



# Le cloud de confiance

Où en est-on en 2025 en France ? Quels sont les freins et les motivations à son adoption ?

exægis. x  
markess



Business

# Avant-propos

Sans sécurité de l'information et du cloud, la transformation numérique des entreprises comme des administrations ne peut s'opérer. Néanmoins, les obstacles auxquels se heurtent les institutions publiques et les entreprises dans leur quête de produits et services numériques sécurisés ne font que s'accroître. Dans ce contexte, des qualifications, des certifications ou encore des directives sont mises en place par l'Union européenne et la France pour éclairer le décideur. Malgré les efforts pour éclaircir et cadrer le sujet (en particulier ceux de l'ANSSI avec le référentiel SecNumCloud), le concept de cloud de confiance reste flou pour une majorité d'entreprises et connaît des évolutions rapides.

Le cloud offre de nombreux avantages en termes de coût, de flexibilité, d'efficacité, d'optimisation, de sécurité, d'accès à l'innovation et il est devenu incontournable. Mais l'usage du cloud et l'exploitation des données est aussi source d'interrogations lorsqu'il s'agit de maîtrise des dépendances, de préoccupations économiques, géopolitiques voire stratégiques. C'est pourquoi les décideurs recherchent de plus en plus la confiance dans le cloud afin de réduire leur exposition aux différents risques, qu'ils soient juridiques (protection des données sensibles contre un accès autorisé par des législations non européennes à portée extraterritoriale, Cloud Act notamment, géopolitiques (prévenir la dépendance des organisations publiques et privées vis-à-vis des solutions numériques non européennes. Exaegis Markess constate dans ses études que Amazon Web Services, Microsoft Azure et Google Cloud captent plus de 70% du marché du cloud public. Est-ce que les entreprises

utilisatrices peuvent poursuivre leur activité en cas de coupure de services ?) ou encore économiques (favoriser la portabilité et la réversibilité pour maîtriser la dépendance vis-à-vis des stratégies de verrouillage des fournisseurs de cloud en position forte sur le marché du cloud).

Le périmètre retenu par Exaegis Markess pour désigner le cloud de confiance n'est pas restreint à la qualification SecNumCloud. Cette qualification délivrée par l'ANSSI offre le plus haut niveau en termes de sécurité technique, opérationnelle et juridique, mais elle est pour le moment limitée au territoire national. D'autre part, les fortes exigences de la qualification SecNumCloud seront parfois supérieures aux contraintes de certaines organisations dont les informations et les activités sont considérées moins sensibles. Au-delà, Exaegis Markess considère que la transparence et la maîtrise de l'empreinte environnementale du fournisseur sont aussi des éléments de confiance et de durabilité des relations.

L'enquête réalisée dans le cadre de cette étude indique que le cloud de confiance est intégré dans la stratégie numérique de 71% des répondants. Toutefois, ils ne sont que 27% à déclarer utiliser des offres de confiance. L'analyse publiée dans cet ebook tend à présenter les motivations, les cas d'usage et les freins actuels à l'adoption du cloud de confiance.

Ronan Mevel, directeur associé  
Practice Leader Infrastructures digitales et Cloud



# Référentiel utilisé

Le périmètre retenu par Exaegis Markess comprend les offres de solutions cloud de confiance basées sur une infrastructure garantissant la sécurité par le biais de solutions techniques à l'état de l'art et fournissant aux utilisateurs des moyens de contrôle. Cette infrastructure est accessible de manière privée ou publique et est soumise aux normes et qualifications françaises et européennes en matière d'hébergement et de protection des données (qualifiée SecNumCloud ou en cours, HDS, PCI DSS, RGPD, NIS2, ISO 27001, etc). Les offres qualifiées C5 en Allemagne ou ENS en Espagne, disponibles en langue française et respectant l'immunité aux lois non européennes sont également comprises dans le périmètre.

Les fournisseurs de ces prestations ont leur siège social en France ou Europe et proposent leurs services à une clientèle externe à leur organisation, en recherche de conformité, de souveraineté et de durabilité.

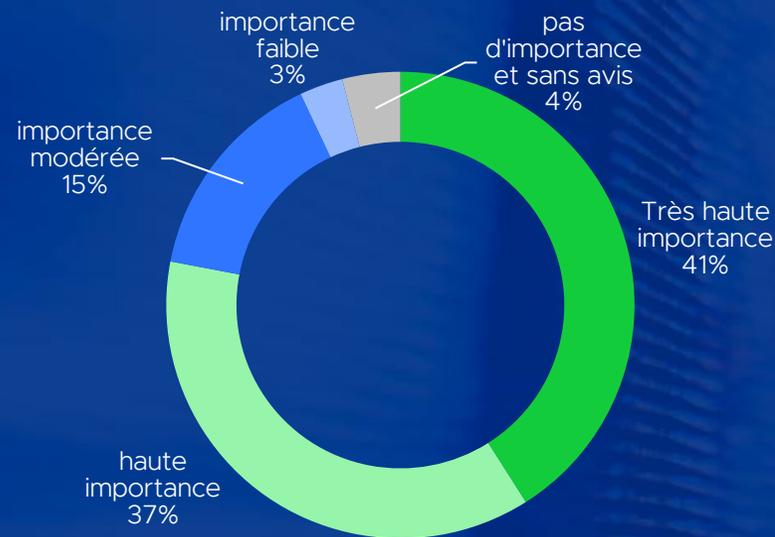
Les fournisseurs de solutions cloud pouvant intégrer ce périmètre sont aujourd'hui Adista, Aruba Cloud, Bleu, Cegedim.cloud, Cheops Technology, Claranet, Clever Cloud, Cloud Temple, Ecritel, Free Pro, Ionos, Numspot, Orange Business, Outscale, OVHcloud, S3NS, Scaleway, SFR Business et Sigma.



