



France
Digitale

Jouons collectif

Étude d'impact économique et stratégique de SecNumCloud

Date de publication : Septembre 2026

Auteurs de l'étude : Flavien Vottero et Jérémy Robiolle, Xerfi

01

Synthèse exécutive

Les messages clés de l'étude

01 | Ne pas faire de SecNumCloud l'instrument d'une politique de souveraineté

Sécurité et souveraineté ne doivent pas être confondues. **Si SecNumCloud est un outil de sécurité, il n'épuise pas à lui seul l'enjeu de souveraineté et de nos dépendances technologiques.**

C'est un outil de sécurisation utile, mais qui ne saurait constituer un instrument de politique industrielle.

02 | Un risque d'application indifférenciée dans les appels d'offres

Le recours à SecNumCloud permet de garantir la sécurité des données les plus sensibles de l'État. Le risque économique vient surtout d'une généralisation par défaut de la qualification dans les appels d'offres, y compris pour des données situées hors du champ de la loi SREN. Pour ces dernières, **une approche graduée doit être maintenue, reconnaissant d'autres moyens de sécurisation des données**, notamment le cadre de confiance dans la santé (HDS, ISO 27001).

Cela suppose une identification stricte des données réellement sensibles, des délais d'adaptation réalistes, et la reconnaissance de garanties alternatives.

Les messages clés de l'étude

03 | Un risque de choc de compétitivité pour les start-up

L'enjeu ne se limite pas à une surprime d'hébergement. Parce que les offres SecNumCloud ne sont, à ce jour, pas techniquement au niveau des besoins des start-up et scale-up les plus avancées, une migration vers une offre qualifiée entraînerait pour elles réécriture applicative, double run, revalidation réglementaire, recrutement de profils infra/cloud ops, perte d'efficience des services managés et ralentissement de la roadmap produit.

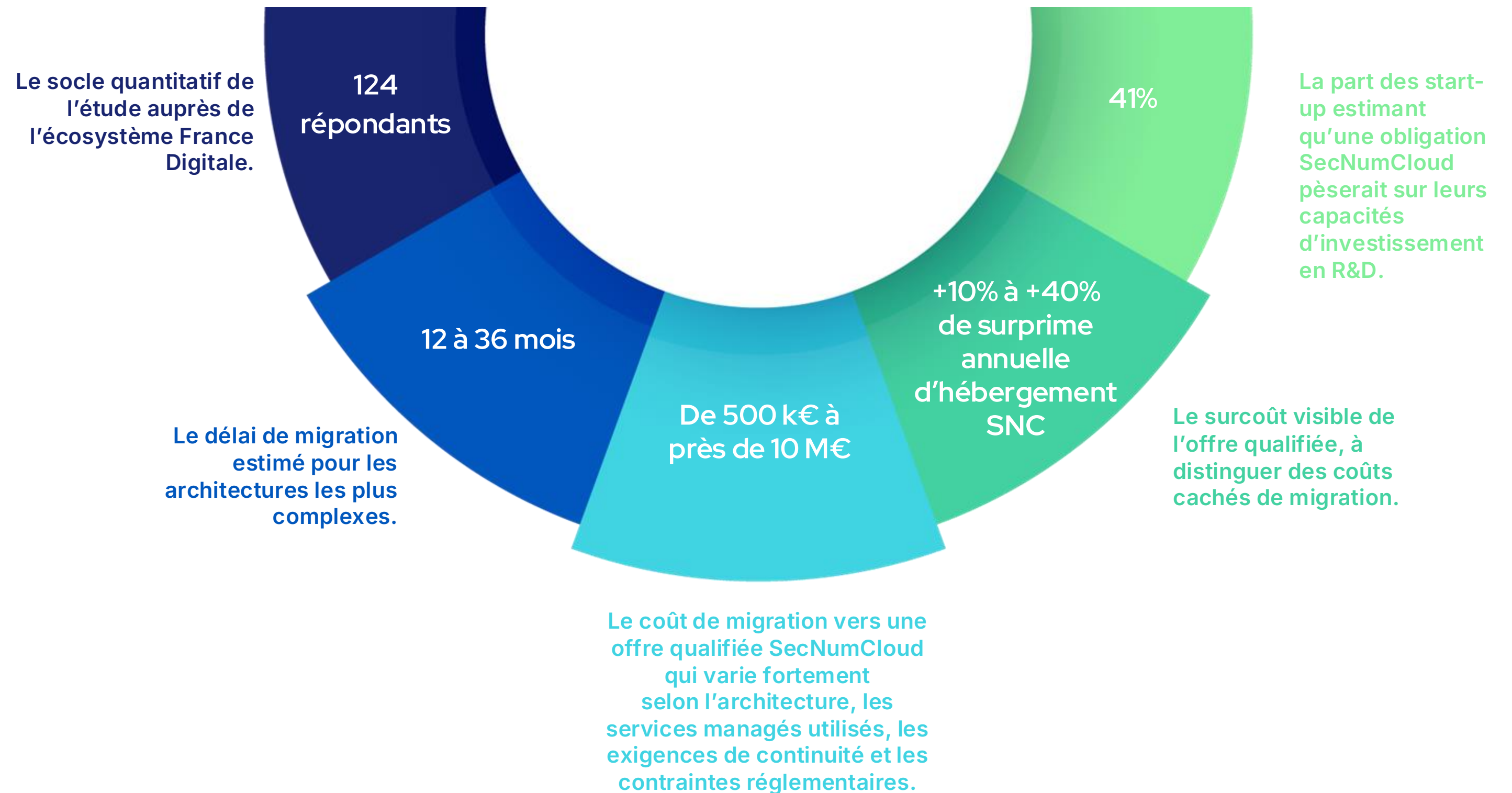
L'impact peut atteindre plusieurs millions d'euros et réduire leur capacité d'innovation, d'internationalisation et de réponse aux marchés publics.

04 | Une harmonisation européenne est indispensable

La fragmentation des certifications de sécurité en Europe fait obstacle à l'expansion de nos start-up sur le marché européen. SecNumCloud doit donc s'inscrire dans une trajectoire de convergence avec le futur schéma de certification harmonisé au niveau européen, l'EUCS.

Il en va de même pour les critères de souveraineté, qui doivent être harmonisés à l'échelle européenne via le CADA.

Les chiffres clés de l'étude



02

Contexte et méthodologie de l'étude

Face au risque d'extension de SecNumCloud, objectiver les faits

Contexte. La qualification SecNumCloud, délivrée par l'ANSSI, constitue aujourd'hui l'un des référentiels français le plus exigeant en matière de sécurité, de confidentialité et de protection contre les risques liés aux législations extraterritoriales. Inscrite dans le cadre de la loi pour sécuriser et réguler l'espace numérique (SREN, mai 2024), elle structure l'accès aux **marchés publics de l'État** lorsque des **données d'une sensibilité particulière** sont concernées.

Ne sont pas concernés : les opérateurs privés, les organismes de protection sociale, les hôpitaux...

Un risque d'extension. Des initiatives parlementaires récentes (PPL Wattebled et Uzenat) ont souhaité étendre le champ de la loi SREN à l'ensemble des marchés publics, sans considération de la sensibilité des données. La diffusion de cette exigence à la commande privée constitue un risque supplémentaire.

Une confusion entre sécurité et souveraineté. SecNumCloud est une qualification de sécurité, conçue pour les données les plus sensibles de l'Etat et les systèmes critiques, pas pour l'ensemble des besoins cloud des entreprises, aujourd'hui non couverts par les offres qualifiées. SecNumCloud n'est pas une qualification de souveraineté en tant que telle.

Enjeu. La souveraineté cloud est un objectif à poursuivre. Mais son déploiement à travers le recours à SecNumCloud est-il le plus pertinent pour atteindre cet objectif ? Ne risque-t-il pas de fragiliser les start-up, scale-up et fournisseurs cloud français ? D'autres voies sont-elles possibles ?

Promesse de l'étude. Face à cette dynamique d'expansion et forte de ses 2000 adhérents start-up et scale-up, France Digitale s'est associée à Xerfi afin d'évaluer l'impact concret du recours à une offre SecNumCloud pour ces entreprises. L'association entend ainsi contribuer à apporter des éléments utiles à la construction d'une souveraineté numérique européenne compatible avec l'innovation et la compétitivité.

Une méthodologie croisant données d'enquête, entretiens qualitatifs et analyse documentaire

01



Enquête quantitative

Une enquête administrée en juin 2026 auprès de l'écosystème France Digitale

- **124 réponses** recueillies auprès de start-up et scale-up françaises
- Profil des répondants : fondateurs, CTO, CFO, directeur affaires publiques
- Un questionnaire structuré autour de quatre axes : profil des entreprises, organisation cloud, exposition au secteur public, impacts potentiels d'une migration vers SecNumCloud.
- Des croisements réalisés par taille d'entreprise, secteur d'activité, niveau d'exposition au secteur public, fournisseurs cloud utilisés, degré de dépendance extra-européenne et niveau de maturité SecNumCloud.

02



Entretiens et contributions qualitatives

Des retours d'expérience d'une dizaine de start-up pour qualifier les mécanismes derrière les chiffres

- Contributions recueillies auprès d'éditeurs SaaS, d'acteurs exposés à des secteurs régulés et de fournisseurs cloud souverains.
- Profil des répondants : CTO, directeur des affaires publiques
- Objectif : documenter concrètement les dépendances techniques, les coûts de migration, les contraintes de double run, les limites fonctionnelles, les enjeux de co-développement et les trajectoires de transition.
- Les contributions ont été **anonymisées** et mobilisées comme preuves transversales, sans présentation nominative d'entreprises.

Une étude empirique d'impact

Cette étude réalisée par Xerfi et commanditée par France Digitale vise à documenter les impacts économiques, techniques et stratégiques potentiels de SecNumCloud à partir des pratiques réelles et des stratégies mises en œuvre par les start-up et scale-up interrogées.

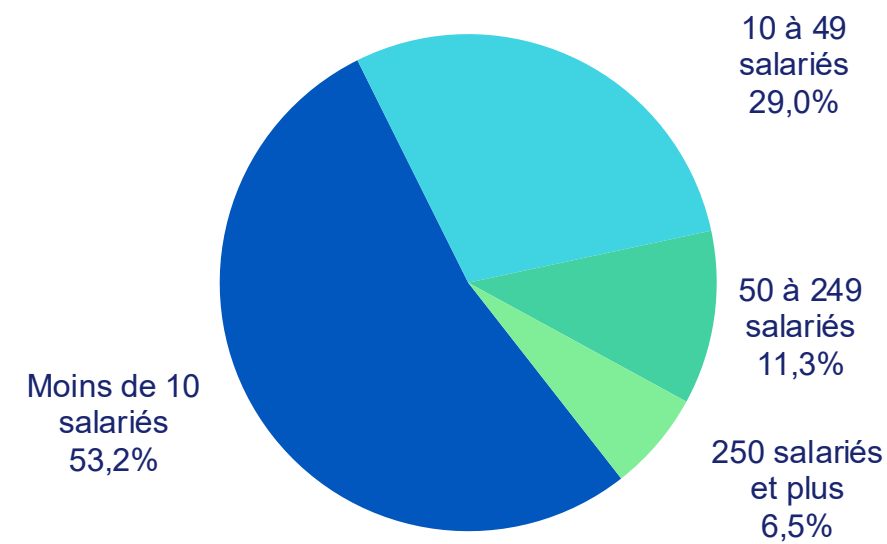
Elle privilégie une approche empirique croisant enquête quantitative, retours d'expérience, entretiens approfondis et analyse documentaire. Les résultats déclaratifs permettent d'identifier des mécanismes, des profils d'exposition et des ordres de grandeur.

Ils n'ont pas vocation à produire une extrapolation statistique de l'impact de SecNumCloud à l'ensemble des start-up françaises, ni à établir un chiffrage macroéconomique global. Les estimations prospectives doivent être interprétées comme des scénarios déclarés par les entreprises dans les conditions techniques et réglementaires observées au moment de l'enquête.

