile de savoir qui a besoin d'accéder à quelles ressources. À l'inverse, l'accès Zero Trust est appliqué à tous les niveaux, ce qui permet de garantir que seuls les utilisateurs humains ou non humains autorisés peuvent accéder aux données dont ils ont besoin (et uniquement ces données), au moment où ils en ont besoin. Dans les référentiels Zero Trust, un « périmètre défini par logiciel » fournit un accès à privilèges aux utilisateurs humains et non humains, quels que soit leur emplacement géographique, la machine ou le terminal utilisé, et quel que soit l'emplacement d'hébergement des données et des charges de travail (sur site, dans le cloud ou dans les environnements hybrides).



## Comment implémenter l'accès Zero Trust dans votre organisation



Il n'existe pas une seule technologie Zero Trust. Les stratégies Zero Trust efficaces s'appuient sur un mélange de technologies et d'approches existantes, comme l'authentification à plusieurs facteurs (**MFA**), la gestion des identités et des accès (**IAM**), la gestion des accès à privilèges (**PAM**) et la **segmentation** du réseau, pour une défense exhaustive et en profondeur. L'accès Zero Trust valorise également les stratégies de gouvernance telles que le principe du **moindre privilège**.

Pour construire des architectures modernes conformes au modèle Zero Trust, les organisations adoptent souvent une approche programmatique par phases au fil du temps, qui implique certaines ou l'ensemble des étapes suivantes.

# Comment implémenter l'accès Zero Trust dans votre organisation



## Protéger les comptes à privilèges puissants.

Il est établi que la majorité des menaces internes et des attaques externes se basent sur une utilisation abusive des accès à privilèges. Les organisations doivent identifier les comptes à privilèges, les identifiants et les secrets les plus importants dans leur environnement et déterminer leurs faiblesses et vulnérabilités potentielles, qui pourraient mettre en péril leurs données sensibles et leur infrastructure critique. À partir de ces renseignements, elles peuvent mettre en œuvre des contrôles d'accès pour protéger les comptes à privilèges qui posent le plus grand risque dans le modèle Zero Trust. Au fil du temps, elles peuvent étendre cette protection aux autres utilisateurs et applications dans toute l'entreprise, dans le cloud, sur les terminaux et dans le pipeline DevOps.

## Mettre en œuvre l'authentification en plusieurs étapes pour les actifs stratégiques.

Dans les modèles Zero Trust, les actifs de niveau 0 doivent être protégés avant tout le reste. Une authentification à plusieurs facteurs (MFA) permanente est essentielle pour réduire la question de la confiance vis-à-vis des utilisateurs et des appareils. De plus, l'authentification incrémentielle ou juste à temps, et les processus d'autorisation par la direction qui permettent d'authentifier les utilisateurs à privilèges au niveau exact du point d'accès, réduisent les risques d'attaques basées sur les identifiants à privilèges.

## Renforcer la sécurité des terminaux.

Si un attaquant ou un acteur interne mal intentionné parvient à accéder à des identifiants à privilèges, il prend l'apparence d'un utilisateur de confiance. Cela rend plus difficile la détection des activités à risque. En complément des outils de détection et de réponse, des antivirus/NGAV, des correctifs pour applications et systèmes d'exploitation, les organisations peuvent réduire le risque d'attaque en gérant et en sécurisant les privilèges sur les terminaux. De plus, il est conseillé aux organisations d'implémenter des modèles de restrictions qui font uniquement confiance à des applications spécifiques, exécutées par des comptes spécifiques et dans des circonstances spécifiques. Cette démarche aidera à réduire le risque d'attaque par rançongiciel et injection de code.

## Surveiller le parcours des privilèges.

La surveillance continue du parcours des accès à privilèges empêche les acteurs internes malveillants et les attaquants externes à progresser dans leur attaque. Les organisations doivent installer des contrôles stricts autour des éléments auxquels les utilisateurs finaux peuvent accéder. Elles doivent créer des couches d'isolation entre les terminaux, les applications, les utilisateurs et les systèmes, le tout en surveillant les accès en continu afin de réduire la surface d'attaque.



