Gagner et conserver la confiance de vos clients tout en stimulant la croissance, dans le respect des enjeux de souveraineté numérique

Juin 2023

Auteurs :
Sudhir Rajagopal
Research Director, Future of Customer Experience
Grace Trinidad
Research Director, Future of Trust
Cyrille Chausson
Senior Research & Consulting Analyst, Custom Solutions

Un InfoBrief IDC, sponsorisé par

Business

Créez une entreprise résiliente et performante en vous adossant à un socle qui garantit durablement la confiance des clients

Les entreprises doivent redoubler d'efforts pour capter chaque euro dépensé par leurs clients. Utiliser les données pour encourager la fidélité des clients, mais sans négliger leur protection, est devenue le principal facteur de différenciation sur le marché.

L'échange de valeur repose sur les données qui constituent la clé pour gagner et conserver la confiance des clients.

Les entreprises sont confrontées à une mosaïque de règlementations créées par les gouvernements du monde entier.

Les entreprises peuvent bâtir un socle de confiance depuis l'infrastructure jusqu'à l'engagement client. Travailler en collaboration avec un partenaire de confiance peut aider les entreprises à industrialiser les gains tirés de la confiance des clients et à les passer à l'échelle.

La France est à l'avant-garde des mesures en matière de souveraineté numérique, de résilience et de confiance en Europe. Les opérateurs de services locaux sont essentiels pour répondre aux besoins des entreprises françaises.

Investir dans un socle de confiance porte ses fruits : une étude menée par IDC montre qu'investir dans la sécurité, la confidentialité, la conformité et la gouvernance environnementale et sociale (ESG) se traduit par de meilleurs résultats et un meilleur retour sur investissement.

En tant que guides sur leur marché, les partenaires de confiance se démarquent de leurs concurrents par leur capacité à offrir une expérience de mise en œuvre améliorée et grâce à leurs solutions riches en matière de sécurité, de conformité et d'ESG.

Les entreprises doivent redoubler d'efforts pour conserver leurs clients. La façon dont elles utilisent et protègent les données pour s'assurer de leur fidélité est le principal facteur de différenciation sur le marché.

Une incertitude économique grandissante dans toutes les industries

1

En France, les stratégies commerciales sont principalement affectées par les risques liés à l'inflation, à la fluctuation du taux de change et au manque de matériel informatique. Il en résulte une diminution du pouvoir d'achat des consommateurs et une intensification de la concurrence. Les principales préoccupations des chefs d'entreprise français qui auront des conséquences sur leur stratégie technologique sont[1] :

43 %

Inflation tarifaire impactant les budgets

22 %

Fluctuation monétaire impactant le pouvoir d'achat local

20 %

Impossibilité d'accéder au matériel informatique (par ex. : PC, périphériques, infrastructure de datacenter) en raison de tensions de la chaîne d'approvisionnement

L'échange de valeur entre les clients et les entreprises sera ancré dans les données

2

- Les entreprises « Digital-first » considèrent que les indicateurs provenant des données clients et opérationnelles sont le principal moteur pour générer davantage de valeur commerciale. Ces indicateurs permettent de fidéliser les clients grâce à l'excellence du service et de vendre (cross-sell ; up-sell) une gamme plus large de produits et de services.
- Selon les prévisions d'IDC Global Datasphere, le volume de données dans le monde devrait doubler d'ici 2026 (actuellement plus de 100 000 exaoctets). Les données sont essentielles pour anticiper les besoins et les problèmes des clients et pour devenir plus résilient dans un marché confronté à des perturbations.

Les clients font confiance aux entreprises qui comprennent leurs besoins et qui protègent leur vie privée

3

83 %[2] des clients déclarent que la façon dont les entreprises traitent et protègent leurs données influence leur niveau de confiance.

L'atténuation des risques qui menacent la confiance numérique est le premier défi des entreprises. Il est essentiel de trouver le juste équilibre entre l'utilité des données (s'assurer que les données sont accessibles, complètes et contextualisées) et la confidentialité des données (y compris la protection des flux de données entre le cloud hybride, edge et l'infrastructure sur site).

- Alors que l'application du RGPD et des lois et réglementations régionales et sectorielles est de plus en plus forte, la souveraineté numérique est essentielle pour les entreprises et devient la pièce maîtresse des travaux en matière de confiance.
- La confidentialité est l'un des piliers de la confiance, et un niveau de confiance élevé est nécessaire pour que les clients acceptent de partager leurs données personnelles. Ces dernières sont indispensables pour générer, à partir d'IA/ML, des indicateurs pertinents et de haute qualité.
- Limiter la collecte de données au strict nécessaire permet de réduire le besoin en stockage. Cela a un impact positif sur l'environnement et offre des avantages en matière de coûts.

L'augmentation des menaces a des conséquences directes sur les résultats : les violations et les compromissions de données dégradent la confiance

4

- L'enquête *CEO Sentiment Survey* réalisée par IDC montre que 30 % des PDG considèrent que les nouveaux risques liés au partage de données et à la conformité auront des conséquences les plus lourdes sur leur activité d'ici 2024. Des études externes estiment que le coût moyen d'une violation de données pourrait atteindre 4 millions de dollars d'ici 2024.
- Investir dans des programmes de confiance (associés à la sécurité, la confidentialité, la conformité et les technologies ESG) permet d'améliorer les résultats clés de l'entreprise.

[1]2023 IDC Future Enterprise Resilience and Spending Survey, Wave 1
[2]IDC 2022 B2B Technology Buyer Survey

L'échange de valeur repose sur les données qui constituent la clé pour gagner et conserver la confiance des clients

La confiance des clients est essentielle pour pérenniser la résilience et la croissance de l'entreprise

La confiance est le résultat d'un cycle vertueux d'excellentes expériences client rencontrées avec une marque. Les marques de confiance sont davantage achetées, utilisées et recommandées. Elles finissent par avoir plus de clients fidèles et sont plus rentables. Une étude menée par IDC montre que les actions des entreprises en matière de sécurité, de confidentialité (la façon dont les données clients sont utilisées et protégées) et les travaux en matière de gouvernance environnementale et sociale ont des conséquences importantes sur la confiance des clients.

Susciter la confiance des clients :

Trouver le bon équilibre : données et confidentialité

79 % des clients souhaitent que les entreprises interagissent avec eux de façon contextualisée, grâce aux données.

Mais 59 % des clients ont des inquiétudes quant à la confidentialité de leurs informations.

Assurer l'intégrité des données pour les clients

En matière d'engagement client et de décision d'achat, la confiance accordée à une entreprise quant à son utilisation des données client est **aussi importante que** les caractéristiques ou les performances du produit.

83 % des clients déclarent que la façon dont les entreprises protègent leurs données a des conséquences sur la confiance qu'ils leur accordent.

