



**Comment le cloud  
m'aide à lancer de  
nouveaux services  
plus rapidement ?**



**Business  
Services**

# Introduction

**Le cloud computing devient la norme : 20% des entreprises européennes de plus de 500 salariés ont migré plus de la moitié de leurs applications dans le cloud, et 44 % devraient l'avoir fait à l'horizon 2020 <sup>1</sup>.**

**Mais s'appuyer sur le cloud comme vecteur de transformation digitale pose des défis organisationnels et techniques.**

Pour les entreprises, la promesse du cloud computing a de quoi séduire : un service performant à coût maîtrisé. Mais lorsqu'elles intègrent les exigences de sécurité des données, la conformité réglementaire et les attentes des utilisateurs sur les performances, cette promesse peut devenir un mirage.

Certes, le déploiement progressif de quelques applications dans le cloud permet aux équipes informatiques de développer leur expertise au rythme qui leur convient. Mais l'introduction du cloud dans l'ADN de l'entreprise (pour tous les processus métiers et flux de données) relève d'une stratégie globale et pérenne.

Cet eBook réalisé par les experts d'Orange Business Services propose des réponses pragmatiques aux 6 enjeux d'un projet de transformation de l'IT vers le cloud computing :

- **Définir sa stratégie cloud** (page 3)
- **Acquérir les compétences pour une migration réussie** (page 5)
- **Offrir une expérience utilisateur inégalée dans l'environnement cloud** (page 7)
- **Protéger les données et respecter les réglementations** (page 9)
- **Gérer les niveaux de service dans le cloud** (page 11)
- **Maîtriser les budgets** (page 13)



# Définir sa stratégie cloud

## L'enjeu

La stratégie cloud de l'entreprise reflète le niveau de maîtrise et de responsabilité qu'elle souhaite conserver.

Lorsqu'elle se tourne vers un fournisseur SaaS (software as a service), celui-ci assure la performance de l'ensemble du dispositif de cloud computing : infrastructures, middleware et applications. Le fournisseur PaaS (platform as a service) ne se porte garant que du middleware et des infrastructures, alors que l'IaaS (infrastructure as a service) concerne uniquement les infrastructures.

Pour l'entreprise qui s'apprête à migrer son SI dans le cloud, ces responsabilités ne sont pas forcément les mêmes selon les applications métiers. Par exemple, une application de collaboration standard pourra fonctionner en mode SaaS, alors qu'une application industrielle développée en interne, plus critique, sera probablement en mode PaaS ou IaaS.

L'entreprise doit également prendre en considération d'autres critères :

- **Financiers** : quel est le coût de revient global ? Pour chaque application pouvant basculer dans le cloud, analysez les composantes de ses coûts (licences, maintenance évolutive, corrective, stockage des données, ressources humaines de supervision, liaisons d'accès réseau, dispositifs de sécurité, maintenance des interfaces...). Si cette application passait dans le cloud, quelles seraient les modalités de facturation des fournisseurs ? Privilégiez la facturation à l'usage.
- **Fonctionnels** : quelles fonctionnalités applicatives et quels niveaux de services sont nécessaires à votre activité ? Analysez les volumes de trafics actuels, attendus et les exigences de qualité de service (disponibilité, temps de réponse, SLA). Pouvez-vous différencier les SLA selon la criticité opérationnelle des usages ? Certaines fonctionnalités anciennes sont-elles toujours utiles ?
- **Réglementaires** : comment protéger les données des clients et des collaborateurs ? Quelles mesures sont nécessaires pour sécuriser la propriété intellectuelle ? Quelles catégories de données sont soumises à quelles réglementations dans chaque pays ? Quels impacts sur les contrats avec les fournisseurs de cloud ?

Le meilleur moyen d'optimiser l'ensemble de ces critères est souvent de procéder par groupe d'applications et d'adopter une stratégie « multi-cloud », combinant des choix de services IaaS, PaaS ou SaaS de plusieurs fournisseurs et s'appuyant sur des architectures publiques, privées ou hybrides.

Ces configurations confèrent aux équipes informatiques une position de « courtiers de services cloud » pour les métiers de l'entreprise, permettant de satisfaire développeurs et utilisateurs, et de déployer de nouvelles fonctionnalités à la demande.



## Pourquoi adopter une stratégie multi-cloud ?

Face aux incertitudes du marché du cloud (pérennité des stratégies de certains acteurs, conformité à l'évolution du cadre réglementaire ou aux politiques de sécurité des entreprises, niveau d'autonomie des entreprises vis-à-vis de certains acteurs ...), de nombreuses entreprises souhaitent garder leur liberté de choix en retenant plusieurs acteurs.

