Le cloud de confiance

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

exægis. markess × adista

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 et peut paraître trop exigeante pour des organisations peu éduquées en la matière ou contraintes budgétairement. 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

exægis. markess

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.

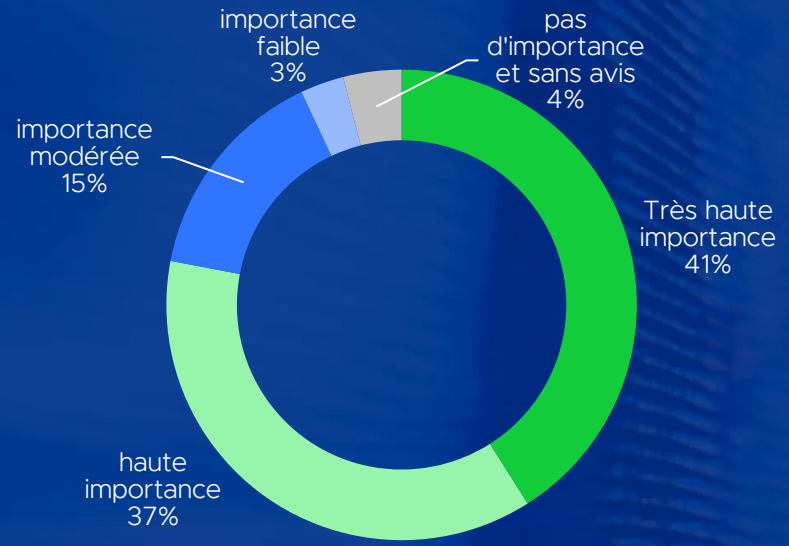
Les fournisseurs de solutions cloud pouvant intégrer ce périmètre sont aujourd'hui Adista, Aruba Cloud, Bleu, Cegedim.cloud, Cheops Technology, Claranet, Clever Cloud, Cloud Temple, Ecritel, Free Pro, Ionos, Numspot, Orange Business, Outscale, OVHcloud, S3NS, Scaleway, SFR Business et Sigma.

exægis. markess

La protection et le contrôle des données dans le cloud

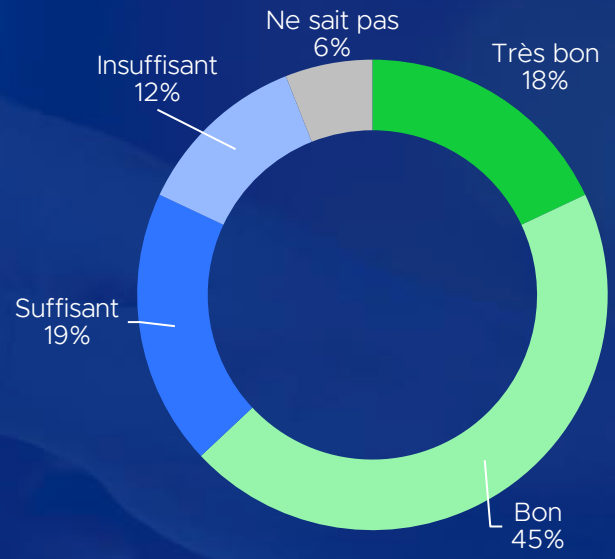
Une haute importance qui n'est pas mise en pratique

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 ?



