[sfeir]

en colloboration avec

PAC

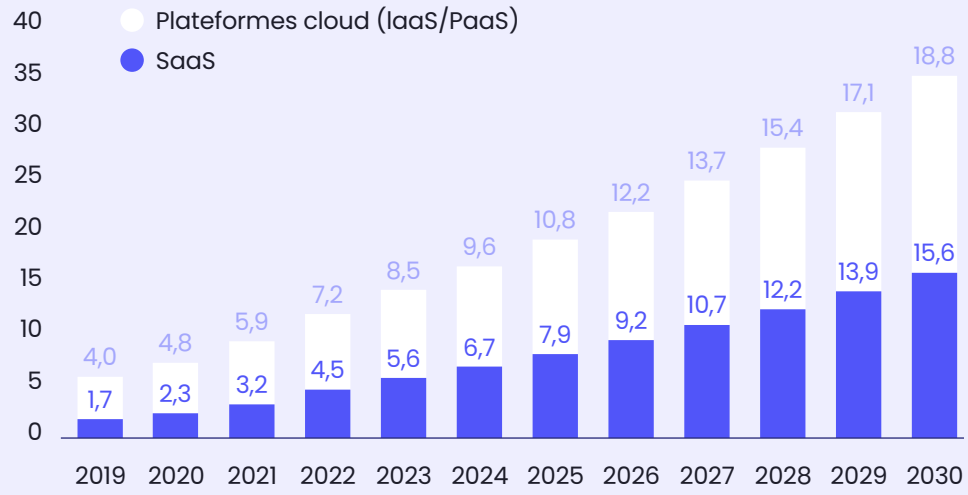
De la souveraineté forteresse à la résilience

Le cloud de confiance permet d'allier innovation et sécurité

En 2025, pour la première fois, plus de 50 % des dépenses IT des entreprises auront été investies dans des solutions cloud, que ce soit pour leurs infrastructures (IaaS/PaaS) ou pour moderniser leurs logiciels d'entreprise (SaaS). PAC estime que la croissance devrait demeurer soutenue, à +12,6% en moyenne sur la période 2026-2030, portée par plusieurs dynamiques structurelles.

Cet investissement permet aux entreprises de gagner en agilité et de réduire le time-to-market de leurs nouveaux services. L'explosion des volumes de données rend aussi indispensables des infrastructures scalables et résilientes. Enfin, l'essor de technologies comme l'intelligence artificielle repose largement sur des environnements cloud capables de fournir une puissance de calcul et des services à la demande.

Évolution des dépenses cloud (IaaS/PaaS et SaaS) en France
(en Md€)



[Avant-propos]

Le cloud de confiance permet d'allier innovation et sécurité

Cette dynamique s'accompagne toutefois d'une prise de conscience croissante des enjeux de souveraineté alors que le marché du IaaS/PaaS est dominé par les hyperscalers américains et que SAP est le seul éditeur de logiciels européens apparaissant dans le top-10 mondial. En effet, dans un environnement géopolitique incertain, la question de la maîtrise des données et des infrastructures devient critique. Longtemps perçue comme un sujet théorique ou réglementaire, la souveraineté numérique s'impose désormais comme un enjeu opérationnel et devient un critère structurant dans les décisions d'architecture IT.

des grandes entreprises françaises envisagent une migration vers des solutions de cloud de confiance à court terme

Les entreprises ont pleinement intégré ces enjeux. Selon une enquête menée auprès de 150 grandes sociétés françaises (PAC CxO Survey - Digital Sovereignty 2025 and beyond), 7% d'entre elles ont déjà migré certains workloads vers des solutions de cloud de confiance et 36% envisagent de le faire à court terme.

Cette évolution traduit une volonté de reprendre le contrôle, tout en conciliant les impératifs de performance et d'innovation.

Pour autant, la souveraineté doit être appréhendée dans toute sa complexité. Elle ne se limite pas à la localisation des données, mais repose sur différents critères, que ce soit la nationalité des hébergeurs, la souveraineté opérationnelle, qui concerne le contrôle des opérations et des accès, ou la souveraineté technologique, qui renvoie à la dépendance à des solutions et à des fournisseurs non européens. Il est donc important de comprendre les besoins de chaque entreprise et de chaque workload, afin d'éclairer au mieux les choix et d'adapter les stratégies en fonction des niveaux de criticité et des usages.