# La protection et le contrôle des données dans le cloud

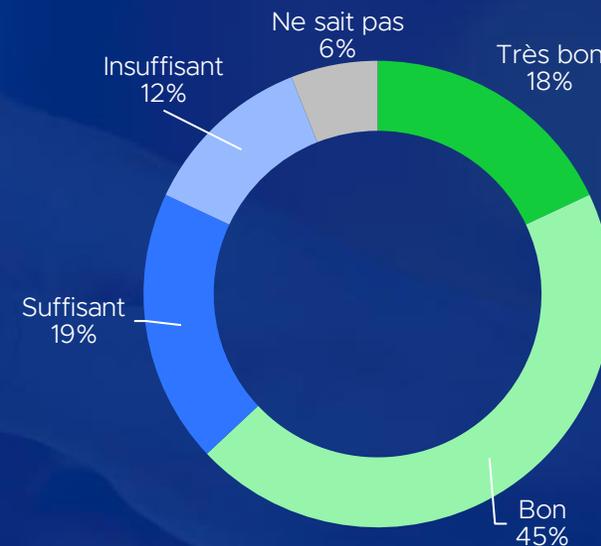
## Une haute importance qui n'est pas mise en pratique

Comment jugez-vous l'importance de la protection et du contrôle de vos données dans le cloud ?



N=122  
©Exaegis Markess, 2025

Comment évaluez-vous le niveau actuel de contrôle et de protection de vos données dans le cloud ?

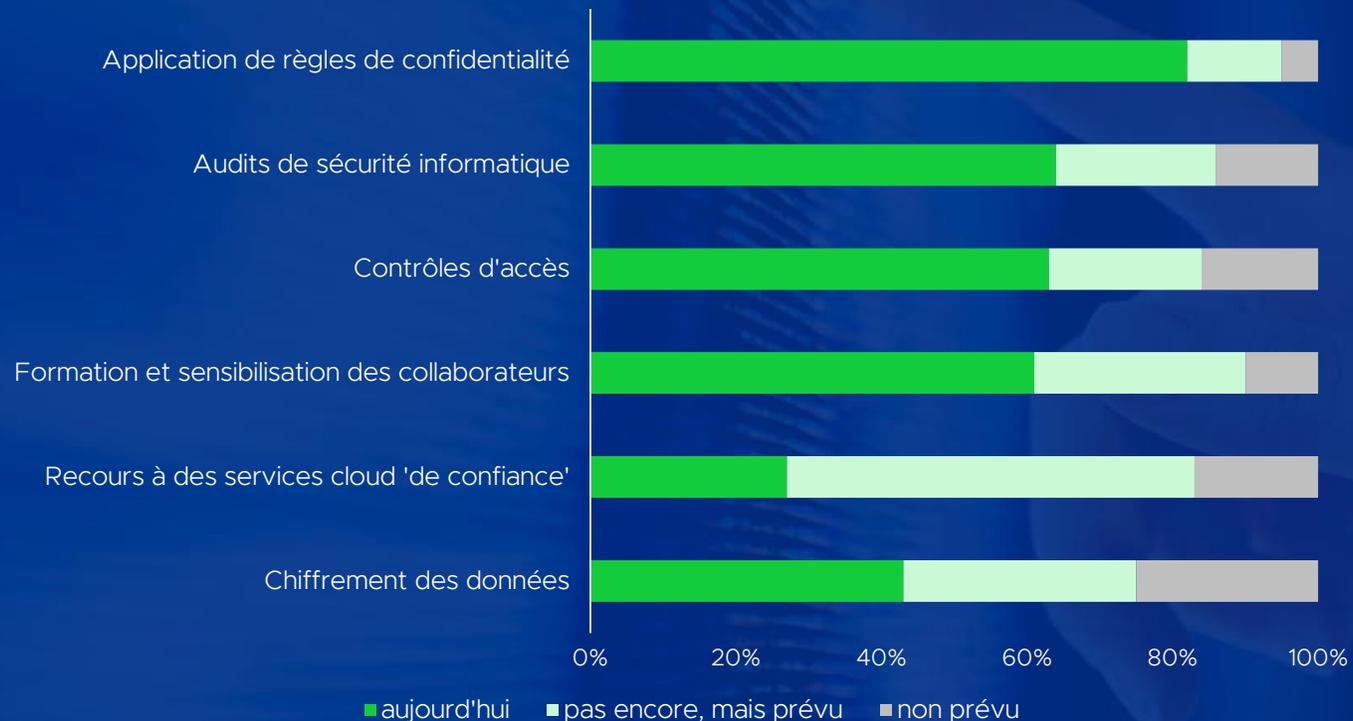


N=122  
©Exaegis Markess, 2025

# Les mesures visant à protéger et contrôler les données

## Un recours au cloud de confiance qui devrait nettement s'accélérer

Quelles mesures instaurer pour renforcer le contrôle et la protection de vos données dans le cloud ?