Se préparer aux réglementations plus strictes en matière de confidentialité et de sécurité

Plus de la moitié (55 %) des entreprises déclarent que la conformité réglementaire (par ex. : le RGPD) est le principal facteur qui détermine la manière et l'emplacement de stockage des données.

48 % des entreprises déclarent que la souveraineté des données est un facteur déterminant dans les décisions en matière d'architecture technologique.

Les entreprises sont confrontées à une mosaïque de règlementations créées par les gouvernements du monde entier.

Les entreprises doivent gérer un environnement de plus en plus complexe et doivent :

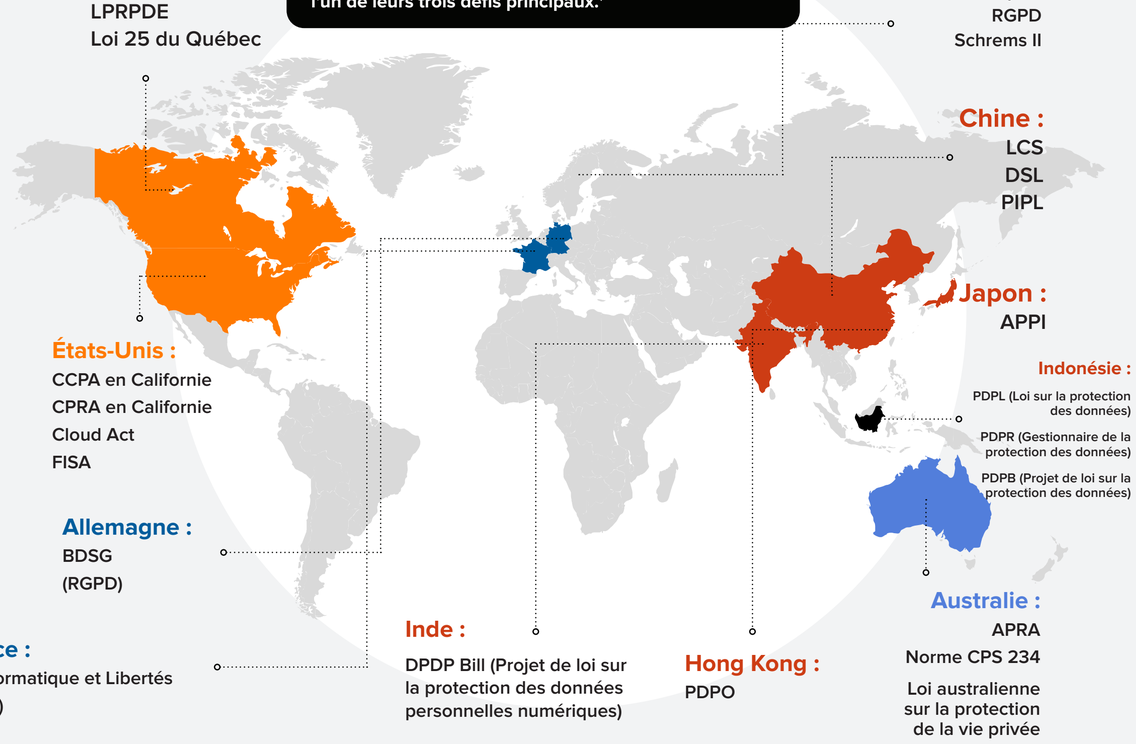
Garantir une infrastructure plus robuste et plus résiliente pour sécuriser les informations

Protéger la confidentialité des personnes

Fournir un consentement individuel et un contrôle sur l'utilisation des données personnelles : collecter, utiliser et divulguer l'utilisation des données personnelles à des fins légitimes et ne conserver ces données que le temps nécessaire

- Schrems II vérifie les lois relatives à la protection des données des pays destinataires : les entreprises doivent s'assurer que la protection des données est équivalente à celle de l'UE et documenter leur évaluation de tous les risques. Les principales opérations à réaliser sont les suivantes :
  - Mettre à jour les clauses contractuelles types (CCT) pour les transferts de données internationaux
  - Mettre à jour la cartographie du traitement des données transfrontalières : mise à jour des descriptions des opérations, destinations, destinataires, outils de transfert, types de données personnelles et catégories des personnes concernées
  - Éviter les traitements des données qui impliquent le transfert de données personnelles vers les États-Unis
- Le Cloud Act permet aux administrations des Etats-Unis, avec l'autorisation d'un juge, d'accéder aux données personnelles notamment hébergées hors des Etats-Unis. Une demande d'accès doit être liée à une enquête, cibler une ou plusieurs personnes identifiées, ne concerner que les faits liés à cette enquête, sur le laps de temps associé à ces faits. Par ailleurs, le Foreign Intelligence Surveillance Act (FISA), loi américaine sur la surveillance et le renseignement extérieur, permet aux Etats-Unis de surveiller physiquement et électroniquement des entités identifiées, si elles se trouvent en dehors des Etats-Unis. Cela se concrétise par les programmes ECHELON, PRISM ou encore Upstream mis en place par l'alliance des services de renseignement Five Eyes (Australie, Canada, Nouvelle-Zélande, Royaume-Uni et États-Unis).
- Les lois chinoises sur la sécurité des données (DSL, Data Security Law) et sur la protection des informations personnelles (PIPL, Personal Information Protection Law) stipulent que les données « principales » et « importantes » stockées en Chine ne peuvent pas être livrées à l'étranger, quel que soit l'endroit où les données ont été initialement collectées. La provenance des données est surveillée de près. Leur vérification et les enregistrements des transactions doivent être conservés. Il faut obtenir le consentement des personnes pour transférer des informations personnelles à des tiers.
- Il existe également de nombreuses normes de gouvernance et de confidentialité des données spécifiques aux secteurs industriels. La norme PCI DSS, par exemple, est la norme mondiale à laquelle doit adhérer toute entité qui transmet, stocke, gère ou accepte des données de carte de crédit.

Lors de l'adaptation et de la mise en application des principes et des processus liés à la souveraineté numérique, **32 % des entreprises européennes considèrent que gérer les exigences parfois contradictoires et conflictuelles entre les juridictions nationales et régionales est l'un de leurs trois défis principaux.**[1]



La France concrétise la souveraineté numérique dans une série de mesures

La France inclut le concept de souveraineté numérique à ceux de l'autonomie de l'économie et de la survie nationale. La cybersécurité et la cyber-résilience sont étroitement liées à la souveraineté numérique. L'agence nationale française de la sécurité des systèmes d'information (ANSSI) a créé « SecNumCloud » pour garantir un haut niveau de sécurité du cloud et établir une norme de souveraineté du cloud. SecNumCloud est la base du « cloud de confiance » utilisé par les administrations publiques françaises et les entreprises privées hautement réglementées et critiques.