Dans ce contexte, les entreprises de services du numérique (ESN) comme SFEIR jouent un rôle clé, et PAC se montre optimiste quant à la croissance du secteur. En effet, au-delà de la mise en œuvre technique, leur valeur réside dans leur neutralité et leur aptitude à définir des trajectoires adaptées, à arbitrer entre les différents modèles de cloud et à construire des environnements hybrides conciliant innovation, performance et souveraineté.

Eric Baudet
Senior Analyst PAC

La Souveraineté IT, un questionnement stratégique

C'est une réalité en ce début d'année 2026 : la "souveraineté IT" n'est plus seulement un sujet qui anime les conversations sur Linkedin mais un questionnement réel et sensible au sein des DSI. Une préoccupation qui s'inscrit dans une réflexion plus globale sur la dépendance stratégique IT de l'Europe envers les États-Unis.

Ce questionnement est d'abord motivé par le refroidissement transatlantique sur le terrain du numérique (et pas seulement malheureusement) avec une Union Européenne qui assume davantage ses règlements (DMA, DSA), et des États-Unis qui brandissent plus facilement leur outillage de rétorsion (les taxes douanières) quand ils estiment que leurs champions sont visés.

Cette rhétorique internationale prend un relief particulier à l'heure de la révolution de l'intelligence artificielle générative qui accélère cette dépendance. Quand l'IA devient la nouvelle chaîne de montage de l'ingénierie logicielle, les questions de dépendance qui en découlent font écho à celles sur la montée en puissance du cloud et des hyperscalers.

Les DSI, et plus largement les COMEX, se retrouvent aux prises avec cette double tension : tandis que la géopolitique éloigne pour l'heure les États-Unis de l'Europe, parfois jusqu'au flirt avec des lignes de rupture, l'innovation technologique, moteur de croissance, les lie toujours plus fortement.

À la clé, une crainte : voir les technologies de nos systèmes d'information devenir une composante parmi d'autres des deals inter-États… Et une question : comment penser la souveraineté IT pour lui donner corps et la rendre opérable ? Une question à nos yeux trop souvent mal posée.

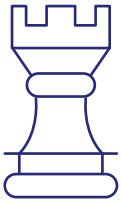
Face aux risques de vendor lock-in et aux effets de bords des tensions entre les États-Unis et l'Europe, SFEIR plaide pour une résilience, composée de scénarios gradués selon la sensibilité des données. Entre cloud de confiance et souverain, entre architectures open source et modèles propriétaires, l'objectif n'est plus l'autarcie, mais la capacité à rester maître de sa trajectoire technologique sans sacrifier la compétitivité.

[Au menu]

01

Un enjeu mal posé et des malentendus

La souveraineté IT, version forteresse nationale



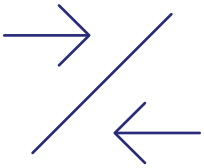
Historiquement, les débats autour de la souveraineté ont été dominés par une vision défensive, dans un esprit de "forteresse nationale". Être souverain, cela voulait dire s'appuyer sur des technologies conçues, développées et opérées sur le territoire national, avec des capitaux nationaux. Un discours souvent couplé à celui sur le logiciel libre et à la perspective du développement d'une dynamique communautaire nationale du libre suffisamment puissante pour assurer une forme d'autarcie.

Cette vision de la souveraineté s'est vite révélée inopérante face au rythme de l'innovation logicielle portée par les acteurs commerciaux (Américains mais pas uniquement). La complexité croissante des systèmes d'information, la nécessité de disposer d'une puissance de calcul élastique à l'échelle mondiale ("hyperscale") et l'émergence de l'intelligence artificielle générative (GenAI) ont rendu l'approche autarcique non seulement coûteuse, mais aussi dangereuse pour la compétitivité des organisations.

La réalité le rappelle au quotidien : l'enjeu n'est pas tant de décréter une pureté technologique que d'arbitrer des dépendances au regard du risque, du coût et de la vitesse d'innovation. De fait, une entreprise qui s'interdirait aujourd'hui l'accès aux modèles de langage les plus performants ou à une infrastructure cloud au nom d'une vision jusque-boutiste de la souveraineté risquerait une obsolescence rapide, au prix de sa souveraineté… économique.

La notion de souveraineté IT n'est pas anachronique, loin de là – le contexte international justifie pleinement une réflexion sur le sujet – mais son appréhension sur le mode historique de la forteresse nationale se heurte à un principe de réalité. Et appelle un autre paradigme capable de concilier souveraineté et compétitivité.

La souveraineté IT, un rapport de force



Tenter de penser de manière opérable la souveraineté IT en 2026, c'est d'abord regarder les risques auxquels expose une perte de souveraineté.