N=122

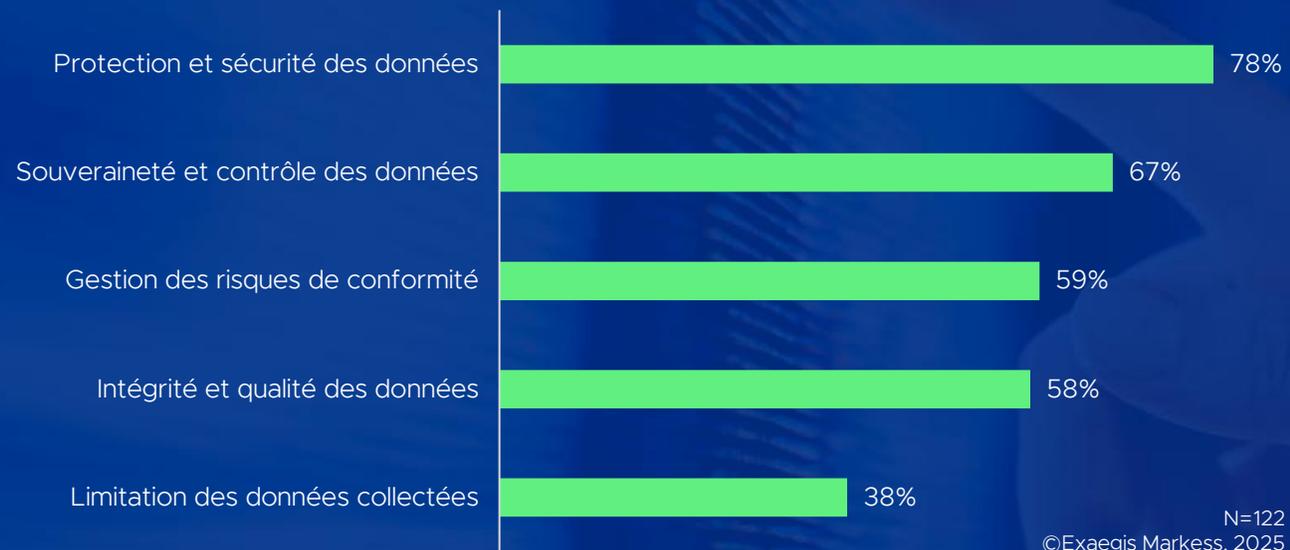
©Exaegis Markess, 2025

Pour 78% des répondants, la protection et le contrôle des données est un sujet de haute importance. Or, ces mêmes répondants ne sont que 18% à déclarer très bon le niveau actuel de contrôle et protection. Le recours au cloud de confiance est considéré par 56% comme une mesure permettant de renforcer le contrôle et la protection des données, devant le chiffrement des données cité par 32% des décideurs.

Au-delà, les réponses sont relativement classiques en termes de sécurité informatique mais démontrent tout de même une faible maturité des décideurs vis-à-vis de la protection des données dans le cloud (formation et sensibilisation limitée à 61% des répondants notamment).