Cette décision peut être renforcée par le besoin de se réappropriier des services qui auraient été souscrits en sandow IT : en réintégrant de telles prestations d'acteurs de cloud public, la DSI peut se remettre au centre du jeu comme interlocuteur privilégié des métiers.

Le multi-cloud se révèle alors souvent comme la meilleure solution pour les équipes informatiques et les utilisateurs, et ses bénéfices sont :

- **Plusieurs choix possibles** : en répartissant les applications sur plusieurs solutions clouds de plusieurs fournisseurs, vous répondrez plus finement aux besoins fonctionnels des utilisateurs et aux nécessités de souveraineté et de sécurité des données, sans vous lier à un fournisseur unique.
- **Optimisation des coûts** : en migrant son IT sur les serveurs virtualisés de différentes solutions cloud et en généralisant le paiement à l'usage, les coûts sont optimisés.
- **Résilience** : le recours à plusieurs fournisseurs de cloud réduit le risque de points individuels de défaillance.
- **Flexibilité** : le multi-cloud est souvent suffisamment flexible pour accompagner vos nouvelles initiatives digitales, telles que l'analyse big data, les plateformes d'objets connectés (IoT), les chatbots et l'intelligence artificielle...qui auront leurs propres exigences.

Par ailleurs, lors d'une fusion/acquisition, le mode multi-cloud s'impose aux équipes de la DSI.

En définitive, le challenge pour une entreprise ne sera plus tant plus de garder une liberté de choix, mais de gérer la complexité naturellement induite par la juxtaposition de plusieurs services cloud.

Dans ces conditions, est-il souhaitable de gérer ces multiples interfaces ou confier à un tiers de confiance le rôle d'agrégateur de ces services, pour mieux se concentrer sur le rôle d'interlocuteur des métiers et de prescripteurs pour les innovations que l'entreprise souhaite engager ?

**90%** des entreprises prévoient de s'appuyer sur plusieurs solutions de cloud computing.<sup>2</sup>

## Analysez vos applications pour bien choisir leur modèle de cloud

Le multi-cloud vous permet de répartir vos applications chez plusieurs fournisseurs et selon plusieurs modèles (IaaS, PaaS, ou SaaS, stockage public ou privé). Pour faire les bons choix, analysez bien vos applications, une par une.



### Les coûts

Le cloud public est souvent bien adapté pour optimiser les coûts de certaines applications (telles que les applications sur étagères, standardisées, ou celles aux usages très variables selon la demande ou sujettes à des pics d'activité). Il nécessite un investissement initial relativement faible.



### Les volumes de trafic de données

Mais lorsqu'une application génère beaucoup de trafic ou que ses données doivent être cryptées, les coûts de WAN et les risques en matière de performance rendent les clouds publics peu avantageux. Toutefois, certains fournisseurs de services cloud publics offrent, à un prix supérieur, des solutions à plus faible latence réseau.



### Confidentialité, sécurité des données, conformité réglementaire

Lorsqu'une application doit répondre à des exigences de confidentialité (application RH, base clients, e-commerce...), le cloud privé permet généralement une sécurité renforcée. Et il s'adapte plus aisément aux procédures opérationnelles et besoins régionaux de votre organisation.

Mais après l'investissement initial dans un cloud privé, pour en tirer tous les avantages, votre équipe informatique devra en maximiser l'utilisation en y migrant d'autres applications.

L'option du cloud hybride offre le double bénéfice du traitement des données dans un cloud public et de leur stockage dans un cloud privé.



### Le maintien de vos standards IT

Si le contexte technique de cloud computing qui vous est proposé s'appuie sur des plateformes (de serveurs, de stockage et/ou de protection des données) similaires à celles de votre système existant, vous aurez moins de modifications à apporter à vos architectures applicatives et à vos configurations. Vos coûts de migration en seront réduits. C'est en cela qu'un cloud privé est généralement intéressant pour les applications historiques.



### Réversibilité

Pour certaines applications placées chez un fournisseur de cloud, il convient de penser au coût et à la complexité de la récupération des données en cas de réversibilité. Ce facteur est souvent négligé alors que, sur certaines plateformes publiques, ces coûts peuvent être considérables. Pour vos services en SaaS, vérifiez comment vous pourrez récupérer vos données à partir du nuage, sous quel format et vérifiez que d'autres fournisseurs prennent en charge ce format.

# Les compétences pour réussir sa migration

## L'enjeu

La migration de vos applications dans le cloud est l'étape clé de votre transformation numérique.

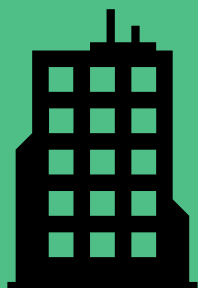
Pour y parvenir, les entreprises doivent conduire des arbitrages selon la typologie de leurs applications.