Un panel reflétant la diversité de l'écosystème France Digitale

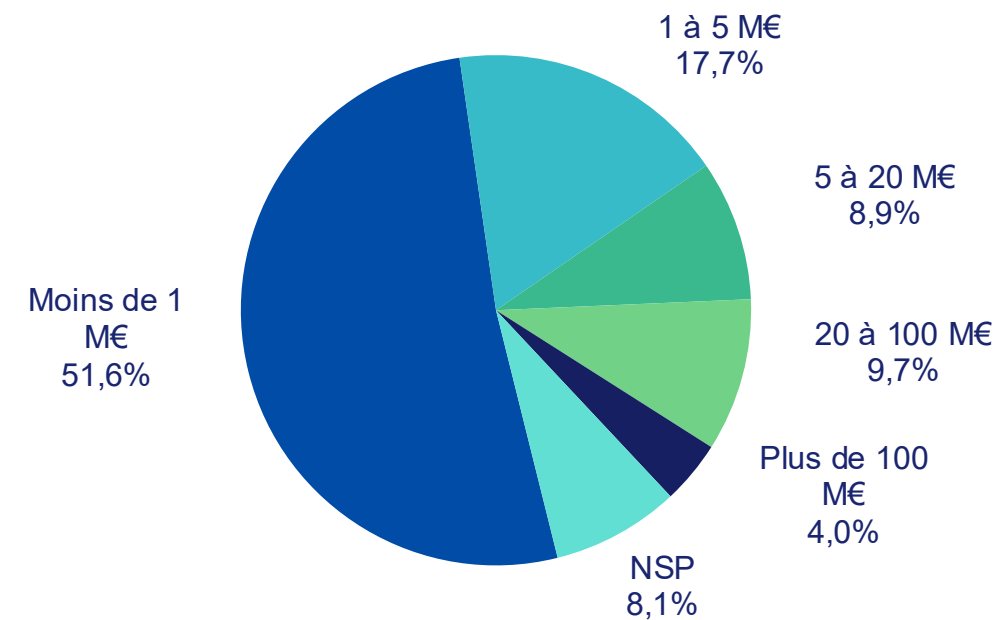
01

Effectifs



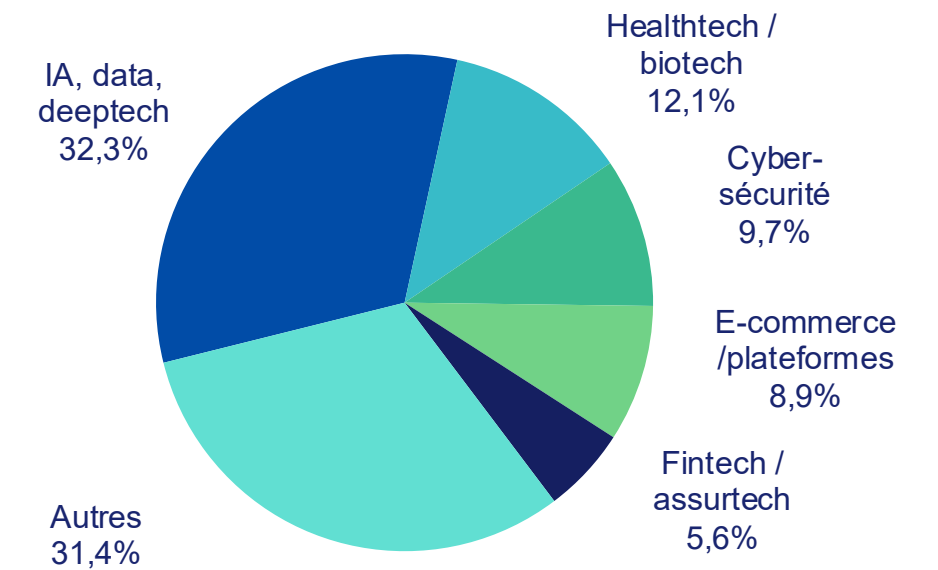
02

Chiffre d'affaires consolidé



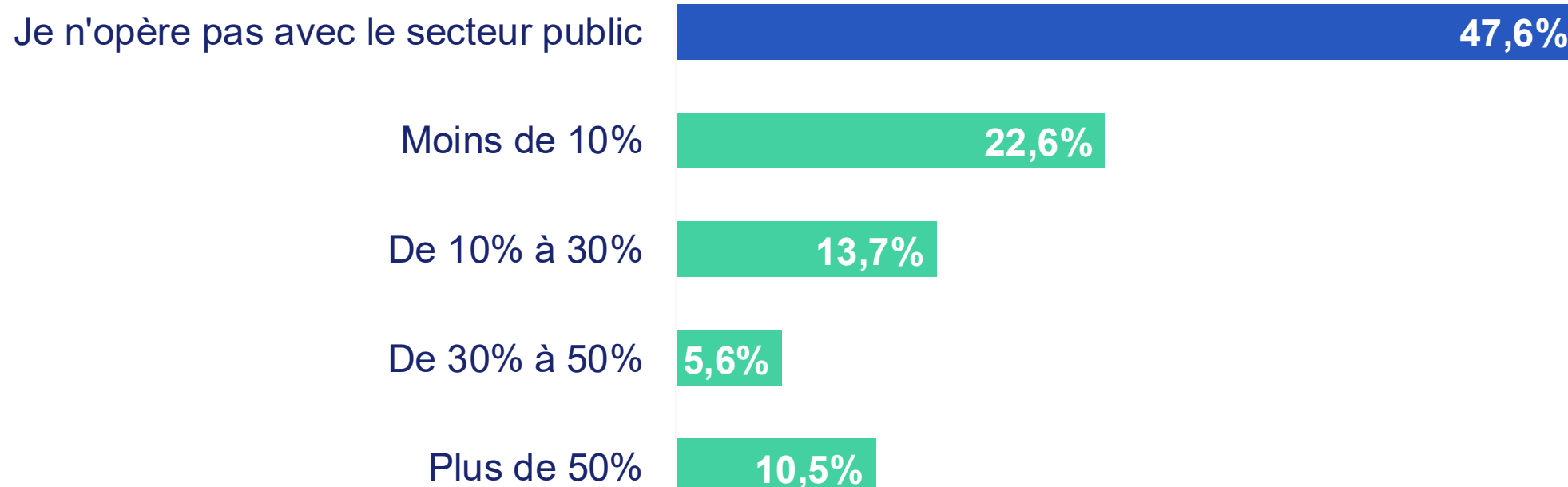
03

Secteur d'activité principal



L'exposition publique est suffisamment large pour transformer une exigence SNC mal calibrée en choc de marché

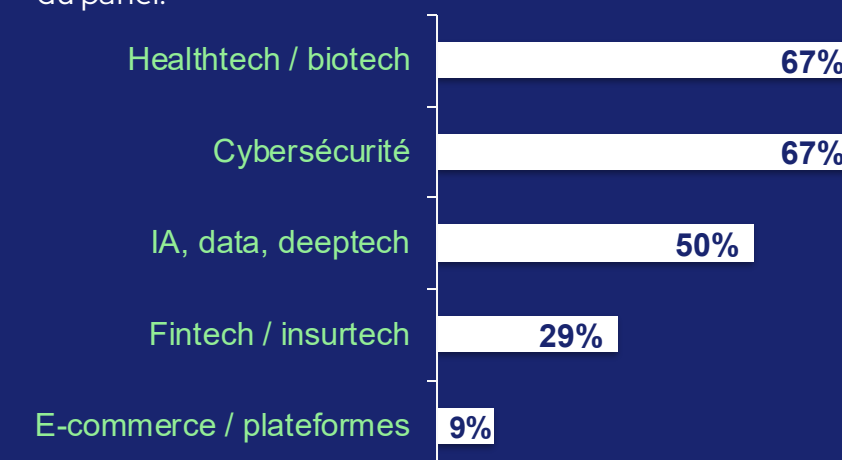
Quelle part de votre chiffre d'affaires consolidé est réalisée avec des clients publics ou parapublics en France ?



Une application contractuelle trop extensive de la loi SREN pourrait générer des effets économiques significatifs, mais très différenciés selon les profils de start-up, notamment si les acheteurs publics généralisent SecNumCloud au-delà des données sensibles visées par la loi.

Le taux de dépendance au secteur public selon la spécialisation

Note : poids du secteur public dans le chiffre d'affaires France des start-up du panel.

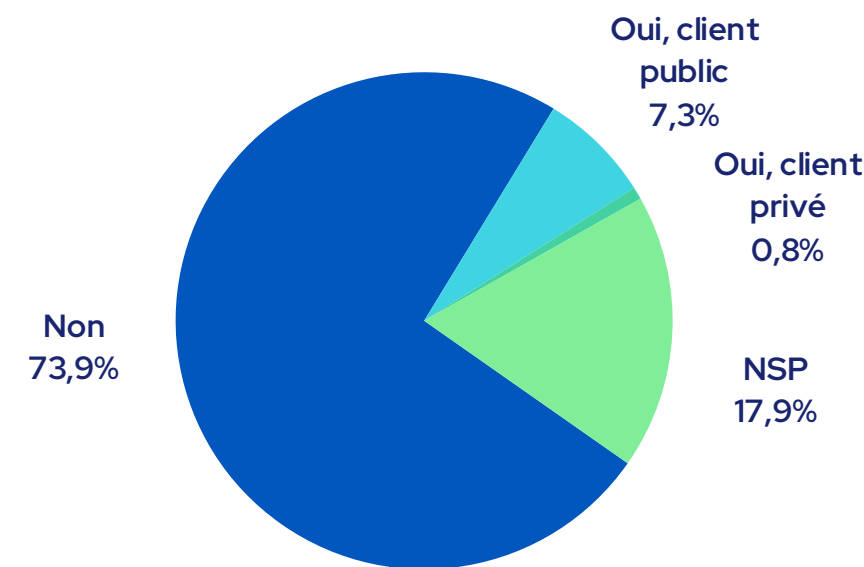


SecNumCloud ne crée pas un risque homogène pour tout l'écosystème

Il crée un risque concentré sur les start-up dont l'accès au marché dépend de clients publics, parapublics ou régulés (notamment les healthtech interrogées dans le cadre du panel) et un risque latent pour les autres si les clauses de confiance se diffusent par capillarité dans les appels d'offres privés.

Un signal commercial encore étroit, mais qui se durcit par poches

Au cours des 12 derniers mois, avez-vous perdu un contrat ou une opportunité commerciale parce que le client exigeait explicitement un hébergement sur un cloud souverain / cloud de confiance ?



Nature de l'exigence formulée en cas d'opportunité perdue
(taille proportionnelle au nombre d'occurrences de la réponse)

Sans fournisseur américain (AWS, Azure, GCP)

Recours à une offre SecNumCloud

Hébergement en Europe

Hébergement en France



Ce que montre le sondage

Le signal commercial SecNumCloud / souveraineté reste encore étroit : seuls 7,3% des répondants déclarent avoir perdu une opportunité avec un client public pour ce motif, mais quand cette perte existe, l'exigence SecNumCloud est bien le facteur dominant.



Ce que disent les entretiens

La demande client reste hétérogène. Hors cas sensibles, les exigences portent surtout sur l'hébergement en France, le HDS, le RGPD renforcé, le chiffrement ou l'absence de Cloud Act, davantage que sur SecNumCloud explicite. Les start-up répondent généralement en documentant leurs garanties de sécurité, de localisation et de continuité de service. La pression se renforce toutefois dans la santé (établissements hospitaliers, ARS, etc.). Elle reste plus faible dans le privé et dans plusieurs marchés publics, où d'autres critères (coût, performance, intégration au SI, continuité, voire RSE) peuvent encore primer.

SecNumCloud n'est pas encore une demande de marché généralisée. Il s'agit d'une exigence émergente, concentrée sur certains acheteurs publics et secteurs sensibles, mais susceptible de devenir problématique si elle se diffuse sans gradation.

