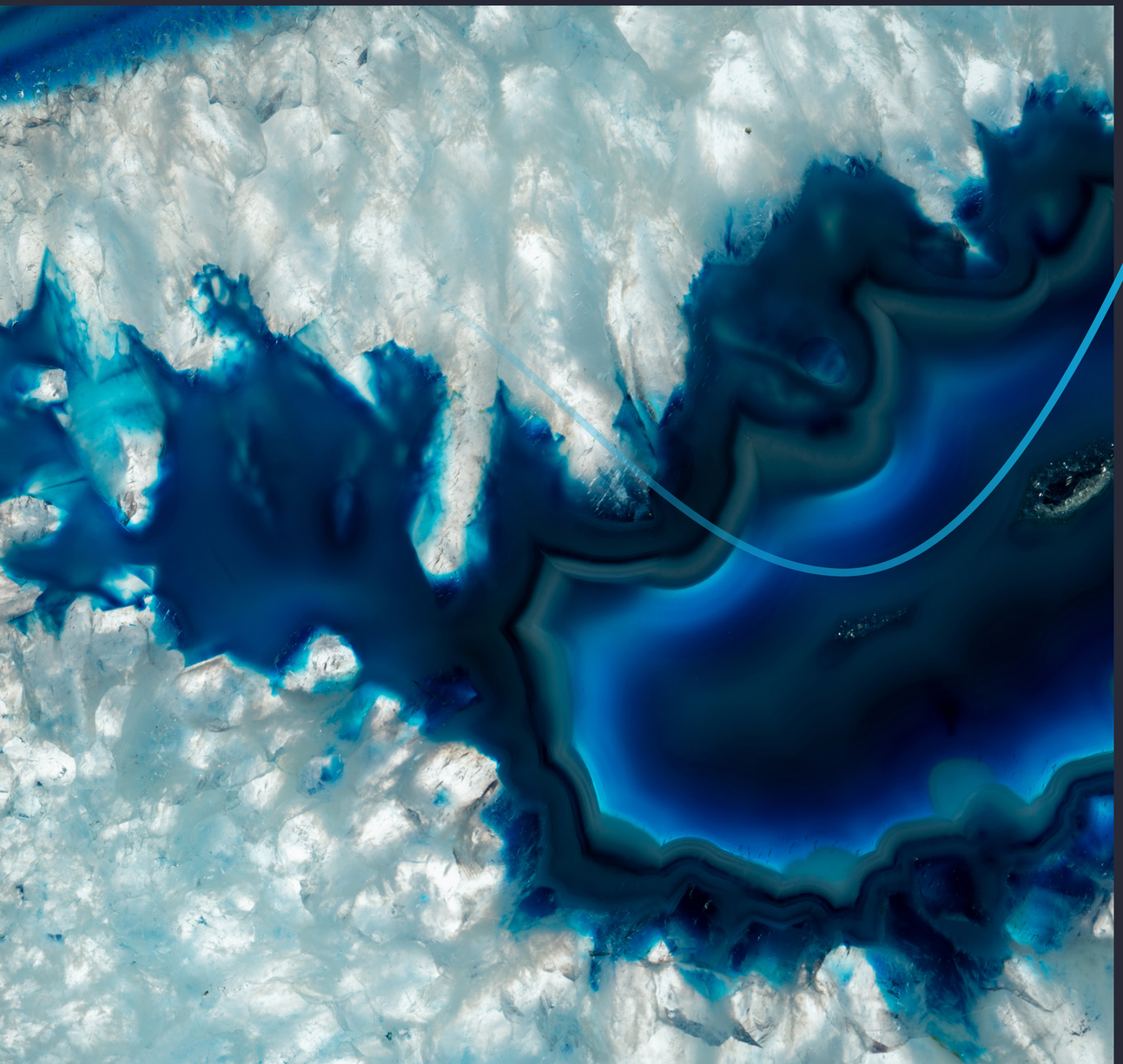
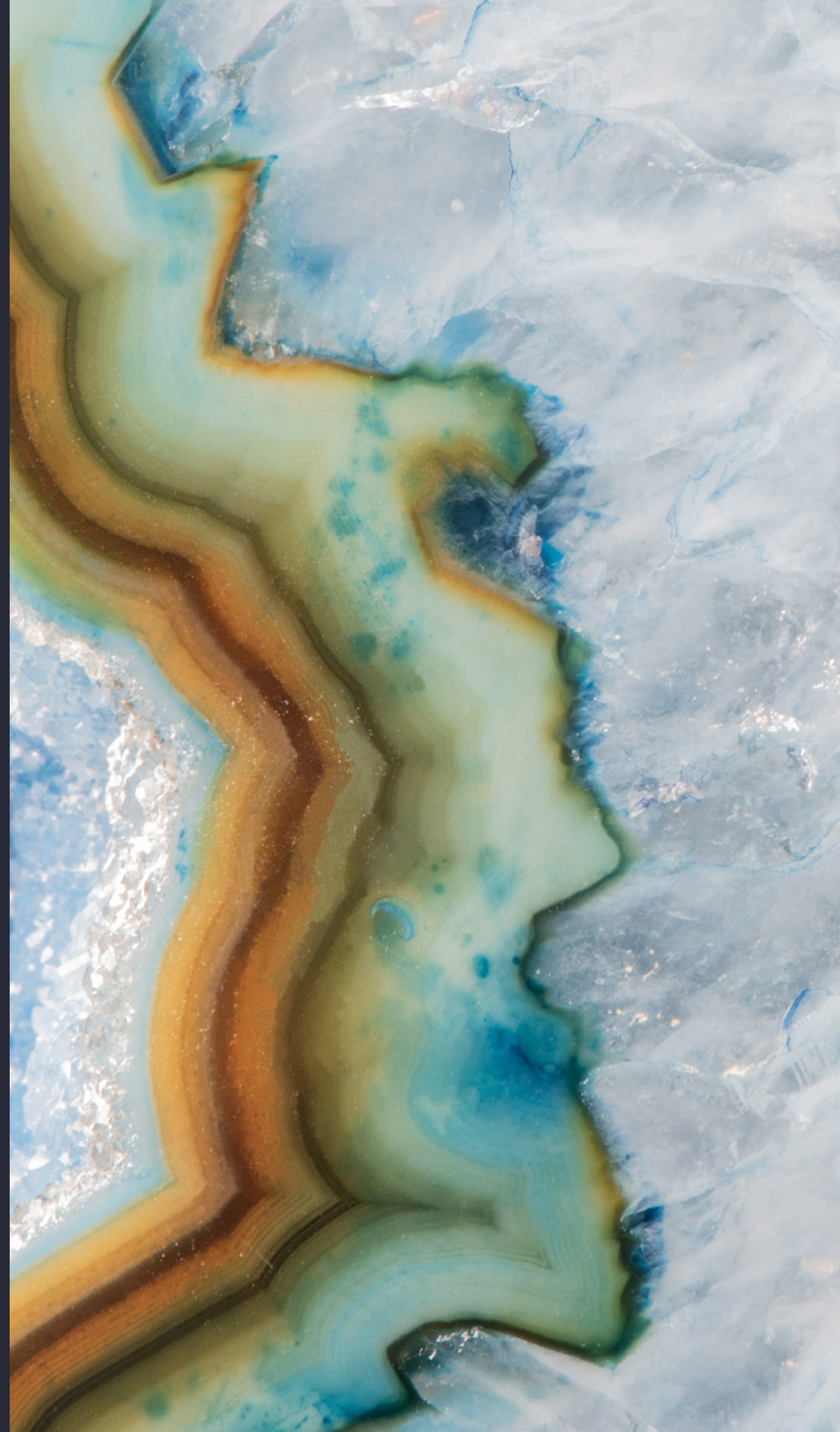


Le cloud de *confiance*

Allier performance,
innovation et sécurité

Capgemini

Table des *matières*



Choisir n’est plus renoncer

Le cloud est une équation complexe aux multiples variables. La migration vers le cloud sert en effet des enjeux qui pouvaient jusqu’à présent paraître antagonistes : d’une part, elle offre la possibilité d’innover dans le traitement des données pour améliorer la performance et l’expérience client ; d’autre part, elle permet d’optimiser les coûts opérationnels, créant ainsi un équilibre essentiel pour les entreprises.

Dans un monde où les défis se multiplient et s’intensifient, la souveraineté s’impose comme l’un des meilleurs boucliers contre des risques de diverses natures, notamment légaux, économiques et réputationnels.

Le cloud de confiance devient une alternative ou complément pertinent aux cloud publics et privés qui dominent aujourd’hui le marché, en garantissant une sécurité renforcée et une conformité aux normes qui régissent la protection des données françaises et européennes. C’est d’ailleurs la première fois que la réglementation (et non pas les besoins métiers ou la technologie) pilote une telle évolution.

Le cloud de confiance apporte aux entreprises un équilibre entre la nécessaire protection de leurs informations sensibles, la performance de leur écosystème et leur capacité d’innover, tout en se prémunissant contre une dépendance aux fournisseurs de cloud extra-européens, qui détiennent aujourd’hui la majorité du marché.