Parmi les applications traditionnelles, une première distinction s'opère entre les applications éligibles à la transformation cloud et les applications historiques (« legacy »).

Les premières sont celles qui ont déjà fait l'objet d'une évolution lors de la virtualisation des infrastructures IT, de sorte que le passage au mode cloud est souvent bien balisé chez les acteurs cloud qui offrent des prestations de services d'aide à la migration.

En revanche, les applications « legacy » sont celles dont les spécificités éditeurs interdisent souvent cette évolution. L'alternative est alors de les conserver en l'état jusqu'à leur fin de vie (si celle-ci est envisageable à un horizon proche) ou de les réécrire en mode cloud si le coût associé peut se justifier en regard de son usage et son caractère stratégique.

A côté des traditionnelles, certaines applications sont plus naturellement appelées à fonctionner sur plusieurs cloud, par exemple pour répartir les risques ou s'appuyer sur des infrastructures géographiques plus locales. C'est fréquemment le cas des applications récentes de la vague digitale, souvent dotées d'une app mobile. Il est alors intéressant de les développer en tant que « cloud native application », c'est-à-dire en intégrant les nouveaux concepts du développement logiciel, tel que le développement agile, le DevOps, les conteneurs, le déploiement continu et les microservices. Les applications ainsi développées pourront s'adapter d'un cloud à l'autre généralement sans difficulté. Vous pouvez vous faire aider par des prestataires qui vous formeront et vous aideront à maîtriser ces concepts et technologies.



# 37%

des entreprises s'inquiètent de ne pas posséder les bonnes compétences pour gérer les environnements cloud et en tirer tous les avantages.<sup>3</sup>

## Les 5 compétences clés pour la migration d'applications

Rôle	Responsabilités
1. <b>L'architecte</b>	Collabore avec les autres entités de la DSI pour porter la feuille de route de la migration et veiller au respect des exigences en matière d'infrastructures, de stockage des données et de sécurité.
2. <b>Le transition manager</b>	Coordonne le projet de transformation dans le cloud, en minimisant l'indisponibilité des applications critiques. Il travaille avec les directions métiers.
3. <b>L'application and data manager</b>	Définit les tâches ETL (Extract, Transform and Load) du stockage de données, grâce à sa connaissance des données applicatives.
4. <b>Le spécialiste migration</b>	Sélectionne les outils pour migrer les données non-structurées et structurées, ainsi que les images de machines virtuelles, convertissant le format des données si nécessaire. Il évalue s'il convient de migrer les applications en ligne pour éviter leur indisponibilité, ou si une migration offline avec copie initiale des données suivie d'une synchronisation du delta des données est possible.
5. <b>Le chef de projet</b>	Gère la migration, évalue le temps requis en fonction de la bande passante disponible et l'impact de la latence du réseau sur les applications sensibles.

Évaluez vos capacités (expertises, disponibilité) et définissez la répartition des rôles avec votre prestataire cloud à travers une matrice RACI (responsible, accountable, consulted, informed) adaptée à votre propre situation.

## 4 étapes préalables pour migrer dans le cloud en toute sérénité

- 1. Connaître vos actifs :** utilisez un outil d'asset management pour répertorier vos applications, les numéros de versions et surtout les détails de leur configuration. Puis inventoriez les flux entre applications, les échanges avec des bases de données distantes ou des annuaires centralisés.
- 2. Adapter les applications :** certaines applications historiques devront être dotées d'une nouvelle architecture, voire partiellement réécrites pour fonctionner dans un environnement cloud.
- 3. Choisir votre méthode de migration, on-line ou off-line :** ce choix dépend de la tolérance des applications ou bases de données à l'indisponibilité, à la déconnexion, et de la bande passante de la connexion vers le cloud.
- 4. Prioriser :** Migrez d'abord les applications non-critiques, telles que celles ayant moins de connexions avec applications tierces ou des bases de données distantes. Commencez par les applications dont les impacts opérationnels sont les moins graves en cas d'indisponibilité.

## Rester réactif pendant la migration des applications

Orange collabore avec un fournisseur de services de santé, qui hébergeait des données sensibles de patients dans une base de données.

Le maintien de cette application historique accaparait la majorité du budget informatique, d'autant plus que différentes versions étaient utilisées dans chaque région.

Orange a aidé l'entreprise à consolider l'application et à rationaliser les versions antérieures en identifiant les charges et les flux de travail. Ce faisant, Orange a découvert des éléments non migrables en l'état, qu'il a fallu modifier avant de les transférer dans le cloud.

Au final, les coûts d'administration ont été réduits et le data center du client a libéré de la capacité.