Le risque économique tout d'abord. Une entreprise cesse d'être souveraine dès lors qu'elle est contrainte d'accepter des conditions qu'elle refuserait si elle était libre. C'est donc ici un enjeu de **souveraineté économique et entrepreneuriale**.

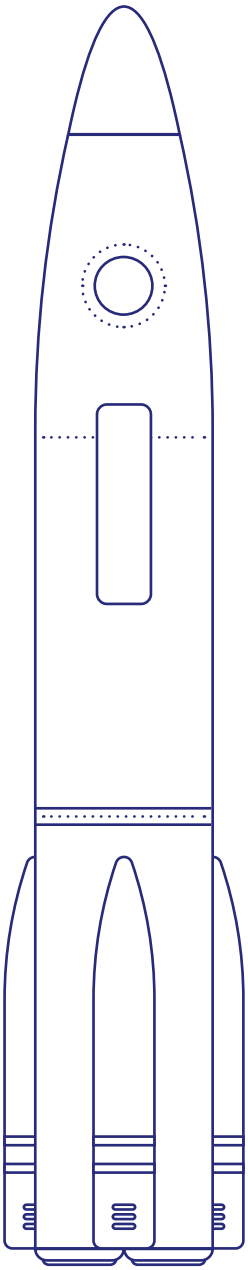
Les exemples ne manquent pas. Cas emblématique, le rachat de VMware par Broadcom. Une acquisition qui s'est soldée par la suppression des licences perpétuelles au profit de modèles pay-as-you-go et d'abonnements sur trois ans avec une tarification prédéterminée. Notons aussi que la bascule de l'industrie logicielle vers le modèle SaaS favorise ces risques. À défaut d'une réversibilité à portée de moyens, de nombreuses organisations subissent les augmentations tarifaires de leurs abonnements SaaS.

Le risque économique n'est pas le seul auquel expose une perte de souveraineté. Pour être complet, il faut évoquer aussi un autre risque parfois laissé dans l'ombre que l'on pourrait nommer "la perte de **souveraineté de valeurs**". Un sujet devenu très concret quelques semaines seulement après le début du second mandat de Donald Trump.

Pour rappel, dans la foulée des annonces mettant fin aux programmes de diversité, plusieurs entreprises de la tech, des éditeurs et de grands acteurs du conseil et des services, ont adopté le ton et les éléments de langage du président nouvellement élu et ont renoncé à leurs objectifs ou programmes en matière de diversité.
La dépendance ici peut conduire une organisation à se retrouver de fait associée à un partenaire dont les valeurs sont bien éloignées des siennes.

Souveraineté économique ou souveraineté de valeurs, l'histoire reste la même : celle d'un rapport de force. Sans alternative, le client subit la loi du plus fort. Et l'actualité des derniers mois rappelle qu'aucune entreprise ne peut faire l'économie d'une réflexion et d'un plan d'actions.

La souveraineté IT, une fusée à 3 étages



Prenons le temps d'un détour par les fondamentaux. Le temps de rappeler que la souveraineté IT, dans son acceptation la plus courante, se compose de plusieurs souverainetés.

1

La souveraineté des données.

Soit le droit et le contrôle qu'exerce une organisation sur ses données, en vertu des lois du territoire où celles-ci sont collectées, traitées et stockées.

2

La souveraineté opérationnelle.

Soit la capacité d'une organisation à garder le contrôle complet sur le management, la maintenance et l'exploitation de son système d'information.

3

La souveraineté technologique.

Soit la capacité d'une organisation à maîtriser les outils et plateformes sur lesquels elle s'appuie, en réduisant la dépendance envers un fournisseur unique ou un ensemble de technologies étrangères.

Ces trois composantes renvoient à des questions distinctes et ne peuvent donc être traitées avec le même outillage. Surtout si l'on souhaite aboutir, ce qui est le cas ici, à des réponses actionnables.

La souveraineté IT, une fusée à 3 étages

1.

Concernant **la souveraineté des données**, l'enjeu est connu. Les hyperscalers américains sont soumis au **Cloud Act américain**. Autrement dit, les autorités des États-Unis peuvent demander à tout prestataire de services soumis au droit américain de fournir des données, même si ces données sont stockées dans des centres de données situés à l'étranger. Le fait pour un prestataire américain de disposer de "régions" en France ne résout donc pas le problème (sauf si ce cloud est dissocié du cloud "mondial" et opéré par une filiale de droit local). Mais une solution existe : des acteurs de droit français (on y revient) déploient des offres cloud sur lesquelles les données sont hors d'atteinte de l'extraterritorialité des lois américaines.

2.