L’objectif de ce livret est de définir les contours du cloud de confiance, d’explorer ses opportunités et ses défis, ses avantages et ses coûts, afin de stimuler une réflexion globale sur cette solution en plein développement et son intégration dans une approche multicloud.

Nous vous souhaitons une lecture enrichissante.

Pierre Albert
Entreprise Architect - Capgemini

Ambroise Lelievre
Directeur Business Technology
Capgemini Invent

La *souveraineté* s’acquiert et se conserve

Près de neuf organisations sur dix voient le sujet du cloud souverain gagner en importance dans le futur et 52% d’entre elles s’apprêtent à inclure la souveraineté dans leur stratégie cloud selon une étude du Capgemini Research Institute[1].

Covid-19, conflit en Ukraine, tensions sur le marché mondial de l’énergie, des utilities et des matières premières… En France et plus largement en Europe, la souveraineté est devenue un enjeu politique, géostratégique et économique majeur. Si le mot est sur toutes les lèvres, quelle est sa définition exacte ? Elle s’entend comme le caractère d’un État qui n’est soumis à aucun autre État. On cherche l’indépendance. Or, le marché du numérique est dominé par une poignée d’entreprises américaines.

Ainsi, l’écrasante majorité des dépenses cloud en Europe sont consacrées à Amazon, Google ou Microsoft. En parallèle, l’usage du cloud (IaaS, PaaS, y compris le cloud privé) et le développement massif des données progressent à grande vitesse. L’équation à résoudre se pose alors dans les termes suivants : comment permettre l’innovation apportée par les technologies cloud tout en maîtrisant les risques ?

Les trois axes de la souveraineté numérique :

La souveraineté numérique se définit comme la capacité – pour les pays, les organisations et les individus – à s’autodéterminer sur le sujet du numérique.

Cela a un triple impact sur :

La technologie
notamment la réversibilité,

Les données
la localisation géographique des serveurs,

Les opérations
qui les exécute, dans quel pays et avec quel niveau de sécurité ?

[1] *The Journey to Cloud Sovereignty,* Capgemini Research Institute, Juin 2022

Cloud de confiance, un label et des garanties

Pour répondre à de nombreux risques opérationnels, économiques, légaux, réputationnels et de cybersécurité, l'ANSII a établi un cahier des charges exigeants, baptisé SecNumCloud 3.2[2].

Les fournisseurs qui rempliront ces exigences auront le droit d'utiliser le label Cloud de Confiance. Il s'agit pour eux d'exécuter des services cloud depuis le territoire national, par l'intermédiaire d'une entité de droit français, dans le strict respect des lois et des normes françaises. La version 3.2 du référentiel offre en outre une protection contre les risques juridiques liés à l'application de lois extraterritoriales (notamment les règlements américains FISA et Cloud Act).

Dans une *stratégie multicloud*, le cloud de confiance vient compléter le continuum de souveraineté entre deux extrêmes : le cloud public et le cloud privé. Le premier encourage l'innovation mais n'offre pas de protection contre les lois extraterritoriales s'il est opéré par l'un des principaux fournisseurs de cloud (hyperscalers). Le second est bien souvent souverain par construction mais se trouve rapidement limité du point de vue de l'innovation par un catalogue de services limité. Pour surmonter ce dilemme, le cloud de confiance permet aux entreprises américaines de concéder des licences sur leur technologie à des entreprises françaises.

Cloud de confiance, comment se lancer ?

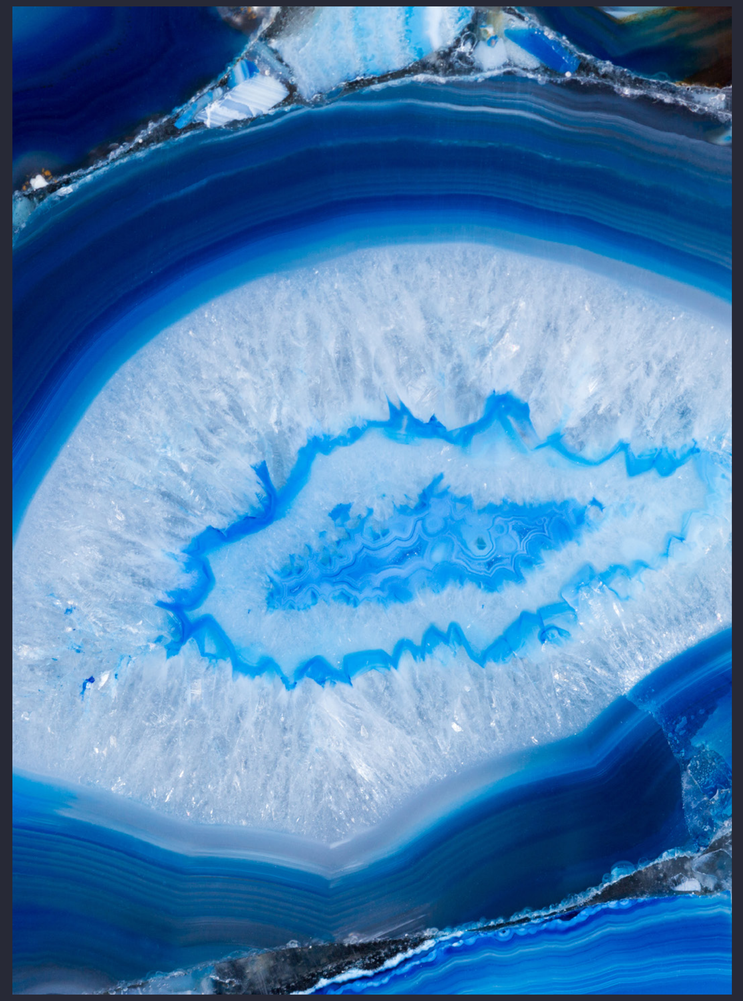
Dans une transformation vers le cloud de confiance, la première étape consiste à établir un *recensement des risques à couvrir*. Cette analyse ne peut se faire de façon macroscopique : il s'agit de descendre aux niveaux des îlots de données et des applications.

Une fois cet état des lieux établi, une stratégie cloud de confiance peut être définie. Elle permet de déterminer quelles données et quels traitements ont vocation à rester sur site (on premise) ; lesquels sont candidats à un cloud de confiance et, enfin, lesquels peuvent sans risque rejoindre un cloud public.

Cette stratégie se décline ensuite en un projet de migration vers le cloud (move to cloud), qui nécessite des points d'attention particuliers. Par exemple, le sujet du chiffrement des données et la gestion des clés associée mérite un traitement spécifique du fait de la sensibilité des données. Pour certaines organisations, le volet collaboratif (messagerie et outils collaboratifs) peut représenter une part importante de la *migration vers un cloud de confiance*.

Si la migration des bonnes données et des bons traitements vers un cloud de confiance est un premier enjeu, le maintien dans le temps de la souveraineté numérique acquise est le deuxième objectif à avoir à l'esprit dès le début du voyage.

[2] *Version 3.2 du référentiel SecNumCloud*, ANSII, 8 mars 2022



Une conduite du changement au long cours

La souveraineté ne s’use que si l’on ne s’en sert pas ! Une fois la migration vers un cloud de confiance réalisée, il convient également de concevoir et d’implémenter les bonnes pratiques relatives aux opérations quotidiennes (run) qui permettent d’inscrire la souveraineté numérique sur le temps long.

4 disciplines sont à traiter dans ce domaine :

1. **La modification des pratiques d’architecture** :
   qui établit la souveraineté par sa conception même (by design).

2. **Les opérations de confiance ou « SovOps »** :
   comment opérer des traitements et comment gérer des données hébergées dans un cloud de confiance ? Avec quel personnel ?

3. **La cybersécurité dans le cloud de confiance** :
   à distinguer de la cybersécurité du cloud de confiance lui-même assurée par le fournisseur. Comment durcir les bonnes pratiques pour prendre en compte la criticité des données et des traitements ?

4. **La maîtrise financière et de l’impact environnemental** :
   comment s’assurer que les coûts d’usage et l’empreinte environnementale du cloud de confiance soient sous contrôle ?

Cinq risques à *anticiper*

Afin de bénéficier des avantages de performance et d'innovation du cloud, les organisations se doivent d'acquérir une compréhension fine des risques associés à l'usage du cloud dans un contexte économique et réglementaire mouvant.