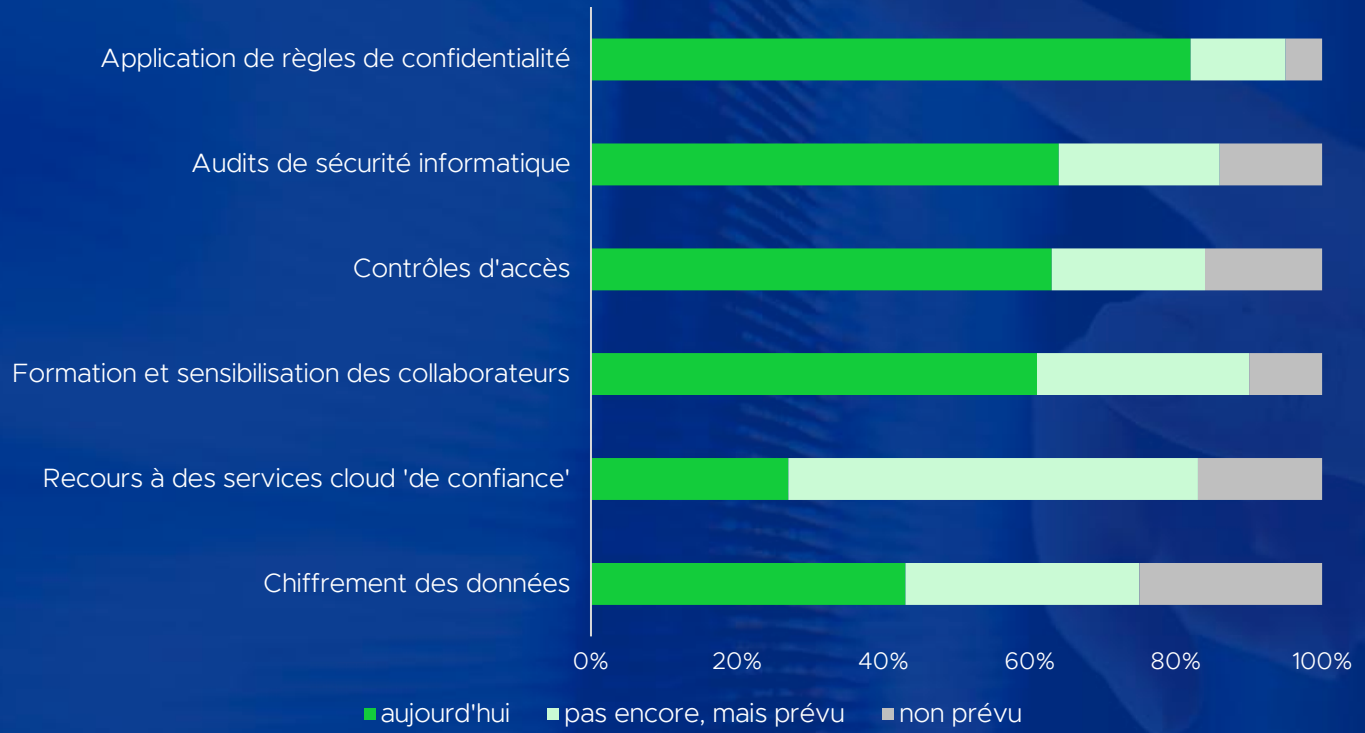
N=122
©Exaegis Markess, 2025

exægis. markess

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

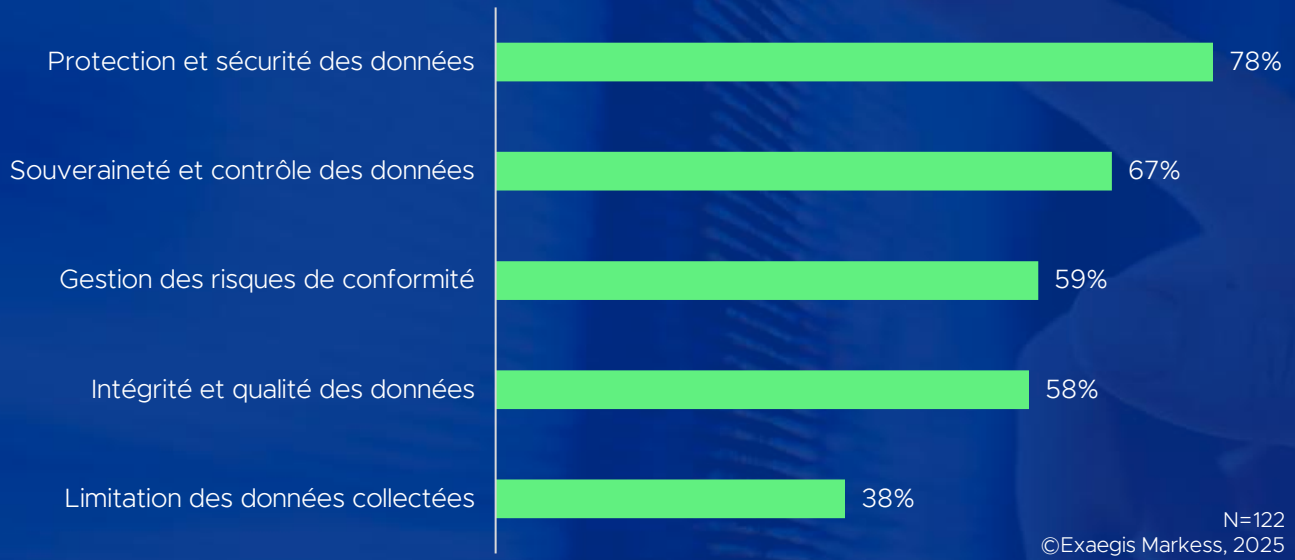
Pour 78% des répondants, la protection et le contrôle des données est un sujet de haute importance. Or, ces mêmes répondants ne sont que 18% à déclarer très bon le niveau actuel de contrôle et protection. Le recours au cloud de confiance est considéré par 56% comme une mesure permettant de renforcer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