« Les entreprises qui adoptent la transformation cloud doivent anticiper les nouvelles compétences. »

# Offrir une expérience utilisateur inégalée

## L'enjeu

Dans un environnement non cloud actuel, les applications historiques sont souvent distribuées sur différents serveurs dans le monde pour minimiser les délais sur les réseaux, déterminés par la distance séparant le serveur de l'utilisateur.

A contrario, la plupart des applications cloud en SaaS reposent sur une unique instance mondiale, située près du plus grand nombre d'utilisateurs. Les utilisateurs situés plus loin des sites centraux doivent parfois patienter pendant le chargement de leurs données ou leur sauvegarde par leur solution SaaS (sans parler des interruptions dues à des délais trop élevés et aux applications qui atteignent leur « time-out » prématurément). Pour une entreprise dont l'activité dépend de l'efficacité de son flux d'informations, cette situation est inacceptable.

La connectivité au cloud constitue donc le facteur le plus déterminant de l'expérience utilisateur. Le réseau doit être bien conçu, flexible, et sa performance régulièrement suivie.



## Des technologies qui améliorent l'expérience utilisateur

Lorsque les utilisateurs et le fournisseur SaaS ne sont pas situés dans un même pays, ou lorsque les infrastructures Internet du pays ne sont pas robustes, la connectivité locale est inadéquate pour la plupart des scénarios d'usage du cloud. En effet, les performances varient au cours de la journée, et dépendent de facteurs incontrôlables tels que les conditions locales d'utilisation d'Internet et les niveaux de congestion régionaux.

Heureusement, il existe des solutions alternatives.



**Connectivité directe au fournisseur SaaS**  
Certaines applications SaaS gourmandes en bande passante et sensibles à la latence du réseau nécessitent des connexions dédiées, à un prix plus élevé. Certains fournisseurs de WAN proposent aussi de tels accès directs.



**WAN sécurisé avec accès Internet répartis**  
Il est possible d'utiliser un WAN privé et sécurisé entre les sites d'une entreprise, avec une ou plusieurs sorties vers l'Internet, et des dispositifs de sauvegarde de trafic en mode cache pour améliorer les temps de réponse.

Certains fournisseurs de WAN proposent des liens directs vers les principaux éditeurs SaaS, IaaS ou PaaS, ainsi que les centres d'hébergements des clouds privés. Ceci garantit d'excellentes performances, sans exposition aux cyber-menaces présentes sur l'Internet.



**Optimisation du trafic et « network as a service »**

Les solutions d'optimisation du trafic (virtualisés ou sur site) compressent les données envoyées sur les liaisons WAN, optimisent certains protocoles gourmands, et réduisent ainsi les volumes de données à transférer. Elles permettent aussi de prioriser les trafics des applications selon les priorités de l'entreprise et son agenda, et de mesurer les flux de données pour les contrôler finement.

Les fournisseurs de « network as a service » permettent de configurer rapidement les solutions d'optimisation ainsi que de modifier en temps réel les caractéristiques réseaux (bande passante, classes de service, options de sécurité...), ce qui est très pratique pendant les périodes de migration ou de pointe de trafic.

## 4 étapes pour optimiser la performance des applications dans le cloud

### 1. Modélisez les niveaux d'utilisation prévus

Utilisez un outil de modélisation de la bande passante qui prend en compte les usages des différentes catégories d'utilisateurs, les tailles typiques des fichiers et les pointes de trafic des applications.

### 2. Choisissez votre connectivité par application et par catégorie d'utilisateur

Utilisez des outils d'optimisation pour gérer les questions de latence ou de perte de paquets.

Dans certaines situations, il est possible de déployer une application SaaS en mode hybride, avec certaines composantes hébergées mondialement et d'autres dans vos centres de données ou chez un fournisseur tiers, de manière à surmonter les problèmes de performance et de sécurité. Un prestataire de services peut vous guider dans la conception de telles architectures.

**3. Pensez aux sites isolés et aux collaborateurs nomades**  
Dans certaines parties du monde, l'Internet peut souffrir d'une performance constamment insatisfaisante, du fait du filtrage des contenus par les autorités publiques. Dans ces conditions, une connexion WAN privée peut être la meilleure option. De même, la bande passante peut être irrémédiablement insuffisante pour les collaborateurs nomades utilisant des connexions cellulaires ou satellite. L'optimisation du WAN s'avère alors précieuse pour réduire fortement les besoins de bande passante.

### 4. Mesurez l'expérience utilisateur

Les équipes de maintenance ne devraient pas attendre les signalements au service d'assistance pour découvrir que leurs collègues souffrent de difficultés d'accès aux applications cloud. Les technologies de suivi de la performance du réseau et des applications (NPM/APM) permettent de gérer la capacité ou de résoudre certains dysfonctionnements. Combinées à des sondes disposées chez les clients, elles permettent de suivre la performance véritablement ressentie par chaque utilisateur du cloud, telle que la perte de paquets, et offrent un tableau de bord de la qualité pour toute l'entreprise.