La souveraineté opérationnelle, quant à elle, renvoie à la capacité d'exploiter, de maintenir, de faire évoluer et, au besoin, de migrer ou d'arrêter un système d'information, tout en garantissant la continuité d'activité, la sécurité et la conformité. Et cela sans se retrouver contraint ou empêché par un fournisseur, une localisation d'infrastructure ou un cadre juridique étranger.

Dans le détail, la souveraineté opérationnelle ouvre donc un large éventail de sujets :

- **La maîtrise des opérations quotidiennes** : contrôle des processus d'exploitation, supervision, sécurité, mises à jour, gestion des incidents et reprise après sinistre..
- **La capacité d'audit des opérations** : visibilité sur où et comment sont opérés les services, possibilité d'accès et de contrôle des centres de données et des équipes qui les exploitent.
- **La possibilité de maintenir, faire évoluer ou changer de solution** sans être bloqué par des contraintes techniques (formats

• • •

3.

Enfin, la **souveraineté technologique.** Le sujet sans doute le plus délicat. Prise au pied de la lettre, en mode “forteresse”, la quête d’une souveraineté technologique peut conduire à n’utiliser que le code que l’on produit soi-même pour s’assurer d’en maîtriser chaque ligne et éviter ainsi toute dépendance. Dans la pratique, nous l’avons vu, c’est un vœu pieux ou, en tout cas, difficile à exaucer à l’échelle d’un système d’information. Mais entre "n’utiliser que le code que l’on produit" et "utiliser du code tiers les yeux fermés", il existe toute une graduation de scénarios. Et avec eux, différentes manières de concilier exigence de souveraineté et compétitivité.

Le changement de paradigme commence déjà ici. Par une conception de la souveraineté IT qui va au-delà d’un statut ou d’un label et s’attache davantage à la considérer comme une dynamique. À nos yeux, la souveraineté IT en 2026 désigne davantage la capacité d’une organisation à dessiner une trajectoire pour rester maître de son destin numérique sans oblitérer sa capacité d’innovation et sa compétitivité. Et, bonne nouvelle, il existe de nombreuses manières de cultiver une telle dynamique.

fermés, absence d’interopérabilité) ou contractuelles (clauses limitant la réversibilité, dépendance à un éditeur extra-européen, etc.). Ici, le sujet se confond avec celui de la souveraineté technologique (voir ci-dessous)

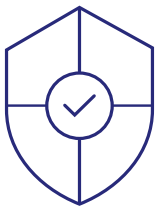
- **La connaissance de la localisation de la chaîne de valeur** : infrastructures, opérateurs, sous-traitants. Objectif : s’assurer qu’ils sont situés dans des juridictions maîtrisées (en clair : européennes)

- **La maîtrise par les compétences internes**. Ce qui suppose le maintien d’un socle minimal de compétences et de gouvernance en interne pour piloter les prestataires, comprendre les risques et être en capacité d’arbitrer les choix technologiques. Un défi au regard de la complexité des architectures contemporaines, mais loin d’être hors d’atteinte pour une organisation volontaire et engagée à investir dans la valeur de ses équipes.

02

Souveraineté et cloud

SecNumCloud 3.2 : l'étalon de l'immunité



En matière de souveraineté et de sécurité cloud, il existe un étalon, ou plutôt un référentiel élaboré par l'ANSSI et qui s'avère être le plus exigeant d'Europe : SecNumCloud. Si la version 3.1 proposée en 2018 avait pour vocation première l'alignement avec le RGPD, la version 3.2* introduite en mars 2022 a placé la protection contre les lois extraterritoriales au cœur des textes. L'article 19.6 établit un cadre juridique strict protégeant les données européennes contre les ingérences étrangères, notamment face au CLOUD Act américain. Contrairement à la version 3.1, les prestataires doivent être basés en Europe avec un contrôle majoritaire européen pour être éligibles.

Le référentiel travaille en fait deux dimensions. D'une part la **sécurité**, avec des exigences fortes sur l'architecture (cloisonnement, contrôle des accès), le chiffrement, la supervision de sécurité, la gestion des incidents, la continuité d'activité, etc. Et d'autre part la **souveraineté**, avec un hébergement des données requis dans l'Union européenne et une immunité vis-à-vis des lois extraterritoriales, avec un prestataire sous contrôle européen (siège, capital, gouvernance).

