accenture

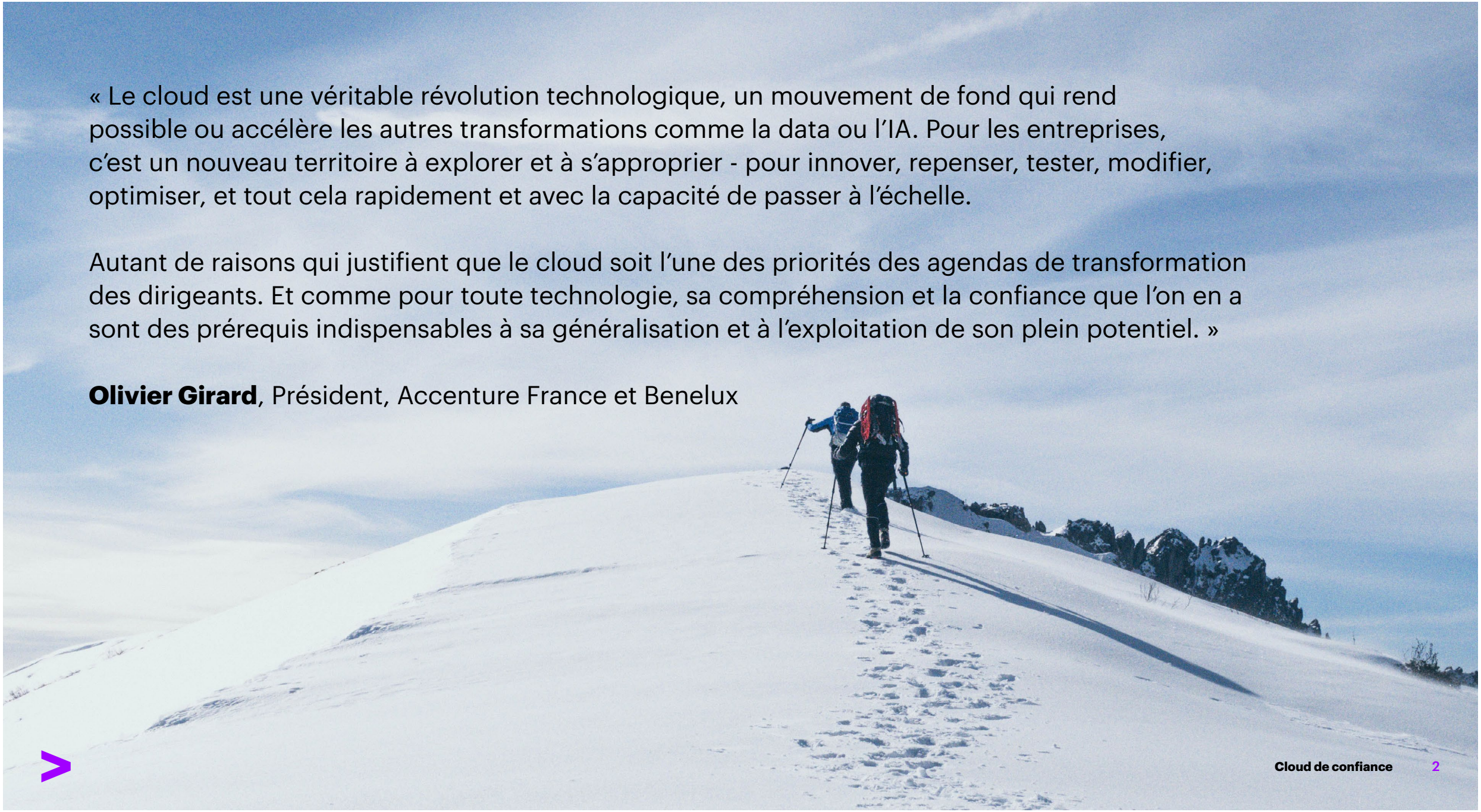
Cloud de confiance

Maîtriser une rupture technologique stratégique

« Le cloud est une véritable révolution technologique, un mouvement de fond qui rend possible ou accélère les autres transformations comme la data ou l'IA. Pour les entreprises, c'est un nouveau territoire à explorer et à s'approprier - pour innover, repenser, tester, modifier, optimiser, et tout cela rapidement et avec la capacité de passer à l'échelle.

Autant de raisons qui justifient que le cloud soit l'une des priorités des agendas de transformation des dirigeants. Et comme pour toute technologie, sa compréhension et la confiance que l'on en a sont des prérequis indispensables à sa généralisation et à l'exploitation de son plein potentiel. »

Olivier Girard, Président, Accenture France et Benelux



Le cloud est une technologie mature qui accélère ici et maintenant la transformation digitale des entreprises et des institutions. Les conditions (collecte et maîtrise des données, connectivité…) qui en limitaient parfois le bénéfice sont aujourd'hui maîtrisées. Le cloud exprime désormais toute sa puissance transformative et simplifie l'accès à un univers applicatif infini, qui resterait hors de portée des moyens individuels de R&D de la majorité des acteurs du marché. C'est une révolution absolument majeure en termes d'usage, de bénéfices et de gouvernance.