exægis. markess

Le cloud de confiance privilégié pour la protection et la souveraineté

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



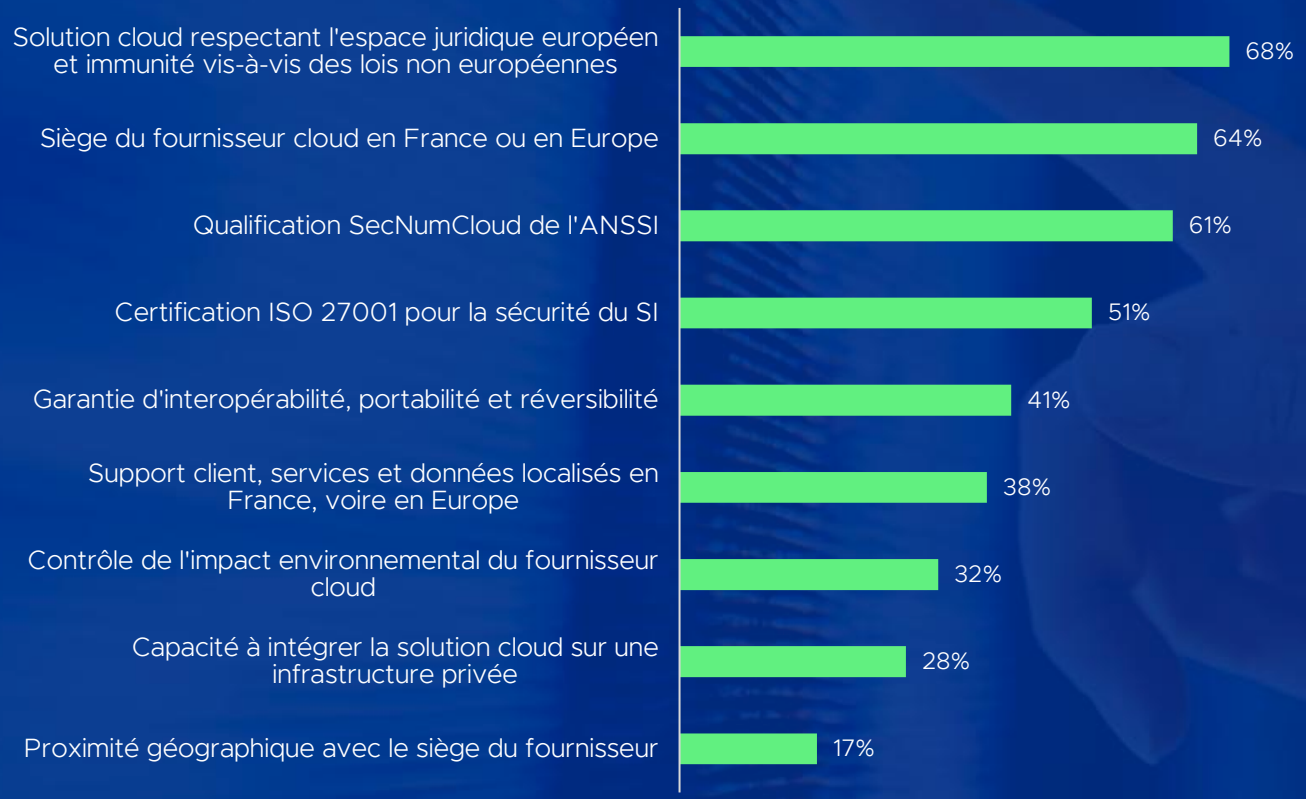
N=122

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 la garantie la souveraineté et le contrôle de ces données.

exægis. markess

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 ?



N=122