Les piliers de la souveraineté numérique en France

Une doctrine pour préciser le cloud de confiance. Le gouvernement français a développé sa doctrine « Cloud au centre » pour que le cloud soit intégré à tous les nouveaux projets numériques de l'État. Dans ce cadre, tous les projets et services numériques doivent être hébergés sur l'un des deux clouds interministériels (basés sur OpenStack). Des plateformes de cloud commerciales peuvent également être utilisées. Cependant, celles-ci doivent répondre à des critères de sécurité stricts, être certifiées SecNumCloud par l'ANSSI, être exemptées des réglementations hors-UE (incluses dans SecNumCoud 3.2) et être conformes au RGPD. Les traitements qui impliquent des données sensibles et critiques relatives aux agents publics de l'État doivent, selon la Doctrine Cloud au centre, être hébergés sur le cloud interne de l'État ou sur un cloud commercial qualifié SecNumCloud par l'ANSSI et protégé contre toute réglementation extracommunautaire.

Promouvoir l'utilisation de logiciels libres. Le gouvernement français encourage l'utilisation de logiciels libres et Open Source pour minimiser la dépendance technologique et servir de base à la souveraineté numérique. L'Open Source constitue un support pour une stratégie numérique de confiance basée sur des données ouvertes, la transparence, les principes du gouvernement ouvert et de nouveaux services numériques.

La résilience de l'infrastructure numérique critique. Depuis 2013, la France a renforcé la sécurité des infrastructures essentielles du pays face à l'augmentation des cyberattaques. L'ANSSI aide certaines entreprises et institutions, publiques et privées, classées comme OIV (opérateurs d'importance vitale) et OSE (opérateurs de service essentiel) à protéger leurs environnements IT. Ces entreprises sont considérées comme essentielles pour maintenir la résilience.

La souveraineté numérique dans les organisations en France :

76 % des entreprises françaises considèrent que la souveraineté numérique est importante et adaptent leurs opérations ou leurs stratégies informatiques en conséquence.[1]

37 % des institutions gouvernementales françaises considèrent que les principes et les directives de souveraineté numérique sont un objectif important.< <175[2]

Une combinaison gagnante de solutions fondamentales et d'un partenaire de confiance peut aider à mieux contrôler les risques connus et inconnus.

Les entreprises doivent coordonner une série de solutions de confiance, depuis l'infrastructure jusqu'à l'engagement client. Un partenaire de confiance peut mettre en œuvre une large gamme de solutions et opérer les changements culturels nécessaires pour récolter les gains d'une stratégie de confiance à grande échelle.

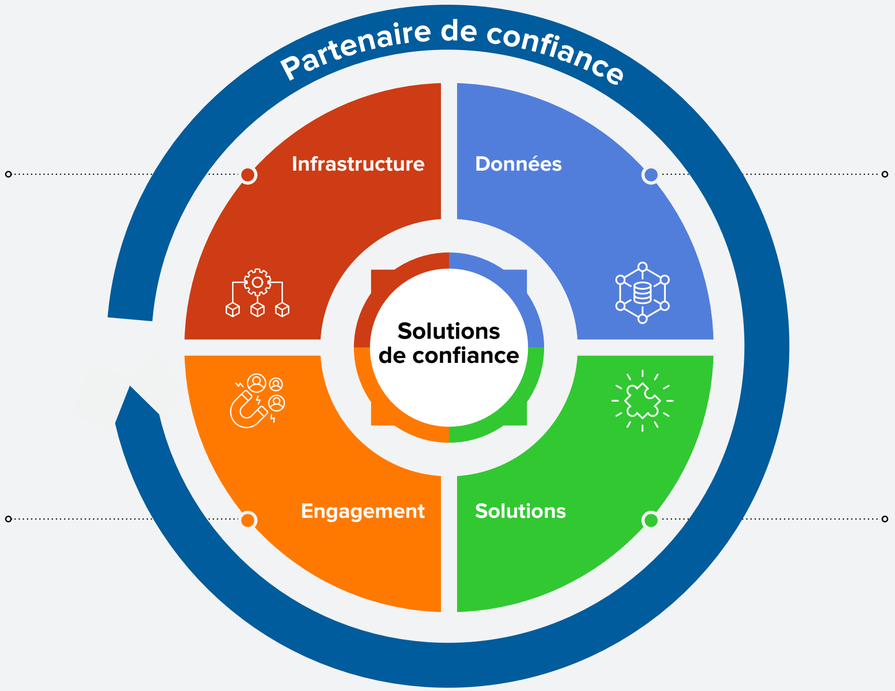
Infrastructure résiliente et sécurisée :

- **Associer les capacités de sécurité** à la sensibilité de l'information
- **S'assurer que sa procédure de continuité d'activité (résilience)** prend en compte le coût des interruptions de service de chaque application
- Envisager le **chiffrement** pair à pair dans le cadre d'une solution réseau de cloud hybride
- **Avoir plus de visibilité sur les données de sécurité** à partir des terminaux, du trafic réseau et des logs pour détecter et répondre plus rapidement aux menaces
- Mettre en place une sécurité **Zero Trust** pour accorder l'accès aux ressources en fonction de l'identité et du contexte

Engagement des clients :

- **Informer les clients (transparence)** que leurs données sont collectées, à quelles fins et pendant combien de temps elles seront conservées
- Les clients doivent être informés sur la façon dont les données sont conservées et sur la durée de conservation
- Apporter **des options de consentement à l'utilisation des données**
- Utiliser des jetons de données pour permettre aux clients de partager des données anonymement
- **Développer des messages visant à gagner et renforcer la confiance des utilisateurs. Communiquer sur les violations de données éventuelles.**

Quatre éléments fondamentaux que les entreprises doivent rechercher auprès d'un partenaire de confiance



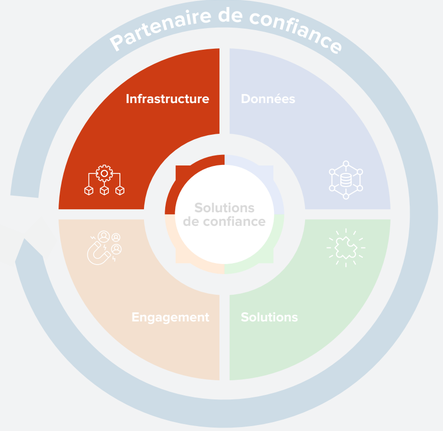
Gestion du cycle de vie des données :

- **Collecter des données à des fins spécifiques** uniquement
- Surmonter l'enjeu des données « shadow » grâce à une **architecture de data mesh**
- S'assurer de pouvoir partager des données en interne et entre les écosystèmes métiers
- Éviter les excès de données, réduire les coûts et son empreinte carbone grâce à la suppression de données
- Accélérer l'analyse des données à l'aide de l'IA/ML
- Promouvoir **une IA éthique** et réduire les biais
- Utiliser l'Edge computing pour gagner en réactivité et visibilité accrues