Après quelques années d'expérimentation, les entreprises françaises et organismes de l'Etat accélèrent leur adoption à l'échelle du cloud. **Il est attendu que 70%[1] de la capacité informatique de calcul ait basculé sur le cloud d'ici 2024**. Cette tendance structurelle a été encore amplifiée par la crise de la Covid-19 qui a contribué à démontrer la puissance du cloud pour assurer la continuité du fonctionnement des entreprises et l'absorption des pics de volumes engendrés par l'explosion de l'activité digitale dans le e-commerce ou les services bancaires. Mais **le recours aux cloud publics pose aussi de nouvelles questions : sécurité et confidentialité des données qui y sont injectées, éventuelle dépendance technologique envers les fournisseurs de cloud…**

[1] Source : Accenture Cloud Ascent and Future Systems for the World Economic Forum

L’acceleration de l’adoption du cloud suppose une confiance forte entre les acteurs

Avec ce transfert massif des systèmes d’information dans le cloud, les entreprises prennent aujourd’hui la mesure du gain de performance qu’il procure, mais aussi des nouveaux risques opérationnels qui l’accompagnent. Dans ce contexte nécessairement évolutif du point de vue technologique comme réglementaire, un besoin nouveau émerge sur le marché : les entreprises entendent en effet **profiter « en confiance » des bénéfices du cloud**, c’est-à-dire en maîtrisant les risques, posés notamment en termes de souveraineté et mis en lumière par la dépendance technologique aux fournisseurs de cloud américain ou chinois. C’est la raison pour laquelle se dessine une tendance forte autour d’**un cloud hybride qui articule briques de confiance pour les applications sensibles et puissance du cloud public, au service de la transformation digitale des organisations et des modèles**.

Cette problématique du cloud de confiance est aujourd’hui centrale, car elle est la condition décisive de l’accélération de l’adoption du cloud.

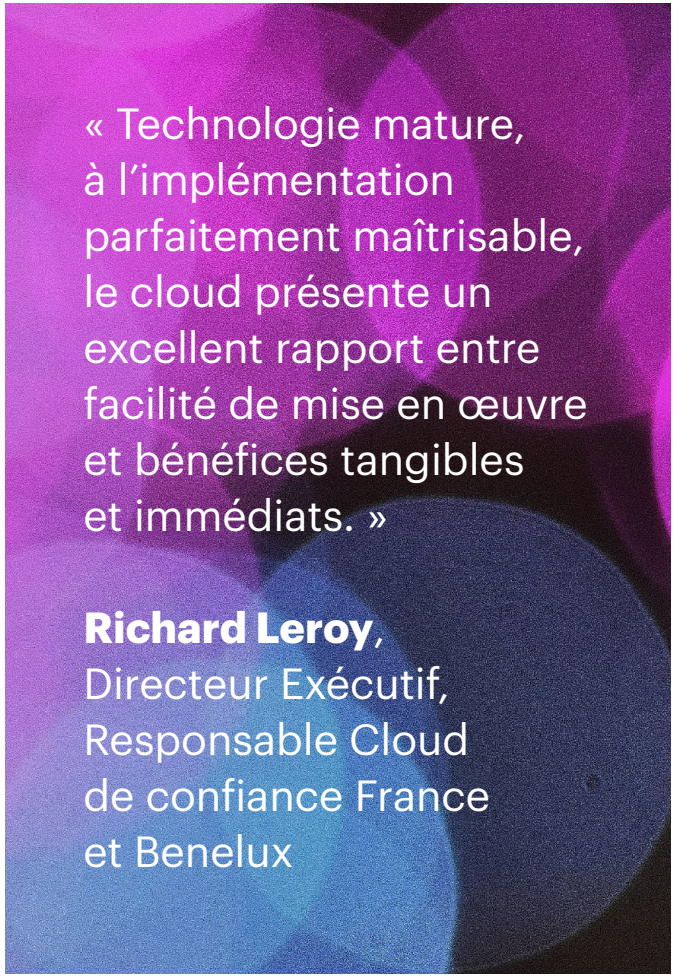
Ce que nous entendons montrer ici, c’est qu’**une démarche de cloud hybride permet d’apporter une réponse aux problèmes et aux risques potentiels, tout en exprimant le potentiel immense du cloud** pour les entreprises et les institutions, toute sa puissance transformative en termes d’innovation, de performance, de résilience et d’agilité.

Le chemin vers une transformation digitale réussie et maîtrisée

Inégalement engagé, le passage au cloud est cependant largement installé. Ce sont 40% des entreprises qui accélèrent drastiquement leur trajectoire cloud, tandis que Gartner prévoit que le marché du cloud représentera 16 milliards de dollars en France, en Belgique et au Luxembourg et 650 milliards de dollars dans le monde d'ici 2024[2] ; mouvement amplifié encore par la pression sur les coûts liés à la crise de la Covid-19[3]. Derrière les chiffres, deux tendances lourdes. La première est l'**usage bien plus large du cloud public**, jusqu'ici limité à des environnements hors production et à l'innovation sous forme de proof of concept. La seconde, intervenant en parallèle ou en séquence, est un virage vers l'**utilisation de technologies cloud de type PaaS**, notamment pour permettre les nouveaux développements et la modernisation des patrimoines applicatifs.

Le cloud représentera 45% des dépenses IT d'ici 2024[4]

Aujourd'hui, de nouvelles trajectoires en rupture font d'ores et déjà leur apparition, par exemple des transitions massives vers le cloud public poursuivant des objectifs d'**innovation**, de **transformation applicative** et d'**économies** sur fond de comblement de **dette technique** et d'**élasticité**. Ce constat se manifeste dans la plupart des secteurs d'activités avec quelques exemples iconiques de sources publiques (Deutsche Bank, Intesa San Paolo…). Et depuis le début de l'année 2020, les entreprises ont entrepris un mouvement structurant d'innovation dans et par le cloud public. C'est une prise de conscience nouvelle, qui change tout.