1. Les risques légaux

L'écosystème cloud évolue dans un paysage réglementaire et juridique complexe. Les États légifèrent depuis plusieurs décennies sur le traitement et l'hébergement de données personnelles et industrielles. Les administrations et entreprises s'engagent alors dans une bataille normative qui leur impose de concilier souveraineté et innovation. En ce sens, les risques légaux se structurent autour de deux grands enjeux liés à la donnée :

- **Les transferts de données non maîtrisés en dehors de la juridiction nationale.** À titre d'exemple, deux accords sont successivement venus encadrer ces transferts entre l'Union européenne et les États-Unis afin de définir des principes de respect de la vie privée : le Safe Harbor et le Privacy Shield. Ils ont été invalidés à tour de rôle par la CJUE[1] (arrêts Schrems I & Schrems II) car jugés non-conformes avec la vision européenne de protection des données personnelles (et notamment le RGPD[2]). En mars 2022, la Commission européenne et les États-Unis ont convenu d'un accord de principe « sur un nouveau cadre transatlantique de protection des données personnelles »[3] afin d'apporter une réponse au flou juridique laissé par ces invalidations. Dans cette continuité, le décret exécutif signé par Joe Biden le 7 octobre 2022 devrait s'ensuivre d'une validation par la Commission Européenne au cours des prochains mois.[4]

- **La captation de données par un organisme étranger,** via l'usage d'un outil extraterritorial par un État. L'extraterritorialité peut être définie comme l'exercice d'une autorité législative au-delà de son territoire ; dans notre contexte, cela signifie la capacité d'un État « non européen d'accéder à tout ou partie des données et des traitements hébergés par un offreur »[5]. C'est ce que permet notamment la loi américaine Cloud Act (Clarifying Lawful Overseas Use of Data Act) – sous certaines conditions néanmoins strictes. Dans une autre mesure, les amendements de la section 702 du FISA (Foreign Intelligence Surveillance Act) – aussi visés par l'arrêt Schrems II en 2020 – constituent un risque d'ingérence sur des données européennes.

[1] Cour de Justice de l'Union Européenne
[2] Règlement General Sur La Protection Des Données
[3] *Déclaration conjointe de la Commission européenne et des États-Unis sur le cadre transatlantique de protection des données personnelles, 25 Mars 2022*
[4] *FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework*
[5] *Panorama De La Menace Informatique 2021, ANSSI*

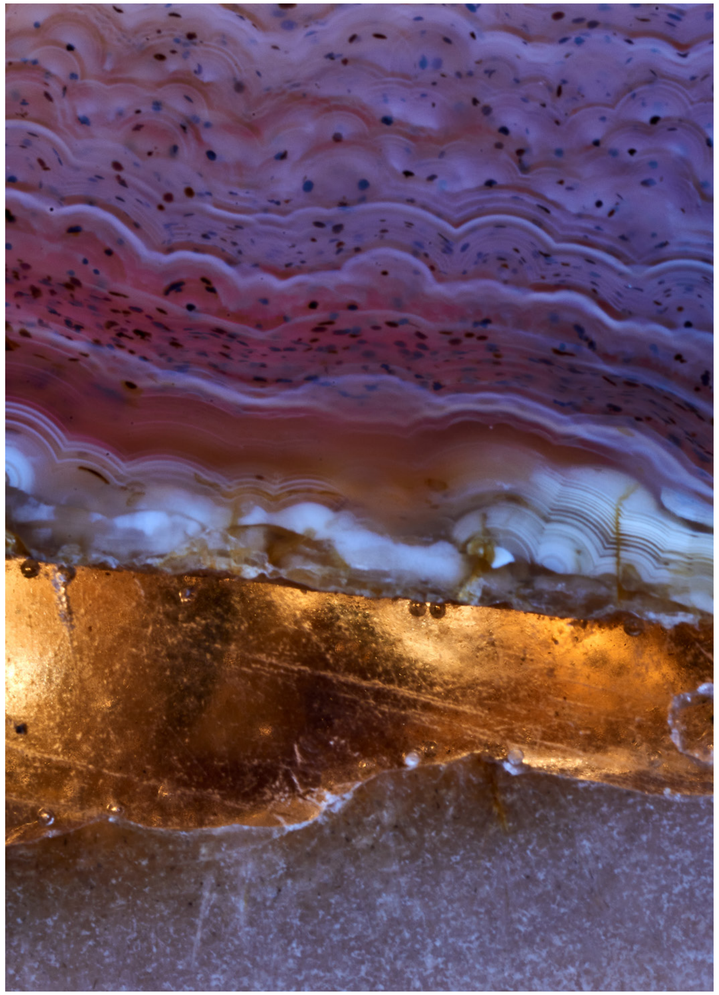
2. Les risques opérationnels

Il s'agit de l'ensemble des risques liés à une éventuelle restriction d'accès aux services cloud. Du fait de leur nature stratégique et/ou régalienne, certaines organisations ne peuvent tolérer aucun incident ni défaillance, ces derniers pouvant avoir « un effet disruptif important sur la fourniture »[6] de leurs activités stratégiques (tout particulièrement les secteurs d'importance vitale comme l'énergie, l'industrie ou la santé).

La dépendance à une technologie ou à des services cloud étrangers augmente fortement ces risques, notamment en cas de tensions et de crises géopolitiques. Ces éléments conjoncturels ont pour effet d'accélérer les réflexions des États et gouvernements à ce sujet. À titre d'exemple, le contexte de guerre en Ukraine a accéléré les réflexions des États européens au sujet de « la résilience des infrastructures télécoms et la protection du cyberespace européen ».[7] Les entreprises et administrations devraient prochainement pouvoir inclure les fruits de ces réflexions afin de mieux appréhender ces incertitudes.

3. Les risques de sécurité

En matière de cloud, la notion de souveraineté repose sur la capacité à contrer différents niveaux de menaces : activistes, cybercriminelles et étatiques. La prévention des risques relève pour partie de la responsabilité des fournisseurs de service mais aussi des organisations utilisatrices.



[6] *Directive NIS*
[7] *Cybersécurité, résilience des réseaux télécoms : la stratégie de l'UE précipitée par la guerre en Ukraine*

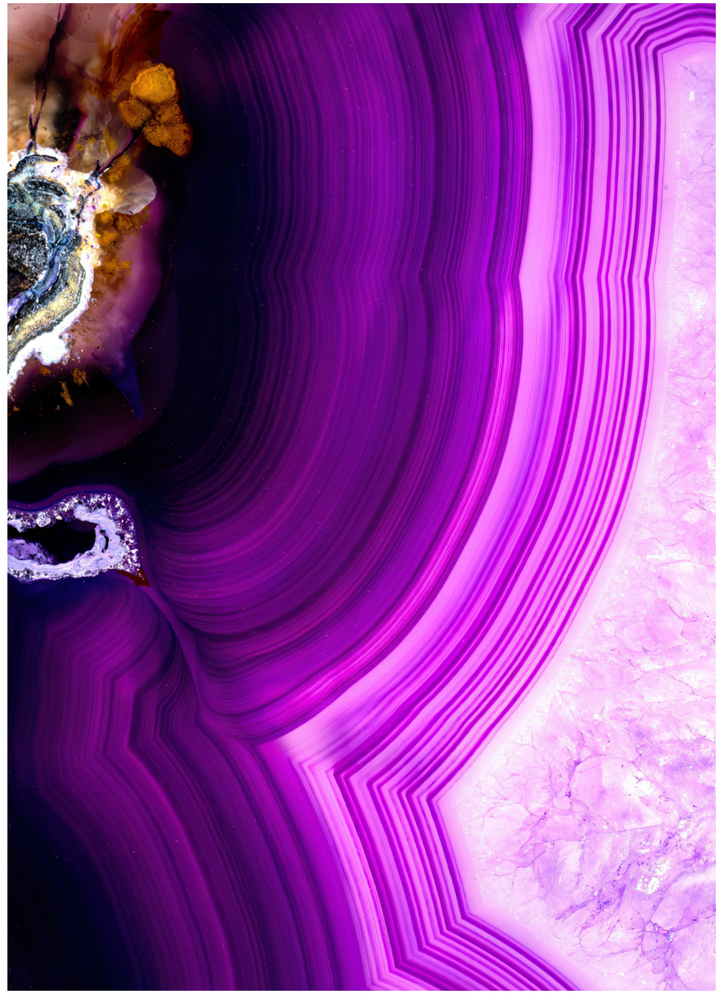
Cybermenaces : un partage des responsabilités entre fournisseurs et utilisateurs

La sécurité du cloud :

relève du fournisseur de cloud (Cloud Service Provider ou CSP). Des certifications existent pour garantir cet aspect, à l'instar de la qualification SecNumCloud en France. Cette catégorie inclut également les risques physiques de perturbation liés à la chaîne d'approvisionnement des services et des composants d'infrastructure qui exposent les organisations à des failles de sécurité multiples (sans compter l'instabilité opérationnelle qu'induit la dépendance à des fournisseurs étrangers). Le défaut de maîtrise des équipements physiques et des serveurs doit être également considéré, afin de limiter le risque d'exposition à des activités d'espionnage. La sécurité dans le cloud, qui fait référence aux dispositifs adoptés par les organisations utilisatrices pour sécuriser les données hébergées et les traitements exécutés dans le cloud. Ces dispositifs peuvent soit être totalement à la charge du client (chiffrage des données externes), soit se baser sur un modèle de responsabilité partagée (le fournisseur met à disposition des services de sécurité qu'il convient au client de configurer et d'opérer).

La sécurité dans le cloud :

qui fait référence aux dispositifs adoptés par les organisations utilisatrices pour sécuriser les données hébergées et les traitements exécutés dans le cloud. Ces dispositifs peuvent soit être totalement à la charge du client (chiffrage des données externes), soit se baser sur un modèle de responsabilité partagée (le fournisseur met à disposition des services de sécurité qu'il convient au client de configurer et d'opérer).