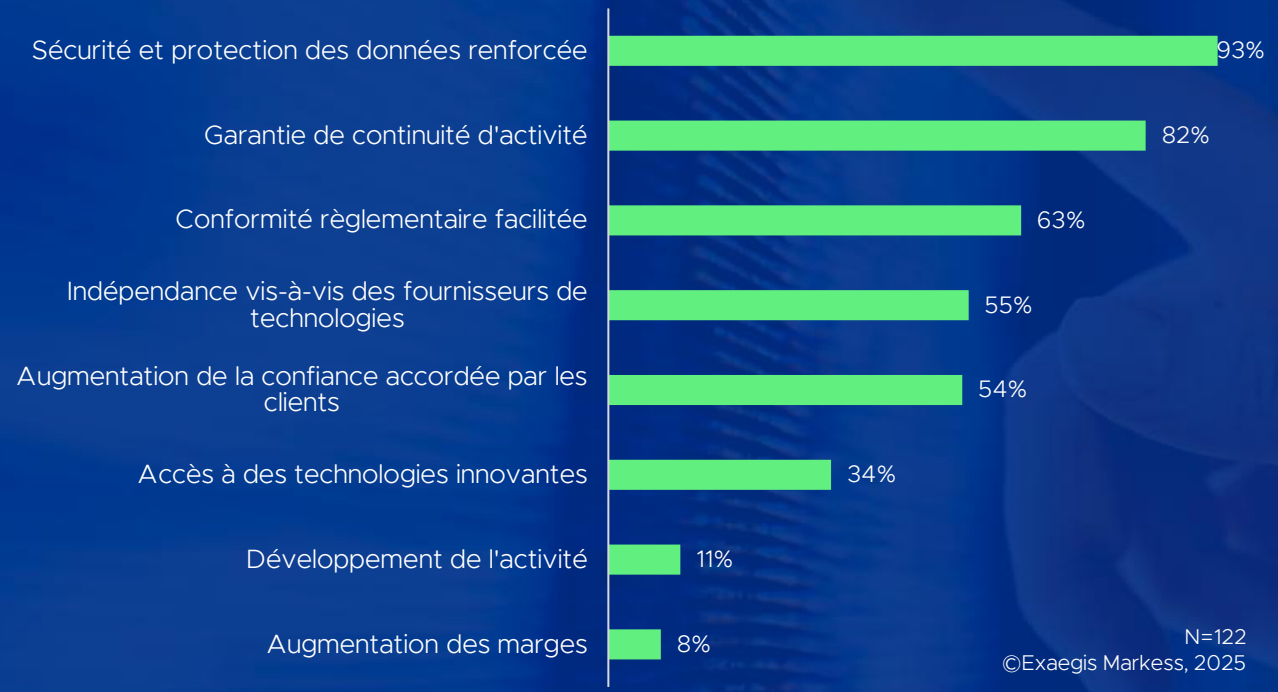
Au-delà des mesures proposées par un fournisseur de solutions cloud pour garantir la confiance (sécurité opérationnelle, cybersécurité, transparence, réversibilité et portabilité), c'est la présence européenne et l'immunité vis-à-vis des lois extraterritoriales qui développent la confiance. Les certifications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