[2] Source : Gartner - Forecast: Public Cloud Services, Worldwide, 2018-2024, 1Q20 Update – May 2020
[3] Source : Insee variation du PIB 2020 -90%
[4] Source : Gartner Market Trends : Cloud Shift - 2020Through 2024

Enjeux stratégiques et risques systémiques pour les entreprises

Dans ce contexte, **le cloud de confiance a pour objectif de répondre aux problématiques de souveraineté induites par la croissance exponentielle de l'usage du cloud public**. Trois axes majeurs se dessinent en ce début d'année 2021 : **la sécurité de la donnée sous toutes ses formes**, la **conformité aux réglementations** européennes en général et françaises en particulier, la **protection face à la dépendance technologique** notamment vis-à-vis des fournisseurs de services de cloud public, GAFA ou BATX en position oligopolistique.

> **Le cloud n'est pas un risque en soi pour l'entreprise, mais une reponse plurielle et modulaire à des enjeux plus ou moins critiques.**

L'utilisation des services de fournisseurs de cloud public qu'ils soient français ou étrangers pose en premier lieu des questions simples de **sécurité** (malware, fuite ou corruption de données...) et de **disponibilité**. Ne plus avoir la technologie « sous la main » dans les propres data centers de l'entreprise induit souvent une méfiance vis-à-vis des fournisseurs de cloud public, même si les mécanismes de sécurité et la disponibilité effective des systèmes cloud sont en général bien supérieurs à ce que proposent les systèmes en propre des entreprises. C'est essentiel : le cloud embarque nativement un niveau sécurité qui est le standard nécessaire de l'« économie de la confiance», c'est-à-dire de l'économie digitale, de l'économie de plateforme.

Les fournisseurs de cloud public implantés en Europe étant principalement américains (AWS, Microsoft, Google), l'utilisation de leurs services présente aussi des risques plus complexes, liés aux problématiques de souveraineté. Les entreprises fortement présentes en Asie auront à traiter des problématiques équivalentes sur les cloud chinois (Tencent, Alibaba). Ces risques sont :

01

Divulgation d'information :

une entreprise américaine ou exerçant une activité économique sur le territoire américain peut être amenée à divulguer des informations, sur demande de la justice américaine (application du Cloud Act dans le cadre d'une suspicion de crime ou de terrorisme) quel que soit le lieu de stockage et de traitement de ces informations. Un citoyen français client d'une banque française logeant les données de compte de ses clients chez un fournisseur de cloud américain pourrait voir ses informations transmises sans accord préalable de la justice française. Ce risque même s'il est hypothétique met les fournisseurs de cloud public américains en non-conformité au RGPD.

02

Espionnage :

accès par des agences d'intelligence aux informations stockées dans le cloud – données sensibles dans le domaine du nucléaire, technologies confidentielles dans le secteur aéronautique, etc.

03

Limitation de l'accès aux nouveaux services :

décision unilatérale de la part des États-Unis de limiter l'accès aux services les plus innovants, de limiter le niveau de service lors de tension sur les ressources comme constaté pendant la crise de la Covid-19, voire de couper l'accès lors de tensions entre États.

04

Réputation :

certaines entreprises françaises sont très soucieuses de ne pas avoir à justifier auprès de leurs clients le fait que leurs données soient hébergées sur des cloud étrangers, si un « Cloud-gate » venait à éclater dans les médias en France. D'autres s'inquiètent de ce que l'Etat français pourrait leur demander en termes d'implication dans un cloud souverain français.