### Mettre en œuvre le principe du moindre privilège.

Il est essentiel de savoir qui (parmi les utilisateurs humains et non humains) a accès à quoi, à quel moment et quelles sont les interactions possibles. Les organisations doivent appliquer le principe du moindre privilège de façon générale en parallèle de contrôles d'accès basés sur les attributs qui combinent les stratégies au niveau de l'entreprise avec des critères utilisateur spécifiques afin de trouver un équilibre entre sécurité et facilité d'utilisation.

# Gouvernance des données – Aspect juridique



Le Cloud Act, aussi dit le Clarifying Lawful Overseas Use of Data Act, est une loi fédérale des États-Unis adoptée en 2018 sur la surveillance des données personnelles, notamment dans le Cloud. Elle permet aux forces de l'ordre de contraindre les fournisseurs de services américains à fournir les données demandées stockées sur des serveurs, qu'ils soient situés aux États-Unis ou pas.

L'adoption du Cloud Act aux États-Unis a relancé le débat sur l'extra-territorialité des mandats américains sur des données hébergées dans des datacenters à l'étranger.

## Le Cloud Act entre-il en conflit avec le RGPD?

Les grands acteurs américains du Cloud (Amazon, Google, Microsoft) disent respecter le RGPD. Le gouvernement n'a pas accès aux données – il faut le demander à un juge et il faut qu'il y ait un acte criminel. Dans tous les cas, les fournisseurs conseillent aux clients de chiffrer leurs données ainsi que la seule chose qu'ils pourront transmettre à un juge sont des données chiffrées et donc inutilisables (car seul le client a la clé du chiffrement). En chiffrant ses données, le client devient le garant de la sécurité de ses données.



Le RGPD, règlement général sur la protection des données, est un règlement de l'Union Européenne relatif à la protection des données à caractère personnel, entré en application en mai 2018. Le RGPD établit des règles sur la collecte et l'utilisation des données personnelles et impose à toute entreprise de connaître les traitements qu'elle effectue sur les données personnelles qu'elle récolte.

L'EBA (European Banking Authority) formule des recommandations\* en ce qui concerne l'externalisation vers des fournisseurs de services Cloud (décembre 2017). L'EBA n'interdit pas aux sociétés européennes de se transférer sur le Cloud, mais recommande d'être d'autant plus vigilant lors de la conclusion d'accord conclus avec une contrepartie non européenne et alerte sur les risques liés au Cloud.

En outre, l'EBA rappelle les bonnes pratiques sur le Cloud en matière de sécurité comme la gestion des accès et des identités, les clés de chiffrement, l'authentification (notamment avec le multi-facteur). Le contrôle de la configuration technique des infrastructures est « d'une importance vitale ».

Ameur

Kais

\* V

o  
i  
r

A  
n  
n  
e  
x  
e

-

F  
i  
n  
a  
l

R  
e  
p  
o  
r  
t

E  
B  
A

R  
e  
c  
o  
m  
m  
a  
n  
d  
a  
t  
i  
o  
n  
s

o  
n

C  
l  
o  
u  
d

O  
u  
t  
s  
o  
u





Une solution pour la protection des données migrés sur le Cloud peut être le chiffrement de ces données.

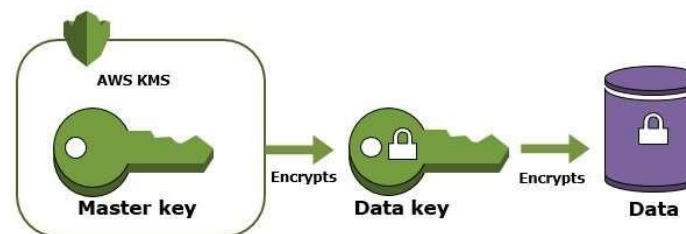
Les clés de chiffrement permettent au fournisseur de crypter des données stockées en ligne par leurs clients. Il existe différentes clés de chiffrement et donc différents niveaux de sécurité. Il existe deux types de chiffrement pour crypter les données dans le Cloud :