4. Les risques économiques

L'espionnage industriel[8] visant à acquérir des données stratégiques fait également courir d'importants risques économiques aux organisations[9]. En parallèle, le manque de transparence de certains services cloud cristallise les inquiétudes quant à la captation de la valeur dans un contexte de marché dominé par des acteurs principalement américains. Certaines industries et administrations étatiques peinent à développer des cas d'usages innovants tout en garantissant la protection et la confidentialité de leurs « données sensibles », et ce, en raison du manque de solutions de confiance – ce qui impacte leur niveau de compétitivité.

Le manque de réversibilité et de portabilité s'avère également être un frein à l'exploitation de la valeur de ces données via des services cloud. Enfin, les risques économiques sont également liés au risque de non-conformité légale et réglementaire, à titre d'exemple une situation de non-conformité au RGPD peut induire des sanctions financières s'élevant jusqu'à 4 % du chiffre d'affaires annuel mondial d'une entreprise.[10]

5. Les risques réputationnels

Ces risques concernent toute potentielle dégradation d'image causée par l'interruption d'un service, qu'elle soit fortuite (désastre naturel) ou intentionnelle (cyberattaque). Ils sont là encore exacerbés par la dépendance technologique et économique à des acteurs étrangers. Ces risques sont également accrus en Europe où les citoyens sont sensibles à la gestion de leurs données et à la protection de leur vie privée.

[8] Ibid
[9] *Principaux incidents dans l'UE et dans le monde – ENISA, 2020*
[10] *CNIL*

Cloud de confiance : un subtil équilibre à trouver entre sécurité et innovation

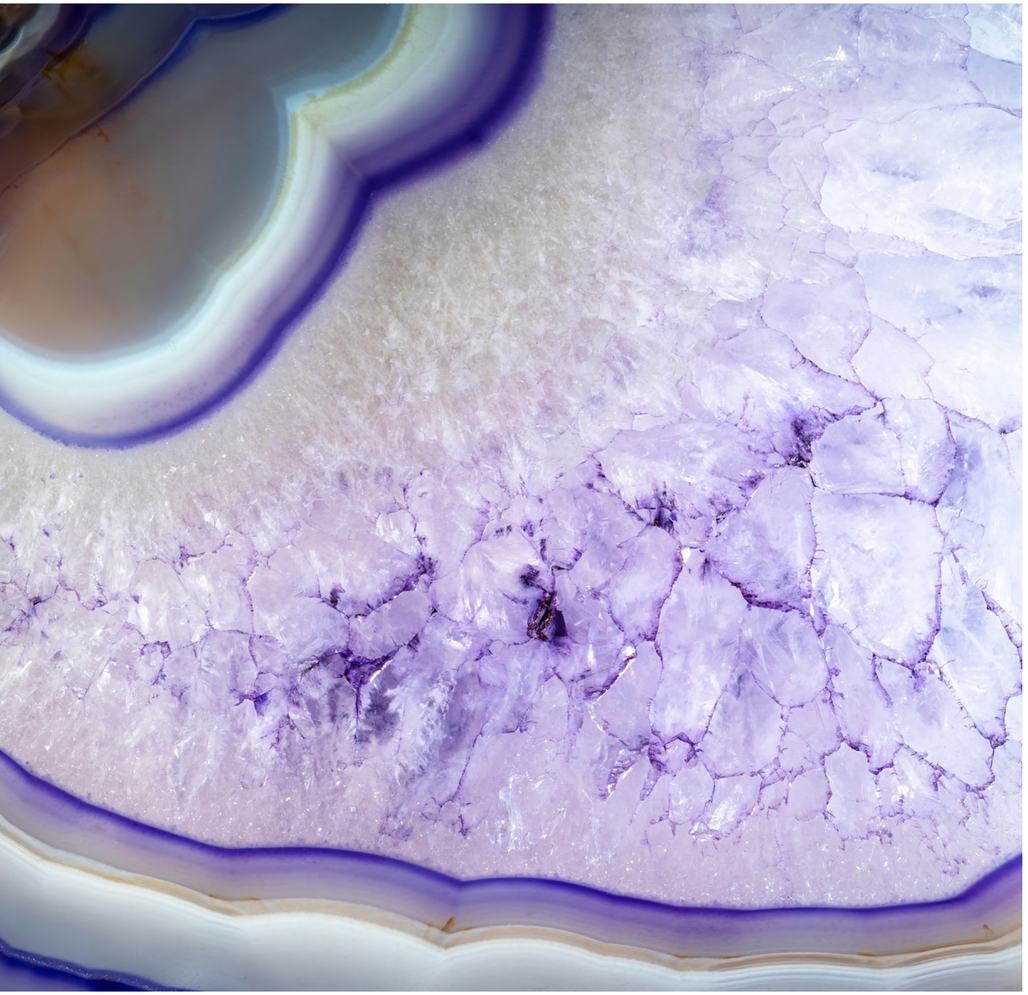
Les organisations doivent donc prendre connaissance de toutes les exigences en matière de conformité imposées par leur pays ainsi que celles applicables à leur secteur d'activité[11]. La conformité du cloud se définit en effet comme le respect des normes de traitement et d'hébergement issues des lois et règlements locaux (par exemple la loi de programmation militaire[12]), européens (RGPD) et sectoriels (à l'instar du cas spécifique des données de santé). Il est également impératif d'identifier et de comprendre les risques relatifs aux réglementations à portée extraterritoriale (par exemple, si les données sont hébergées au sein d'un cloud détenu par une société étrangère). Au vu du caractère mouvant des régulations, une veille doit être instaurée afin de maintenir la conformité dans le temps. Cette phase doit être soutenue par une expertise juridique.

Ensuite, la réflexion doit tendre vers la définition d'un périmètre éligible à la migration dans un cloud de confiance. Cette étape de fléchage doit être construite conjointement avec plusieurs acteurs de l'organisation (incluant les équipes métiers & IT) — dont les CDO (Chief Data Officers) et DPO (Data Protection Officers) — et doit s'intégrer pleinement au sein d'une stratégie hybride et multicloud plus large. La classification des données doit prendre en compte deux principaux éléments : les risques précités et le niveau de sensibilité des données. Cette réflexion doit être tournée vers des cas d'usages métiers.

Au terme de cette réflexion, le choix des offres cloud les plus adaptées peut être réalisé, en phase avec les contraintes de sécurité (accès aux données, techniques de chiffrage, management des clés), de souveraineté (restrictions de localisation, technologie utilisée, gestion des opérations, résilience), et l'ambition d'innover (catalogue de services, écosystème de partenaires, etc.). La transformation vers le cloud de confiance doit également inclure un arbitrage comprenant les contraintes liées à une architecture multicloud ou hybride, incluant les enjeux d'interopérabilité, d'interconnexion, de conformité « bout-en-bout » et les coûts associés[13].

Le cloud de confiance permet ainsi de mitiger ces différents risques interconnectés, tout en permettant aux entreprises et administrations de bénéficier de l'état de l'art technologique impliquant innovation, vélocité et performance.

[11] *The Journey To Cloud Sovereignty* – Assessing cloud potential to drive transformation and build trust, Capgemini Research Institute, 2022
[12] Loi de Programmation Militaire, 2013
[13] *The Journey To Cloud Sovereignty* – Assessing cloud potential to drive transformation and build trust, Capgemini Research Institute, 2022



Cloud confiance : quels sont ses *bénéfices* ? Et à quel coût ?

Le cloud de confiance offre une alternative aux services de cloud public pour les organisations confrontées à des contraintes réglementaires et/ou de souveraineté. Pour autant, elles doivent réussir à piloter ses coûts pour en maximiser sa valeur.

Le cloud de confiance présente des avantages notables :

- la sécurité et la protection contre les lois extraterritoriales. Par son caractère souverain, il est étanche aux lois non-européennes- (Cloud Act américain…) ;
- une protection renforcée du cloud avec des infrastructures robustes et des mesures de défenses efficaces, à l'état de l'art, contre les menaces extérieures ;
- une sécurité optimale dans le cloud. Il intègre des mécanismes avancés de contrôle d'accès, de chiffrement et de surveillance, permettant aux entreprises de protéger efficacement l'intégrité et la confidentialité de leurs données ;
- une sécurité optimale dans les moyens et processus de sécurité disponibles nativement – contrairement aux cloud publics classiques. Il est ainsi possible de limiter l'investissement et la maintenance des solutions de sécurité tierces.

Des coûts supplémentaires

Cependant, les bénéfices ont un coût. Avec le cloud de confiance, les clients peuvent s'attendre à une facture plus élevée de 10 à 20 % par rapport aux offres de cloud public classiques, en raison des mesures de sécurité et de conformité renforcées.

En outre, la mise en place d'un modèle opérationnel de confiance engendre des coûts supplémentaires : former les équipes futures utilisatrices, mais aussi déployer des processus spécifiques pour garantir la sécurité dans le cloud.