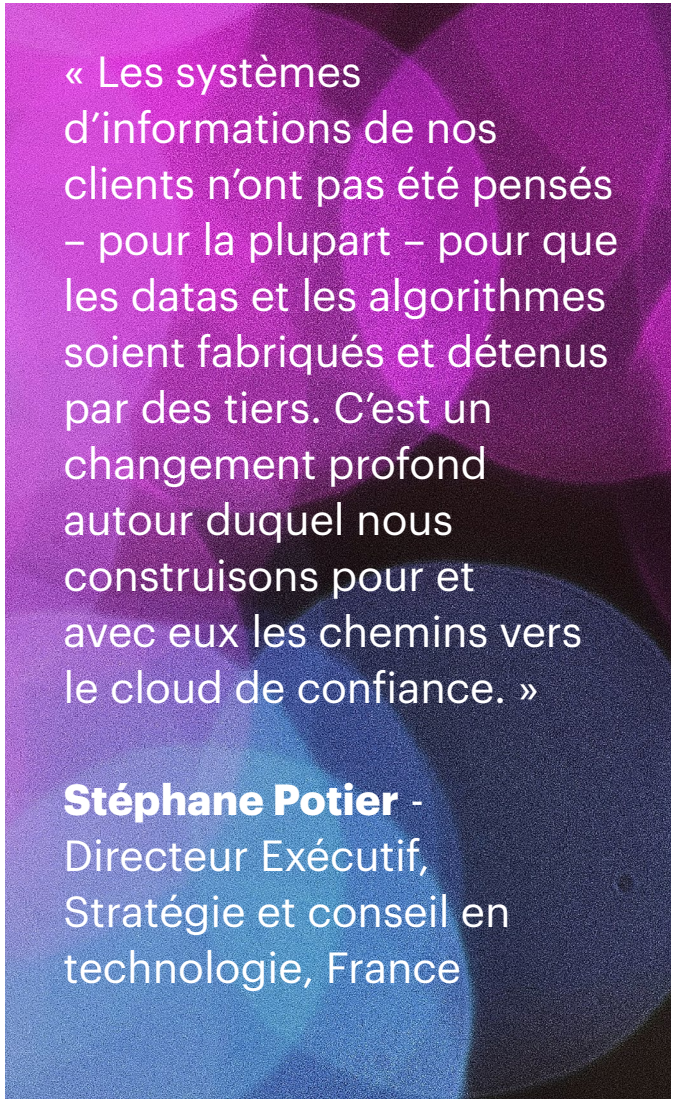
Un équilibre à définir et à construire

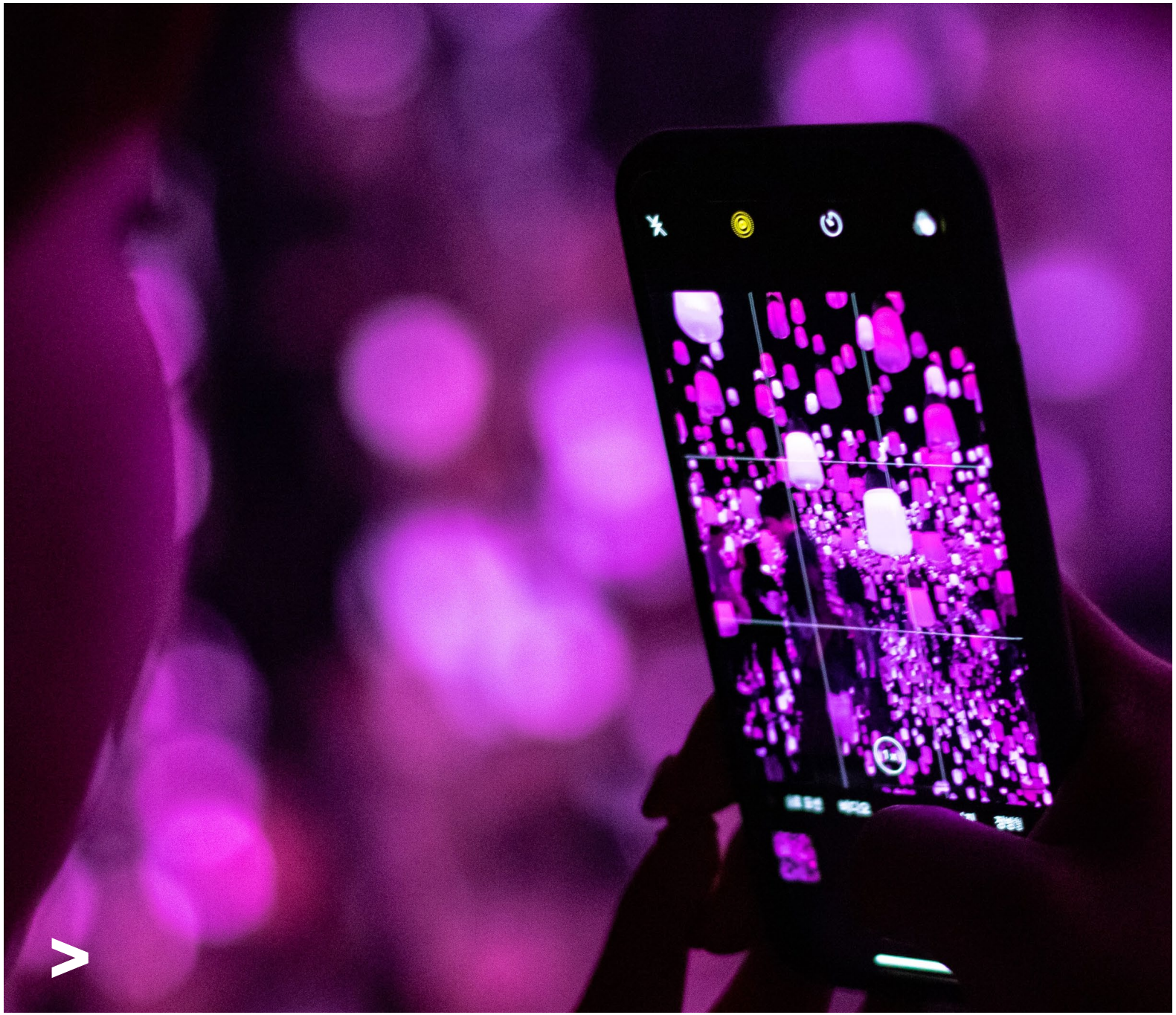
Face à ces risques et à la demande des entreprises de solutions de mitigation, l'offre de cloud de confiance se structure. Il faut tout d'abord noter que l'émergence d'un cloud strictement français (stockage des données, conformité, opérateurs et technologies de traitement des données rigoureusement français et à performances équivalentes aux actuels acteurs) est pour le moment peu probable. Et l'utilisation sans limite des prestations de fournisseurs de services de cloud public américains ou chinois l'est tout autant.

Dans le même temps, il faut bien comprendre que la dynamique de transfert des SI vers le cloud est un mouvement déjà engagé de manière très nette et qui va encore s'accélérer. La confiance est la condition de cette adoption, elle n'est pas un frein.

> **L'enjeu des entreprises est donc de déterminer la zone de juste équilibre entre la préséance d'une logique sécuritaire qui freinerait l'innovation et une logique d'ouverture sans contrôle qui exposerait trop au risque.**

La réponse cloud de confiance n'est pas uniforme et va dépendre de deux grands facteurs. Tout d'abord de **la sensibilité aux risques** : les choix faits par les ministères, de la défense par exemple, seront différents de ceux de la santé, de l'énergie, des banques ou de la grande distribution. De ce point de vue, l'appartenance au secteur public ou privé appelle des stratégies très différentes. En second lieu, de l**a nature des capacités cloud sollicitées** : les usages Métier vont appeler la consommation de formes de cloud diverses, simples (IaaS), plus complexes (PaaS) voire avancées (modules de machine learning) en passant par des solutions intégrées (SaaS) qui sont autant de leviers de souveraineté numérique et de confiance potentiels.