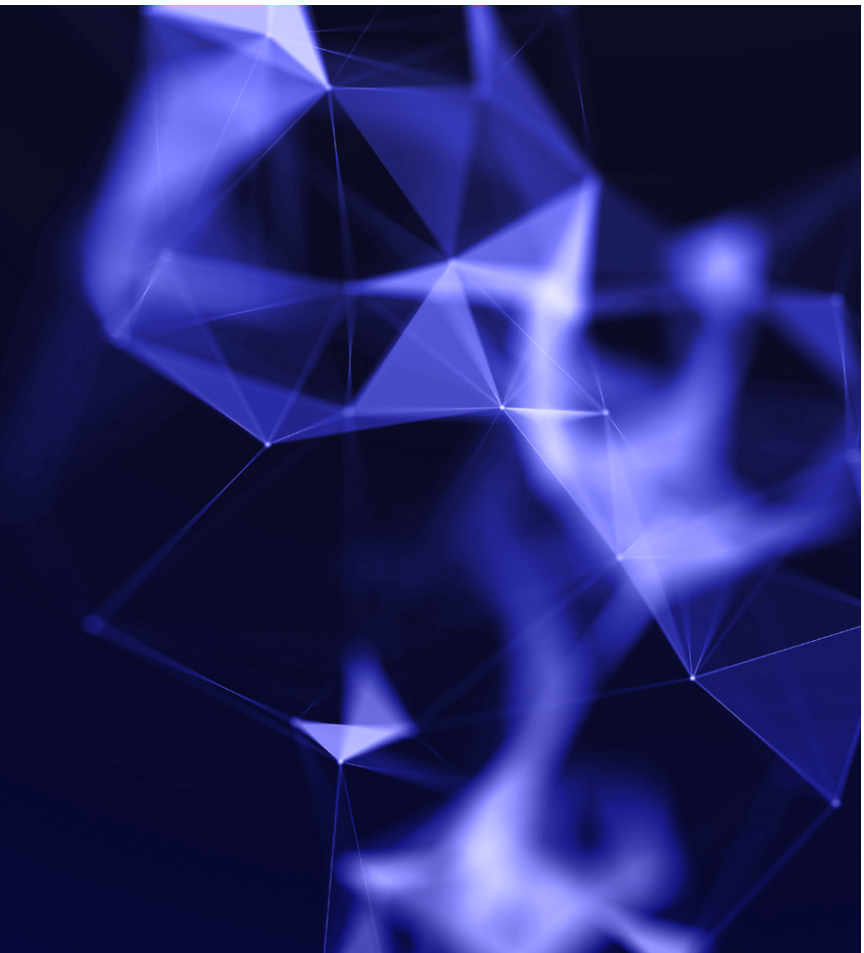
Objectifs affichés : réduire les risques de fuite, d'altération ou d'indisponibilité des données et mettre ces dernières à l'abri d'actions imposées par des autorités non-européennes. Peut-on en déduire que SecNumCloud est un label de souveraineté ? Pas tout à fait. Il serait plus exact de dire que la qualification SecNumCloud désigne un standard de sécurité cloud qui inclut des exigences de souveraineté (juridique, et géographique notamment). Un socle pour un **cloud de confiance**.

Aujourd'hui (mars 2026), une dizaine d'acteurs ont obtenu la certification SecNumCloud 3.2 pour un service cloud et, parmi eux, le cloud de confiance de S3NS.

*À savoir : SecNumCloud 3.2 devrait servir de modèle pour les niveaux les plus exigeants de la certification européenne EUCS (European Union Cybersecurity Certification Scheme for Cloud Services).

Du cloud de confiance au cloud souverain : une multitude de modèles

Nous l'avons vu, des questions juridiques, technologiques et organisationnelles s'entremêlent à travers la notion de souveraineté IT et questionnent des enjeux d'autonomie et de résilience.



Pour y répondre, plusieurs solutions sont d'ores et déjà activables dans le paysage français et européen.
Des solutions sur lesquelles le groupe SFEIR s'est positionné pour répondre au mieux aux besoins de ses clients.
Les entreprises doivent aujourd'hui naviguer entre deux objectifs parfois divergents : d'une part, accéder aux innovations les plus avancées du marché pour maintenir leur compétitivité ; d'autre part, veiller à ne pas devenir dépendantes d'écosystèmes propriétaires au point de subir (des évolutions techniques ou commerciales) et de perdre toute liberté.
À chaque entreprise ici de définir la perspective et la formule qui lui correspond. Il existe une multitude de formules.
Pour illustrer le champ des possibles, voici deux perspectives :

Du cloud de confiance au cloud souverain : une multitude de modèles

PERSPECTIVE #1

Concilier innovation de pointe et immunité juridique

Pour les organisations dont la priorité est de ne pas renoncer aux environnements éprouvés des hyperscalers, la solution réside dans le **contrôle opérationnel d'une technologie tierce**. C'est la réponse apportée par **S3NS** (filiale de Thales et totalement contrôlée par l'entreprise française). L'enjeu est ici de résoudre le "dilemme français" : bénéficier de Google Cloud Platform tout en garantissant une protection contre les lois extraterritoriales américaines.