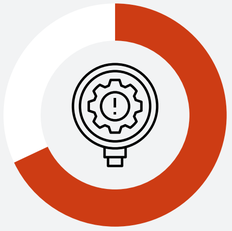
Solutions de confidentialité des données :

- Utiliser des catalogues de données et des outils d'intégration pour améliorer la découverte de données
- Cartographier les relations entre entités de données et réduire les redondances
- **Évaluer les risques liés aux données** (y compris au niveau des fournisseurs tiers) et automatiser les demandes formulées par des personnes (DRS, Data Subject Requests)
- **Mettre à jour ses clauses contractuelles types (CCT) de protection des données** avec des informations géo-spécifiques

Infrastructure : La confiance repose sur une infrastructure sécurisée et résiliente



La confiance repose sur une infrastructure solide et sécurisée. Sans une base solide en matière de sécurité, les autres éléments qui forment la confiance (confidentialité, conformité, gouvernance environnementale et sociale) ne sont pas possibles. Protéger les données des employés, des clients et des partenaires est essentiel pour être une entreprise citoyenne. La loi européenne sur la gouvernance des données (DGA) impose un environnement sécurisé pour le stockage et le traitement des données.



Une étude menée par IDC révèle que

68 % des personnes interrogées considèrent que **la sécurité est l'élément où le risque est le plus élevé pour la confiance numérique**[1]. Pour les entreprises françaises, les principales fonctions de sécurité portent sur la détection et la réponse aux menaces, les vulnérabilités de la chaîne d'approvisionnement du matériel et du logiciel, et la gestion du chiffrement et des clés.[2] Les entreprises de confiance, qui ont investi pour renforcer leur posture de sécurité, constatent une plus forte résilience opérationnelle.

Domaines de sécurité classés par importance

	France	EMEA	Monde
1	Détection et réponse aux menaces (terminal, réseau, etc.)	Sauvegarde et reprise après sinistre	Sauvegarde et reprise après sinistre
2	Vulnérabilités de la chaîne d'approvisionnement du matériel et du logiciel	Vulnérabilités de la chaîne d'approvisionnement du matériel et du logiciel	Gestion du chiffrement et des clés
3	Gestion du chiffrement et des clés	Gestion du chiffrement et des clés	Détection et réponse aux menaces (terminal, réseau, etc.)

Selon une étude menée par IDC, les entreprises françaises placent la capacité de détection et de réponse aux menaces comme principale priorité en matière de sécurité IT. La gestion des vulnérabilités de la chaîne d'approvisionnement du matériel et du logiciel est le second domaine auquel elles accordent de l'importance. Dans la zone EMEA, en revanche, la sauvegarde et la reprise après sinistre sont les domaines de sécurité les plus importants lors de l'évaluation des fournisseurs de cloud.

[1]IDC Future Enterprise Resilience and Spending Survey, juillet 2021
[2]IDC Future of Trust Survey, janvier 2022

Données : Les partenaires de confiance gèrent la confidentialité et la sécurité des données tout au long du cycle de vie, de la collecte à la destruction, en passant par le stockage, l'utilisation, le partage et l'archivage

En vertu du RGPD, les personnes (data subjects) ont désormais le droit de savoir quelles données les concernant ont été collectées et quels traitements ont été opérés. Ils disposent du droit de transférer des données personnelles, du droit d'apporter des modifications à des données inexactes, du droit de retirer leur consentement et du droit de demander la suppression de données personnelles. Les données ne peuvent pas être traitées sans avoir obtenu un consentement au préalable. Schrems II a invalidé le Privacy Shield (le mécanisme *Safe Harbor*), ce qui a accéléré l'adoption d'outils de cartographie des données et de rapport de transfert.

Selon une enquête réalisée par IDC France et publiée en 2022, **77 % des entreprises françaises estiment que la souveraineté des données est importante pour mener leurs activités** (66 % pour les entreprises privées contre 89 % pour les organisations publiques)[1]. 49 % des entreprises françaises considèrent que la restriction du stockage et du transfert de données à des zones géographiques spécifiques est un critère associé à la souveraineté numérique et à une chaîne d'approvisionnement technologique de confiance.[2]

Cycle de vie des données

Création/collecte des données	Le moment où les données sont créées ou importées dans le système. Idéalement, les données sont classées à ce stade, après quoi le niveau de sécurité approprié peut être appliqué.
Stockage des données	Le stockage est le processus où des contrôles de sécurité sont appliqués pour protéger les données, définir les contrôles d'accès, le chiffrement et l'audit des données.
Utilisation des données	Les données en cours d'utilisation sont vulnérables aux fuites ou risquent d'être compromises. Le manque de coordination ou la mauvaise configuration de l'accès ou de l'authentification entre différents services peut compromettre les données. Un problème important avec les données « shadow » a été détecté. Il peut être résolu à l'aide de solutions telles que le data mesh.
Partage des données	Les données quittent le système et ne sont plus sous la supervision et le contrôle du système d'origine. La prévention de la perte de données (DLP, Data Loss Prevention) et la gestion des droits relatifs à l'information (IRM, Information Rights Management) peuvent être utilisées pour détecter des anomalies lors du partage et empêcher toute modification non autorisée des données.
Archivage des données	L'archivage à long terme basé sur les règles de l'entreprise et les exigences réglementaires doit garantir une bonne récupération et lecture des données archivées.
Destruction des données	Destruction permanente des données en fonction de la demande de l'utilisateur ou du niveau de sensibilité.

Pour mettre en musique la souveraineté numérique, les entreprises françaises investissent pour :

- Améliorer les mesures de confidentialité et leur mise en œuvre
- Améliorer les processus intégrés de gestion des risques pour inclure des paramètres géographiques
- Travailler plus étroitement avec leurs fournisseurs IT et de communications pour réduire les risques [3]

Dans un monde arbitré par les données et déterminé par l'IA, les entreprises doivent contrôler la façon dont leurs données sont collectées et leur origine. **Les données à partir desquelles les entreprises prennent leurs décisions doivent être complètes et représentatives pour réduire le risque de biais en matière d'IA/ML.** Une confiance élevée est un prérequis pour que les clients acceptent de partager des données personnelles qui livrent de précieux indicateurs.

[1]IDC France, Observatoire de la cybersécurité 2022
[2]IDC EMEA Future Enterprise Resilience and Spending Survey, 2021, Wave 8
[3]IDC, Future Enterprise Resilience and Spending (FERS) Survey, mai 2022

Solutions : Des solutions de confidentialité et des technologies émergentes existent pour aider les partenaires de confiance à se conformer au RGPD et à la réglementation Schrems II

Au niveau européen, une série de services se met en place pour répondre aux exigences de gestion des données du RGPD et de Schrems II. Ces services sont spécialisés dans l'évaluation des risques liés au transfert de données, l'évaluation des risques fournisseurs, la cartographie du flux de données, la surveillance et le suivi du consentement, la conformité aux cookies, les demandes des personnes (DSR) et leurs demandes d'accès, les demandes de rectification et de suppression des données.