03

SecNumCloud : mythes
et réalités d'une qualification
de sécurité (et non de
souveraineté)

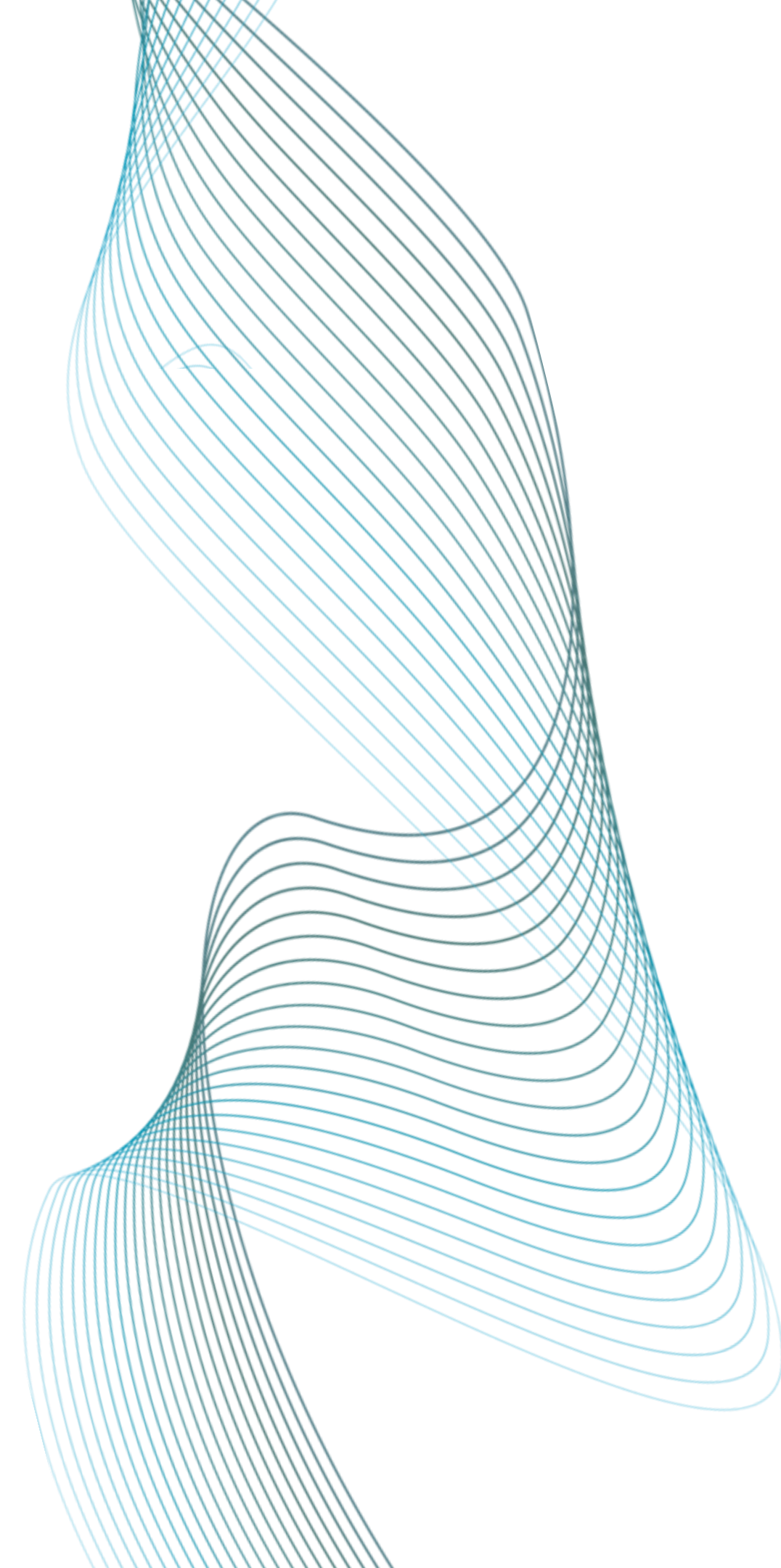
SecNumCloud, qu'est-ce que c'est ?

Définition. Une qualification délivrée par l'ANSSI pour une offre donnée (et non l'ensemble d'un opérateur cloud), pour une durée de 3 ans, selon un référentiel avec plus de 360 exigences.

Une qualification de souveraineté limitée. Pour obtenir la qualification sur une offre, un hébergeur doit être de droit européen : capital protégé contre les prises de contrôle non européennes (max 24 % pour un acteur non-UE, 39 % collectivement); aucun transfert de données hors UE; autonomie d'exploitation garantie.

Les offres hybrides : la question de la dépendance non résolue. Le seuil des 24 % permet à des joint-ventures comme Bleu (Capgemini-Orange et Microsoft) et S3NS (Thales et Google) de viser la qualification tout en s'appuyant sur des technologies américaines (Azure pour Bleu, Google Cloud pour S3NS). SecNumCloud garantit l'autonomie d'exploitation, pas l'indépendance de la technologie elle-même

Un outil de politique industrielle en trompe-l'œil. Si les acteurs souverains du cloud, premiers à avoir obtenu la qualification, ont pu bénéficier d'un accès privilégié à la commande publique pour les données dans le champ de la loi SREN, ceux-ci se trouvent directement concurrencés par les offres hybrides. Ces dernières sont souvent plus attractives pour les scale-up d'ores et déjà hébergées chez des hyperscalers (réduction du coût de réarchitecture, limitation des risques opérationnels...). L'effet d'entraînement pour les fournisseurs cloud français s'en trouve d'autant plus limité.



Des exigences cloud encore confuses : cloud de confiance, souveraineté et sécurité se mélangent

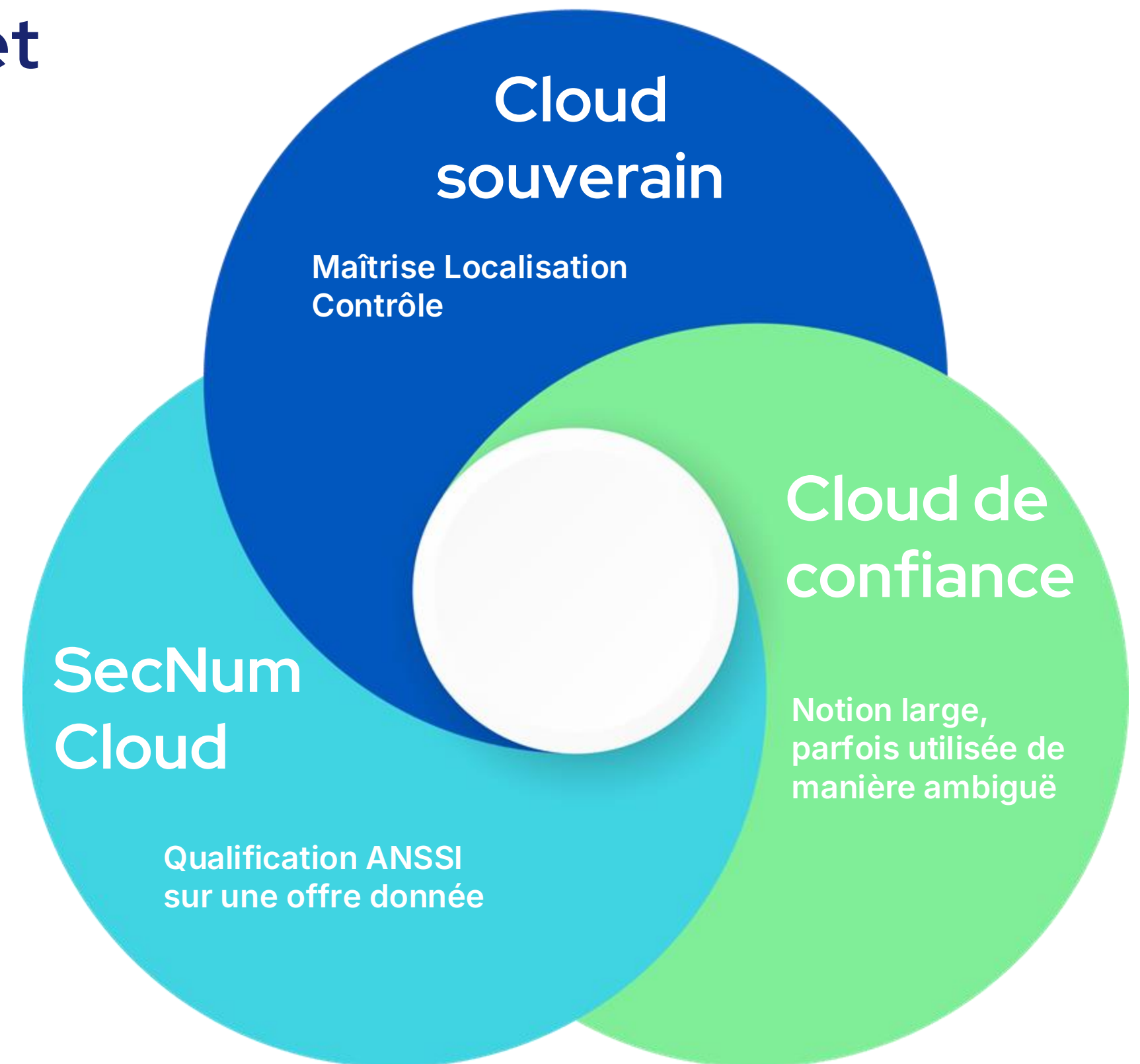


Ce que disent les entretiens

Les entretiens montrent une forte hétérogénéité des demandes clients : "hébergement en France", "cloud souverain", "pas de fournisseur américain", "HDS", "RGPD renforcé", "SecNumCloud" ou "cloud de confiance" sont souvent employés comme des notions interchangeables. Cette confusion brouille les objectifs poursuivis : sécurité opérationnelle, protection contre les lois extraterritoriales, maîtrise technologique, continuité d'activité ou préférence économique européenne.

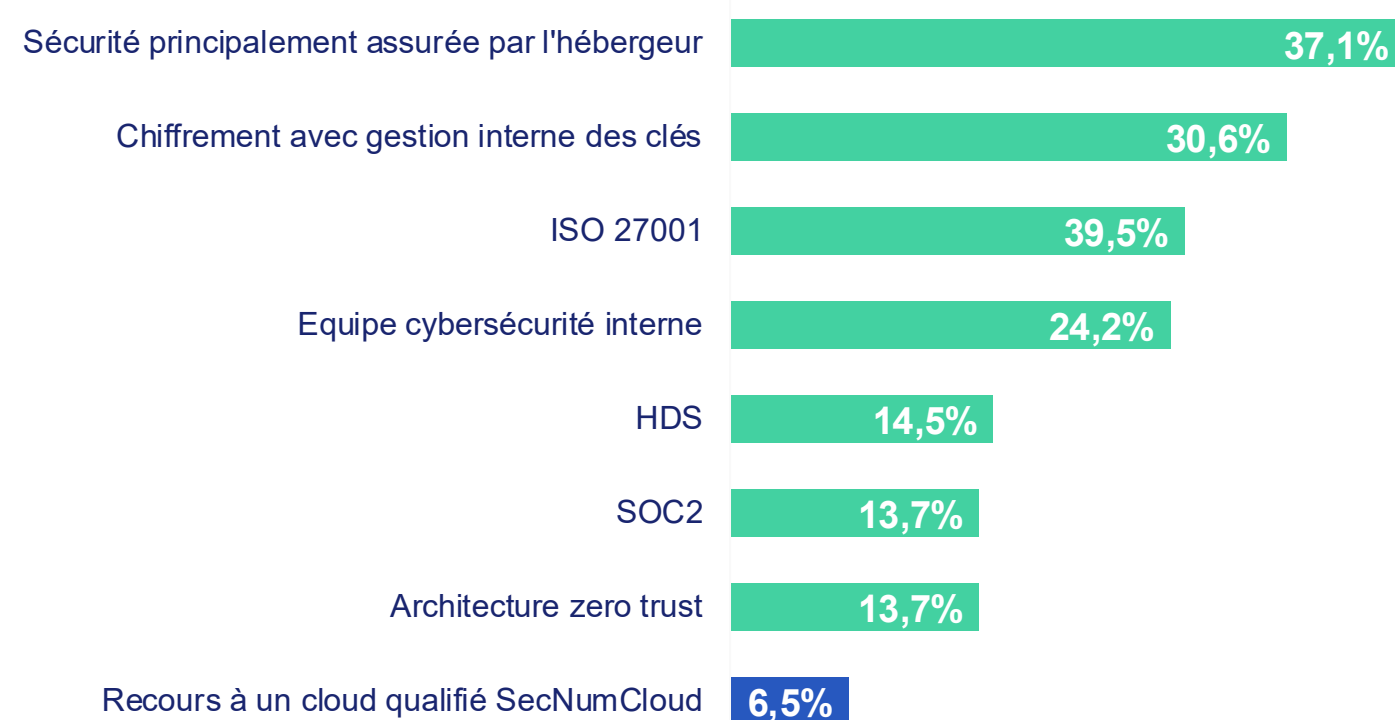
SecNumCloud est un outil de cybersécurité, mais ne peut constituer une politique industrielle en tant que telle.