« La performance des applications cloud est essentielle à la productivité des collaborateurs et à la satisfaction des clients. »

« Faute de considérer la connectivité au cloud comme une exigence majeure, les impacts sur l'expérience utilisateur peuvent être considérables »

## Optimiser la performance des applications en période de pointe

Chaque succès apporte son lot de difficultés. Lane Crawford, un distributeur chinois de marques de luxe, enregistrait une forte croissance de ses ventes en ligne. Mais il souffrait du manque de flexibilité du système de gestion des ventes, Oracle, en période de soldes et lors des pics d'activité.

Orange a migré la solution sur le service cloud d'Orange, en y ajoutant l'optimisation de la performance. L'équipe de mise en œuvre a utilisé un générateur de trafic pour tester le système dans les scénarios d'utilisation prévus.

Satisfait du résultat, le client a ensuite migré d'autres modules de commerce électronique sur le service cloud d'Orange.

# 32%

des professionnels des réseaux considèrent l'accès aux services de cloud public comme un facteur important d'évolution de leur réseau, et

# 25%

la priorisation des applications business critiques <sup>4</sup>



# Protéger les données en conformité avec la réglementation

## L'enjeu

Les entreprises font face à un double défi. D'une part, les attaques sur leurs données sont de plus en plus agressives et ciblées. D'autre part, les réglementations se renforcent. Combinés aux conséquences potentielles d'une attaque réussie, ces défis font de la sécurité le plus gros enjeu du cloud computing actuellement.

Pour protéger les données de leurs clients, collaborateurs et partenaires qui sont hébergées dans le cloud, les entreprises doivent dorénavant adopter des programmes efficaces et visibles en interne.

## 4 enjeux de sécurité et de conformité du cloud

### 1. Les réglementations

De très nombreux pays, de l'Australie à la Russie, de la France à la Chine, ont adopté des réglementations rigoureuses en matière de protection des données. Beaucoup d'entre elles exigent des entreprises qu'elles stockent les données personnelles des ressortissants sur le territoire national.

### 2. Les exigences sectorielles

Mais les réglementations varient selon le secteur d'activité. Ainsi, les organisations de la santé sont soumises à des normes plus strictes de confidentialité des données des patients, et les enseignes de distribution doivent s'adapter fréquemment aux évolutions de la norme PCI-DSS (paiements par carte).

### 3. Le Règlement Général sur la Protection des Données (RGPD / GDPR : General Data Protection Regulation)

A partir de mai 2018, toute entreprise ou organisme public employant des salariés dans l'Union européenne ou traitant des données de citoyens de l'UE devra se conformer au RGPD. Ce règlement européen est identique dans chaque pays et prévoit des amendes pouvant atteindre 20 millions d'euros ou 4% du chiffre d'affaires.

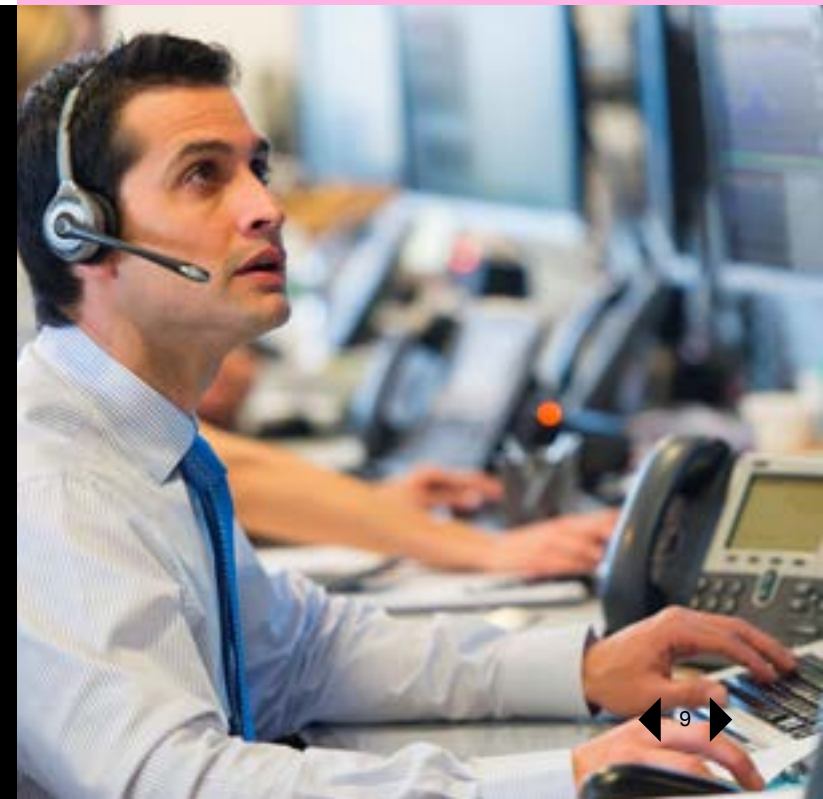
### 4. Des volumes d'informations sur les systèmes en augmentation