Domaines de confidentialité classés par importance

	France	EMEA	Monde
1	**Obfuscation/confidentialité des données et intégrité des données (comme le masquage, la randomisation, le chiffrement)**	Conservation, suppression et divulgation conformément aux réglementations en matière de confidentialité	DLP/IRM
2	**Conservation, suppression et divulgation conformément aux réglementations en matière de confidentialité**	DLP/IRM	Autorisations et contrôle de l'utilisation des données
3	**Surveillance, reporting et transparence des politiques de confidentialité**	Découverte, classification et catégorisation des données	Découverte, classification et catégorisation des données

La prévalence des environnements de travail hybrides accélère l'adoption de frameworks Zero Trust pour réduire la vulnérabilité des ressources auxquelles les employés doivent accéder. Même s'il reste encore beaucoup d'éducation à réaliser en matière de technologies Zero Trust, **une entreprise française sur cinq envisage un déploiement de ce type ou le mettra en œuvre au cours des 12 prochains mois**.[1]

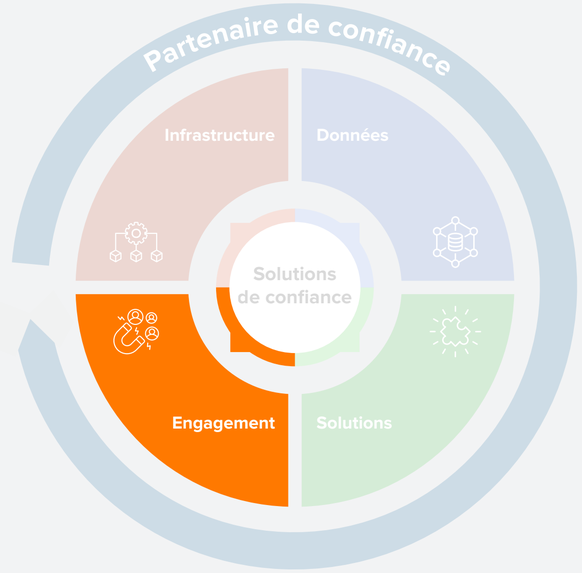
Principes fondamentaux du Zero Trust : vérification, accès au moindre privilège et chiffrement de bout en bout

Éléments d'organisation à prendre en compte lors de la mise en œuvre du Zero Trust : gestion de la surface d'attaque, sécurité des données et gestion des identités et des accès

Outils de protection des données et de confidentialité pour répondre aux exigences réglementaires

Enjeu	Technologie
Découverte de données	Découverte des ressources et des données
Cartographie des données	Traçabilité des données et automatisation de la confidentialité des données
Identification des données	Intelligence des données
Reporting sur les risques liés aux données	Cartographie des données et évaluations des fournisseurs
Gestion du consentement	Automatisation du consentement aux données
Demandes d'accès des personnes	Automatisation des demandes d'accès des personnes (DSR)
Protection des données en cours d'utilisation	Sécurité Zero Trust (y compris l'informatique confidentielle et les identités décentralisées)

Engagement : Les entreprises doivent devenir des gestionnaires éthiques des données clients, de la confidentialité, de la sécurité et de l'environnement pour conserver la confiance



Alors que les entreprises continuent d'innover avec de nouveaux produits et services numériques, anticiper les besoins et les problèmes des clients et garantir la résilience sont des éléments essentiels pour conserver la confiance. En parallèle, les données client ne constituent plus un droit commercial. Les clients sont prêts à partager leurs données en échange de meilleurs produits et services. Les entreprises doivent rassurer leurs clients sur la façon dont leurs données sont gérées et sur le respect des pratiques de conformité réglementaire.

Selon un étude IDC,

69 % des entreprises européennes pensent que **la souveraineté numérique renforce la confiance accordée par les clients**.[1]

S'engager sur des résultats autorisés (et donc garantis)

- **56 %** des entreprises européennes considèrent que les réglementations en matière de collecte, d'utilisation et de stockage des données clients sont leur priorité n°1.[2]
- En outre, les entreprises devraient centraliser les politiques de confidentialité et de consentement des clients et suivre, d'une entreprise à l'autre, le consentement des clients et les accès des personnes.
- Les entreprises devraient également créer un schéma de métadonnées pour représenter et mesurer les dimensions des différents types de données, en plus des paramètres qui régissent leur utilisation tels que la notion de temporalité des usages, l'expiration, la priorité et le consentement.

Intégrer la transparence des données clients

- Les grandes entreprises partagent en toute transparence leur utilisation des données clients dans leurs processus d'engagement et proposent des options de consentement. Par conséquent, ces entreprises bénéficient **d'un niveau plus élevé de confiance mutuelle** avec leur clientèle.

Lutter contre les biais

- **39 %** des entreprises considèrent les réglementations relatives à une utilisation équitable et éthique de l'IA[2].
- Selon IDC, d'ici 2025, 40 % des entreprises classées au Forbes Global 2000 encourageront l'utilisation éthique de l'IA et des données dans le marketing et d'autres initiatives ESG. Une façon de garantir la confiance des clients. Cela devrait augmenter leur part de marché de 5 %.

[1]IDC EMEA Future Enterprise Resilience and Spending Survey 2021, Wave 8

IDC EMEA Future Enterprise and Resilience Spending Survey 2022, Wave 12

Les études montrent qu'investir dans la confiance se traduit par de meilleurs résultats et un meilleur retour sur investissement

Pourquoi étudions-nous la confiance ? La confiance a été décrite comme un « rapport sûr avec l'inconnu ». L'incertitude règne dans notre monde complexe et en constante évolution. Etre considéré comme un partenaire de confiance contribue à atténuer les pertes des entreprises en cas d'événements imprévisibles. Une confiance élevée crée un avantage concurrentiel et favorise la fidélité des clients. Construire une relation de confiance est nécessaire pour surmonter la réticence des consommateurs à partager leurs données personnelles.

Dans une enquête européenne menée en 2022 par IDC, 74 % des personnes interrogées ont déclaré qu'investir dans des programmes de confiance était une priorité ou une priorité élevée pour 2023. **77 % des Français interrogés déclarent la même chose.**[1]

Selon une étude menée par IDC, les investissements prioritaires dans des programmes de confiance ou dans la sécurité, la confidentialité et la conformité, sont fortement associés à l'amélioration de la résilience commerciale, de l'efficacité opérationnelle et du développement durable dans le monde.[2]

En utilisant une analyse de régression, nous pouvons étudier la relation entre deux ou plusieurs variables d'intérêt.