La souveraineté cloud peut aussi reposer sur d'autres leviers : localisation des données, chiffrement, maîtrise des clés, réversibilité et recours à des offres européennes (dites souveraines) non qualifiées SNC.



Une solution de sécurité... parmi d'autres

Parmi les options suivantes, lesquelles s'appliquent à vos pratiques en termes de sécurité des systèmes et données ?
(plusieurs réponses possibles)



Ce que montre le graphique

Les start-up mobilisent déjà plusieurs leviers de cybersécurité au-delà du choix de l'hébergeur : ISO 27001, chiffrement avec gestion interne des clés, équipes cyber internes, HDS, SOC2 ou architecture Zero Trust. Le recours à un cloud qualifié SecNumCloud reste minoritaire dans le panel, ce qui ne signifie pas une absence de sécurité, mais une autre combinaison de dispositifs techniques, organisationnels et contractuels.

SecNumCloud apporte une garantie forte sur l'environnement cloud qualifié, mais il ne couvre pas l'ensemble du risque cyber. Les start-up mobilisent déjà d'autres leviers de sécurité : ISO 27001, HDS, SOC2, chiffrement avec gestion interne des clés, équipes cyber internes ou architecture Zero Trust. La sécurité effective dépend donc moins d'un seul label que d'une combinaison de dispositifs techniques, organisationnels et opérationnels.

Une start-up non hébergée sur SecNumCloud peut déjà disposer d'un niveau élevé de maturité cyber. Réduire la cybersécurité à la qualification de l'hébergeur déplacerait le débat de la réduction effective des vulnérabilités vers une logique de conformité formelle.

Souveraineté cloud et SecNumCloud : deux réalités à ne plus confondre



Souveraineté et SecNumCloud sont deux notions distinctes qui ne peuvent pas être traitées comme un seul et même sujet. La confusion entre les deux notions conduit à des raccourcis analytiques qui faussent le diagnostic et, in fine, les décisions publiques.

La souveraineté recouvre des enjeux de protection des données, de maîtrise technologique et de maîtrise opérationnelle. SecNumCloud est avant tout un référentiel de sécurité, comportant des milliers de critères techniques, qui n'intègre qu'une poignée de critères souverains. Il s'agit de deux périmètres, deux niveaux d'exigence, deux réalités de marché.

La souveraineté n'est pas structurellement synonyme de surcoûts. Cette assimilation est inexacte et constitue un frein majeur à l'adoption. Le surcoût réel est celui de la qualification SecNumCloud, qui s'explique par le niveau de sécurité exceptionnel qu'elle impose, et non par la souveraineté en tant que telle.

Verbatim issu d'un entretien réalisé avec un hébergeur souverain

04

Mesure d'impact du recours
à SecNumCloud : une offre
technologique limitée

SecNumCloud : une offre technologique limitée

SecNumCloud n'est pas encore prêt pour les usages avancés. Bien que les offres qualifiées progressent rapidement, elles ne couvrent pas, à périmètre fonctionnel constant, toutes les briques nécessaires aux start-up cloud-native (services managés, KMS, IAM, recherche, IA/GPU ou traitement temps réel). Une obligation trop rapide risquerait de précéder l'industrialisation du marché.

Le choix des offres correspond à un arbitrage technique. Les fournisseurs cloud sont d'abord et avant tout choisis pour leur performance, la richesse fonctionnelle et le time-to-market. L'accès rapide à des services managés, à des environnements data/IA, à des niveaux élevés de disponibilité et à des dispositifs de sécurité opérationnelle difficiles à reconstituer en interne, s'avère souvent décisif.

La maturité technologique accroît l'adhérence cloud. Plus une start-up est mature, plus son architecture est optimisée, automatisée et imbriquée dans des services avancés. Cette maturité augmente la performance industrielle de l'entreprise, mais rend aussi la migration vers une offre qualifiée plus complexe.

Une dépendance pilotée, mais rarement totalement réversible. Les start-up ne sont pas passives face au risque cloud ; elles arbitrent, documentent et sécurisent. Mais la capacité à changer de fournisseur dépend moins d'une décision stratégique que de la disponibilité effective d'équivalents techniques, économiques et réglementaires.

Une offre SecNumCloud qui existe, mais peu profonde sur les briques cloud avancées

Le marché qualifié est en croissance, mais reste concentré sur quelques familles de services, loin de la profondeur fonctionnelle des hyperscalers.

De plus en plus de services qualifiés

En mars 2026, le catalogue de l'ANSSI recensait 17 services d'informatique en nuage qualifiés SecNumCloud, proposés par 10 fournisseurs et couvrant désormais plusieurs catégories de services cloud.

Scaleway vise une première offre SecNumCloud au S2 2026, d'abord centrée sur l'IaaS puis élargie aux PaaS et services cloud-native. Cette trajectoire peut réduire l'écart avec les hyperscalers, sous réserve de qualification effective des briques avancées.

OVH vient d'annoncer la qualification d'une troisième offre : SNC Cloud Platform (offre de cloud public de confiance).

Numspot a quant à elle obtenu sa première qualification SNC, après avoir obtenu la certification ISO 27001 ainsi que la certification HDS.

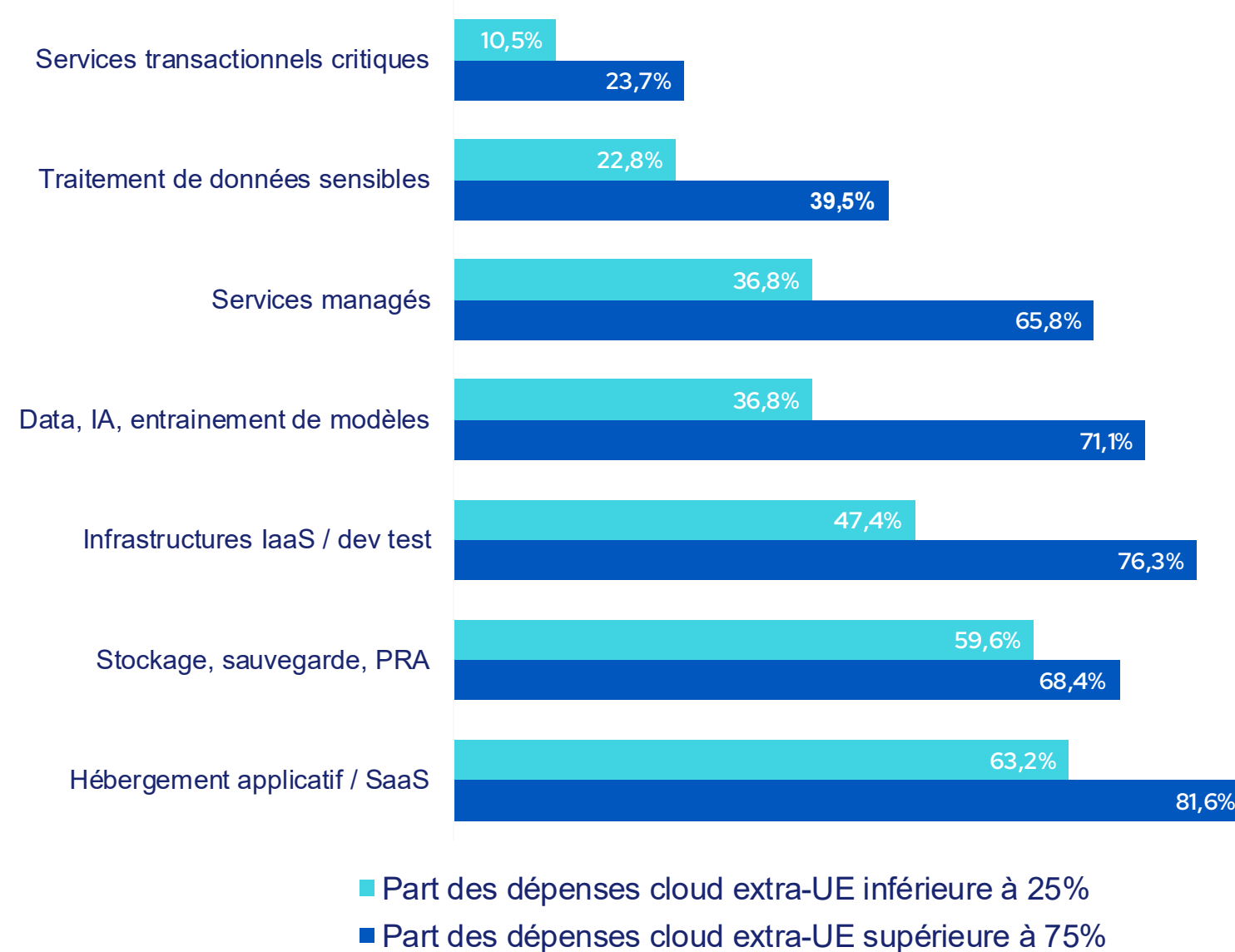
Mais la couverture fonctionnelle reste limitée

L'offre qualifiée répond déjà à certains besoins standards : hébergement applicatif, cloud privé, stockage, sauvegarde, collaboration sécurisée, services métiers. Elle ne peut cependant couvrir les briques les plus critiques pour les start-up cloud-native : services managés, bases de données avancées, KMS, streaming, IoT, observabilité, recherche, IA/GPU.

L'enjeu n'est pas l'absence d'offre SecNumCloud, mais celui de son inadéquation aux architectures start-up et scale-up. Pour les usages standards, des solutions existent déjà. Pour les scale-up fortement utilisatrices des services managés, la question porte moins sur l'hébergement que sur la disponibilité de briques équivalentes, qualifiées et industrialisées.

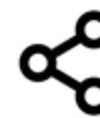
Les briques cloud avancées sont un levier de scalabilité, de sécurité et de time-to-market

Pour quels usages principaux recourez-vous au cloud ?
(plusieurs réponses possibles)



Ce que montre le graphique

Les usages cloud les plus avancés (IA/data, GPU, services managés, traitements critiques, stockage complexe ou infrastructures de scalabilité) sont davantage associés aux hyperscalers.



Implication

Le verrou n'est pas seulement l'hébergement des données. Il réside dans l'accès aux briques qui font fonctionner le produit : bases managées, KMS, observabilité, streaming, recherche, IoT ou GPU. Une trajectoire souveraine crédible doit donc porter sur la disponibilité de ces services, pas uniquement sur la localisation des serveurs.