Les entreprises collectent et stockent de plus en plus de données sur l'utilisation de leurs systèmes (origine des connexions, durées...). Pour les équipes de cyberdéfense, cette masse de données rend plus difficile l'identification des incidents de sécurité.



# 53%

La sécurité est le premier des soucis concernant le cloud computing pour 53% des décideurs.<sup>5</sup>



## Comment sécuriser un environnement cloud



### Protégez les données

Évaluez les modalités de chiffrement et de déchiffrement des données pendant leur stockage et leur transfert. Mettez en place ou confiez à un tiers un processus rigoureux de production et de protection des clés, et assurez-vous que vos fournisseurs de services cloud n'y ont pas indûment accès. Pour les données plus critiques (commerciales, RH, financières...), envisagez des moyens supplémentaires (chiffrement des transactions, anonymisation...).



### Contrôlez les droits d'accès au cloud

Exigez l'utilisation de mots de passe robustes sur tous les terminaux et ajoutez un deuxième facteur d'authentification sur les plus sensibles. Accordez l'accès aux utilisateurs qui en ont réellement besoin et prohibez les comptes partagés. Accordez une attention particulière aux comptes privilégiés qui accèdent aux services clouds où sont sauvegardées vos données les plus sensibles. Évaluez la réputation des adresses IP qui se connectent à vos SI et conservez la trace des connexions et tentatives.



### Protégez vos applications migrées dans le cloud

Maintenez la disponibilité des sites web et autres applications critiques migrées dans le cloud en les protégeant contre les attaques en dénis de service. Préservez l'intégrité de leur données en les protégeant contre les injections de code malicieux, les vols de données, les défacements, et autres attaques transitant par le web pouvant avoir un fort impact sur votre business (entreprise resource planning indisponible, site web aspiré, infection de site e-commerce...).

Les solutions de pare-feu applicatif et de protection anti-DDOS intégrés aux accès Internet peuvent être déployés en amont de vos applications. De telles solutions sont généralement disponibles chez votre fournisseur de cloud (à un coût supplémentaire) et chez certains fournisseurs spécialisés en cyberdéfense.



### Miser sur la prévention et la détection des menaces en amont

Avec des mécanismes d'intelligence artificielle, les solutions de SIEM (security intelligence and event management) permettent d'analyser les événements de sécurité liés à l'activité des serveurs, des utilisateurs et des terminaux, ainsi que les données en transit, les signaux faibles ou les activités anormales sur les réseaux.

Pour contrôler finement les applications et les données dans le cloud, de nouvelles méthodes et technologies sont récemment apparues (CASB : cloud access security broker, API...).

Conjuguées à un Security Operations Center (SOC) qui apporte l'expertise humaine pour surveiller l'ensemble de votre environnement cloud, toutes ces solutions permettent de détecter et ainsi contenir les menaces avant qu'elles ne provoquent de dégâts.



## Utiliser un cloud privé pour les informations sensibles

L'Agence spatiale européenne (ESA) manipule des données très sensibles et ses exigences en matière de sécurité sont plus strictes que chez la plupart des entreprises. Orange a mis en place un cloud privé et des contrôles des accès différenciés selon les applications et les collaborateurs, ce qui évite l'utilisation abusive des comptes.

« Certains pays exigent des entreprises qu'elles stockent les données personnelles de leurs clients et citoyens sur le territoire national. »

# Gérer les niveaux de service dans le cloud

## L'enjeu

Les entreprises ont souvent besoin de gérer toute une gamme de services informatiques, de manière traditionnelle ou dans le cloud. Elles doivent s'assurer que les garanties sur les niveaux de service (Service Level Agreements – SLA) sont respectées : disponibilité et rétablissement des services, utilisation des systèmes, temps de réponse des applications...

De plus, la gestion du changement est devenue cruciale. Autrefois, les entreprises devaient gérer des réorganisations et des évolutions occasionnelles des systèmes informatiques. Aujourd'hui, à l'époque du renouvellement et de l'amélioration continue des plateformes technologiques, l'agilité des processus SI est devenue essentielle.



## 5 étapes de la gestion des services informatiques dans le cloud

### 1. Déterminez vos indicateurs de performances

Suivez ce que font vos applications. Fonctionnent-elles correctement ? S'approchent-elles d'un niveau de saturation ?