# Le cloud de confiance privilégié pour la protection et la souveraineté

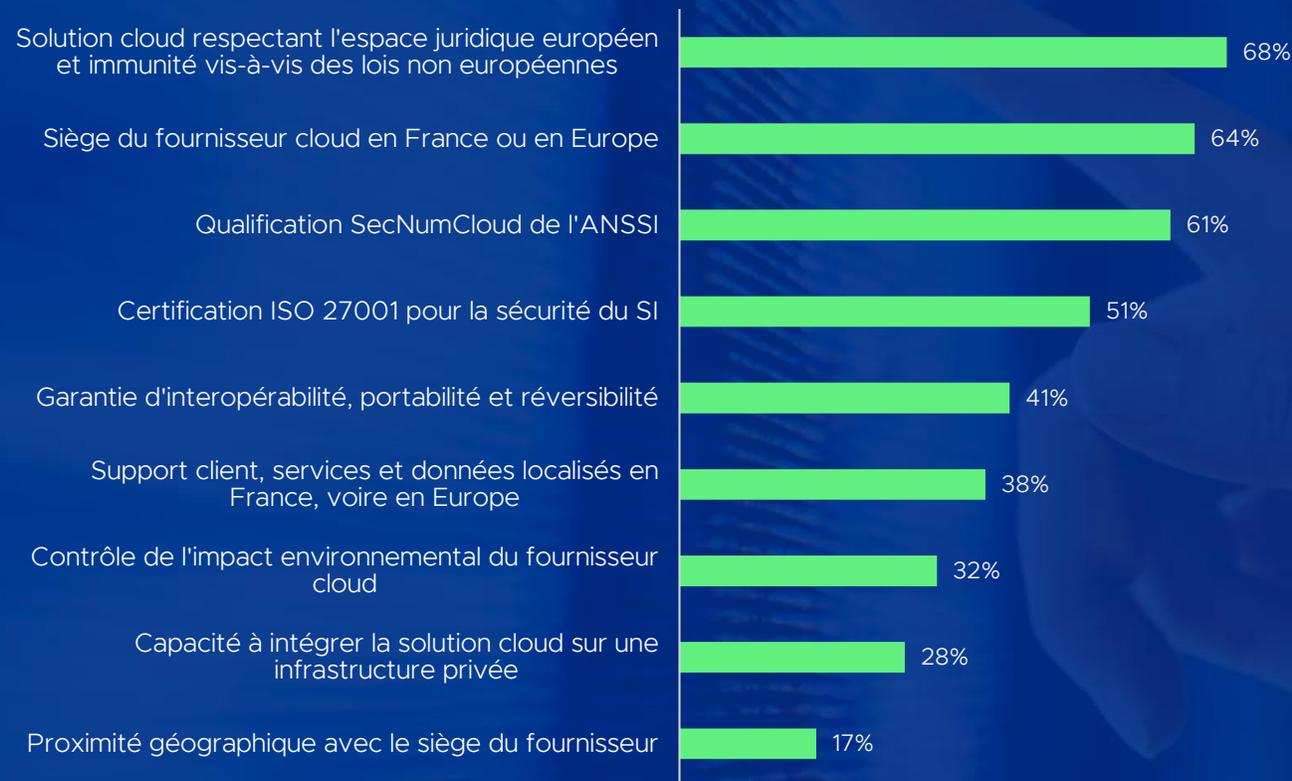
Quels sont aujourd'hui vos besoins en termes de cloud de confiance ?



Lorsqu'elles font appel ou désirent faire appel à une offre de cloud de confiance, les entreprises et organisations publiques le font principalement pour des besoins de protection et de sécurité des données ainsi que pour garantir la souveraineté et le contrôle de ces données.

# La sécurité juridique et les certifications dominent lors du choix du fournisseur

Quels sont aujourd'hui vos critères de sélection pour le cloud de confiance ?



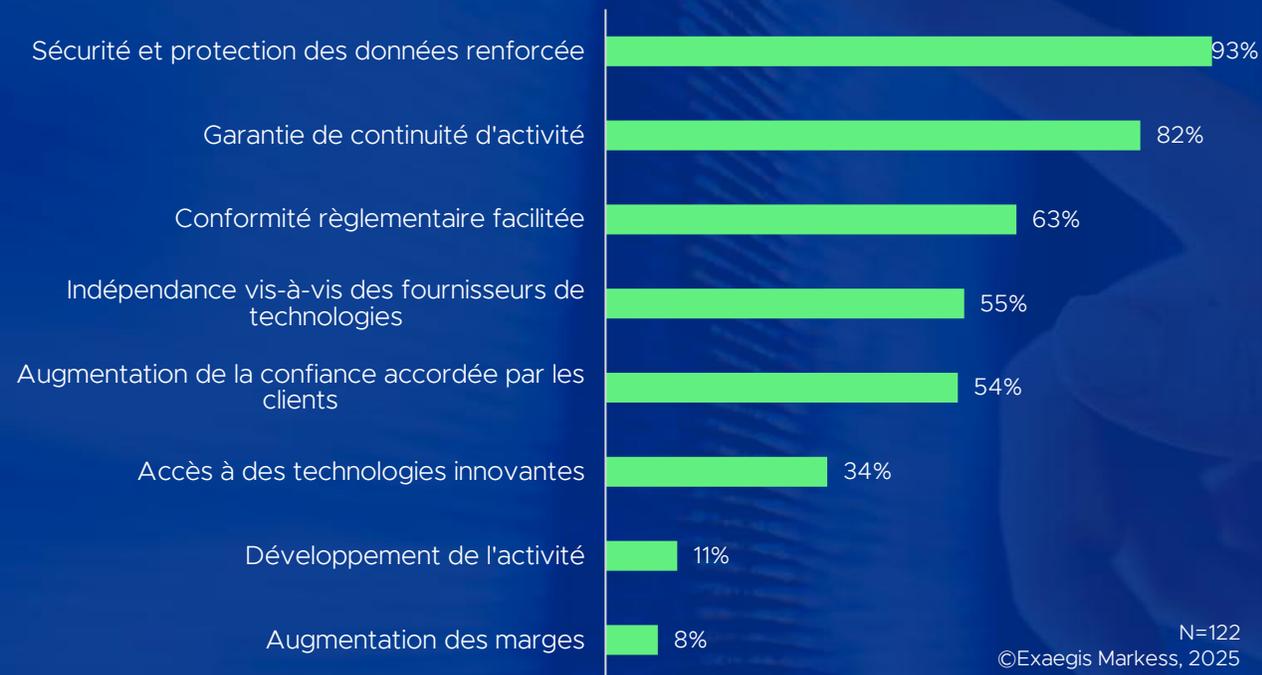
Au-delà des mesures proposées par un fournisseur de solutions cloud pour garantir la confiance (sécurité opérationnelle, cybersécurité, transparence, réversibilité et portabilité), c'est la présence européenne et l'immunité vis-à-vis des lois extraterritoriales qui développent la confiance. Les certifications et qualifications sont également des éléments forts pour sélectionner un fournisseur.