Nous répondons aux questions suivantes : Quels facteurs sont les plus importants ? Lesquels pouvons-nous ignorer ? Comment ces facteurs interagissent-ils les uns avec les autres ?

Objectifs opérationnels améliorés* grâce à l'investissement dans des programmes de confiance

Productivité des employés	Les personnes interrogées dans la région EMEA constatent une augmentation de la productivité des employés (R^2 = 0,05) grâce à leurs investissements dans des programmes de confiance.
Résilience de l'entreprise	Au niveau mondial, les investissements dans des programmes de confiance améliorent la résilience des entreprises (R^2 = 0,03). Les entreprises qui investissent dans la confiance mettent en place les infrastructures de sécurité et de confidentialité nécessaires pour établir une relation de confiance et rétablir leurs activités plus rapidement après une cyberattaque.
Efficacité opérationnelle	Dans le monde (en particulier dans la zone Asie - Pacifique), l'investissement dans des programmes de confiance améliore l'efficacité opérationnelle (au niveau mondial : R^2 = 0,02 ; Asie/Pacifique : R^2 = 0,06), réduit le volume de données collectées et favorise des approches plus structurées en matière d'utilisation et de confidentialité des données.
Développement durable	Au niveau mondial, (R^2 = 0,02), l'investissement dans des programmes de confiance favorise le développement durable. Les initiatives liées à l'ESG forment un pilier de la confiance et sont de plus en plus importants dans les décisions d'achat.

[1]IDC EMEA Future Enterprise Resilience and Spending Survey, Wave 5, juin 2022
[2]IDC, Future Enterprise Resilience and Spending Survey, Wave 5, juin 2022

* Niveau d'importance défini sur p < 0,05

La souveraineté est un pilier essentiel de l'accélération du cloud en France

La souveraineté numérique est un accélérateur de cloud en France :

Pour **42 %** des entreprises françaises, la souveraineté numérique va accélérer leur utilisation du cloud au cours des deux prochaines années.[1] Les entreprises françaises mettent en place des bases technologiques pour améliorer leur sécurité, leur résilience et leur confiance.

31 % des entreprises françaises utilisent déjà un cloud souverain. Mais ce n'est que la partie émergée de l'iceberg, car **40 % prévoient de le faire dans les deux prochaines années et 18 % l'envisagent**.[2] Les solutions de cloud souverain devraient progressivement faire partie des stratégies hybrides ou multicloud.

La conformité aux législations nationales et régionales constitue un facteur premier de souveraineté

- **33 %**[2] des entreprises françaises citent la législation nationale ou régionale comme premier facteur d'utilisation d'un cloud souverain. Au niveau européen, les entreprises considèrent le cloud souverain comme un moyen de mettre en musique leur stratégie de travail hybride postpandémie sans minimiser la conformité.
- Elles considèrent également le cloud souverain **comme un instrument et un critère pour développer leur activité et étendre leurs opérations au-delà de leurs frontières**. L'expansion à l'international est le deuxième facteur d'utilisation du cloud souverain en France (voir ci-dessous).

Facteurs d'adoption du cloud souverain en France et en Europe

France	Europe
1 Législation nationale ou régionale	1 Développement de l'utilisation du cloud (pour supporter davantage le télétravail)
2 Expansion à l'international	2 Conformité et réglementations du secteur
3 Conformité et réglementations du secteur	3 Législation nationale ou régionale
4 Développement de l'utilisation du cloud (pour supporter davantage le télétravail)	4 Protection contre les demandes de données extraterritoriales
5 Protection contre les demandes de données extraterritoriales	5 Problèmes précédents liés à la conformité et à la sécurité

Se protéger contre les règles d'extraterritorialité incluses dans les réglementations étrangères (par ex. : le Cloud Act) est un facteur d'utilisation d'un cloud souverain pour **26 % des entreprises françaises**.[2]

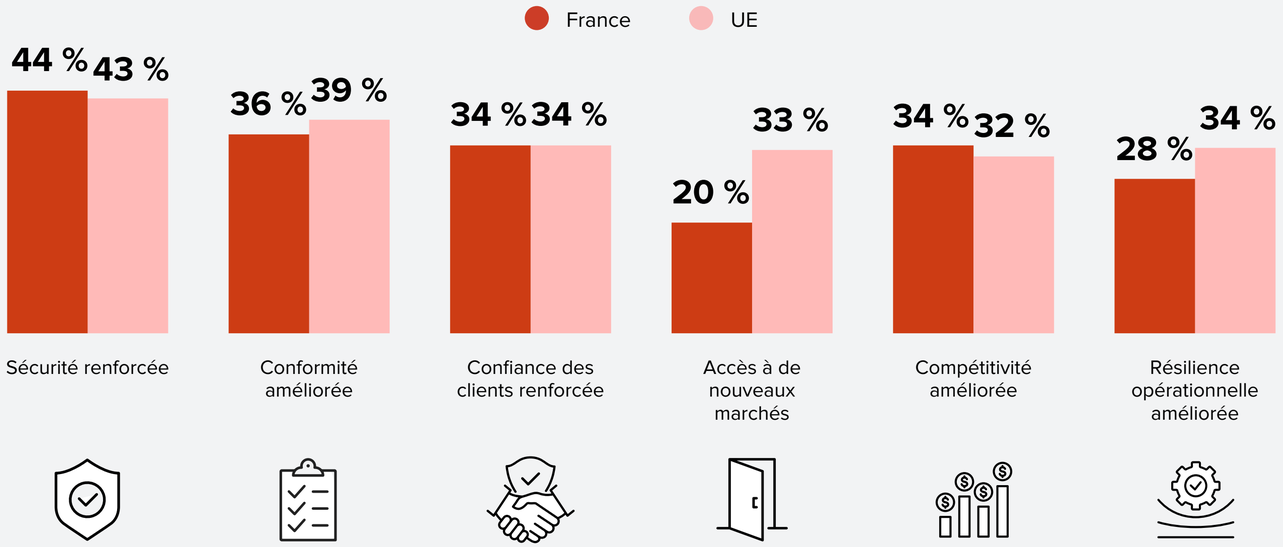
[1]IDC Europe Multicloud Survey 2022
[2]IDC European Future Enterprise Resilience and Spending Survey, 2023

Les entreprises françaises considèrent le cloud souverain comme un atout précieux de leur stratégie commerciale et de leur croissance

Confiance et sécurité : les bénéfices pour lesquels les entreprises sont prêtes à payer davantage