Cela étant posé, et en tenant compte des risques et de la demande des entreprises en termes de solutions de mitigation, l'offre de cloud de confiance émerge en ce début d'année 2021 autour de trois axes :

#1 **Technologique :**
chiffrement des données, détention des algorithmes et clés de chiffrement

#2 **Opérationnel :**
territorialité des centres de données (en France) et nationalité des opérateurs et de leur personnel

#3 **Juridique :**
obligation de transparence des accès aux données, respect des réglementations applicables à l'entreprise cliente

Conditions et contraintes du cloud de confiance

De façon générale, l'adoption de solutions de confiance s'accompagnent aussi dans l'immédiat de conditions et de contraintes qui doivent être considérées au regard de leurs bénéfices stratégiques, et notamment :

Surcoûts pouvant aller de 10% à 30% pour des solutions aux normes les plus restrictives, en comparaison des normes du cloud public.

Accès dégradé aux services avancés et aux nouvelles innovations. Néanmoins les grands fournisseurs de cloud investissent pour minimiser cet écart. A date, le terrain de jeu du cloud de confiance s'étend des services IaaS au CaaS/PaaS et à l'orchestration qui s'y rattache, à condition toutefois d'utiliser des solutions « privatisées » provenant des fournisseurs de cloud américains (Outposts, Anthos, Azure Stack ou Openshift).

Élasticité limitée de la puissance disponible, scalabilité moins rapide.

De façon plus spécifique (à un Etat, à une industrie par exemple), d'autres éléments doivent être pris en compte.

Un **cadre juridique** commercial et national protège contre des actions permettant l'accès aux données, la limitation à l'accès au service opérationnel ou la limitation à l'accès aux nouvelles technologies. Des clauses contractuelles (Standard Contractual Clause pour le RGPD) permettent d'encadrer la gestion des données clients par le fournisseur cloud et établit les responsabilités des « data processor » et « data controler ».

En règle générale, **pour un cloud de confiance, l'accès aux données de l'entreprise par des personnels du fournisseur de services est strictement limité aux besoins impérieux d'administration technique**. Le fournisseur de cloud s'engage à fournir régulièrement la liste des personnels qui ont eu accès aux données client. Par ailleurs, les clients sont en mesure à tout moment de récupérer leurs données et leurs applications.

Plusieurs **freins réglementaires** différent en fonction du type de données. En Europe, le RGPD est le plus connu et encadre la protection des données personnelles, chaque pays a maintenant des restrictions additionnelles. A noter que le **RGPD** et le Cloud Act américain ne sont pas en harmonie, accentué encore par la dénonciation du Privacy Shield (décision dite « Schrems II » par la cour de Justice de l'UE, le 16 juillet 2020).

Des exigences spécifiques de cyberdéfense s'appliquent aux Opérateurs d'Importance Vitale (OIV) suite à la promulgation de la Loi de Programmation Militaire[5] qui charge l'Agence nationale de la sécurité des systèmes d'information (ANSSI) d'accompagner les OIV dans la mise en place des mesures organisationnelles et techniques adéquates. A noter que l'ANSSI réalise des préconisations non contraignantes par exemple de respect des règles SecNumCloud et que des nuances apparaissent souvent entre la législation, les règles de normalisation et la réalité de mise en œuvre.

Dans le milieu bancaire en particulier, l'European Banking Authority encadre les risques liés à l'externalisation (et le cloud), avec la notion de service critique et important. Plusieurs réglementations encadrent le secret bancaire, en France mais surtout au Luxembourg et en Suisse.

[5] Source : Gouvernement loi n°2018-607 relative à la programmation militaire

Perspectives de court et moyen termes

A court et moyen termes et de manière concrète, l'offre de cloud de confiance va se structurer autour de 3 grands pôles :

#1 **Des offres de cloud américaines**, renforcées sur le chiffrement et assorties de garanties juridiques spécifiques

#2 **Des offres partenariales entre cloud américains et sociétés françaises**, appuyées par les pouvoirs publics qui permettront un niveau plus élevé de mitigation des risques

#3 **Des offres spécifiques, sans doute par secteur (santé, défense, bancaire…) fournissant le maximum de mitigation des risques** et barycentrées sur des cloud d'acteurs nationaux

La verticalisation des problématiques par type d'industrie

La probabilité est forte que la réponse apportée à la problématique du cloud de confiance ne soit pas unique mais dépende de l'industrie concernée et, au sein de chaque industrie, appelle des stratégies différenciées, acteur par acteur. En effet, la réponse à la problématique est encadrée par les contraintes réglementaires de l'industrie, mais aussi par la posture du secteur et des acteurs face au couple risque / bénéfices du cloud, incluant les contraintes structurantes du cloud de confiance ainsi que par l'existence d'une réponse sectorielle qui pourrait se dessiner.

> **Il n'existe pas une stratégie cloud pour l'ensemble des entreprises. La clé est de centrer la démarche sur le business, la valeur, pas sur la technologie.**

Une première cartographie des spécificités par industries distingue début 2021 :

01

Les industries de la défense

pour lesquels le cloud revêt une réalité « produit » (le cloud opérationnel du théâtre d'opérations ou des systèmes d'intelligence) et de « gestion » (le cloud de gestion faisant fonctionner les ERP, les PLM, les CRM sur lesquels des informations confidentielles ou sensibles peuvent transiter). Les services publics régaliens tels que la justice, la police, la défense, et plus généralement les activités civiles permettant la continuité d'activité de l'Etat s'inscrivent dans la même perspective.