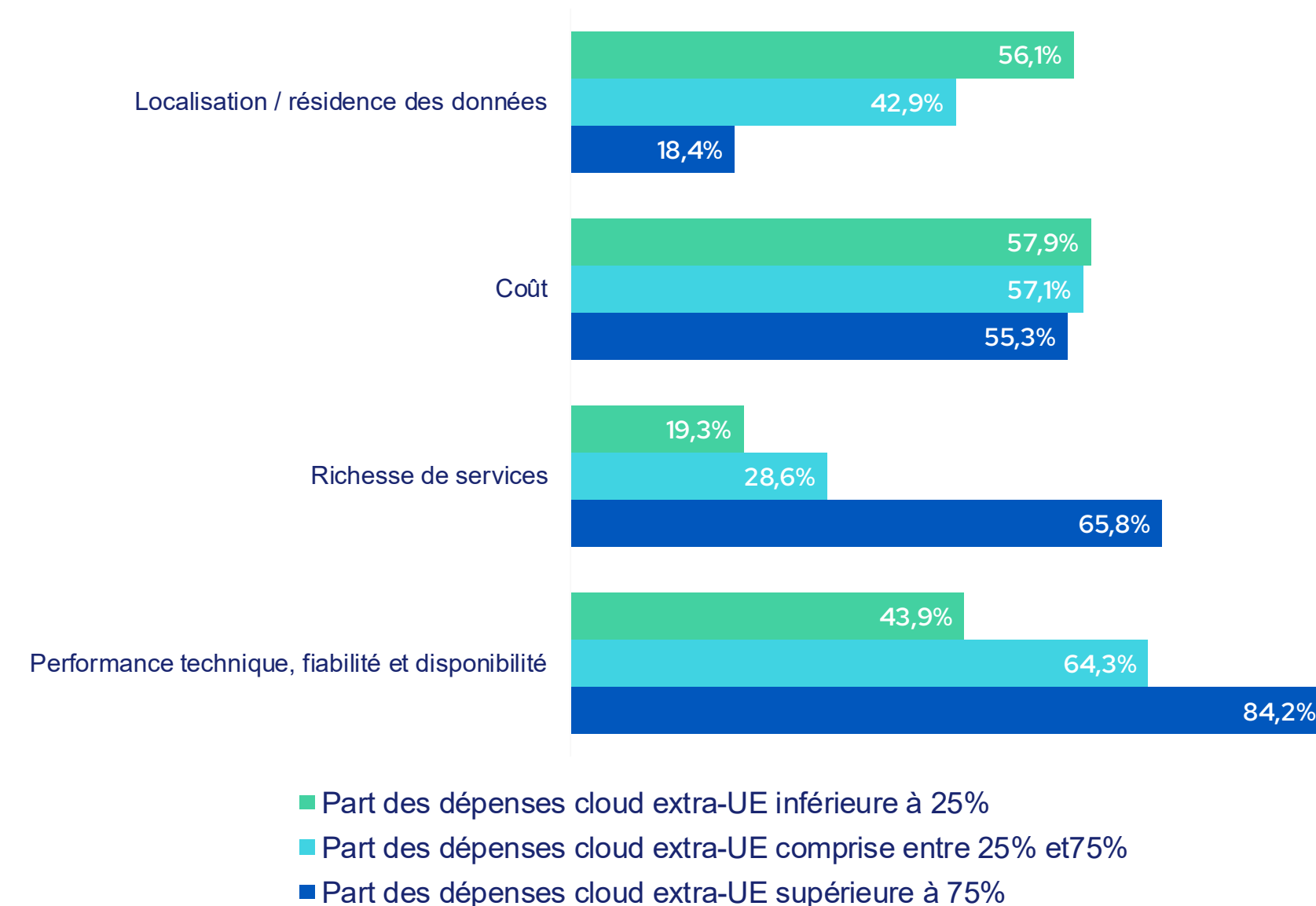
Lecture qualitative

Les entretiens confirment que les dépendances les plus "collantes" concernent les services managés intégrés au produit : flux temps réel, moteurs de recherche, chiffrement, data pipelines ou calcul IA. Leur remplacement implique rarement un simple changement d'hébergeur ; il suppose souvent une réécriture applicative.

Le débat n'est pas seulement « où sont hébergées les données ? », mais « quelles briques permettent au produit de fonctionner ? »

Les principaux critères de sélection d'une offre cloud sont les services et la performance

Quels sont vos critères de choix d'un hébergeur ? (les répondants devaient classer les critères) (part de réponses dans le top 3)



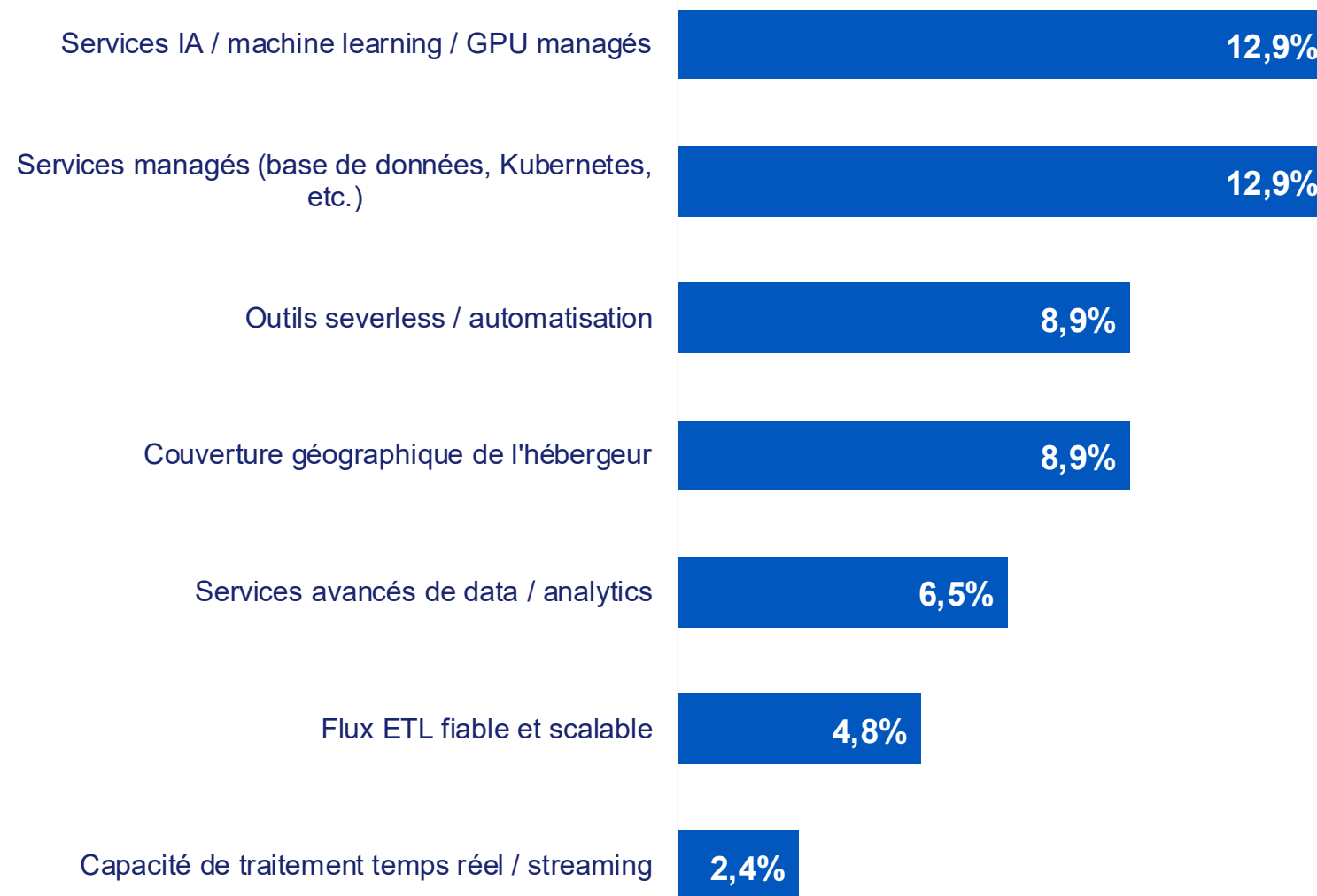
Ce que montre le graphique

Les répondants ayant choisi de recourir aux acteurs extra-européens pour la majorité de leurs dépenses cloud privilégient nettement la performance et la richesse fonctionnelle. À l'inverse, ceux dont la part des dépenses extra-UE est faible placent plus souvent la localisation des données comme principale raison de leur choix. Ce résultat est central pour l'étude : le recours à un hébergeur souverain ou non relève d'une hiérarchie de choix technico-économiques.

Les fournisseurs cloud extra-européens sont d'abord et avant tout choisis pour leur performance, la richesse fonctionnelle et le time-to-market. En miroir, la localisation des données constitue un critère plus important dans le choix d'un cloud européen.

Les services avancés concentrent les verrous de migration

Quels sont aujourd'hui les services cloud nécessaires à votre produit indisponibles chez les offres qualifiées SecNumCloud ?



Ce que montre le graphique

Les services manquants ou limités concernent d'abord les usages cloud les plus avancés : services managés, bases de données avancées, KMS, IAM, logs, streaming temps réel, IoT, recherche, observabilité, IA/GPU. Ces briques ne sont pas des "options" pour les start-up cloud-native : elles sont intégrées au produit, à la performance et parfois aux engagements de service.

Le débat ne porte pas sur l'existence d'une offre SNC, mais sur la disponibilité de briques équivalentes, qualifiées et industrialisées.

La difficulté n'est pas seulement de remplacer une brique technique au moment de la migration. Lorsqu'un service managé critique disparaît ou n'a pas d'équivalent qualifié, la start-up doit reconstruire, superviser et maintenir elle-même des fonctions jusque-là externalisées. Le coût devient récurrent : compétences, incidents, sécurité, supervision et complexité inter-cloud.



Une trajectoire de progrès existe, mais les obligations doivent attendre des offres réellement industrialisées



Ce que montre le verbatim

Les hébergeurs d'offres qualifiées SNC ne nient pas le différentiel de profondeur fonctionnelle avec celles des offres non qualifiées. Leur position est plus nuancée : les usages standards sont déjà largement couverts, mais le périmètre qualifié doit encore s'étendre aux briques cloud-native. Le point critique est donc le calendrier exigé.

Les offres souveraines, chez (information confidentielle), couvrent plus de 80 % des services cloud les plus utilisés sur le marché. Tous ne sont pas nécessairement qualifiés SecNumCloud, mais ils restent souverains by design.

S'agissant des services qualifiés SNC, certains segments sont déjà largement matures et bien couverts : notamment l'hébergement applicatif, la sauvegarde, le cloud privé et le Bare Metal.

D'autres services accusent encore un retard en matière de qualification : en particulier les services managés (Kubernetes, le stockage objet de type S3 ou les bases de données), ainsi que certains enablers associés tels que le KMS, l'IAM, le load balancing ou la gestion des logs.

Ainsi, sur le périmètre SecNumCloud, la couverture fonctionnelle reste en construction. Toutefois, de nombreuses offres sont actuellement en cours de qualification et les lacunes identifiées tendent à se réduire rapidement. L'écosystème des fournisseurs qualifiés a fortement progressé ces derniers mois, et cette dynamique devrait permettre de combler l'essentiel des manques.

Verbatim issu d'un entretien réalisé avec un hébergeur souverain

05

Mesure d'impact du recours
à SecNumCloud : un choc
économique

Un risque de choc de compétitivité pour les start-up

L'impact dépend d'abord de l'adhérence cloud. Il serait erroné de raisonner en coût moyen de migration. Les start-up souveraines by design, les architectures hybrides et les scale-up cloud-native n'ont ni les mêmes contraintes, ni les mêmes délais, ni les mêmes coûts. Plus l'entreprise dépend de services managés et de briques hyperscalers intégrées au produit, plus la migration devient longue et coûteuse.

Le coût principal n'est pas toujours la prime d'hébergement. La surprime d'infrastructure est visible, mais elle ne résume pas l'impact économique. Les coûts les plus structurants résident souvent dans la réécriture applicative, le double run, la revalidation réglementaire, la montée en compétence des équipes, la supervision de nouveaux environnements et la perte d'efficacité sur les services managés.

Les verrous sont techniques, humains et organisationnels. Les difficultés se concentrent sur les briques cloud avancées : KMS, IAM, logs, streaming temps réel, IoT, bases de données spécialisées, observabilité, recherche, IA/GPU. Leur remplacement peut transformer un coût de migration en coût d'exploitation récurrent, avec davantage de maintenance, d'incidents, de supervision et de besoins en compétences rares.

Le coût d'opportunité est central. Une migration SecNumCloud peut mobiliser les meilleures équipes pendant 18 à 36 mois sur un chantier qui ne crée pas de nouvelles fonctionnalités. L'impact ne se limite donc pas aux factures cloud : il se mesure aussi en roadmap ralentie, projets IA/R&D reportés, recrutements différés, internationalisation freinée et capacité de croissance réduite.

Trois couches de coûts à distinguer

Le coût SecNumCloud ne se résume pas à une prime d'hébergement : il combine des coûts de migration, une hausse potentielle du coût complet d'exploitation et un coût d'opportunité lié à la mobilisation de ressources rares.