- Utiliser un cloud souverain a des conséquences directes sur les modèles économiques des entreprises françaises. Ces avantages comprennent l'amélioration de la sécurité (46 %), de la conformité (36 %), de la confiance des clients et de la compétitivité (31 % respectivement).[1]
- Malgré des budgets limités (en raison de l'inflation et des incertitudes politiques et économiques), deux entreprises françaises sur trois sont prêtes à payer entre 11 % et 30 % en plus pour répondre aux enjeux de confiance, de sécurité et de conformité auxquels elles sont confrontées. 9,3 % seraient prêtes à payer une surprime comprise entre 31 % et 50 %, tandis que près de 5 % seraient prédisposées à débourser un supplément de 50 %.[3]

Les avantages à utiliser un cloud souverain en France et en Europe



Les entreprises françaises indiquent que **les coûts élevés (40,5 %) et la complexité (35 %)** sont les principaux défis liés à la souveraineté des données.[2]

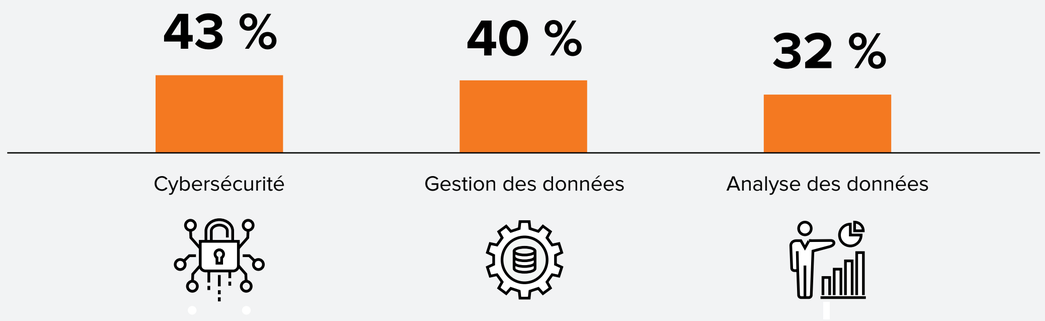
Pour les organisations françaises, la souveraineté numérique entraîne une redistribution des applications et services et nécessite davantage de compétences et de nouveaux partenaires

Une migration en cours vers des fournisseurs locaux pour les applications et les données :

- Les entreprises françaises sont sur le point de modifier la répartition actuelle de leurs applications et services entre les environnements SaaS, PaaS et IaaS pour répondre aux exigences de la souveraineté numérique. 44 % des entreprises accorderont la priorité à un fournisseur de cloud local pour leurs outils de développement et de gestion des données (PaaS), 40 % pour leurs applications métiers et 37 % pour leur infrastructure (IaaS). Sans surprise, le stockage et la sécurité seront les domaines les plus affectés par cette nouvelle répartition des applications et services.[1]

Cybersécurité et données : adapter les compétences aux enjeux de souveraineté

- La mise en œuvre de la souveraineté numérique entraînera des coûts supplémentaires pour les entreprises. Elles devront en particulier investir dans des compétences IT pour accompagner les déploiements. Seules 5 % des entreprises françaises déclarent qu'aucun changement en compétences n'est nécessaire.
- De nombreuses entreprises devront s'appuyer davantage sur leurs fournisseurs pour répondre aux exigences de souveraineté numérique.



Panorama de la souveraineté du cloud en France

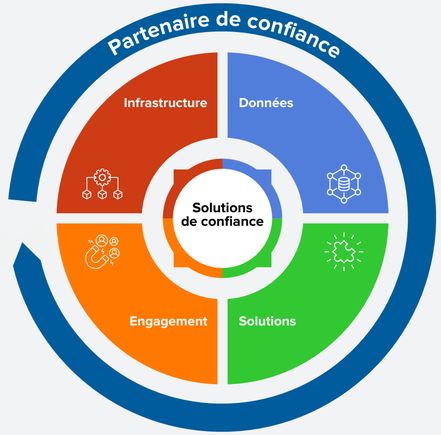
L'approche française de la souveraineté numérique et le « cloud de confiance » ont changé le paysage du cloud dans le pays. Ces clouds ciblent les besoins spécifiques de l'État français, des organismes publics, du secteur de la santé publique, des autorités locales et régionales, des OIV et des OSE, ainsi que d'autres entreprises dans des secteurs très réglementés. En France, les offres de cloud souverain peuvent être réparties en trois catégories :

Fournisseurs de services et de cloud locaux	Alliance locale	Alliance entre les fournisseurs de services et de cloud locaux et les hyperscalers
Fournisseurs français de cloud, de services et de télécommunications disposant d'une certification SecNumCloud et d'une entité commerciale juridique exploitée en France. Exemples : OVHCloud Outscale Orange Business (en cours)	Alliance de fournisseurs et d'entités publiques basés en France pour proposer un ensemble de services (certifiés SecNumCloud) centrés sur la confiance et la souveraineté numérique pour le marché français Exemples : NumSpot ; Dassault Systèmes, Bouygues Telecom et Banque des Territoires	Alliance de fournisseurs de services ou de télécommunications basés en France et d'hyperscalers basés aux États-Unis pour fournir une nouvelle entité juridique basée en France et exploitée par une équipe française, mais utilisant la technologie de l'hyperscaler. C'est cette nouvelle entité juridique qui sera responsable de l'offre souveraine (certifiée SecNumCloud). Exemples : Bleu : une future joint-venture entre Orange et Capgemini et un partenariat technique avec Microsoft (2024) Sens : Thalès, Google Cloud (2024)

Source : IDC Future Enterprise Resilience and Spending Survey Europe, 2022

[1]IDC Future Enterprise Resilience and Spending Survey Europe, 2022

Les fournisseurs dont les offres permettent d'améliorer la livraison, la sécurité, la conformité et les critères ESG sont considérés comme des partenaires de confiance



L'IDC Trust Perception Index mesure les performances des fournisseurs, en demandant aux entreprises de classer ce qui compte le plus pour elles et d'évaluer la performance des principaux acteurs. Au-delà de la confidentialité et de la gestion des données, les partenaires de confiance se distinguent des autres acteurs par leur proposition de valeur en matière de sécurité, de confidentialité, de conformité, d'ESG et de facteurs basés sur l'expérience. Pour développer des partenariats à long terme, les capacités et la culture d'un fournisseur feront la différence .

Core

Sécurité et conformité

La sécurité et la conformité sont essentielles, mais constituent la base. Selon l'IDC Trust Perception Index, les principaux fournisseurs se valent en matière de protection des données, conformément à toutes les réglementations applicables en matière de confidentialité et de gouvernance des données. Les fournisseurs considérés comme des leaders de confiance excellent dans la sauvegarde et la reprise après sinistre, la disponibilité de compétences et leadership en matière de cybersécurité, la gestion des identités, des identifiants et des accès, ainsi que la gestion du chiffrement et des clés. Les acteurs les plus performants se distinguent également en fournissant des certifications de conformité conformes aux normes mondiales, nationales et sectorielles.