02

Les Opérateurs d'Importance Vitale (OIV)

dont il n'y a pas de liste officielle, désignent les acteurs de certains secteurs stratégiques (eau, santé, énergie, finance, transports, communication, industrie, recherche, aérospatiale). Certains d'entre eux sont proches des pouvoirs publics et joueront certainement un rôle important dans l'émergence de cloud souverains, en raison du volume d'affaires et d'opérations qu'ils représentent. Le projet Gaia-X cristallise une partie de ces attentes et de ces réflexions autour de l'émergence d'un acteur cloud européen capable de rivaliser avec les champions américains et chinois du secteur. En France, le projet Gaia-X est porté par le CIGREF. Le 29 mars dernier, GAIA-X a annoncé ses 212 premiers membres, ainsi qu'une série de règles qui s'applique pour tous, y compris les GAFAM et un fournisseur chinois qui a été accepté comme membre. Pour aller plus loin, un label GAIA-X devrait être défini dans les prochaines semaines, celui-ci s'appliquera à la maille d'un service ou d'une prestation et non de l'entreprise qui la délivre.

03

Les acteurs de la santé

qui au-delà de faire partie des OIV présentent des problématiques spécifiques liées aux données médicales

04

Les secteurs banques-assurances

qui sont soumis à une réglementation spécifique

05

Les acteurs des filières d'excellence

qui doivent protéger leur propriété intellectuelle et leur recherche

Comment aborder la problématique du cloud de confiance pour une entreprise ?

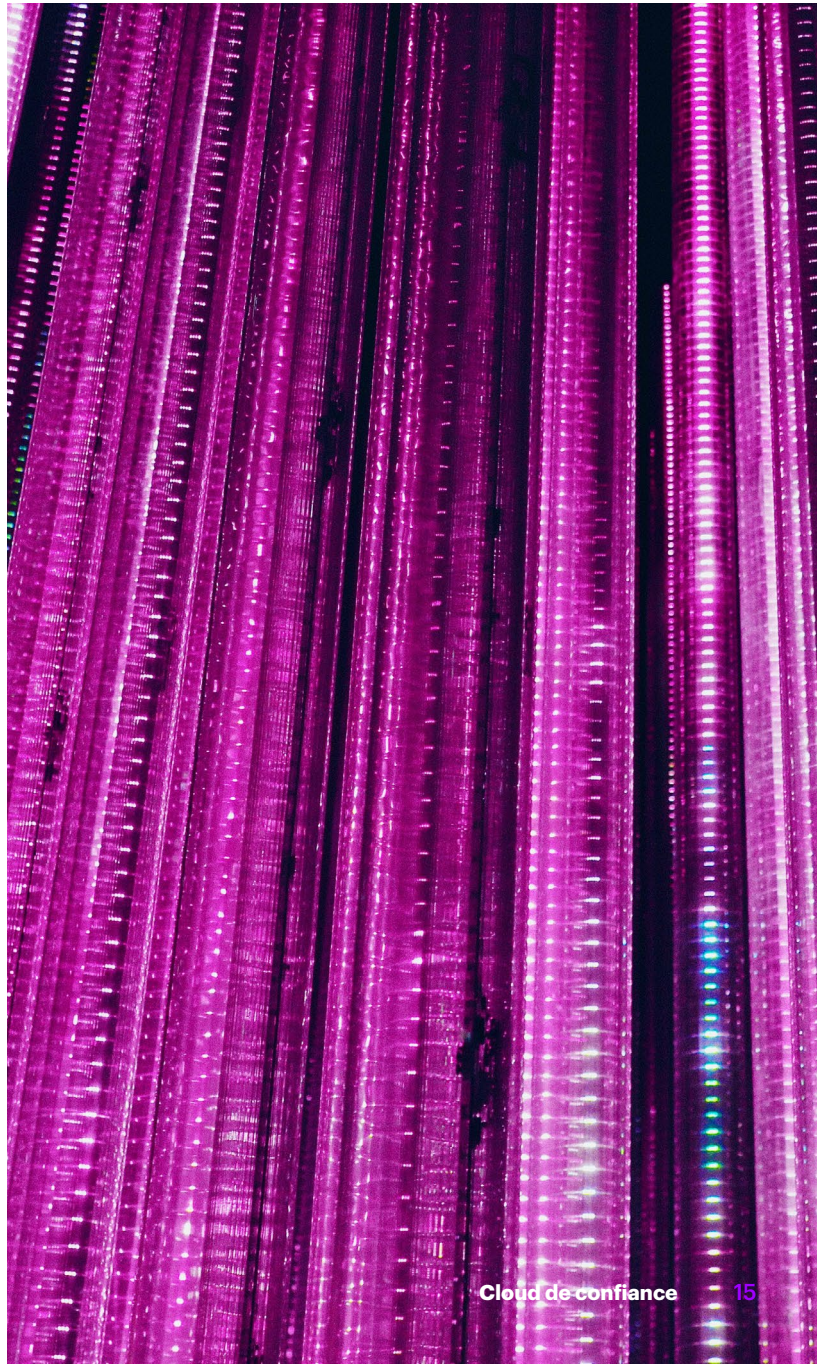
Définir la stratégie cloud de confiance :

Réaliser une phase d'exploration des risques, de définition d'une doctrine mettant en balance ces risques avec les contraintes structurantes du cloud souverain, puis décliner cette doctrine au sein de l'entreprise par division et patrimoine de données et d'application.