Il est enfin intéressant de noter que l'impact environnemental du fournisseur et sa transparence vis-à-vis de son empreinte participent aussi à porter la confiance.

N=122  
©Exaegis Markess, 2025

# Les avantages perçus du cloud de confiance

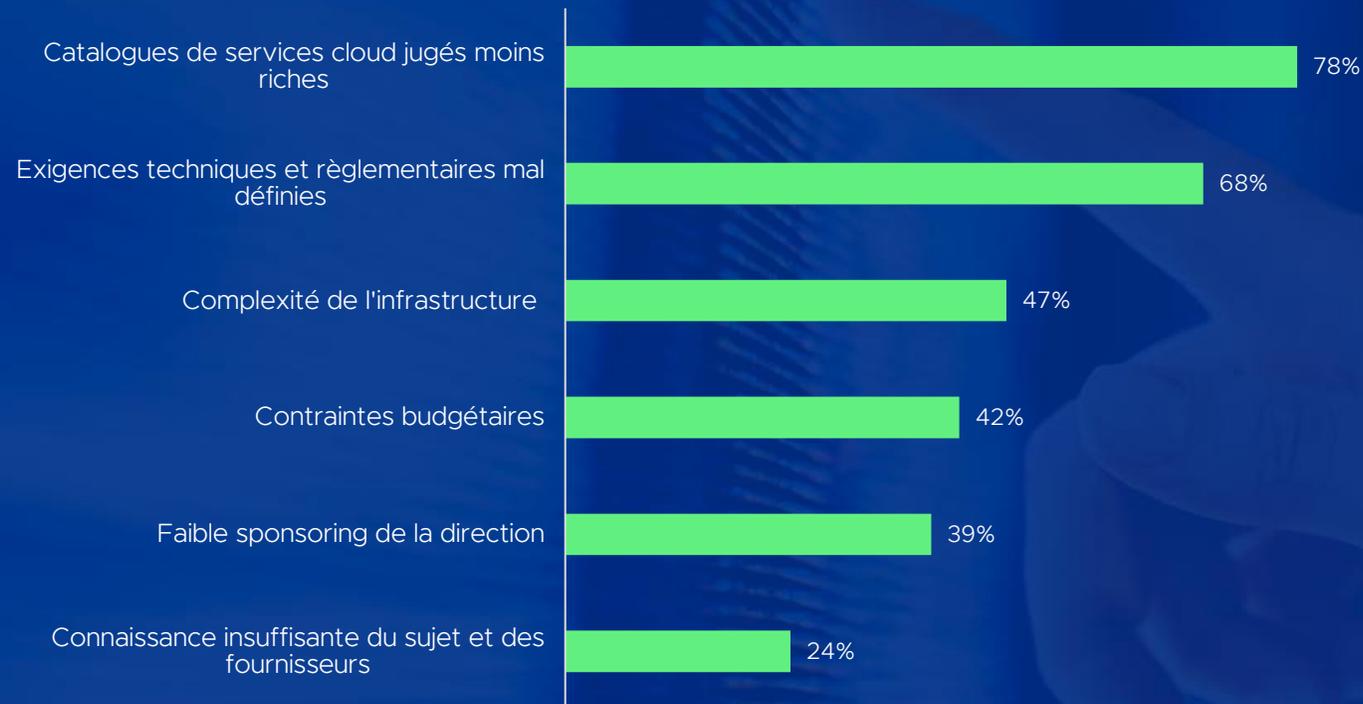
Quels sont pour vous les principaux avantages d'une solution de cloud de confiance ?



Le recours au cloud de confiance n'est pas, aujourd'hui, perçu comme un élément qui permettrait de développer l'activité, les marges ou l'innovation. Il est vrai qu'une offre de 'confiance' n'aura que peu d'impact direct sur les ventes et le développement de l'entreprise. En revanche, et comme cela est démontré dans les réponses, les solutions de confiance visent à garantir la poursuite d'activité face à des risques cyber et opérationnels. Elles facilitent également la mise en conformité règlementaire des organisations utilisatrices et in fine participent à développer la confiance dans des écosystèmes clients – fournisseurs.

# Et les freins à l'adoption

Quels sont les freins à l'adoption du cloud de confiance ?



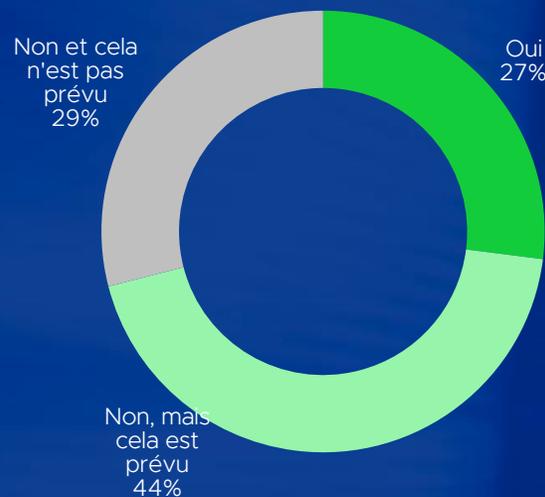
N=122  
©Exaegis Markess, 2025

« Le cloud de confiance est trop cher », une citation souvent entendue mais qui ne semble pas refléter la réalité. En effet, la contrainte budgétaire n'est citée qu'à 42% parmi les freins à l'adoption du cloud de confiance.