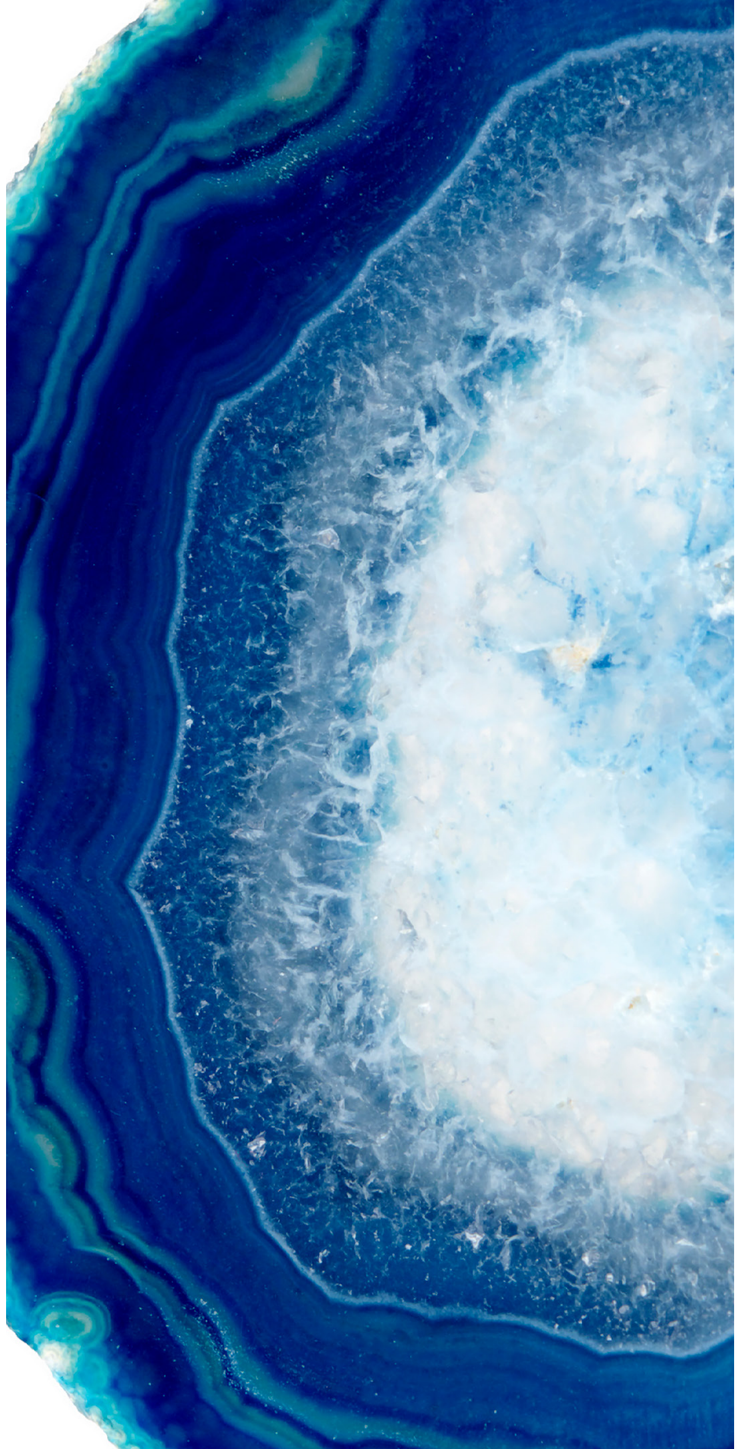
Enfin, l'intégration et l'interopérabilité avec les systèmes d'information des entités et filiales situées hors de l'Union européenne peuvent également entraîner des coûts additionnels. Les entreprises doivent alors déployer des moyens d'interconnexion entre leurs plateformes cloud.

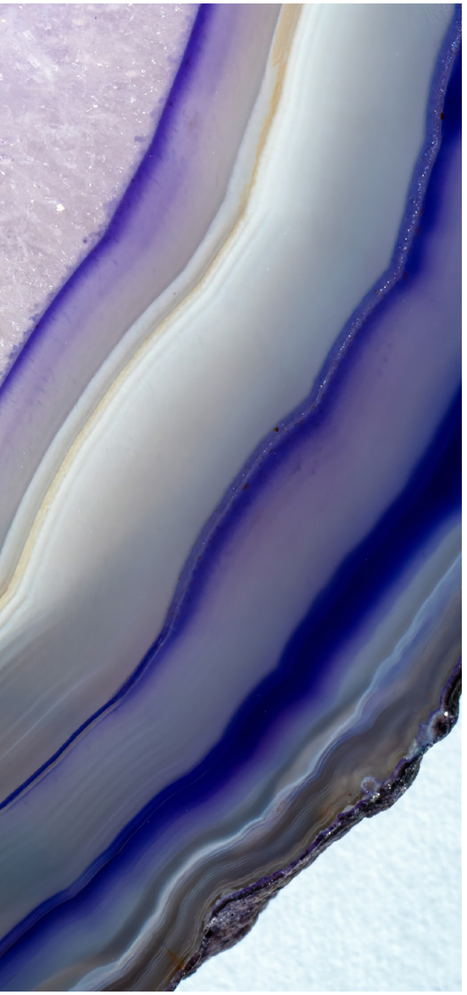
Un arbitrage bénéfices/coûts en faveur du cloud de confiance

Malgré ces coûts additionnels, l'équation économique du Cloud de Confiance peut s'avérer favorable pour les organisations qui souhaitent allier souveraineté, sécurité, agilité et innovation.

La plupart des cas induisent une bascule d'un existant déjà optimisé. L'estimation des coûts associés à la souveraineté doit bien prendre en compte l'état des systèmes d'information existants, souvent déjà optimisés voire amortis, qu'ils soient hébergés dans le cloud public ou pas.

Une réflexion approfondie est nécessaire pour déterminer la stratégie la plus adaptée à l'entreprise, qu'il s'agisse d'adopter un modèle multicloud, de basculer entièrement vers le cloud de confiance, ou d'opter pour une approche hybride en conservant une partie des systèmes sur site (on -premise).





Maximiser la valeur de son cloud de confiance

Pour tirer le meilleur du cloud de confiance tout en limitant ses coûts, les organisations doivent débuter cette réflexion dès la genèse du projet et poursuivre tout au long une démarche FinOps vertueuse.

La migration vers un cloud de confiance offre l'opportunité aux organisations qui auraient déjà réalisé une première migration cloud de repartir d'une page blanche et se remettre à l'état de l'art. Pour maximiser la valeur de cette transition, plusieurs éléments sont à considérer :

- **Piloter** les études d'opportunité (business case) de manière extrêmement précise et assidue pour suivre l'évolution des coûts et bénéfices tout au long du projet et assurer la matérialisation de la valeur attendue.
- **Concevoir** des jalons (landing zones) efficients pour faciliter la migration des applications et optimiser leur gestion une fois déployées dans le cloud de confiance.
- **Anticiper** une latence au démarrage, notamment dans le cas de solutions SaaS qui ne seront pas disponibles immédiatement en version « de confiance ».
- **Automatiser** au maximum les processus (notamment autour du provisioning) pour réduire les coûts et accroître l'agilité de l'organisation.
- **S'appuyer** sur des architectures hybrides pour tirer parti des meilleures fonctionnalités de chaque environnement et assurer une transition en douceur.
- **Anticiper** les négociations contractuelles : il n'y aura probablement pas de vases communicants entre les contrats cadres des principaux fournisseurs de cloud (hyperscalers) et leur équivalent « de confiance ».