Certains pans d'activité nécessiteront des solutions très sécurisés, d'autres plus proches des standards de marché. La conformité réglementaire joue un rôle déterminant dans ces classifications et les secteurs avancés montrent l'importance d'une discussion proactive avec les organismes réglementaires.

Activer la transformation vers le cloud de confiance :

Ajuster l'approche classique de transformation vers le cloud notamment en termes de cadre de sécurité, de catalogue de services spécifiques de cloud de confiance (ex. provisionner un serveur en configuration standard ou de confiance), d'outillage d'aide à la décision de placement vers un cloud public standard ou de confiance, de formation des personnels au cloud de confiance, de suivi automatisé et fréquent de la conformité au cadre du cloud de confiance défini par l'entreprise.



Un contexte en pleines (r)évolutions

Le terrain technologique, concurrentiel et réglementaire qui structure la réflexion autour du cloud de confiance évolue très rapidement et très régulièrement. Des changements sont notamment attendus pour 2021 dans un contexte en permanente redéfinition qui doit amener les entreprises à s'approprier la problématique en profondeur, pour définir sa posture propre et de pouvoir décoder de manière agile tous ces changements.

Face à ce besoin, Accenture a bâti une offre de « Sovereign Cloud Navigator »

Sovereign Cloud Navigator bénéficie tout d'abord de la position de neutralité d'Accenture par rapport aux cloud providers mais aussi de la profondeur technologique d'Accenture et de l'accès à de nombreux cas clients. Après la sélection des partenaires, le « Journey To Sovereign Cloud » est pour l'essentiel analogue à son équivalent classique, mais avec quelques particularités en matière de sécurité, gouvernance, compétences et suivis opérationnels.

Cette offre dérivée s'appuie sur un écosystème d'Alliances avec les fournisseurs de cloud et de solution de sécurité qui positionne Accenture comme leader sur le marché du cloud de confiance.

NAVIGATEUR

Evaluation des risques de souveraineté en fonction des besoins et du contexte, en particulier :

- Identification de **la segmentation** et de l**a classification des données** et des **applicatifs**
- Identification et qualification des **scénarios de risques** (en fonction des menaces, vulnérabilités et de la probabilité du risque)
- Synthèse du **cadre stratégique**
- **Principales exigences** et **mesures** à mettre en œuvre (conformité, sécurité opérationnelle & applicative, gouvernance, etc.)

Stratégie cloud de confiance et Blueprint opérationnel.

JOURNEY TO CLOUD

Accompagnement à la mise en œuvre de la stratégie de cloud de confiance:

- Conception et implémentation **des cadres et des outils**
- **Accompagnement au choix des acteurs du cloud de confiance** (hyperscalers, opérateurs locaux, tiers de confiance)
- Conception et implémentation **des plateformes** clou de confiance
- Sécurisation **des applicatifs et des données**
- **Acculturation** au cloud de confiance
- Mise en place du **modèle opérationnel**

Construction du cloud de confiance.

Accenture et le cloud de confiance

Accenture intervient auprès de grandes entreprises de tous les secteurs d'activités pour les accompagner dans leur stratégie cloud de confiance et dans les choix à réaliser en termes de souveraineté (cloud public, cloud de confiance et cloud privé) en fonction de la nature des services cloud ciblés et de l'aversion au risque des entreprises. Nous avons notamment mis au point une approche de la criticité et des risques afin de déterminer la meilleure stratégie à adopter.

Nous aidons nos clients à mettre en place les fondations opérationnelles et technologiques, notamment les fonctions régaliennes qui permettent une utilisation maîtrisée du cloud public et sommes au cœur de projets de transition vers le cloud de confiance au travers notamment de la structuration de Centres d'Excellence Cloud.

Accenture Cloud 1st

Accenture possède en son sein une entité (Cloud First) dédiée au cloud computing, composée de 70,000 collaborateurs experts. L'investissement initial de 3 milliards de dollars annoncé par Julie Sweet CEO du groupe au dernier trimestre 2020, donne un élan aux innovations et engagements au niveau de l'ensemble de l'écosystème clients et partenaires d'Accenture. Nous nous appuyons sur la puissance du change management dans notre modèle opérationnel alliant l'ensemble de nos spécialités depuis Stratégie et consulting jusqu'aux services managés pour créer une valeur nouvelle en plaçant le cloud au cœur de l'activité de nos clients. Nous donnons ainsi la priorité aux besoins de l'entreprise au travers des spécificité de l'industrie, en utilisant notre expérience unique et notre envergure mondiale. Dans le but toujours d'une transformation pertinente et réussie de l'organisation et des modèles de nos clients.

Les leviers de différentiation Accenture

Accenture est positionné comme leader sur le cloud par IDC[6]et Gartner[7] de par sa capacité à construire et à mettre en œuvre les stratégies cloud, notamment :