- Chiffrement des données **stockées et transférées** : dans ce type de chiffrement, les **données transférées sont cryptées**. Ainsi, un pirate ne pourra pas intercepter un document/mot de passe, etc. Le cryptage des données stockées en ligne offre une **protection supplémentaire**. Néanmoins, dans ce cas, le fournisseur de service Cloud dispose de la clé de chiffrement et de déchiffrement et peut donc « voir » les données. Lorsque le prestataire est français, cela ne pose pas vraiment de problème puisque la loi sur la protection des données est stricte en France. Par contre, lorsqu'il s'agit d'un fournisseur américain, comme les géants du Cloud grand public, cela soulève la question de la sécurité (étant donné qu'ils sont soumis au Cloud Act).
- Chiffrement de **bout en bout** : dans ce type de chiffrement, le fournisseur de solution Cloud ne peut pas accéder aux fichiers : les données sont chiffrées et déchiffrées **en local**. Avec ce type de chiffrement, les données sont en sécurité et leur confidentialité est respectée.

Le service AWS propose **3 niveaux de chiffrement des données** (KMS – Key Management Service)

- AWS détient **toutes les clés** : Dans ce cas-là, l'espace reste vulnérable étant donné que le service de stockage Cloud peut être compromis par une attaque où ceux qui l'ont initiée peuvent accéder aux clés de chiffrement des utilisateurs et donc à leurs données.
- **Client génère les clés / Clés sont hostés chez AWS** (hostés à un autre endroit que data).
- **Clés gardées chez client** : dans ce cas là, le client ne peut pas utiliser toutes les fonctionnalités AWS. Les fichiers sont illisibles sans cette clé.

KMS permet de gérer un **double niveau de chiffrement** : celui des données à proprement parler et celui des clés utilisées à ces fins. C'est le principe du chiffrement « en enveloppe ».



Avec le recours au chiffrement, le risque est transféré des données aux clés. Pouvoir sécuriser la gestion, le stockage et l'utilisation de ces clés de chiffrement est donc essentiel. Le **déploiement d'une plateforme de gestion du chiffrement** de niveau d'assurance élevé est indispensable pour protéger ces clés. Cette approche repose sur la génération de clés fortes, la gestion des clés de l'entreprise, une administration centralisée des ressources de chiffrement et l'utilisation de dispositifs matériels de confiance.



### ➤ 4.5 SECURITE DES DONNEES ET SYSTEMES

15.[...] le contrat d'externalisation devrait obliger le fournisseur de services externes à protéger la confidentialité des informations transmises par l'établissement financier. [...] les établissements devraient mettre en place des dispositions visant à assurer la continuité des services fournis par les fournisseurs de services externes. [...] les besoins respectifs des établissements pratiquant l'externalisation en matière de qualité et de performance devraient être pris en considération dans les contrats d'externalisation écrits et les accords de niveaux de service. Ces questions liées à la sécurité devraient également faire l'objet d'un suivi permanent.

16. Aux fins du point précédent, avant l'externalisation et afin d'éclairer la prise de décision, l'établissement devrait au moins effectuer les opérations suivantes :

- a) Recenser et classifier ses activités, ses processus et les données et systèmes connexes en matière de sensibilité et de protection requise;
- b) Procéder à une sélection minutieuse, fondée sur les risques, des activités, des processus et des données et systèmes connexes susceptibles d'être externalisés vers une infrastructure informatique en nuage;
- c) Définir et décider d'un niveau approprié de protection de la confidentialité des données, de continuité des activités externalisées, ainsi que d'intégrité et de traçabilité des données et des systèmes dans le cadre de l'externalisation en nuage envisagée. Par ailleurs, les établissements devraient examiner des mesures spécifiques, le cas échéant, applicables aux données en transit, aux données en mémoire et aux données au repos, telles que l'utilisation de technologies de cryptage associées à une architecture de gestion des clés appropriée.