exægis. markess

Les avantages perçus du cloud de confiance

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



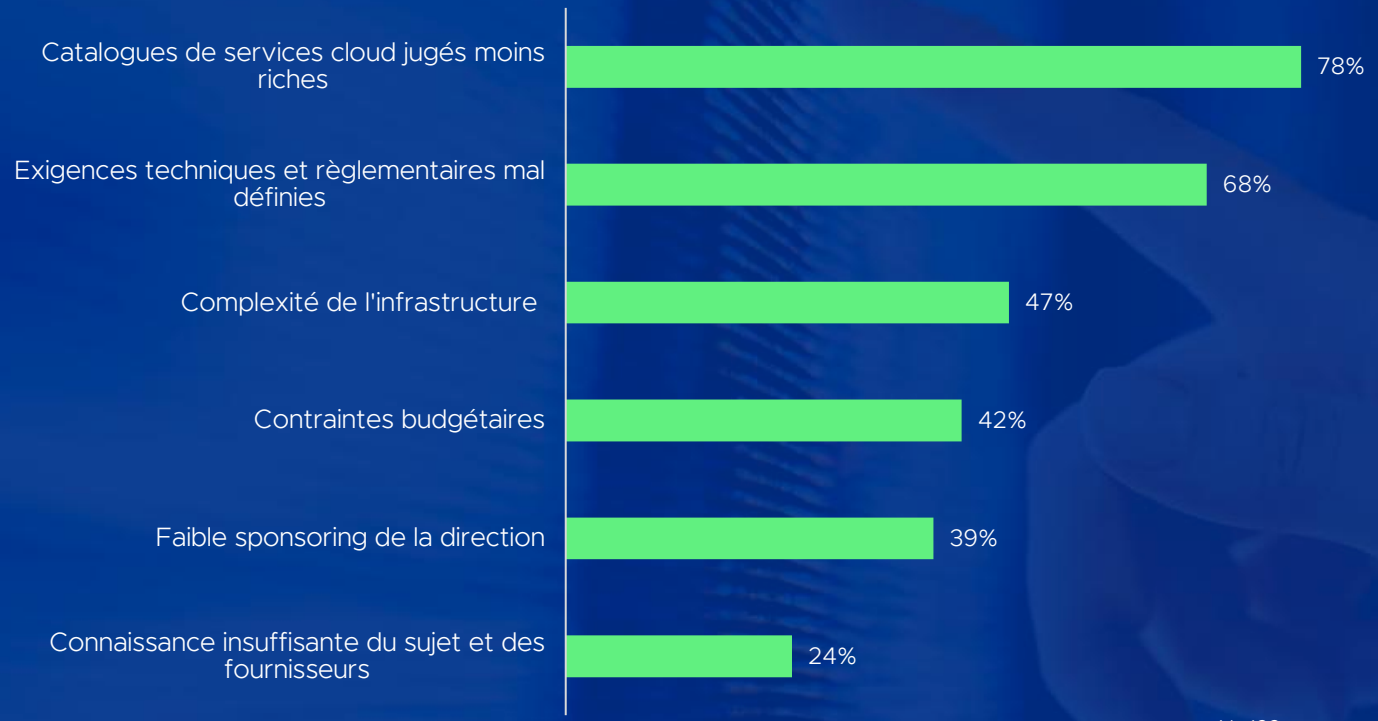
N=122

Le recours au cloud de confiance n'est pas, aujourd'hui, perçu comment 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.

exægis. markess

Et les freins à l'adoption

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



N=122

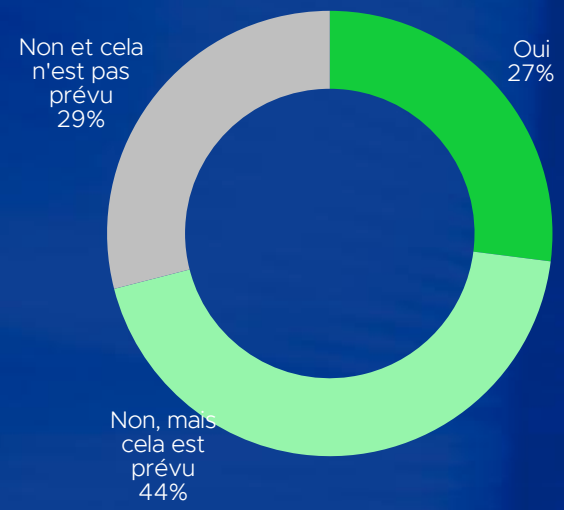
« Le cloud de confiance est trop cher », une citation souvent entendue mais qui ne semble pas refléter la réalité. En effet, la contrainte budgétaire n'est citée qu'à 42% parmi les freins à l'adoption du cloud de confiance.