La plus faible richesse du catalogue de services est en revanche est vrai frein et cité à 78%. Et il est vrai que les offres de cloud de confiance, françaises et européennes, ne rivalisent pas aujourd'hui avec les services proposés par AWS, Azure et Google Cloud. Mais les toutes les données des organisations ne sont pas sensibles et il est souvent bénéfique d'avoir recours à des hyperscalers ET à un cloud de confiance.

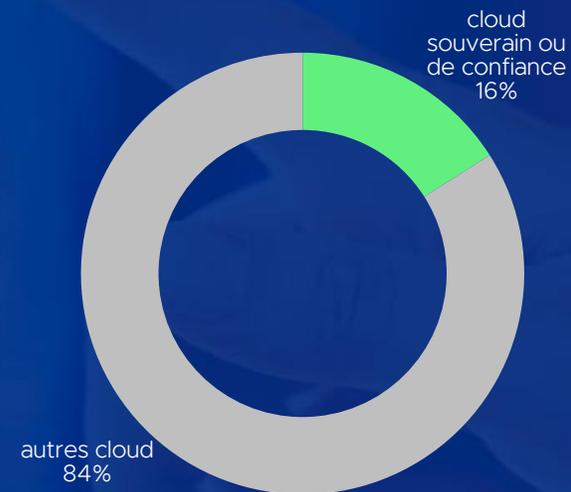
# Des budgets alloués au cloud de confiance qui restent faibles

Faites-vous aujourd'hui appel à un fournisseur de cloud de confiance ?



N=122  
©Exaegis Markess, 2025

Quelle proportion de votre budget cloud est consacré aux solutions de confiance ?



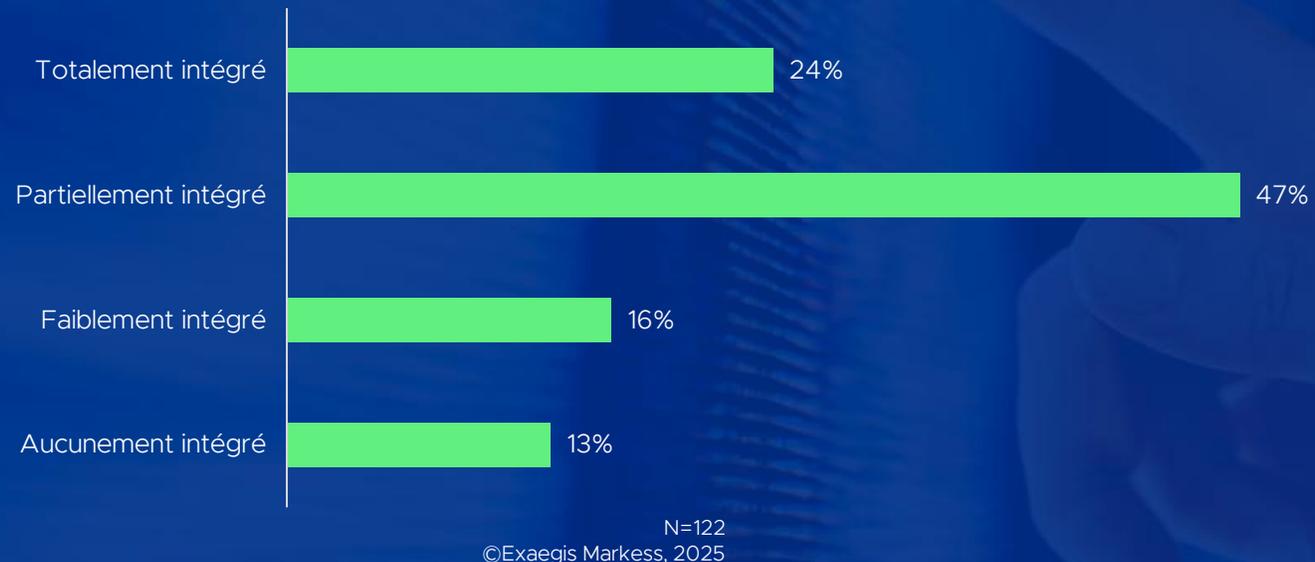
N=122  
©Exaegis Markess, 2025

Le marché du cloud privé et public en France en 2024 était de 6 milliards d'euros d'après les études Exaegis Markess. Les ventes de solutions de cloud de confiance, selon le référentiel utilisé dans l'étude étaient de 385 M€.

Le cloud de confiance serait en réalité plus proche de 6% du marché total du cloud.

# La confiance ancrée dans la stratégie numérique des organisations

De manière générale, comment le cloud de confiance s'inscrit dans votre stratégie numérique ?



Le cloud de confiance s'inscrit dans la stratégie numérique de 71% des entreprises et organisations publiques interrogées.