Une optimisation en continu avec le FinOps

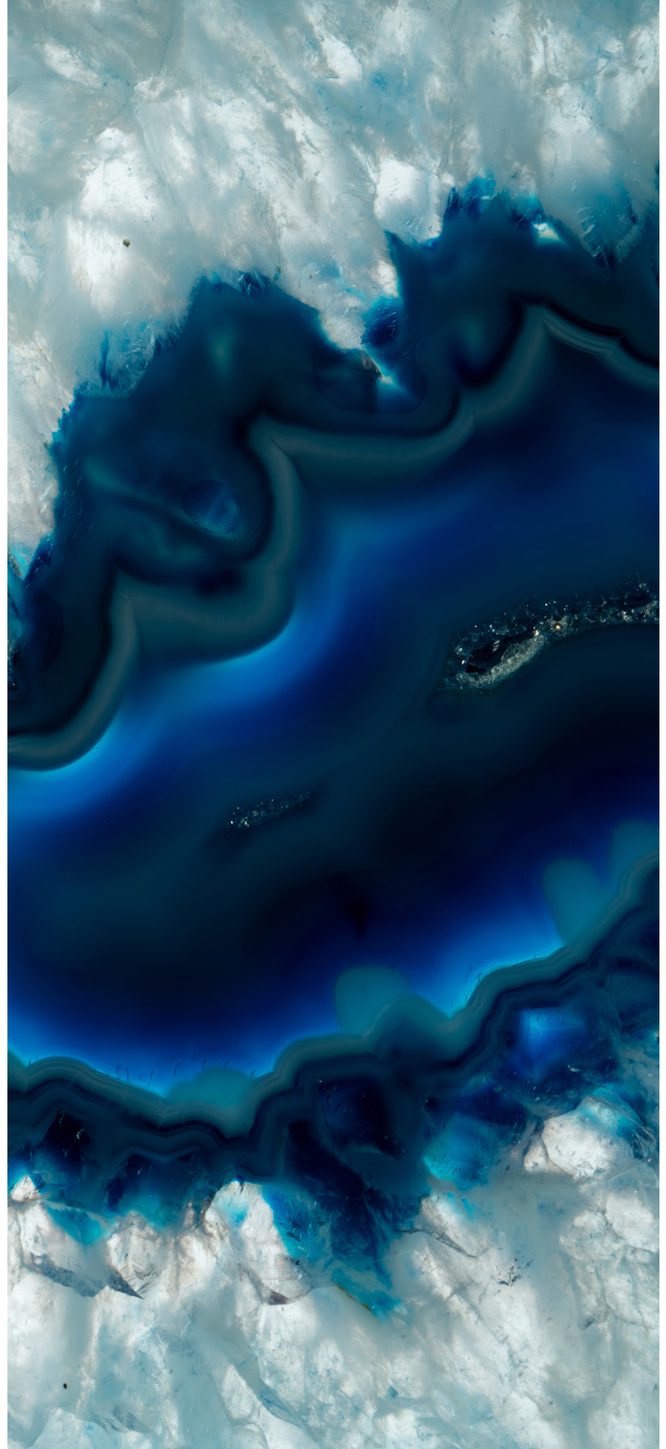
Le cloud de confiance offre certes des avantages majeurs en termes de souveraineté et sécurité des services et données mais sans optimisation, il peut engendrer des coûts supplémentaires. Pour en maximiser la valeur, une approche proactive est nécessaire dès le début des projets, avec l'implication de toutes les parties prenantes dont les responsables métiers, garants des dépenses engagées sur leurs périmètres. Les équipes doivent être formées à ses bonnes pratiques pour une utilisation efficiente des ressources et services.

Il est également essentiel d'appliquer des politiques strictes en ce qui concerne la sélection des niveaux de sécurisation dans une logique de maîtrise des coûts et de conformité.

Enfin, il convient de systématiser les principes du FinOps. Cela passe par la mise en place de tableaux de bord et d'alertes pour suivre de près l'évolution des coûts et des performances. Une automatisation de l'application des principes FinOps (policy as code) fait particulièrement sens ici.

FinOps : des freins encore à lever

Tous les outils et services du FinOps (notamment SaaS) ne seront pas disponibles immédiatement sur les clouds de confiance. Des alternatives devront être analysées : utiliser les services proposés nativement par les fournisseurs (similaires au cloud public), déployer d'autres progiciels ou réaliser des développements internes.



Les piliers d’une *migration* vers le cloud de confiance

Les enjeux sont nombreux pour les organisations : innovation métier, efficacité opérationnelle et organisationnelle, résilience IT et cybersécurité sans oublier souveraineté et durabilité. De multiples variables s’ajoutent à une équation déjà complexe que peu d’acteurs semblent encore maîtriser dans son ensemble.

Maturité numérique

La maturité des entreprises et institutions publiques concernées est très hétérogène. Certaines sont déjà confortablement installées sur des clouds publics (avec des stratégies cloud-first ou cloud-native), d’autres complètent leur SI sur site (on premise) ou leur cloud privé avec du cloud public mais uniquement pour certains cas d’usages spécifiques (cloud hybrides, interopérabilité). Une troisième catégorie d’entreprises a fait le choix de ne s’interfacer avec aucun des géants américains et opère encore intégralement sur leur cloud privé/sur site en complète autonomie.

Diagnostic de l’existant

Chaque projet de migration débute par une phase de diagnostic de l’existant qui vise à réaliser un état des lieux détaillé du parc applicatif, technologique et de l’organisation actuelle. Il conviendra dans un premier temps d’évaluer les risques et aussi d’identifier, qualifier et classifier les données, les traitements et les applications afin de déterminer leurs destination (sur site, cloud de confiance, cloud public).

Quelles données faire migrer ?

Le périmètre des données sujettes à migration sur un cloud de confiance relève d'une combinaison de paramètres : leur sensibilité (de très secret à non-protégé), leur typologie (données stratégiques métiers, économiques, personnelles et santé), la profondeur et les ambitions de la migration (IaaS, PaaS ou SaaS). Cet exercice crucial, qui participe du diagnostic de l'existant, permettra ainsi d'identifier les jeux de données candidats à la migration vers un cloud de confiance.

Quels partenaires choisir ?

Il existe aujourd'hui une petite dizaine d'offres cloud de confiance en Europe, avec des catalogues plus ou moins riches (du IaaS au SaaS qualifiés SecNumCloud SNC). La majorité de ces offres s'appuie naturellement sur Azure, Google, OVHcloud, Outscale, Bleu ou S3NS. Cependant, elles semblent encore assez limitées pour répondre aux process métiers de bout-en-bout (à l'été 2024, les solutions SaaS de confiance étaient encore en cours de qualification SecNumCloud), ce qui pourrait frustrer certaines ambitions de migration pour les acteurs les plus appétents et donc renforcer le recours à une stratégie multicloud à court terme.

Dans un marché qui évolue aussi vite que celui du numérique de confiance, les organisations éprouvent des difficultés à concrétiser leurs projets. Comment établir la bonne stratégie de migration et la feuille de route associée alors qu'une offre plus adaptée pourrait sortir à tout moment ? Il est dès lors essentiel de prévoir une veille concurrentielle et d'être en mesure de faire rapidement pivoter sa stratégie vers la solution la plus adaptée.

Quand l'automatisation *renforce* la souveraineté numérique

Grâce à l'automatisation, les entreprises peuvent répondre aux enjeux de sécurité et de souveraineté numérique avec du personnel français ou européen, et ce, à des coûts acceptables, tout en s'inscrivant dans une démarche durable.

De nombreuses entreprises veulent bénéficier d'infrastructures informatiques fiables et sécurisées, tout en soutenant l'économie locale. L'automatisation et les outils de gestion des infrastructures permettent la relocalisation des activités sur le territoire français avec des coûts de mise en œuvre compétitifs par rapport aux solutions offshore actuelles. Cette orientation permet de répondre à la fois aux enjeux de souveraineté par la localisation en France d'activités à forte valeur ajoutée, à l'augmentation de la vélocité de l'exécution (delivery), à la fiabilisation des actions de gestion des infrastructures, à l'évolution des systèmes et à la réduction des coûts de gestion de ces mêmes infrastructures.

L'hyperautomatisation vise à automatiser les processus et fonctions de gestion des infrastructures informatiques de bout-en-bout, sans intervention humaine :

- observabilité du système d'information ;
- service management (gestion des incidents, des problèmes, des changements, etc.),
- AIOps (opérations intelligentes telles que les corrélations, les analyses de causes racines ou d'impacts, les prévisions de fonctionnement des services métier, les services intelligents de traitement de tâches, etc.)
- reporting et de tableaux de bord des services. Tous ces éléments sont orchestrés et interconnectés par des outils d'automatisation modernes et récents ainsi que d'autres bus d'échanges d'entreprise.
- Cette approche permet de gagner en rapidité (temps de traitement), en fiabilité (réduction des erreurs) et en efficacité (précision des opérations).