17. Par la suite, les établissements devraient veiller à disposer d'un accord écrit avec le fournisseur de services en nuage dans lequel figurent notamment les obligations qui incombent à ce dernier en vertu du paragraphe 16 (c).

18. Les établissements devraient assurer le suivi permanent de l'exécution des activités et des mesures de sécurité, conformément à l'orientation 7 des orientations du CECB, y compris les incidents, et, le cas échéant, vérifier si l'externalisation de leurs activités est conforme aux points précédents. En outre, ils devraient prendre sans délai les mesures correctrices requises.



### ➤ 4.6 LOCALISATION DES DONNÉES ET TRAITEMENT DES DONNÉES

19.[...] les établissements devraient prendre des précautions particulières lorsqu'ils concluent et gèrent des accords d'externalisation convenus en dehors de l'EEE, en raison des risques potentiels pour la protection des données et pour le contrôle effectif par l'autorité de surveillance.

20. L'établissement pratiquant l'externalisation devrait adopter une approche fondée sur le risque concernant la localisation et le traitement des données lorsqu'il recourt à l'externalisation vers un environnement en nuage. L'évaluation devrait porter sur la possible incidence des risques, y compris les risques juridiques et les questions de conformité, ainsi que sur les limites de la surveillance dans les pays où les services externalisés sont fournis ou susceptibles de l'être et les données stockées ou susceptibles de l'être. L'évaluation devrait tenir compte de considérations relatives à la stabilité politique et sécuritaire plus large des juridictions en cause, aux lois en vigueur au sein de ces juridictions (y compris la législation relative à la protection des données), et aux dispositions sur l'application des lois en vigueur dans ces juridictions, y compris les dispositions relatives à l'insolvabilité qui s'appliqueraient en cas d'erreur de la part du fournisseur de services en nuage. L'établissement pratiquant l'externalisation devrait veiller à ce que ces risques soient maintenus dans des limites acceptables et proportionnées au caractère significatif de l'activité externalisée.

# Compétences et responsabilités de la DSI pour travailler dans le Cloud



## Compétences de la DSI

L'éventail des compétences attendues englobent les qualités suivantes :

- Expertise technique
- Veille technologique
- Management des hommes (notamment, former les collaborateurs aux nouveaux outils)
- Gestion des budgets et ressources
- Optimisation des achats
- Négociation
- Conseil
- Consultant fonctionnel
- Coordinateur des projets
- Accompagnement du changement (nécessite entre autre d'avoir une vision précise du métier de ses collaborateurs)
- Et last but not least : Maître d'Œuvre de la Transition Numérique

## Responsabilités de la DSI :

- **Management des nouveaux projets** : Le management des nouveaux projets est vraisemblablement le cœur même de la question posée autant par la gouvernance des SI que par les exigences de l'accomplissement de la stratégie d'entreprise. Les contraintes techniques ne sont plus les seules à occuper l'esprit des acteurs de la DSI. Un projet d'intégration des technologies se doit d'une manière ou d'une autre de contribuer à la création de valeurs.
- **ROI Projet** : Garantir et assurer un ROI du projet effectif est désormais part intégrante des nouvelles responsabilités de la DSI.
- **Responsabilité commerciale** : La gestion des contrats commerciaux et le suivi de la qualité de services (QoS).
- **Responsabilité juridique** : Les contrats, la gestion des risques et la sécurité. Garanties de la gestion des données personnelles (notamment avec le RGPD).
- **Responsabilité éthique** : Jusqu'où ne faut-il pas aller pour éviter les atteintes aux libertés individuelles lors de la collecte ou du rapprochement des informations personnelles ? Le rapprochement de fichiers n'est pas qu'une préoccupation technique. Les conséquences des enseignements que l'on pourra en tirer sont directement de la responsabilité de ceux qui l'ont rendu possible. C'est ainsi.