Les statistiques (historiques et en temps réel) sont indispensables pour comprendre la performance des applications dans la durée, les améliorer et prévenir tout incident.

### 2. Gérer vos services

Un expert en service management de cloud aidera vos équipes informatiques au cours des différentes phases opérationnelles :

- Programmation des déploiements, des mises à jour et réplication des données dans le cloud
- Gestion et suivi des versions de systèmes d'exploitation, des applications, des middlewares, des ressources de calcul, de stockage et réseau
- Orchestration des flux et répartition des charges inter-cloud
- Sécurisation des données avec des politiques précises et en programmant des alertes.

### 3. S'adapter à un monde en perpétuelle évolution

Un audit en amont permet de bien programmer les évolutions nécessaires de l'infrastructure informatique. Il réduit les risques d'impacts potentiels sur les activités opérationnelles grâce à la mise en place d'analyses, d'évaluations et de processus spécifiques. Par exemple, le « suivi des changements » répertorie toutes les évolutions réussies et constitue un historique de référence sur les processus répliquables et auditables.

### 4. Améliorer le self-service et l'automatisation

Les outils de self-care que vos fournisseurs cloud proposent doivent vous permettre de commander, provisionner et configurer automatiquement vos services cloud et de suivre les coûts (facturation à la consommation). Cette approche vous permet de résoudre plus rapidement les éventuels problèmes (manque de capacité, stockage insuffisant...). Elle réduit par ailleurs la charge de travail manuel de l'équipe informatique ainsi que les risques d'erreurs humaines.

### 5. Encourager l'interaction

Les services cloud doivent être gérés de bout en bout, et non par silos organisationnels (WAN, LAN, serveurs du cloud, baies de stockage, postes de travail, bases de données...). L'entreprise et ses fournisseurs de services doivent travailler en étroite collaboration.

## Gestion de la capacité lors de fusions et acquisitions

Pour développer sa croissance à l'international, une entreprise a adopté une ambitieuse stratégie d'acquisition. Son équipe informatique devait gérer les enjeux d'un déploiement rapide. Mais elle ne savait ni comment anticiper les ressources IT dont auraient besoin les nouveaux collaborateurs ni comment intégrer de nouvelles applications logicielles.

En collaborant avec Orange, l'entreprise a su anticiper bien en amont la demande de ressources IT et les mettre en place pour faire évoluer son cloud privé, sans interruption des services.



« Créez une infrastructure cloud dotée de la flexibilité nécessaire pour évoluer avec vos nouveaux projets. »



# 56%

des entreprises utilisant le cloud s'appuient, aujourd'hui, sur plusieurs fournisseurs SaaS.<sup>6</sup>

# Maîtriser le coût global du cloud

## L'enjeu

Les entreprises mettent en place des projets cloud pour réduire leurs dépenses d'investissement et de gestion. Et en effet, migrer dans le cloud peut générer des économies, comparé aux systèmes informatiques traditionnels.

Mais pour quantifier précisément ces économies, les entreprises doivent évaluer le projet de bout en bout, de la migration des données à la performance des applications et la sécurité.



# 42%

**des entreprises considèrent que la réduction des coûts d'investissement est clé pour l'adoption du cloud computing, selon le cabinet IDG.<sup>7</sup>**

## 5 leviers pour maximiser le retour sur investissement des projets de cloud computing

### 1. Gestion de projet

Encouragez les phases de test avant d'adopter les solutions qui apportent de véritables avantages opérationnels. Priorisez les fonctionnalités les plus importantes et capitalisez sur les déploiements cloud réussis pour vos nouveaux projets.

Pour vos nouvelles applications, appliquez une stratégie « cloud first ». Et pour un même besoin fonctionnel ou métier, évitez la multiplication des applications : votre gestion en sera simplifiée et vous ferez des économies d'échelle.

### 2. Transferts des données lors des migrations

Un service de transfert d'importantes bases de données via Internet, proposé par votre fournisseur cloud, peut s'avérer coûteux. Souvent, l'utilisation temporaire d'une connexion plus puissante pour migrer permet de réduire le temps de migration et l'indisponibilité des applications, tout en coûtant moins cher.

### 3. Compétences de migration et d'opérations

Travaillez avec des fournisseurs de services expérimentés et certifiés qui vous accompagneront de bout en bout : de la migration des applications à la connectivité pour y accéder et aux dispositifs de sécurité pour les protéger.

Appuyez-vous sur des projets pilotes pour que les équipes de conception et de déploiement montent progressivement en compétence. Vos administrateurs d'infrastructures pourront évoluer vers les métiers de « service manager » ou de « broker de cloud » pour piloter les performances des services de vos différents fournisseurs cloud.