À travers des offres comme *PREMI3NS*, S3NS isole physiquement l'infrastructure et audite chaque mise à jour logicielle fournie par Google. Mais la dépendance technologique demeure puisque le code et ses mises à jour sont bien fournis par Google. On ne peut donc pas parler ici de "solution souveraine".
Et c'est d'ailleurs plutôt la notion de "cloud de confiance" qui est le plus souvent évoquée pour qualifier le positionnement de S3NS.

Du cloud de confiance au cloud souverain : une multitude de modèles

PERSPECTIVE #2

Garantir l'indépendance technologique et la réversibilité

Pour d'autres entreprises, la souveraineté est indissociable de la **liberté de mouvement**. L'objectif prioritaire est ici d'éviter le "vendor lock-in" (l'enfermement propriétaire) et de s'assurer que les capitaux, les équipes et les infrastructures sont exclusivement européens. Une vision portée par **Scaleway**, qui mise à cette fin sur l'**Open Source** pour apporter des garanties* en matière d'interopérabilité et de réversibilité. Avec une ambition clairement affichée : proposer une alternative européenne aux hyperscalers américains.

De fait, en s'appuyant sur une stack open source et sur une implantation géographique européenne (Paris, Amsterdam, Varsovie), Scaleway construit une alternative nativement affranchie du Cloud Act.

Ici, la souveraineté n'est pas une option ajoutée à une technologie étrangère, mais le socle même d'une infrastructure autonome.

Sans surprise, cette démarche suppose aussi de ne pas attendre un portfolio de services forcément équivalent à celui des hyperscalers américains. Ce qui n'empêche pas Scaleway d'afficher d'ores et déjà des services IaaS/PaaS très consistants et d'étoffer son portfolio sur un rythme soutenu avec l'arrivée de plusieurs nouveaux produits chaque mois. Et cela en tenant le cap des engagements pris sur la lisibilité de la tarification, la compatibilité des produits avec l'écosystème cloud basé sur l'open source ou encore l'exhaustivité et l'accessibilité de la documentation pour faciliter la montée en compétences des équipes.

* Scaleway cumule déjà plusieurs certifications (ISO27001, Ecovadis Gold, HDS). La qualification est en cours pour la certification SecNumCloud.

Un éventail de choix pour une souveraineté sur-mesure

Ces deux perspectives ne sont qu'une illustration des choix qui s'offrent aux entreprises.
Bien d'autres sont possibles et il est aussi concevable qu'au sein d'une même organisation, selon la sensibilité des domaines métiers et des données associées, plusieurs modèles cohabitent.
Du cloud de confiance fondé sur la technologie d'un hyperscaler à l'alternative européenne souveraine, les entreprises disposent de quoi aligner leur feuille de route sur leurs objectifs et convictions. Partenaire de S3NS et de Scaleway, **SFEIR se considère d'abord comme le partenaire de confiance de ses clients**. Et, à ce titre, veille à construire et à mettre en œuvre avec eux une trajectoire de résilience sur-mesure.

03

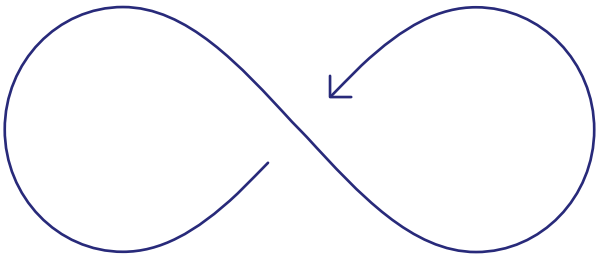
Souveraineté et IA

La voie du “Model-as-a-Service” fondé sur l’open source

La démocratisation de l’IA générative (IAGen) dans le sillage de la mise à disposition de ChatGPT 3.5 en novembre 2022 a contribué à mettre davantage encore sous tension l’enjeu de souveraineté IT. Et pour cause : la conception de grands modèles de langage (Large Language Models, LLM), socles de **l’IAGen**, demande un volume de ressources (puissance de calcul notamment) dont peu d’acteurs disposent. Résultat, parmi le top 10 des LLM en ce début d’année, 7 sont américains, 2 chinois et 1 français (Mistral 3 de Mistral AI). Et sans surprise, Google (avec ses modèles Gemini), Open AI (avec ses modèles GPT), et Anthropic (avec ses modèles Claude) occupent le devant de la scène. Avec leurs LLM mais aussi avec des produits qui accélèrent leur adoption et exploitation pour le grand public comme pour les professionnels.