Coûts transitoires de transformation technique et organisationnelle

Double run

Maintien temporaire de 2 environnements cloud lors de la migration afin d'assurer la continuité de service, de tester les bascules et de sécuriser la migration des données. Ce poste peut doubler une partie des coûts d'infrastructure pendant plusieurs mois.

Réécriture et adaptation applicative

Adaptation du code, refonte d'architectures, remplacement de services managés et tests de compatibilité. Le coût dépend fortement du degré d'adhérence aux briques propriétaires en cas de recours historique à un hyperscaler.

Re-certification et conformité réglementaire

Nouveaux audits, mise à jour des dossiers HDS / MDR / ISO, homologations de sécurité et, dans certains cas, renégociation des engagements clients. Le coût est à la fois documentaire, technique et juridique.

Coûts récurrents d'infrastructure et d'exploitation

Prime d'hébergement SNC

Surcoût éventuel de l'offre qualifiée par rapport à l'infrastructure actuelle. Son niveau dépend du fournisseur, du périmètre migré et de l'intensification de la concurrence entre offres qualifiées.

Renforcement des équipes infra/cloud ops

Besoin durable de profils infra, réseau, sécurité et DevOps pour superviser une architecture plus complexe, gérer les clés, les flux inter-clouds et compenser la moindre automatisation de certaines briques.

Perte d'efficacité opérationnelle

Risque de moindre performance, d'observabilité plus limitée, d'incidents plus difficiles à traiter et d'une dette technique accrue lorsque les alternatives aux services managés historiques sont moins matures.

Coûts d'opportunité, diffus mais stratégiques

Coût d'opportunité stratégique

Réallocation de ressources rares (ingénieurs, CTO, équipes produit, budget d'investissement) vers un projet de conformité et d'infrastructure, au détriment de la R&D, de l'IA, de l'internationalisation ou de l'acquisition client.

Ralentissement de la roadmap produit

Gel ou décalage de développements fonctionnels pendant la migration, avec un impact potentiel sur le time-to-market, la compétitivité **et la capacité à répondre aux demandes clients.**

Deux profils types parmi les entreprises ayant objectivé une migration



Note méthodologique : cette analyse porte uniquement sur les répondants ayant engagé des travaux concrets pour évaluer une migration vers une offre qualifiée SecNumCloud, soit 20,9% du panel. Deux groupes sont distingués : les entreprises ayant déjà effectué ou validé une migration (7,3% du panel) et celles ayant étudié techniquement la migration sans avoir encore pris de décision (13,6% du panel). Au sein de chacun de ces groupes, les répondants présentent des caractéristiques relativement homogènes et déclarent des ordres de grandeur convergents en matière de coûts, de délais et de surcoûts d'infrastructure. Les éléments présentés doivent donc être lus comme des profils représentatifs et des ordres de grandeur observés, et non comme des moyennes statistiques strictes.

Acteur ayant déjà effectué la migration ou validé une migration dans les prochains mois

Profil type :

CA compris entre 1 et 5 M€ / Effectif moyen compris entre 20 et 50 personnes / Entre 10% et 20% du CA avec le secteur public

Surreprésentation d'acteurs opérant dans la cybersécurité

Coopère déjà avec un hébergeur souverain

Une majorité de profil « Start-up avec une architecture hybride à trajectoire souveraine partielle »

Résultat des études technico-économiques :

Durée estimée de la migration : de 12 à 24 mois
Coût estimé de la migration : 150 k€

Surcoût annuel estimé de l'infrastructure : +15%

Services cloud manquants jugés réels, mais techniquement surmontables

Acteur ayant étudié techniquement la migration mais n'ayant pas pris de décision

Profil type :

CA moyen de 75 M€ / Effectif moyen de plus de 250 personnes / CA avec le secteur public compris entre 30% et 50%

Surreprésentation des legaltech et healthtech

Choix historique d'un hyperscaler pour la profondeur fonctionnelle, la scalabilité et l'accès à des compétences cloud pointues.

Une majorité de profil « Start-up avec une architecture cloud-native à forte adhérence aux hyperscalers »

Résultat des études technico-économiques :

Durée estimée de la migration : Plus de 24 mois

Coût estimé de la migration : de 500 k€ à 5 M€

Surcoût annuel estimé de l'infrastructure : +30% à +50%

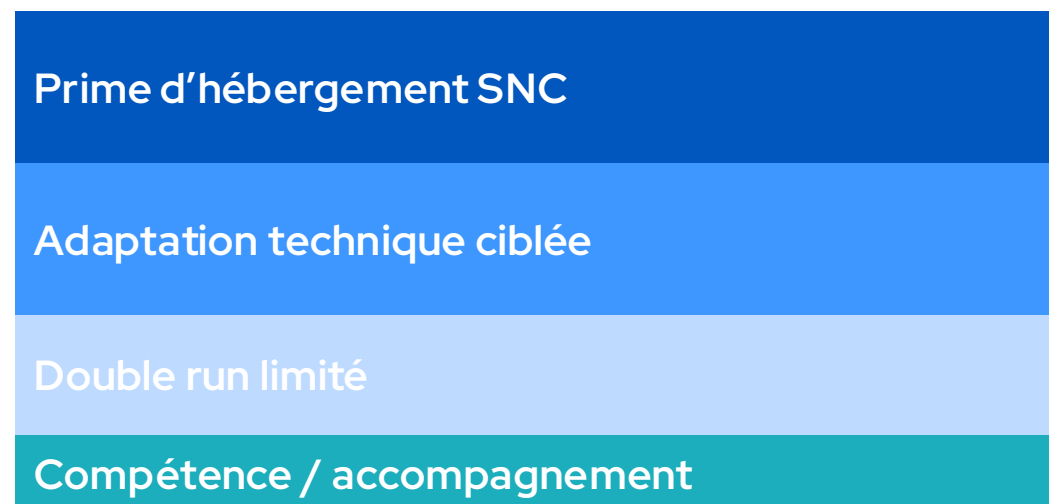
Migration hybride uniquement pour le secteur public jugée difficilement viable économiquement

L'écart entre les deux profils s'explique moins par la taille des entreprises que par leur degré d'adhérence aux architectures cloud existantes : plus la dépendance aux services managés et aux briques hyperscaler est forte, plus la migration vers SecNumCloud devient longue, coûteuse et structurante.

La nature des surcoûts diffère fortement selon le profil

Il serait erroné de présenter une ventilation unique des coûts d'une migration SecNumCloud. Les entretiens font apparaître une forte dispersion des ordres de grandeur, **de quelques centaines de milliers d'euros à plus de 10 M€ pour certaines scale-up internationalisées**. L'enquête et les retours qualitatifs distinguent deux profils : le coût dépend moins du prix facial de l'hébergement que du degré d'adhérence à l'architecture cloud existante.

Start-up avec une architecture hybride à trajectoire souveraine partielle



Coût estimé de la migration : 150 k€

Le coût est surtout **technique et ponctuel**.

La migration peut être absorbée si les workloads sont segmentables et si l'exposition au secteur public justifie l'effort.

Start-up avec une architecture cloud-native à forte adhérence aux hyperscalers



Coût estimé de la migration : de 500 k€ à 5 M€

Le coût ne se limite plus à l'infrastructure.

Il devient **structurel** : transformation du produit, mobilisation des équipes, re-certification, complexité d'exploitation et ralentissement de la roadmap.



Une prime d'hébergement SecNumCloud encore élevée

Le surcoût annuel du recours à une offre qualifiée SecNumCloud varie fortement selon le profil de la start-up. La prime d'hébergement reste le poste le plus visible (+10% à +40%), mais le surcoût récurrent total peut être beaucoup plus élevé lorsque l'entreprise dépend fortement des services managés hyperscalers.

Surprime hébergement SNC

+10% à +40%

Point d'attention pour les pouvoirs publics :

La prime d'hébergement SNC apparaît aujourd'hui élevée pour de nombreuses start-up et constitue un risque de barrière d'accès aux marchés publics ou un frein à l'innovation.

Mais cette surprise n'est pas figée : l'intensification de la concurrence, la montée en puissance de nouvelles offres qualifiées et l'industrialisation des catalogues devraient contribuer à réduire progressivement l'écart de prix. Un hébergeur interrogé indique viser à terme une convergence tarifaire entre ses offres qualifiées SNC et ses offres souveraines classiques.

D'autres surcoûts récurrents difficilement évaluables

Renforcement durable des équipes infra / cloud ops

Réinternalisation partielle de services managés, besoin de profils cloud rares et plus chers, voire quasi-doublement de l'équipe infra dans certains cas.

Double infrastructure / architecture hybride

Si la migration SNC concerne uniquement les services publics, coexistence de deux environnements, coûts réseau inter-clouds, supervision doublée, complexité d'exploitation.

Perte d'efficacité des services managés

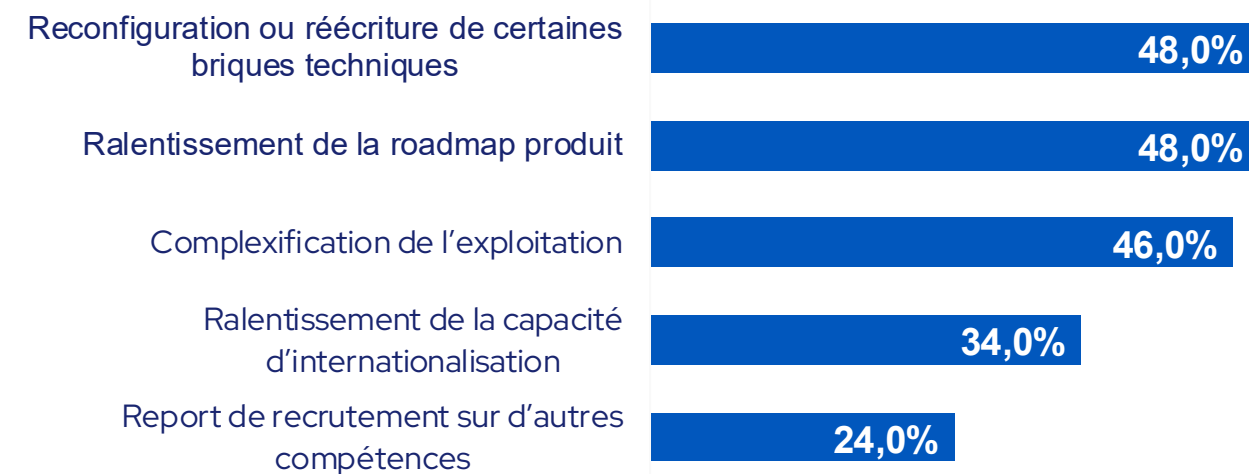
Poste très dépendant de l'architecture. Il devient élevé quand il faut remplacer des briques hyperscalers comme IoT Core, Kinesis, MongoDB Atlas Search, GPU/ML, réplication ou monitoring par des développements internes ou des solutions moins industrialisées. La maintenance de ces services nécessitera des recrutements récurrents.



Le coût de SecNumCloud ne s'arrête pas au cloud : il se paie en innovation, en marges et en croissance

Dans le cas où une migration serait obligatoire, quelles seraient les principales conséquences opérationnelles et techniques ?

(part des entreprises interrogées répondant oui)



Dans le cas où une migration serait obligatoire, quels impacts économiques anticipez-vous ?

(part des entreprises interrogées répondant oui)



Ce que montre le sondage

Les conséquences les plus citées relèvent d'abord de la transformation produit : réécriture de briques techniques, ralentissement de la roadmap et complexification de l'exploitation. Les impacts économiques suivent : hausse des prix, baisse des marges et report d'investissements R&D/IA.

Une exigence SecNumCloud mal calibrée ne renchérit pas seulement l'hébergement : elle détourne les équipes produit, ralentit la roadmap, reporte les investissements R&D/IA et réduit les marges des start-up.