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.

exægis. markess

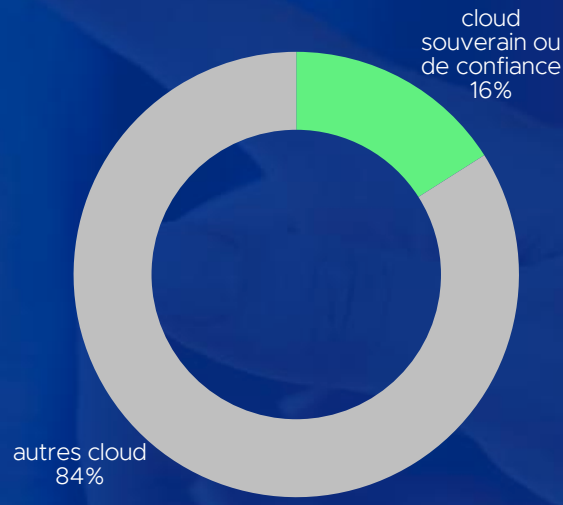
Des budgets alloués au cloud de confiance qui restent faibles

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

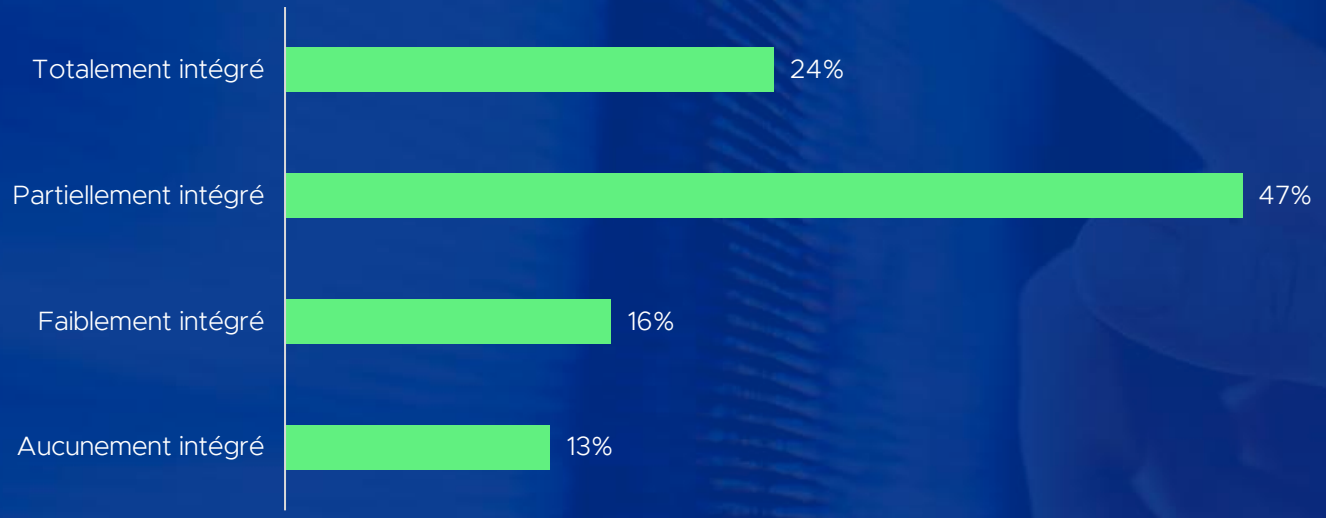
Le marché du cloud privé et public en France en 2024 était de 6 milliards d'euros d'après les études Exaegis Markess. Les ventes de solutions de cloud de confiance, selon le référentiel utilisé dans l'étude étaient de 385 M€.