Comment concilier cette révolution de l’IAGen avec une quête de souveraineté ? Là encore, avec des scénarios gradués et, aussi, en découplant les sujets.

Pour les besoins les plus exigeants et les plus sensibles, le recours à des modèles open source, en provenance de Mistral ou Meta (avec ses modèles Llama) et exploités sur clusters GKE (Google Kubernetes Engine) au sein d’un environnement tel que S3NS Premi3ns apporte des garanties fortes. Mais à un prix élevé puisque, en attendant une offre "LLM as a service" souveraine, il faudra en passer par la mise en place et la gestion d’une infrastructure dédiée de GPU.



La voie du “Model-as-a-Service” fondé sur l’open source

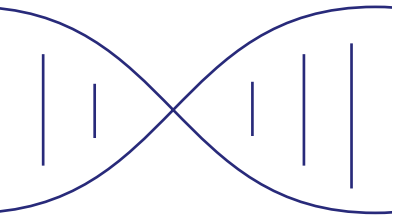
Scaleway de son côté affiche plusieurs offres. Du "**Model-as-a-Service**" pour les usages clés (chat, génération visuelle, audiovisuelle, embeddings). Sans surprise, l’entreprise profite de sa proximité avec l’écosystème d’innovation français pour proposer aussi un modèle Speech-to-Speech comme Moshi du laboratoire Kyutia.
À côté des offres"Model-as-a-Service", des instances GPU (H100 SXM, H100 PCIe, L40S) sont également disponibles.

Dans ces contextes (inférence sur une infrastructure maîtrisée), un modèle tourne sans aucun appel vers l’extérieur. Les compromis concernent davantage les modèles proposés qui ne sont pas toujours les plus récents et les plus performants (par comparaison avec l’offre "publique"). Notons toutefois que l’offre open source s’élargit si l’on étend le sourcing jusqu’à la Chine : les modèles de Moonshot AI (Kimi) ou de Deepseek se démarquent par leur efficience. Des modèles à exploiter sans perdre de vue les biais d'entraînement de ces modèles sur des sujets politiques et sociaux notamment – biais auxquels n’échappent pas non plus les modèles américains comme en témoignent les modèles Grok de xAI.

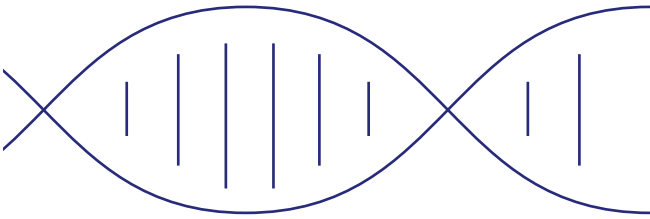
Pour des besoins exigeants mais moins sensibles, d’autres scénarios existent dans lesquels les LLM exploités sont les plus récents et opérés par un acteur comme Google mais les données, elles, sont protégées. Parce que les prompts comme les complétions (données renvoyées) sont chiffrées.
Parce qu’il est possible de choisir la région (Europe, Amérique, ...) où sont stockées les données et où sont effectués les calculs.
Enfin, des garanties contractuelles sont en place pour interdire toute utilisation des données à des fins de réentrainement des modèles.

Dans ces scénarios, le curseur de la souveraineté se déplace donc du modèle aux données pour combiner deux exigences : s’appuyer sur les modèles les plus performants tout en garantissant à une organisation la sécurité et l’exclusivité de ses données.

Investir dans la donnée et l'architecture



Résumons : pour les données critiques, les regards se tournent vers des modèles open source hébergés sur une infrastructure souveraine tandis que pour des usages plus standards le recours à des modèles commerciaux puissants s'envisage, à condition de maîtriser l'anonymisation des données. Ces scénarios illustrent les deux sujets qui comptent en matière d'IA Générative pour éviter les dépendances.



Premier sujet, **l'architecture**. Modulaire, elle doit donner la capacité de découper les briques d'un système pour permettre de changer de fournisseur sans imposer de refonte globale mais, au contraire, en garantissant réversibilité et portabilité. Une telle architecture doit soutenir une gouvernance à la fois multi-LLM et hybride. Cette diversité des modèles et cette capacité à les opérer s'avère décisive pour assurer une "**souveraineté du raisonnement**".