### 4. Coûts récurrents

Les coûts récurrents de développement, traitement, stockage, administration, sécurité, etc. représentent une partie considérable du budget informatique des entreprises. Il convient de varier les solutions en fonction des usages prévus.

Vous pouvez migrer vos environnements de développement et de test dans le cloud lorsque vous n'en avez plus besoin et les désactiver de votre SI traditionnel.

En revanche, les flux de calcul en temps réel nécessitent des ressources plus coûteuses (capacités de traitement et stockage, latence). Les données qui circulent en continu pourront être hébergées sur site.

Si des données sources personnelles doivent être conservées dans un environnement plus sécurisé (et plus coûteux), les données non-critiques ou les données traitées, quant à elles, peuvent parfois être moins rigoureusement protégées, par exemple lorsqu'elles sont anonymisées.

### 5. Usages et métiers

Développez la culture du service en privilégiant la délégation des responsabilités. Instaurez la refacturation interne pour responsabiliser vos différentes directions métiers sur leurs usages IT. Des solutions ou prestataires de service peuvent vous aider à répartir les coûts au plus juste.

« Les projets pilotes permettent un bon apprentissage pour les équipes chargées de la conception et du déploiement des services IT dans le cloud. »

## S'appuyer sur l'expertise de partenaires

Les contrats de services cloud reposent souvent sur une responsabilité partagée entre les fournisseurs de services et le client.

Une entreprise souhaitait gérer elle-même son système d'exploitation, ses applications et son middleware sur une infrastructure fournie par Orange. Mais une application particulière subissait un temps de réponse trop important pour les utilisateurs. A première vue, il aurait pu s'agir d'un problème réseau commun, mais la raison s'est avérée plus complexe.

Les experts Orange ont identifié la cause des ralentissements : la mise à jour de l'antivirus du client se déclenchait en période de pointe d'utilisation du serveur de traitement de données dans le cloud. L'antivirus a été reconfiguré et les collaborateurs ont bénéficié d'une application performante (ouverture et sauvegarde des données rapides et efficaces). Cet audit technique a évité d'investir dans un réseau plus puissant.



# Dès maintenant, migrez vers le cloud

Pour la plupart des entreprises, il n'est plus question de savoir « si » elles doivent aller dans le cloud mais « à quelle vitesse » et « comment ».

Pour rester compétitives, elles peuvent aujourd'hui mettre en place des services multi-cloud, s'affranchir des écueils techniques et trouver le juste équilibre entre besoins opérationnels et coûts.

Orange Business Services propose des services cloud qui prennent en compte les exigences de sécurité et de connectivité, en France et à l'international.

Avec ses entités Orange Cloud for Business et Orange Applications for Business, Orange Business Services peut accompagner et aider les entreprises à migrer leurs applications dans le cloud et y connecter les utilisateurs en permanence.

## La réussite de votre transformation IT dépend de votre adoption du cloud

Accélérez votre transformation digitale grâce à une meilleure maîtrise du cycle de vie, de la performance et de la sécurité des applications IT traditionnelles et cloud ready.

Découvrez comment Orange Cloud for Business peut vous accompagner :

<http://www.orange-business.com/fr/cloud-computing>

## De l'idée à la transformation. Ensemble.

Donnons vie à vos ambitions, avec notre approche centrée sur l'humain, nos partenariats multifournisseurs et nos ressources internationales de déploiement :

<http://www.orange-business.com/fr/transformation-digitale>



**Sources:**

1. <https://www.idgenterprise.com/resource/research/2016-idg-enterprise-cloud-computing-survey>
2. <http://www.idc.com/getdoc.jsp?containerId=prUS42464417>
3. [https://www.scribd.com/document/329518100/IDG-Enterprise-2016-Cloud-Computing-Survey#download&from\\_embed](https://www.scribd.com/document/329518100/IDG-Enterprise-2016-Cloud-Computing-Survey#download&from_embed)
4. <http://www.cbronline.com/news/mobility/security/cloud-performance-issues-costing-firms-600000-a-year-survey/>
5. <http://www.businesswire.com/news/home/20160517005583/en/Report-Reveals-Cloud-Security-Concerns-Rise-Investment>
6. [https://www.slideshare.net/North\\_Bridge/2016-future-of-cloud-computing-study](https://www.slideshare.net/North_Bridge/2016-future-of-cloud-computing-study)
7. [https://www.scribd.com/document/329518100/IDG-Enterprise-2016-Cloud-Computing-Survey#download&from\\_embed](https://www.scribd.com/document/329518100/IDG-Enterprise-2016-Cloud-Computing-Survey#download&from_embed)

**Pour nous contacter :  
info.cloud@orange.com**



**Business  
Services**