Facteurs de différenciation

Confidentialité et ESG

Selon l'IDC Trust Perception Index, les fournisseurs qui se démarquent de leurs concurrents dans le domaine de la confidentialité et des facteurs environnementaux, sociaux et de gouvernance (ESG) sont les leaders de la confiance sur leurs marchés. Les leaders de la confidentialité se distinguent en matière de DLP, IRM ou d'obfuscation et d'intégrité des données. Les leaders dans la mise en œuvre de facteurs ESG se démarquent quant à eux en proposant des prix abordables pour des offres et services durables ou en fournissant des indicateurs clés de performance sur le développement durable et l'impact social.

Facteurs liés à l'expérience

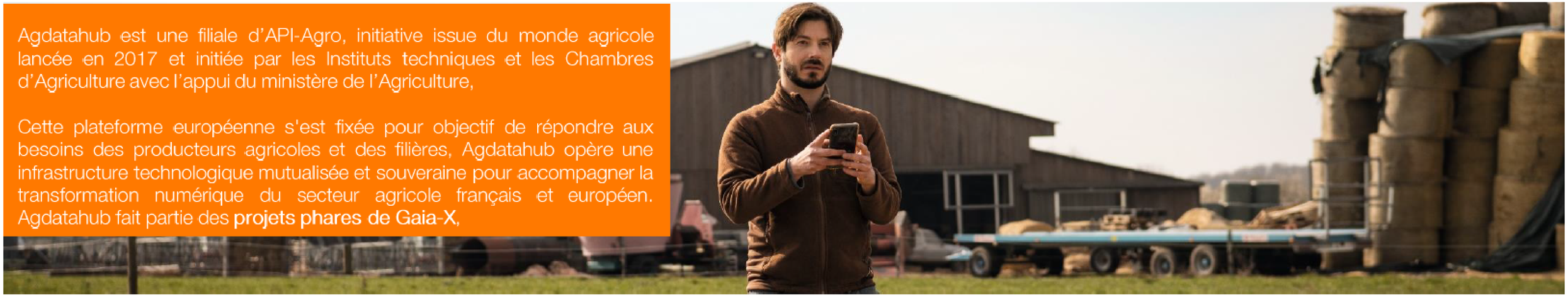
Selon la même étude, dans un contexte économique difficile, les entreprises recherchent un partenaire de confiance capable d'offrir bien plus que de simples solutions. Elles ont besoin d'aide pour réduire la complexité et les coûts liés à la création et à la gestion d'une infrastructure de confiance. À cela s'ajoute une combinaison de services de conseils, d'intégration et d'assistance proposés à un prix juste et accompagnés d'offres sectorielles. L'ensemble doit être proposé via une unique solution.

Agdatahub

Apporter une identité numérique aux agriculteurs et garantir leurs consentements.

Agdatahub est une filiale d'API-Agro, initiative issue du monde agricole lancée en 2017 et initiée par les Instituts techniques et les Chambres d'Agriculture avec l'appui du ministère de l'Agriculture,

Cette plateforme européenne s'est fixée pour objectif de répondre aux besoins des producteurs agricoles et des filières, Agdatahub opère une infrastructure technologique mutualisée et souveraine pour accompagner la transformation numérique du secteur agricole français et européen. Agdatahub fait partie des **projets phares de Gaia-X**,



Enjeux

En France, le secteur agricole est composé de 380 000 exploitations dont 80% d'entre elles sont des TPE / PME. Cette division des exploitations crée une dispersion des données et il est donc très difficile de les utiliser.

Afin de palier à cet obstacle, un projet a été lancé pour la création d'une identité numérique propre à chaque personne physique et morale permettant de certifier les échanges avec les fournisseurs, les clients et l'administration.

Solution

Agritrust, la première identité numérique agricole décentralisée reconnue par l'ensemble du secteur et reposant sur une solution blockchain innovante permet de :

- **Etablir une liaison entre identité de l'agriculteur et exploitation**
- **Héberger et sécuriser les données sur le cloud public d'Orange Business**
- **Mettre à disposition un certificat digital dans un portefeuille numérique (wallet), accessible grâce à un QR code**

Bénéfices

Des données authentifiées et sécurisées grâce à la Blockchain

Un contrôle total de son identité numérique et de ses consentements

Une diminution du risque de fraude envers l'industrie et la Grande Distribution

Un usage qui répond aux normes françaises et européennes

Message du sponsor

Orange Business, l’entité du Groupe Orange dédiée aux entreprises, est un intégrateur réseaux et numérique de référence.

Orange Business s’appuie sur son expertise en matière de connectivité nouvelle génération, de cloud et de cybersécurité, ses plateformes de services ainsi que sur son écosystème de partenaires pour offrir aux entreprises du monde entier des solutions numériques de confiance.

Forts de 30 000 collaborateurs à travers 65 pays, Orange Business orchestre la transformation des entreprises de bout en bout en concentrant sa proposition de valeur sur les infrastructures digitales sécurisées, l’expérience clients, l’expérience salaries et l’expérience opérationnelle. Plus de 2 millions de professionnels, entreprises et collectivités en France et 3 000 multinationales font confiance à Orange Business.

Orange est l'un des principaux opérateurs de télécommunications au monde, avec un chiffre d'affaires de 43,5 milliards d'euros en 2022 et 287 millions de clients dans le monde au 31 décembre 2022. En février 2023, le groupe a présenté son plan stratégique, « Lead the Future », fondé sur un nouveau modèle économique et guidé par la responsabilité et l'efficacité. « Lead the Future » s'appuie sur l'excellence du réseau pour renforcer le leadership d'Orange en matière de qualité de service.

Pour en savoir plus : www.orange-business.com

orange™ Business

À propos d'IDC

International Data Corporation (IDC) est le principal prestataire international dans le secteur de la recherche, du conseil et de l'événementiel sur les marchés des technologies de l'information, des télécommunications et de la technologie grand public. IDC aide les professionnels de l'informatique, les cadres et les investisseurs à prendre des décisions étayées par des informations tangibles, dans le cadre d'achats technologiques et de stratégie d'entreprise. Plus de 1 100 analystes IDC mettent en application leurs connaissances au niveau mondial, régional et local en matière de technologie et de secteur d'activité, dans plus de 110 pays à travers le monde. Depuis 50 ans, IDC fournit un éclairage stratégique afin d'aider ses clients à atteindre leurs objectifs clés. IDC est une filiale d'IDG, leader mondial des supports technologiques, de la recherche et de l'événementiel.

IDC UK
5th Floor, Ealing Cross,
85 Uxbridge Road
Londres
W5 5TH, Royaume-Uni
44 208 987 7100
Twitter : @IDC
idc-community.com
www.idc.com

Siège social
140 Kendrick Street,
Building B, Needham,
MA 02494 États-Unis
508 872 8200
www.idc.com