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

exægis. markess

La confiance ancrée dans la stratégie numérique des organisations

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



N=122

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.

exægis. markess

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.

exægis. markess

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 , Ecritel, 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 ?

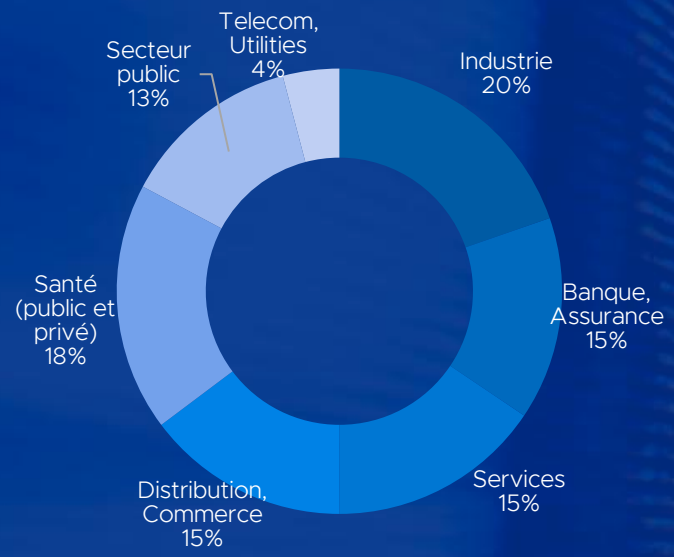
L’analyse présentée ici démontre que le cloud de confiance est privilégié par la majorité des organisations, qu’il est intégré dans les stratégies numériques des entreprises et organisations publiques, pas seulement celles des obligés. Que ces organisations recherchent de l’immunité vis-à-vis de lois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

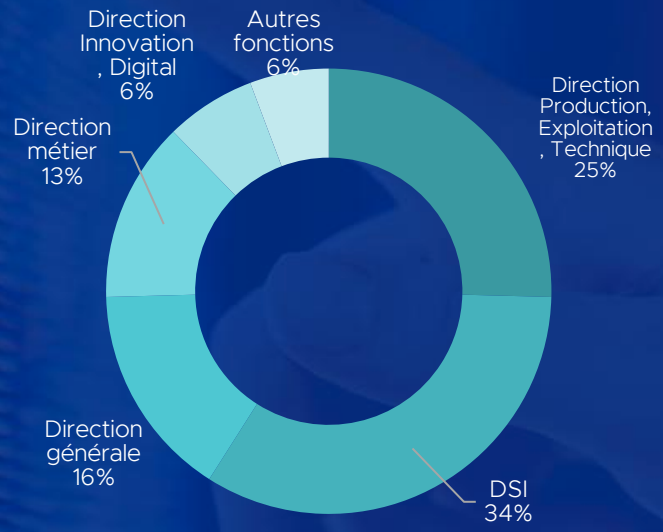
Alors pour soutenir le développement du cloud de confiance, en favoriser l’accès et supporter la croissance des fournisseurs européens, la définition de la confiance dans le cloud mériterait d’être harmonisée, en France comme en Europe.

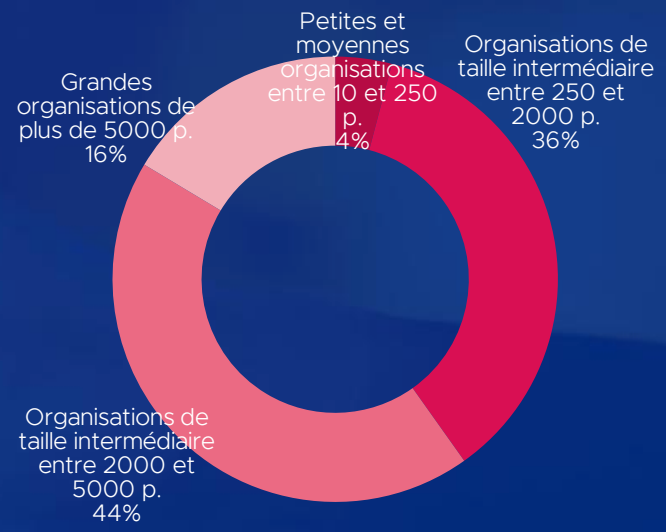
exægis. markess

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.