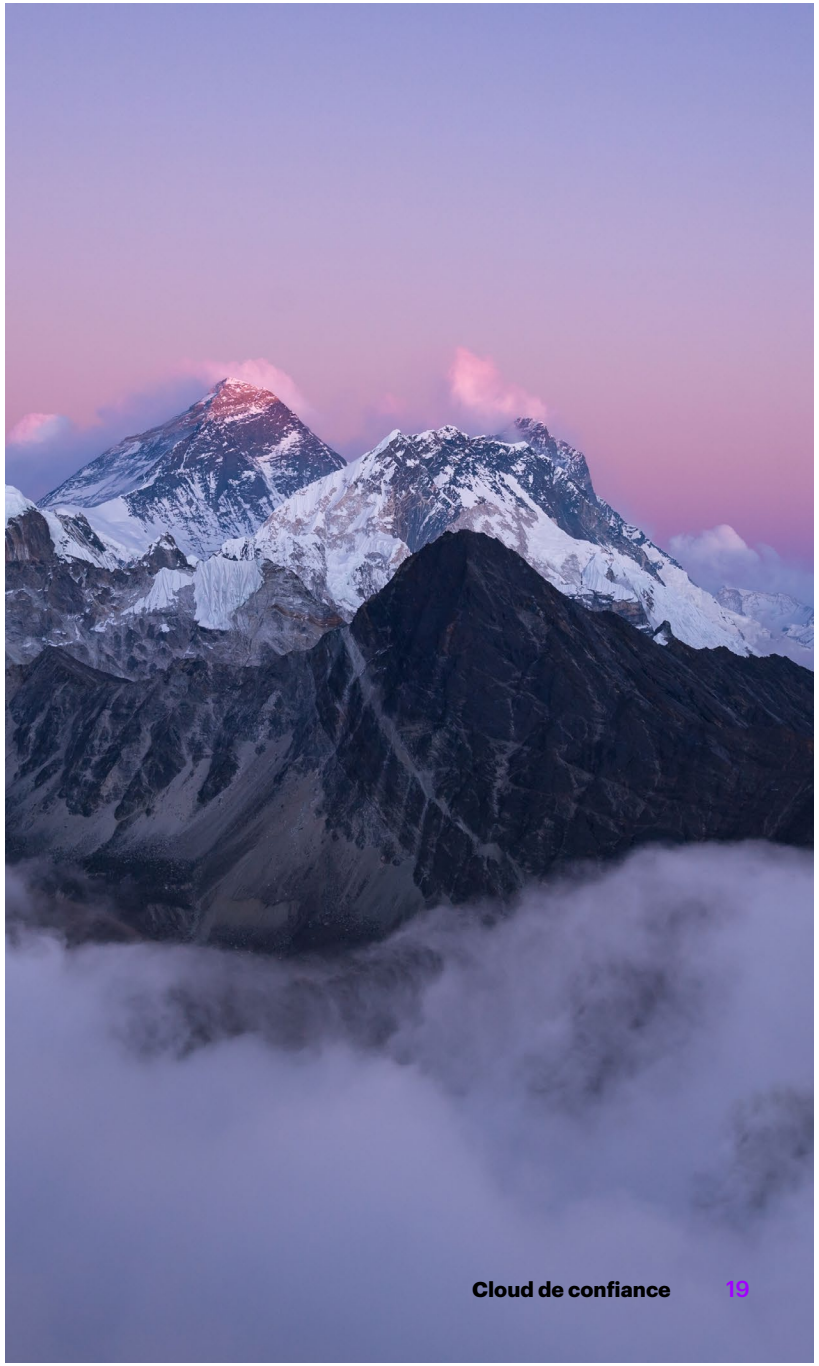
- **Identifier les priorités** et les typologies de transformation cloud,
- **Assister les choix** des différents fournisseurs en fonction des cas d'usage,
- **Identifier les exigences** liées à la conformité et les remédiations associées,
- **Apporter des éclairages** et de perspectives Marché,
- **Réaliser et construire les plateformes** de cloud hybrides,
- **Assister la migration** des patrimoines applicatifs en empruntant les chemins de transformations qui maximisent la valeur.

Accenture a établi des partenariats avec l'écosystème cloud (fournisseurs cloud opérateurs locaux, acteurs de niche, etc.) mais aussi avec les éditeurs tiers connectés aux environnements cloud (solutions Data, réseau, DevOps, ...) et ce dans l'objectif d'apporter des solutions qui répondent de bout en bout aux problématiques des entreprises.

Accenture a augmenté ses savoir-faire et ses capacités de réalisation grâce à des acquisitions et rapprochements stratégiques avec des acteurs spécialisés par « hyperscaler » (Avanade pour Microsoft, Cirruseo pour Google Cloud Platform et Gekko pour Amazon Web Services) et des acteurs spécialisés (Sentelis pour la Data, Opusline pour la santé).

> **Nous sommes engagés auprès de nos clients pour leur fournir un accompagnement neutre et agnostique fondé sur des méthodologies éprouvées et des accélérateurs innovants (Accenture MyNav for Cloud, Incountry).**

[6] Source : IDC MarketScape: Worldwide Cloud Professional Services 2020 Vendor Assessment
[7] Source : Gartner's 2020 Magic Quadrant for Public Cloud Infrastructure Professional and Managed Services, Worldwide



Contacts

Richard Leroy
Directeur Exécutif
Responsable Cloud de confiance, France et Benelux

Stéphane Potier
Directeur Exécutif
Stratégie et conseil en technologie, France

Marc Bousquet
Directeur Exécutif
Cloud First, France et Benelux

À propos d' Accenture :

Accenture est un des leaders mondiaux des services aux entreprises et administrations, avec une expertise de pointe dans les domaines du numérique, du cloud et de la sécurité. Combinant une expérience unique et une expertise spécialisée dans plus de 40 secteurs d'activité, Accenture s'appuie sur le plus grand réseau international de centres de technologie avancée et d'opérations intelligentes pour offrir à ses clients des services Strategy & Consulting, Interactive, Technology et Operations. Avec 537 000 employés, Accenture s'engage chaque jour auprès de ses clients dans plus de 120 pays, à réaliser la promesse de la technologie alliée à l'ingéniosité humaine. Accenture s'appuie sur le changement pour générer de la valeur et créer une réussite partagée avec ses clients, ses collaborateurs, ses actionnaires, ses partenaires et ses communautés. Site Internet : **www.accenture.com/fr**