En effet, si les décideurs ne sont que 27% à déclarer utiliser le cloud de confiance, 56% d'entre eux souhaitent y avoir prochainement recours. En revanche, cette adoption se fera dans le cadre de stratégies de cloud hybride.

# Comment adopter le cloud de confiance



Réaliser une analyse des risques de sécurité et de conformité. Un accent sera mis sur l'analyse des risques liés aux lois extraterritoriales (en particulier Cloud Act aux USA).



Identifier et sélectionner les données et processus sensibles, critiques dans l'organisation.

Définir une stratégie de cloud hybride qui favorisera la mobilité des différents workloads et l'interopérabilité entre les clouds.



Préparer la migration vers un cloud de confiance en cartographiant les dépendances, les applications portables, la stratégie de migration, la formation des équipes.



Sélectionner un fournisseur de cloud de confiance selon ses propres critères et opérer la migration des environnements sensibles.

Identifier un prestataire d'infogérance cloud qui facilitera la gestion uniforme du cloud hybride.

# L'engouement pour le cloud de confiance doit être supporté par une harmonisation des certifications

Garantissant un très haut niveau de sécurité, la qualification SecNumCloud attire les fournisseurs de solutions cloud. Si Cloud Temple, OVHcloud et Outscale étaient précurseurs, la liste des demandes ne cesse de s'allonger avec les arrivées de Cegedim.cloud (qualifié en décembre 2024), NumSpot, Eritel, Free Pro, Orange Business, Scaleway, S3NS, Bleu et SFR Business. Ces fournisseurs souhaitent obtenir le visa leur permettant de valider la sécurité de leurs offres.

En effet, dans un contexte géopolitique très incertain et face à la prédominance des fournisseurs américains dans le domaine du cloud public, les fournisseurs nationaux aspirent à se distinguer par la confiance. En offrant un cadre de confiance, ils souhaitent attirer à eux des organisations publiques et des entreprises privées tenues de garantir la confidentialité de leurs données.

La notion de souveraineté suscite la confusion avec ses contours flous. En revanche, avec la qualification SecNumCloud, l'appellation de cloud de « confiance » ne laisse, en France, aucune place à l'ambiguïté. Mais qu'en est-il dans les autres pays européens ? Un schéma de certification européen des services cloud (EUCS) est en cours d'élaboration, avec des garanties en termes de sécurité juridique proche de la certification allemande C5 et plus faibles que SecNumCloud. Q'en sera-il de la validité de SecNumCloud dans les appels d'offres lorsque l'EUCS sera publiée ? Au-delà, est-il

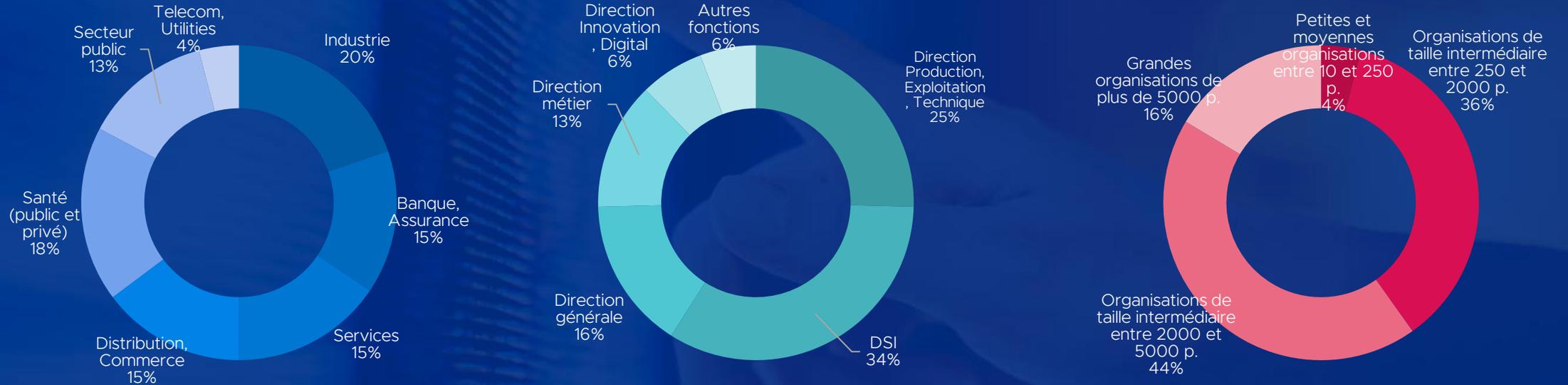
possible d'affirmer qu'un prestataire certifié HDS (Hébergeur de données de santé) et non SecNumCloud ne propose pas de solution de confiance, alors que cette certification HDS vise justement à construire un environnement de confiance autour de la Santé ?

L'analyse présentée ici démontre que le cloud de confiance est privilégié par la majorité des organisations, qu'il est intégré dans les stratégies numériques des entreprises et organisations publiques, pas seulement celles des obligés. Que ces organisations recherchent de l'immunité vis-à-vis de lois extraterritoriales, et des clouds certifiés.