Une migration SecNumCloud : une trajectoire de transformation, pas une bascule immédiate

Start-up avec une architecture hybride
à trajectoire souveraine partielle

De 12 à 24 mois

Qualification du périmètre sensible

1 à 2 mois

Conception de l'architecture hybride cible

2 à 3 mois

Adaptations applicatives ciblées

3 à 6 mois

Migration progressive + double run limité

3 à 6 mois

Stabilisation / preuves de conformité

2 à 4 mois

Start-up avec une architecture cloud-native à forte adhérence
aux hyperscalers

De 24 à 48 mois

Cadrage et choix de l'architecture cible

3 à 6 mois

Réécriture des composants critiques et migration des données

12 à 18 mois

Tests de charge et re-certification

6 mois

Bascule progressive client par client avec double run

3 à 6 mois

Stabilisation

6 à 12 mois



Le passage à SecNumCloud ne peut pas relever d'une mise en conformité immédiate. Il suppose un délai d'application permettant aux start-up de segmenter les workloads sensibles, d'adapter leur architecture et d'absorber les coûts de transition sans interrompre leur trajectoire produit.



Le coût d'opportunité est le principal coût caché d'une migration SNC



Une migration de cette nature mobilise les meilleures équipes pendant 18 à 36 mois sur un projet qui ne crée pas de nouveau produit. Le principal coût n'est pas seulement technique : c'est le coût d'opportunité sur la roadmap, l'internationalisation et l'innovation.

Verbatim issu d'un entretien réalisé avec une scale-up B2B établie



Ce que montre le verbatim

Une migration SecNumCloud absorbe les ressources les plus rares : équipes cloud, produit, sécurité et architecture. Le coût ne se mesure donc pas seulement en factures ou en jours-hommes. Il se mesure en fonctionnalités non développées, marchés non adressés, recrutements différés et projets IA/R&D ralentis.

Le frein n'est pas seulement tarifaire : il est aussi humain et organisationnel



Le déficit de compétences constitue un frein à la migration. Les équipes des DSI sont en effet majoritairement formées aux technologies des fournisseurs américains. Dès lors, la migration vers des environnements alternatifs, quand bien même ils reposent sur des technologies ouvertes, implique un effort significatif de montée en compétence, que de nombreuses organisations peinent à anticiper et à structurer.

Verbatim issu d'un entretien réalisé avec un hébergeur souverain



Ce que montre le verbatim

L'écart de maturité ne se mesure pas uniquement au catalogue de services. Il se joue aussi dans les compétences disponibles, les routines d'exploitation, les outils d'observabilité et la capacité des équipes à résoudre les incidents. Une trajectoire SecNumCloud soutenable suppose donc un accompagnement technique, pas seulement une obligation contractuelle.

06

Nécessaire trajectoire
européenne

Un nécessaire atterrissage européen

À l'heure où chaque État membre définit ses propres référentiels de sécurité et ses propres critères de souveraineté, l'urgence est de traiter ces deux enjeux au niveau européen, via l'EUCS et le CADA. Sans cela, la fragmentation persistante freinera l'expansion de nos start-up, pour lesquelles le marché européen est l'échelle indispensable.

La fragmentation des certifications nationales de cybersécurité : un obstacle majeur à la fourniture de services cloud sur le marché européen

La situation actuelle : chaque État membre applique son propre référentiel national (SecNumCloud en France, C5 en Allemagne, Strategia Cloud en Italie....)

Un frein à l'expansion des offreurs cloudeurs français en Europe : le cumul des certifications duplique les coûts et retarde leur entrée sur le marché, une situation qui profite structurellement aux acteurs déjà certifiés localement et aux grands hyperscalers, au détriment des plus petits acteurs et des nouveaux entrants.

De la même manière, les start-up françaises ne peuvent pas supporter une contrainte nationale plus lourde que leurs concurrentes européennes. Elles ne peuvent pas financer une trajectoire française spécifique, sans garantie de reconnaissance automatique dans les autres États membres.

Un cadre de certification eurooéen à l'horizon : le Cybersecurity Act, dont une proposition de révision a été publiée par la Commission en janvier 2026, devait remédier à cette fragmentation via l'EUCS, un schéma commun de certification de sécurité, et non de souveraineté. Il est désormais urgent que les négociations actuelles au Parlement européen et au Conseil aboutissent en vue de l'adoption du texte.

Une trajectoire de souveraineté à amorcer au niveau européen

La Commission a présenté le 3 juin 2026 une proposition de réglementation Cloud and AI Development Act (CADA) pour renforcer l'écosystème européen du cloud et de l'IA.

En portant des critères de souveraineté harmonisés, afin de conditionner l'accès à la commande publique et aux financements européens, le CADA incite les start-up européennes à construire leurs offres cloud et IA en conformité avec ces exigences en leur donnant accès à un marché de taille critique : le marché européen.

Le défaut d'harmonisation des référentiels de sécurité et de souveraineté, sans garantie de reconnaissance automatique dans les autres États membres, entrave la capacité des start-up à scaler en Europe.

Une trajectoire progressive et européenne doit guider toute transition vers le cloud souverain



Ce que montre le verbatim

L'enjeu n'est pas d'opposer SecNumCloud au cadre de confiance existant, mais de l'articuler avec lui. Une approche graduée permet de concentrer l'exigence maximale sur les données réellement sensibles, sans faire de SecNumCloud un prérequis systématique, notamment dans des secteurs déjà matures sur ces enjeux, comme la santé, où la sensibilité des données a depuis longtemps structuré un cadre de sécurité et de confiance exigeant (HDS, ISO 27001, chiffrement, etc.). Cette approche ouvre une trajectoire européenne en faveur d'une progression des offres souveraines non qualifiées.



La trajectoire la plus réaliste, et celle que nous observons dans la pratique, est la migration progressive. Le passage à SecNumCloud n'est pas une bascule mais un processus qui s'inscrit dans la durée : les applications migrent au fur et à mesure, selon leur architecture propre et la disponibilité des briques qualifiées.

Concrètement, cela se traduit par une segmentation des usages. Les workloads les plus critiques basculent en priorité vers un environnement qualifié, tandis que les autres restent sur des infrastructures souveraines non SNC.

Cette approche permet de sécuriser l'essentiel sans bloquer l'organisation dans l'attente d'une couverture fonctionnelle complète.

C'est avant tout un projet partenarial dans la durée, qui suppose un engagement conjoint entre le client et son fournisseur, ainsi qu'une vision stratégique claire dès le départ pour séquencer les migrations de manière cohérente.

Verbatim issu d'un entretien réalisé avec un hébergeur souverain

07

Focus sur le secteur
des healthtechs

Dans la santé, imposer SecNumCloud viendrait bouleverser un cadre de confiance déjà structuré

HDS : le socle santé

La certification HDS encadre l'hébergement des données de santé à caractère personnel. Elle vise à garantir la sécurité, la confidentialité, la disponibilité et la traçabilité des données médicales. Pour les healthtech, elle structure déjà l'architecture, les processus, les flux et les contrôles associés à la donnée de santé.

SecNumCloud : une garantie cloud différente, quand HDS progresse déjà sur l'extraterritorialité

SecNumCloud qualifie une offre cloud précise et renforce les garanties de sécurité et de protection contre certains risques extraterritoriaux. Mais le décret HDS du 24 mars 2026 (stockage UE/EEE, encadrement des accès distants, transparence contractuelle, mesures d'atténuation) montre que le cadre santé évolue déjà sur ce même risque. Il existe donc une trajectoire graduée de maîtrise du risque au sein même du cadre HDS.

Un secteur déjà fortement encadré



Un secteur qui investit déjà massivement dans la sécurité, au-delà du réglementaire. Les start-up en santé opèrent dans un environnement où la sécurité des données est déjà structurée par des exigences fortes : HDS, RGPD, audits clients, chiffrement, gestion des clés externalisée, procédures qualité, contraintes liées aux dispositifs médicaux. Ces investissements vont bien au-delà des obligations légales : la sécurité est un prérequis et un facteur de confiance vis-à-vis des patients, soignants et établissements de santé, ce qui maintient naturellement un niveau d'exigence élevé, sans qu'une nouvelle certification soit nécessaire.

Une confusion possible côté acheteurs



Dans les appels d'offres hospitaliers, plusieurs notions sont parfois utilisées comme équivalentes : HDS, hébergement en France, cloud souverain, absence de Cloud Act, chiffrement, SecNumCloud. Cette confusion peut conduire à considérer SecNumCloud comme un raccourci global de sécurité.

Un risque de disqualification implicite



Pour les healthtech déjà certifiées HDS sur des architectures existantes, l'ajout de SecNumCloud peut semer le trouble : une architecture audité, sécurisée et certifiée peut être perçue comme insuffisante non pas parce qu'elle serait moins sûre, mais parce qu'elle ne coche pas une nouvelle exigence contractuelle. Le risque est alors de déplacer le débat de la sécurité effective vers la conformité attendue par l'acheteur.

Les healthtech combinent déjà HDS, ISO 27001, chiffrement, gestion des clés, supervision et continuité clinique. SecNumCloud ne comble pas un vide de sécurité en santé : le secteur dispose déjà d'un cadre de confiance exigeant. L'enjeu n'est pas d'ajouter une nouvelle certification.

Indépendamment du coût, SecNumCloud pose une question de couverture fonctionnelle

84,1%

Start-up estimant qu'au moins un service/brique cloud nécessaire à leur produit n'est pas disponible dans les offres qualifiées SecNumCloud.

dont 100% des healthtechs interrogées

La migration vers une offre qualifiée ne dépend pas seulement du prix ou du délai. Elle suppose que les services nécessaires au fonctionnement du produit soient effectivement disponibles, qualifiés et industrialisés. Or l'enquête révèle un niveau élevé d'incertitude sur ce point, particulièrement dans les secteurs les plus sensibles.

Focus sur les healthtech

Dans la santé, le problème n'est pas uniquement le coût d'une migration SecNumCloud. C'est d'abord l'incertitude fonctionnelle : les acteurs ne savent pas si les offres qualifiées couvrent les briques critiques nécessaires à leurs produits, et aucun répondant healthtech ne déclare disposer d'une couverture complète.

Cette incertitude est critique dans la santé : les briques cloud peuvent porter des flux patients, du temps réel, des moteurs de recherche sur données médicales, des dispositifs médicaux, du chiffrement ou des interfaces hospitalières. Une exigence SecNumCloud ne peut donc être généralisée sans vérifier la disponibilité effective de services équivalents, qualifiés et industrialisés.

Cette incertitude ne porte pas sur des fonctionnalités accessoires. Elle concerne potentiellement des services managés, des briques data, de l'IA, du temps réel, etc. Pour les start-up, l'enjeu n'est donc pas seulement de migrer une infrastructure, mais de retrouver un niveau fonctionnel équivalent.

Le recours aux hyperscalers relève souvent d'un arbitrage industriel



«On sait qu'il existe une dépendance, mais elle est arbitrée. Les hyperscalers nous permettent de nous concentrer sur le produit plutôt que de reconstruire nous-mêmes des briques d'infrastructure. La migration vers AWS nous a permis d'obtenir l'ISO 27001 en 9 mois et la certification HDS, deux objectifs inatteignables dans ce délai avec notre architecture précédente.»

Verbatim issu d'un entretien réalisé avec une start-up



Ce que montre le verbatim

La dépendance aux fournisseurs cloud extra-européens est moins ignorée que rationalisée : les start-up acceptent certains risques fournisseurs lorsqu'ils sont compensés par des gains de performance, de sécurité, de certification, de scalabilité et de time-to-market.

08

Recommandations aux pouvoirs publics

Les recommandations aux pouvoirs publics

01 | Maintenir SecNumCloud dans sa vocation de référentiel de cybersécurité

La souveraineté est un objectif légitime, mais ne doit pas être confondue avec un outil de sécurité. La loi SREN a fixé un point d'équilibre : soumettre les données les plus sensibles de l'État à un haut niveau de cybersécurité via SecNumCloud, sans en faire un instrument de politique industrielle.

02 | Ouvrir la conformité à plusieurs référentiels de haut niveau, SecNumCloud compris

SecNumCloud peut être pertinent pour certains risques critiques, mais la sécurité cloud doit être évaluée à partir d'un faisceau de critères : certifications de sécurité, chiffrement, clés, auditabilité, résilience, réversibilité, interopérabilité, continuité de service, création de valeur et maîtrise des dépendances.