exægis. markess

Concilier conformité réglementaire, haute disponibilité et performance au service des métiers

Témoignage client

exægis. markess

Concilier conformité réglementaire, haute disponibilité et performance au service des métiers

CONTEXTE

KRYS GROUP est le leader incontesté du marché français de l'optique avec des enseignes connues et reconnues comme Krys, Le Collectif des Lunetiers et YOU DO, et l'un des acteurs de premier plan de l'audition avec Krys Audition.

KRYS GROUP compte aujourd'hui 10 millions de clients et plus de 1540 magasins implantés dans toute la France, mais aussi à l'international.

Coopérative d'opticiens, KRYS GROUP tire sa force de son modèle exceptionnel, en France, de distributeur-producteur. Pour anticiper les évolutions du marché et consolider sa place de leader de l'optique en France et d'acteur majeur de l'audition, KRYS GROUP a initié en 2023 un nouveau plan stratégique qui s'articule autour de 3 piliers essentiels et d'un quatrième élément : la préférence client, l'accélération de son développement, l'accélération dans l'audio et le renforcement de sa capacité de veille stratégique et d'innovation.

ENJEUX

L'IT chez KRYS GROUP est un élément central de la stratégie, et tous les outils sont développés par et pour les opticiens, notamment le logiciel métier de KRYS GROUP, Konvergence, hébergé dans les centres de données HDS d'adista.

Les enjeux sont multiples :

- Assurer la haute disponibilité des données et applications métiers pour l'ensemble des magasins KRYS GROUP en métropole et dans les DOM TOM,
- Répondre aux obligations des acteurs de la santé en s'appuyant sur un partenaire IT certifié HDS (Hébergeur de Données de Santé), et ISO27001.

Concilier conformité réglementaire, haute disponibilité et performance au service des métiers

SOLUTION RETENUE

KRYS GROUP a opté pour une solution redondée sur 2 centres de données HDS, pour héberger Konvergence, le logiciel métier du groupe, ainsi que les bases de données de la Centrale et de l'ensemble du réseau d'opticien.

Adista est certifié Hébergeur de Données de Santé de Niveau 6, ce qui représente le plus haut niveau de certification et permet de prendre en charge les sauvegardes externalisées, et donc le PRA (Plan de Reprise d'Activité) de KRYS GROUP, qui est testé une fois par an.

Un Service Delivery Manager dédié assure le suivi au quotidien des plateformes en RUN. Véritable voix du client au sein d'adista, il suit les KPIs de performance et de disponibilité, propose des actions correctives et améliorations, organise les routines mises en place avec KRYS GROUP, tels que les comités de pilotage et les CAB mensuels (Change Advisory Board).

BENEFICES

En confiant des informations sensibles et critiques comme les données de santé à caractère personnel à adista, KRYS GROUP a la garantie que toutes les mesures technico-organisationnelles sont mises en œuvre pour garantir les exigences de sécurité (DICT) du secteur de la santé : Disponibilité – Intégrité – Confidentialité des Données – Traçabilité.

KRYS GROUP s'appuie aussi sur KUMBA, Kubernetes Managé par adista, pour moderniser Konvergence et accélérer son déploiement dans un cadre réglementaire HDS.

Le respect du cadre réglementaire va de pair avec des engagements de niveau de service, que ce soit en termes de taux de disponibilité ou de performances des applications critiques de KRYS GROUP.

> « Nous avons une relation privilégiée avec adista : nous sommes en contact direct avec les DBA, ingénieurs systèmes et réseaux qui nous accompagnent au quotidien sur nos différentes demandes, et qui concernent aussi bien les nouveaux déploiements que les incidents à traiter. »

Sébastien Drouet,
Responsable Bases de Données, KRYS Group

adista En savoir plus : www.adista.fr

exægis. markess

exægis.
markess

En savoir plus : markess.com

hub.markess.com (freemium et abonnés)