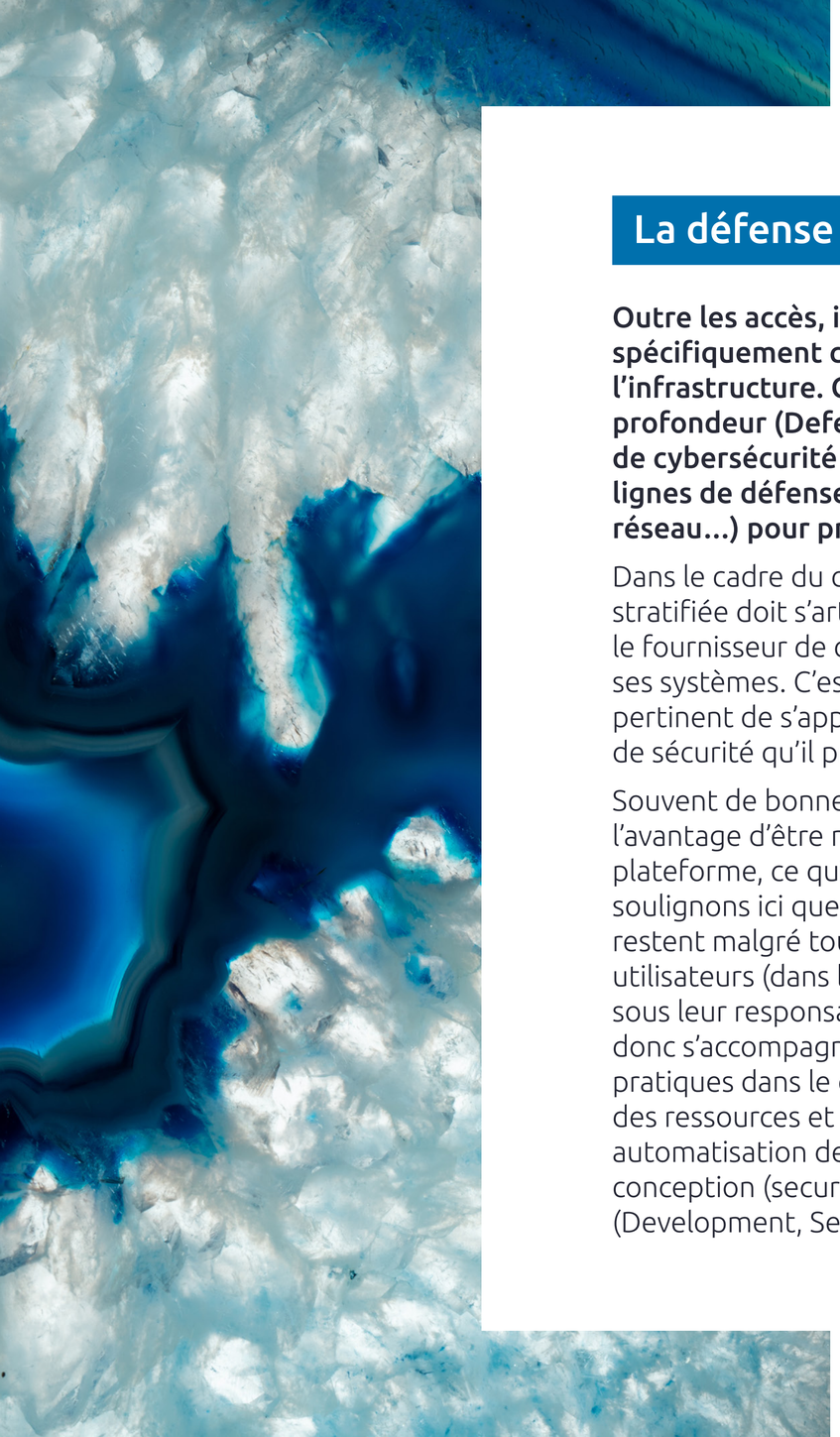
Cybersécurité, une responsabilité partagée

Les entreprises et institutions font le choix du cloud de confiance pour manipuler en toute sécurité des données sensibles. Les services conformes aux exigences SecNumCloud 3.2 et labellisés cloud de confiance apportent nombre de garanties dans la sécurisation de l'environnement, en complément des dispositions prises par les clients (applications, données, processus).

La gestion des identités et des accès

La gestion des identités et des accès (Identity and Access Management, IAM) est la pierre angulaire de la sécurité dans le cloud. Gérant à la fois l'identité, l'authentification et les habilitations, elle garantit que les utilisateurs — humains ou machines —ne peuvent accéder qu'aux seules données et applications qui leur sont autorisées.

Incontournable et omniprésente, non seulement l'IAM conditionne le niveau de sécurité dans le cloud, mais elle favorise aussi grandement la fluidité des échanges, des expériences et des projets. L'IAM est également la clé de voûte du modèle zero trust. Basé sur une vérification systématique des identités et des droits avant chaque action, et pas seulement au moment d'accéder au système, cette approche requiert une gestion des droits très fine, largement automatisée, et qui n'accorde à chaque utilisateur que les autorisations qui lui sont strictement nécessaires. De ce fait, le modèle zero trust peut être envisagé comme une approche globale pour protéger l'environnement cloud et ses composantes (identité, réseau, données…). En outre, la mise en place d'un modèle opérationnel de confiance engendre des coûts supplémentaires : former les futures équipes utilisatrices, mais aussi déployer des processus spécifiques pour garantir la sécurité dans le cloud.



La défense en profondeur

Outre les accès, il convient de sécuriser spécifiquement chacune des couches de l'infrastructure. C'est le principe de la défense en profondeur (Defense in Depth, DiD), une doctrine de cybersécurité qui consiste à dresser plusieurs lignes de défense (au niveau matériel, logiciel, réseau…) pour protéger les informations.

Dans le cadre du cloud de confiance, cette approche stratifiée doit s'articuler avec les mesures prises par le fournisseur de cloud pour protéger physiquement ses systèmes. C'est pourquoi il est souvent pertinent de s'appuyer sur les outils et les services de sécurité qu'il propose (pare-feux, antivirus…).

Souvent de bonne qualité, ces solutions ont l'avantage d'être nativement intégrées à la plateforme, ce qui facilite leur mise en œuvre. Enfin, soulignons ici que les diverses mesures de sécurité restent malgré tout tributaires de la prudence des utilisateurs (dans les limites des couches placées sous leur responsabilité). Leur mise en œuvre doit donc s'accompagner d'un renforcement des pratiques dans le contexte du cloud : destruction des ressources et des données inutiles, automatisation des mises à jour, sécurité par la conception (security by design), DevSecOps (Development, Security, Operations)…

Chiffrement : protéger les données sensibles

Pour protéger efficacement ses données, le chiffrement demeure fondamental. Sa mise en œuvre dans le cadre d'un cloud de confiance, et donc sur des données des plus sensibles, présente cependant quelques spécificités. Il faut ainsi s'assurer que les données resteront en permanence dans l'environnement maîtrisé du cloud de confiance et ne soient pas exfiltrées, au moment de leur traitement, vers une plateforme qui ne bénéficierait pas des mêmes protections juridiques.

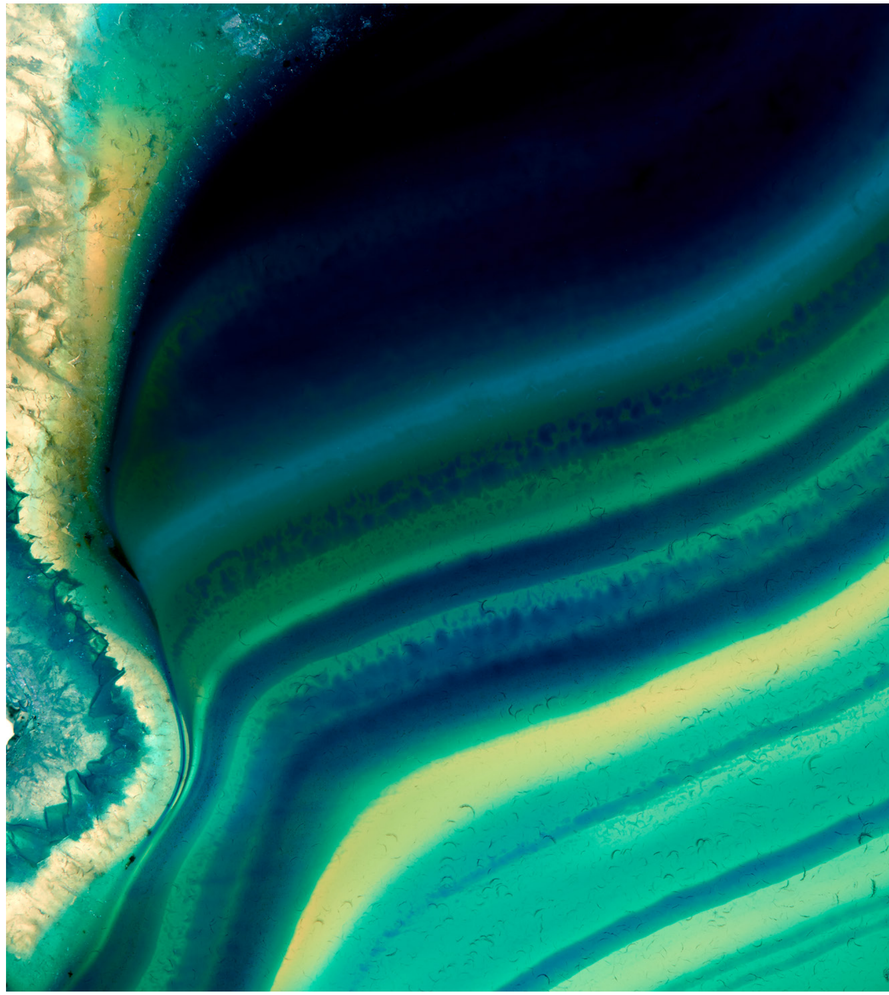
Pour surveiller les fuites et transferts de données d'un environnement à un autre, il est indispensable de mettre en place des outils spécifiques, à l'image des solutions de type CASB (Cloud Security Access Broker) qui s'interfacent avec les services cloud et contrôlent les flux de données tout au long de leur cycle de vie.

Le choix d'outils tiers destinés à manipuler les données doit faire l'objet d'une attention redoublée. On veillera en particulier à ce qu'aucune opération ne soit réalisée en dehors d'un environnement labellisé « cloud de confiance » car tel est bien l'enjeu : la donnée peut circuler entre les systèmes mais elle ne doit jamais sortir, même très brièvement, de ce cadre protecteur. Et il est essentiel de sensibiliser toutes les équipes à cette exigence capitale.

Enfin, dernier point de vigilance concernant les données : veiller à ce que les clés de chiffrement ne soient pas stockées au même endroit que les données pour qu'il soit impossible d'y accéder simultanément. À cette fin, on pourra utiliser un matériel dédié (Hardware Security Module, HSM).