Les recommandations aux pouvoirs publics

03 | Sanctuariser un délai de transition et un soutien aux start-up

Pour tout nouvel impératif de sécurité des données, prévoir des délais de 24 à 36 mois selon la complexité, sous réserve d'une offre qualifiée fonctionnellement équivalente à l'infrastructure actuelle. Soutenir les trajectoires souveraines plutôt que d'en transférer brutalement le coût aux start-up : crédits d'impôt, accompagnement du double run et des audits pour les migrations vers des infrastructures souveraines ou européennes de confiance, y compris non qualifiées SNC, dès lors qu'elles constituent un palier réaliste.

04 | S'inscrire dans les cadres européens de sécurité (EUCS) et de souveraineté (CADA), pour garantir une approche cohérente à l'échelle de l'Union européenne

La France ne doit pas construire de doctrine nationale séparée, mais inscrire SecNumCloud dans le futur schéma de certification européen (EUCS) et soutenir l'adoption de critères de souveraineté harmonisés via le CADA, pour que la trajectoire de nos entreprises s'inscrive dans un cadre commun à l'échelle du marché unique.

Les recommandations aux pouvoirs publics

05 | Renforcer l'offre souveraine, accompagner les transition des utilisateurs

Il est nécessaire de construire, avec les parties prenantes, une stratégie dédiée à l'hébergement souverain, distincte des enjeux de sécurité. Cette stratégie doit tracer une trajectoire claire de renforcement des offres souveraines françaises et accompagner les entreprises utilisatrices dans leur transition vers ces offres. Elle doit tenir compte de la diversité des niveaux de maturité et des contraintes techniques des entreprises concernées.

06 | Garantir la stabilité du cadre de cybersécurité des données de santé

Les start-up en santé doivent bénéficier d'un cadre de certification adapté, stable et durable, garantissant la pérennité du socle HDS.

09

Annexes

Questionnaire quantitatif

A. Profil de l'entreprise

Q1 – Quel est l'effectif actuel de votre entreprise en France ?

Moins de 10 salariés

10 à 49 salariés

50 à 249 salariés

250 salariés ou plus

Q2 – Quel est votre chiffre d'affaires annuel consolidé (Monde) (dernier exercice clos) ?

Moins de 1 M€

1 à 5 M€

5 à 20 M€

20 à 100 M€

Plus de 100 M€

Ne souhaite pas répondre

Q2bis – Quel est votre chiffre d'affaires annuel France (dernier exercice clos) ?

Moins de 1 M€

1 à 5 M€

5 à 20 M€

20 à 100 M€

Plus de 100 M€

Ne souhaite pas répondre

Q3 – Quel est le principal secteur d'activité de votre entreprise ?

IA, data, deeptech

Fintech / Insurtech

Healthtech / Biotech

Cybersécurité

E-commerce / plateformes

Autre (précisez)

B. Exposition au secteur public

Q4 – Quelle part de votre chiffre d'affaires consolidé est réalisée avec des clients publics ou parapublics en France ?

0%

Moins de 10%

10 à 30%

30 à 50%

Plus de 50%

Q5 – Avec quels types d'acteurs publics travaillez-vous ? (plusieurs réponses possibles)

Administration centrale / ministères

Établissements de santé / hôpitaux

Collectivités territoriales

Opérateurs publics / parapublics

Autre (préciser)

Aucun actuellement

C. Organisation et dépendance cloud

Q6 – Quels fournisseurs cloud IaaS utilisez-vous aujourd'hui ? (plusieurs réponses)

AWS

Microsoft Azure

Google Cloud

OVHcloud

Scaleway

3DS Outscale

Bleu

S3NS

Autre (précisez)

Questionnaire quantitatif

Q6bis – Quel est le pourcentage de vos dépenses cloud fléchées vers des fournisseurs cloud extra-européens ? (Bleu et S3NS considérés comme intra-UE)

Moins de 25%

De 25 à 50%

De 50 à 75%

Plus de 75%

Ne sait pas

Q7 – Quelle part vos dépenses cloud représentent-elles dans votre structure de coûts ?

Moins de 5% du CA

5 à 10%

10 à 20%

20 à 30%

Plus de 30%

Ne sait pas

Q8 – Pour quels usages principaux recourez-vous au cloud ? (plusieurs réponses possibles)

Hébergement applicatif / SaaS

Infrastructure technique (IaaS, environnements de dev/test)

Services managés (bases de données, Kubernetes...)

Data, IA, entraînement de modèles

Stockage, sauvegarde, PRA

Traitement de données sensibles

Services transactionnels critiques

Autre (compléter)

Q9 – Quels ont été les principaux critères de choix de votre fournisseur cloud ? (classer par ordre d'importance du plus important au moins important)

Performance technique, fiabilité et disponibilité (SLA)

Richesse des services (data, IA, services managés...)

Coût

Cybersécurité et protection des données

Localisation / résidence des données & souveraineté

Exigences clients

Contrainte réglementaire / conformité

D. Cybersécurité et perception des offres

Q10 – Parmi les options suivantes, lesquelles s'appliquent à vos pratiques en termes de sécurité des systèmes et données ? (plusieurs réponses possibles)

ISO 27001

HDS

SOC2

Équipe cybersécurité interne

Chiffrement avec gestion interne des clés

Sécurité principalement assurée par l'hébergeur

Architecture Zero Trust

Recours à un cloud qualifié SecNumCloud pour tout ou partie des données

Autre (préciser)

Q11 – Au cours des 12 derniers mois, avez-vous perdu un contrat ou une opportunité commerciale parce que le client exigeait explicitement un hébergement sur un cloud souverain / cloud de confiance ? (plusieurs réponses possibles pour Oui)

Oui un client public

Oui un client privé

Non

Ne sait pas / difficile à attribuer

Questionnaire quantitatif

Q11bis – Si oui, quelle était l'exigence ? (plusieurs réponses possibles)

"hébergement en France"

"hébergement dans l'UE"

"sans fournisseur américain (AWS/Azure/GCP)"

"recours à une offre qualifiée SecNumCloud"

autre exigence (préciser)

E. Connaissance de l'enjeu SecNumCloud

Q12 – À propos de SecNumCloud

SecNumCloud est une certification délivrée par l'ANSSI (Agence nationale de la sécurité des systèmes d'information) à certains fournisseurs de services cloud, attestant du respect d'exigences élevées en matière de sécurité et de protection des données.

Des discussions réglementaires portent sur l'extension possible du recours à ces fournisseurs certifiés pour certains marchés publics (État, hôpitaux, collectivités), notamment lorsque des données sensibles sont concernées.

Êtes-vous informé de ces évolutions potentielles ?

Oui, précisément

Oui, partiellement

Non

F. Hypothèse de migration vers SecNumCloud

Q13 – Avez-vous engagé des travaux pour évaluer une migration vers une offre qualifiée SecNumCloud ?

Non, aucun travail engagé

Sujet identifié mais non étudié

Premières évaluations techniques ou économiques réalisées

Etude réalisée et décision prise de ne pas migrer

Décision de migration prise, en cours de mise en œuvre

Migration déjà réalisée (totale ou partielle)

Q14 – Si une migration vers un fournisseur qualifié SecNumCloud devait être engagée, quel délai estimez-vous nécessaire pour la mener à bien ?

Moins de 6 mois

6 à 12 mois

12 à 24 mois

Plus de 24 mois

Difficile à estimer à ce stade

Q15 – Quel serait l'ordre de grandeur de l'ensemble des coûts d'une migration vers un fournisseur qualifié SecNumCloud (frais de transfert, frais techniques, conseil technique externe, potentiel coût d'un double run le temps de la migration....)?

Moins de 100 k€

100 à 500 k€

500 k€ à 1 M€

1 à 5 M€

5 à 10 M€

Plus de 10 M€

Impossible à estimer

Questionnaire quantitatif

Q15 bis – A combien estimez-vous le surcoût annuel d'un passage d'une offre qualifiée SecNumCloud vis à vis de votre prestataire actuel (% du montant de votre contrat actuel) ?

<10%

Entre 10% et 20%

Entre 20% et 30 %

Entre 30% et 50%

> 50%

Impossible à estimer

Q16 – Aujourd'hui, certains services cloud nécessaires à votre produit sont-ils indisponibles chez les offres qualifiées SecNumCloud ?

Non, tous les services nécessaires sont disponibles

Oui, certains services manquent ou sont encore limités

Difficile à évaluer

Q16 bis Si "Oui" : Quels types de services sont concernés ?

Services avancés de data / analytics

Services IA / machine learning / GPU managés

Services managés (bases de données, Kubernetes, etc.)

Flux ETL fiables et scalables

Capacités de traitement temps réel / streaming

Outils serverless / automatisation

Couverture géographique / déploiement international

Autre (préciser)

Q17 – L'option consistant à utiliser une offre qualifiée SecNumCloud uniquement pour vos activités publiques, tout en conservant votre infrastructure actuelle pour les autres activités, vous paraît-elle envisageable ?

Oui, facilement envisageable

Oui, mais avec des contraintes importantes

Non, difficilement envisageable

Difficile à évaluer à ce stade

Q17 bis Si non, Quelles sont les principales raisons ?

Surcoûts d'exploitation / double run trop élevés

Complexité technique / architecture trop difficile à scinder

Limites fonctionnelles (services indisponibles/limités côté offres qualifiées)

Contraintes de performance / latence / disponibilité

Complexité organisationnelle (équipes, exploitation, gouvernance, processus)

Contraintes de sécurité/compliance (exigences difficiles à tenir en hybride)

Exigences clients / contractualisation incompatible

Autre (préciser)

G. Impacts business et compétitivité

Q18 – Si l'obligation de recourir à une offre qualifiée SecNumCloud pour certains marchés publics (État, hôpitaux, collectivités) était actée, quelle serait votre stratégie principale ? (une seule réponse)

Migrer tout ou partie de votre infrastructure vers une offre qualifiée

Renoncer à répondre aux marchés publics contraints

Sortir définitivement de la sphère publique en anticipant une extension des contraintes

Se tourner vers d'autres zones géographiques moins contraignantes

Ne sait pas à ce stade

Je ne suis pas concerné par cette obligation

Questionnaire quantitatif

Q19 – Dans le cas où une migration serait obligatoire, quelles seraient les principales conséquences opérationnelles et techniques ?

Réinternalisation de compétences aujourd'hui externalisées

Recours accru à du conseil ou de l'intégration technique

Reconfiguration ou réécriture de certaines briques techniques

Ralentissement de la roadmap produit

Report de recrutement sur d'autres compétences

Complexification de l'exploitation

Ralentissement de la capacité d'internationalisation / déploiement de nouveaux marchés ou développement de nouvelles offres sur d'autres géographies

Autres (préciser)

Q20 – Dans le cas où une migration serait obligatoire, quels impacts économiques anticipez-vous ? (tableau oui/non)

Hausse des prix facturés aux clients

Impact économique très important / baisse des marges

Report d'investissements (R&D, IA...)

Retard d'expansion internationale

Aucun impact économique significatif

Q21 – Si vous opérez sur d'autres marchés européens, une obligation d'hébergement sur une offre qualifiée SecNumCloud pour vos activités en France vous obligerait-elle à maintenir des infrastructures distinctes entre la France et d'autres marchés ?

Oui

Non

Potentiellement

Je n'opère pas sur d'autres marchés européens

Remerciements

France Digitale et Xerfi remercient l'ensemble des start-up, scale-up, fournisseurs cloud et experts ayant participé à cette étude, par leurs réponses à l'enquête quantitative, leurs contributions écrites et les entretiens approfondis réalisés au cours des travaux. La diversité de ces contributions a permis de confronter les situations, les architectures et les stratégies cloud afin de restituer au plus près les réalités économiques et opérationnelles rencontrées par les entreprises.

Étude réalisée par Xerfi pour France Digitale

Flavien Vottero – Directeur d'études expert, Xerfi

Jérémy Robiolle – Directeur du développement, Xerfi

France Digitale fédère un écosystème de près de 2 000 start-up et scale-up. L'association contribue au débat public sur les conditions de développement, de financement et de compétitivité des entreprises technologiques, en France et en Europe.

francedigitale.org

Xerfi est un groupe d'études économiques et stratégiques. Il accompagne les entreprises, fédérations professionnelles et acteurs publics dans l'analyse de leurs marchés, de leurs environnements concurrentiels et de leurs enjeux stratégiques.

www.xerfi.com