Alors pour soutenir le développement du cloud de confiance, en favoriser l'accès et supporter la croissance des fournisseurs européens, la définition de la confiance dans le cloud mériterait d'être harmonisée, en France comme en Europe.

# Profils des décideurs interrogés

Enquête sur le cloud responsable menée par Exaegis Markess auprès de 122 décideurs au 1er trimestre 2025 via un questionnaire en ligne.



# Accompagner les organisations dans la construction d'un écosystème numérique sécurisé, résilient et souverain.

Avis d'expert



## Business



Comme présenté précédemment, en 2025, le marché du cloud de confiance en France et en Europe poursuit sa montée en puissance, portée par une volonté croissante des entreprises et des acteurs publics de renforcer leur souveraineté numérique. Malgré une forte intégration stratégique dans les plans de transformation digitale, l'adoption concrète reste encore limitée : selon l'étude d'Exaegis Markess, seulement 27 % des organisations déclarent utiliser des offres de cloud de confiance, alors que 71 % l'intègrent dans leur stratégie globale. Ce décalage reflète la complexité et les freins persistants à une adoption plus large.

Les motivations à privilégier ces solutions sont multiples. La sécurité juridique constitue un enjeu majeur : la qualification SecNumCloud, délivrée par l'ANSSI, garantit un haut niveau de sécurité technique, opérationnelle et juridique pour les solutions hébergées en France ou en Europe, évitant ainsi l'application de lois extraterritoriales telles que le Cloud Act américain. La maîtrise juridique et la localisation des données renforcent la confiance et la souveraineté, deux piliers essentiels pour les décideurs.

Par ailleurs, la dépendance aux géants américains du cloud, souvent perçue comme une vulnérabilité stratégique, pousse à rechercher des alternatives répondants à leurs enjeux de souveraineté. La proximité technologique, la localisation des partenariats, et la capacité à garantir la conformité réglementaire deviennent des critères clés dans la sélection des fournisseurs. La transparence sur l'empreinte environnementale et la maîtrise des certifications renforcent également la crédibilité et la durabilité des relations.



**Emmanuel Cacheux,**  
Chief Trust Officer,  
Orange Business

# Accompagner les organisations dans la construction d'un écosystème numérique sécurisé, résilient et souverain.



# Business

AVIS D'EXPERT

Dans ce contexte, Orange Business se positionne comme un acteur de référence du cloud de confiance. Notre plateforme Cloud Avenue SecNum qualifiée SecNumCloud offre une protection maximale des données, en garantissant leur hébergement dans un cadre juridique français. Nos services opérationnels, via des solutions de services managés, apportent des garanties de disponibilités de service sur mesure selon les besoins et la criticité du parc applicatif confié par le client. De plus, nous fournissons des prestations poussées en matière de monitoring, alerting et maintien en condition de sécurité (MCS). Notre approche repose également sur la capacité d'adapter le niveau de sécurité de nos solutions en fonction de la criticité des données, des processus et des ressources sensibles de chaque client, en proposant des solutions hybrides, évolutives et sur-mesure.

En conclusion, la maîtrise de la connectivité de bout en bout constitue une différenciation stratégique majeure pour Orange Business. Nous assurons la sécurité et l'intégrité des données sensibles, non seulement lors de leur stockage, mais aussi tout au long de leur transit, grâce à une gestion intégrée de la connectivité, du réseau et des partenaires locaux. Cette approche garantit une sécurité renforcée, essentielle dans un environnement où la confiance repose aussi sur la maîtrise des flux de données en transit. En combinant cette maîtrise technique avec une forte présence locale, Orange Business accompagne ses clients dans la construction d'un écosystème numérique sécurisé, résilient et conforme aux exigences de souveraineté, tout en assurant une interconnexion fluide et performante. ”



**Emmanuel Cacheux,**  
Chief Trust Officer,  
Orange Business



**exægis.**  
markess

En savoir plus :

[markess.com](https://markess.com)

[hub.markess.com](https://hub.markess.com) (freemium et abonnés)

© 2024 Markess International SAS, et/ou ses sociétés sœurs ou mères. Tous droits réservés. Exaegis Markess est une marque déposée de Markess International SAS, et de ses sociétés sœurs et mères. Cette publication ne peut être reproduite ou distribuée sous quelque forme que ce soit sans l'autorisation écrite préalable de Exaegis Markess . Elle comprend des analyses et des opinions issues de la recherche de Exaegis Markess , qui ne peuvent être interprétées comme des déclarations de fait. Exaegis Markess décline toute garantie quant à l'exactitude, l'exhaustivité ou l'adéquation de ces informations. Les recherches de Exaegis Markess peuvent aborder des sujets juridiques et financiers, néanmoins, Exaegis Markess ne saurait fournir de conseils juridiques ou financiers et ses analyses ou recherches ne doivent pas être interprétées ou utilisées comme telles. Votre accès et votre utilisation de cette publication sont régis par la politique d'utilisation de Exaegis Markess . Exaegis Markess est particulièrement soucieux de sa réputation d'indépendance et d'objectivité. Ses analyses et recherches sont produites de manière indépendante par son équipe d'analystes de recherche, sans contribution ni influence d'une tierce partie.