Présumer la compromission (Assume Breach)

Dans un environnement aussi complexe et mouvant que le cloud, fût-il de confiance, et face à des assaillants extrêmement compétents, équipés et déterminés, la sécurité absolue n'existe pas. Tel est le principe de la posture Assume Breach, qui invite à se montrer réaliste et pragmatique. Puisqu'un incident de sécurité finira toujours par se produire, il faut s'être préparé de manière à pouvoir le détecter et alerter au plus tôt, réagir rapidement et à bon escient pour en limiter les conséquences, puis en réparer les éventuels dégâts et, enfin, en tirer les enseignements. Tout ceci nécessite la mise en place d'un outillage, d'une organisation et de processus appropriés, que des exercices grandeur nature permettront de tester, valider et optimiser.



Sécuriser la migration de données

À l'image d'un déménagement qui nous conduit parfois à laisser des portes grandes ouvertes et des objets sans surveillance, les opérations de migration engendrent des risques importants. Que le point de départ ou d'arrivée soit un cloud de confiance ne peut que les amplifier en éveillant des intérêts malveillants. Même si les opérations sont similaires à celle d'une migration vers le cloud ordinaire, il faut donc procéder avec une rigueur accrue en s'appuyant notamment sur le chiffrement. Il ne faudra aussi pas non plus omettre d'effacer les données de la plateforme d'origine.

Toutes ces solutions et ces bonnes pratiques permettent de doubler les garanties apportées par le cloud de confiance d'un dispositif de sécurité complet et renforcé. Leur mise en œuvre – comme d'ailleurs le choix d'un cloud de confiance – reste toutefois subordonnée à une appréciation en amont des risques, c'est-à-dire du rapport entre la gravité et la probabilité des menaces. Cette analyse permet de déterminer le juste niveau de protection à mettre en œuvre et la priorité des actions à mener en tenant compte de l'ensemble des contraintes et des exigences (réglementaires, budgétaires, opérationnelles…).

La gestion des risques dans le cadre d'une stratégie *multicloud*

La question de la souveraineté numérique n'est pas nouvelle, elle a toujours existé lors de la formulation des stratégies de cloud. L'évolution majeure tient à l'émergence de nouvelles offres.

Au cours des dernières années, la transformation numérique des activités des entreprises faisait l'objet d'un choix binaire : soit elles pouvaient être transférées vers un cloud public, soit elles devaient rester dans une infrastructure sur site, idéalement un cloud privé construit et géré sous le contrôle strict de l'entreprise. L'arbitrage était donc réalisé entre un riche catalogue de services externes sous le contrôle direct d'un tiers, ou une infrastructure contrôlée en interne avec un ensemble de services plus limité. Si ce principe de conception des stratégies de cloud n'a pas fondamentalement changé, les possibilités offertes sont désormais plus étendues et nuancées, permettant des stratégies plus sophistiquées.

Aux côtés des clouds publics et privés, l'arrivée du cloud de confiance conforme au SecNumCloud 3.2 offre une 3e option. Il faut noter que les catalogues de services des fournisseurs de cloud de confiance ont tendance à être riches, avec des maturités différentes et parfois spécialisés, rendant le spectre des possibilités encore plus large.

Souveraineté : l'âge de la maturité pour les organisations

Du point de vue de la gestion des risques, la maturité des entreprises face aux différentes typologies de risques est croissante : économiques, concurrentiels, géopolitiques, réglementaires, réputationnels, pour n'en citer que quelques-uns. Cette nouvelle maturité facilite l'analyse des domaines applicatifs, voire des applications individuelles et des portefeuilles de données. Cette granularité accrue apporte une vision plus précise de ce que la notion de souveraineté signifie concrètement pour chaque organisation.

Des stratégies multicloud dynamiques

Bien que la notion de souveraineté semble immuable, sa mise en pratique dans le secteur du cloud est mouvante, en raison de multiples paramètres :

- **Le paysage concurrentiel** de nombreux secteurs évolue très rapidement, ce qui exige une innovation permanente dans les cas d'usage et d'utilisation des données.
- **Les catalogues de services** des fournisseurs de cloud se développent à une vitesse vertigineuse, tant pour le public que pour le privé.
- **Le paysage réglementaire** évolue en permanence – au niveau national et européen.
- **De multiples fournisseurs** de services innovants de cloud de confiance existent ou sont annoncés dans un espace qui devient rapidement riche d'options.
- **La volatilité liée à la géopolitique** et aux pandémies perturbe les chaînes d'approvisionnement, y compris celles des fournisseurs de cloud. Cela n'est pas sans impact sur l'équilibre de la stratégie – les coûts de l'énergie et les perturbations dans les chaînes d'approvisionnement en semi-conducteurs font partie de l'équation.

Le contexte de chaque organisation a naturellement sa propre dynamique. Cela nécessite une attention continue de la part d'équipes multidisciplinaire (experts cybersécurité, commerce, informatique et architectes) pour conserver l'équilibre entre contrôle et innovation.

Dans le cas spécifique des stratégies multicloud, presque tous les projets seront soumis aux forces en mouvement :

- **Les projets d'adoption de technologies innovantes** proposées par les fournisseurs de cloud, comme l'IA, les données ou le low code/no code (ces plateformes et outils de développement qui permettent aux utilisateurs métier de concevoir et de développer simplement leurs application) ;
- **Les initiatives commerciales existantes et futures** soumises à des réglementations en matière de confidentialité des données ou de résidence qui évoluent au fil du temps ;
- **Les dates de fin des contrats d'externalisation** existants, que ce soient des contrats d'infogérance ou d'hébergement ;
- **Les approches FinOps**, en particulier lorsqu'elles impliquent l'utilisation d'instances réservées sur de longues périodes.

La clé : l'anticipation

La plupart de ces dossiers, y compris les plus ardus (comme l'évolution de la réglementation autour du cloud de confiance et la norme SecNumCloud 3.2) sont d'ores et déjà entre les mains des dirigeants. Pour faire de leur stratégie multicloud un succès, ils doivent assigner les bonnes priorités, mobiliser les bonnes ressources multidisciplinaires tout en accédant aux bonnes informations, le tout dans le tempo stratégique de leurs impératifs métier.

Né à la toute fin des années 1990, **le cloud connaît aujourd'hui un pic de croissance**, avec des investissements qui atteignent chaque année de nouveaux sommets. À cela s'ajoute un contexte réglementaire mouvant, portant sur la sécurité mais aussi sur les exigences qui pèsent désormais sur les entreprises en matière de **responsabilité sociale et environnementale**.

Le cloud de confiance porte une promesse essentielle : il permettra demain aux entreprises de **tirer parti des dernières innovations**, à l'instar de l'IA générative, dans le cadre d'un écosystème de sécurité, avec la certitude de conserver la main sur leurs données.

Le défi pour les entreprises sera de s'adapter à cet écosystème en mutation, de saisir les opportunités et d'épouser les contraintes liées aux nouvelles normes. Pour y parvenir, elles peuvent compter sur le soutien de leurs partenaires technologiques. **Un soutien indispensable, tant le cloud se définit comme une équation complexe, aux multiples variables et en perpétuelle évolution**.

Contributeurs

Pierre Albert
Entreprise Architect
Capgemini

Serge Baccou
Head of South and Central Europe
Azure Cloud COE
Capgemini Invent

Skander Guetari
Expert en Infrastucture
Transformation Services
Capgemini

Thomas Heron
Architecte d'entreprise
Capgemini

Lucas Lauret
Manager Cloud
Capgemini Invent

Ambroise Lelievre
Directeur Business Technology
Capgemini Invent

Abdembi Miraoui
Co-Head of Service Line
"Cloud, Endpoint &
Infrastructure Security"
Capgemini

Thomas Sarrazin
FinOps Offer Leader
Capgemini

Camille Sebire
Consultante offre
Cloud Souverain / Cloud de Confiance
Capgemini Invent

Benoit Thibaut
Group Industrialization
Design Autority Leader
Capgemini

À propos de Capgemini

Capgemini est un leader mondial, responsable et multiculturel, regroupant près de 360 000 personnes dans plus de 50 pays. Partenaire stratégique des entreprises pour la transformation de leurs activités en tirant profit de toute la puissance de la technologie, le Groupe est guidé au quotidien par sa raison d'être : libérer les énergies humaines par la technologie pour un avenir inclusif et durable. Fort de 55 ans d'expérience et d'une grande expertise des différents secteurs d'activité, Capgemini est reconnu par ses clients pour répondre à l'ensemble de leurs besoins, de la stratégie et du design jusqu'au management des opérations, en tirant parti des innovations dans les domaines en perpétuelle évolution du cloud, de la data, de l'Intelligence Artificielle, de la connectivité, des logiciels, de l'ingénierie digitale et des plateformes. Le Groupe a réalisé un chiffre d'affaires de 22 milliards d'euros en 2022.

Get The Future You Want*

*Capgemini, le futur que vous voulez.

Plus d'informations sur
www.capgemini.com/fr-fr