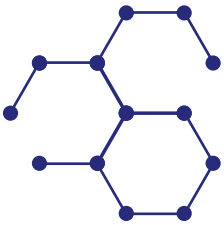
Un nouveau rôle : le Trust Architect

Ces architectures multi-LLM et hybrides légitiment l'émergence d'un nouveau rôle, celui de l'architecte de confiance.

Sa mission ? Définir des politiques de sécurité (Policies-as-Code) et des garde-fous (Guardrails) pour surveiller que l'IA ne dévie pas de sa mission et ne porte pas atteinte à l'intégrité des données.

Investir dans la donnée et l'architecture

Second sujet, **les données**. Avec des LLM de plus en plus accessibles, et qui mécaniquement deviennent une commodité, la valeur glisse du modèle aux données propriétaires de l'entreprise. Autrement dit, pour une organisation la souveraineté se joue de plus en plus sur le "**Context Engineering**", cette capacité à assembler la donnée de l'entreprise pour offrir à l'IA un carburant unique (pour des résultats qui le seront aussi). C'est ici, aussi, que l'investissement doit se concentrer pour rester maître de ce que produit l'IAGen à l'échelle de l'entreprise.



> ***« Investissez dans vos données, pas dans les modèles. »***

POUR EN APPRENDRE PLUS
téléchargez **l'édition 2026 des Tendances Tech de WEnvision**, l'entité conseil du groupe SFEIR3

FOCUS

SFEIR RAISE

l'IA souveraine pour tous

C'est dans cet esprit que SFEIR a développé RAISE (Raise AI Semantic Engine), une plateforme d'IA générative dont l'atout principal réside dans sa modularité et sa capacité à couvrir toute l'échelle des besoins. Ceux qui peuvent se contenter d'une infrastructure cloud internationale comme ceux qui se doivent d'opérer on-premises et avec une immunité totale face au Cloud Act.

Concrètement, dans une architecture souveraine, RAISE agit comme un chef d'orchestre :

- Il se connecte aux modèles de fondation de multiples manières : appel direct à des modèles signés Google, Anthropic ou à des modèles Mistral hébergés sur une infrastructure comme celle de Scaleway. Notons que SFEIR a aussi porté RAISE sur S3NS. Une exploitation on-premises d'un modèle Open Source est aussi à la portée de RAISE.
- Il injecte le contexte métier (RAG - Retrieval Augmented Generation) stocké dans des bases de données selon des scénarios qui offrent différents niveaux de garantie pour la souveraineté des données.
- Selon le scénario global retenu, il peut garantir que les données de l'entreprise ne servent jamais à réentraîner les modèles publics.

Pour SFEIR, RAISE est la preuve par l'exemple que l'on peut faire de l'IA de pointe tout en se conformant à des objectifs de souveraineté (de modèle, de données, d'infrastructure).

6 principes pour une souveraineté agile

1. **Segmenter les workloads** (sensibilité / criticité / contraintes)
2. **Découpler** données, opérations et technologies
3. **Concevoir la réversibilité** (design-to-exit)
4. **Maîtriser** le chiffrement, les clés, la gestion des identités et accès (IAM)
5. **Encadrer contractuellement l'IA** (logs, entraînement, conservation, audit)
6. **Investir dans les compétences** (build/run/secops/finops)

Cap sur **la résilience**

Vous l'aurez compris, pour SFEIR, la quête de souveraineté IT ne doit pas mener à un repli ou à un isolationnisme dans lequel elle deviendrait l'antichambre d'une perte de compétitivité (dont les entreprises européennes n'ont clairement pas besoin). À l'opposé, il n'est pas non plus question d'accepter les dépendances qui conduisent à mettre les patrimoines informationnels des entreprises dans les mains de fournisseurs peu enclins à les relâcher, et encore moins les dépendances qui se traduisent par un renoncement à des valeurs fondamentales.

Une autre voie est possible dès lors qu'on renouvelle son regard sur cet enjeu pour considérer la souveraineté IT d'abord comme un objectif de résilience.

Construire cette résilience, c'est accepter que le monde est incertain et concevoir son système d'information comme un organisme capable de s'adapter grâce à...

- **une résilience technologique** : via des choix de solutions et d'architecture qui évitent le "vendor lock-in"
- **une résilience juridique** : en protégeant les données contre l'extraterritorialité (via le Cloud de Confiance).
- **une résilience par l'expertise** : en investissant dans la compétence des équipes pour les mettre en capacité de tenir durablement le rênes du système d'information

Aujourd'hui, l'écosystème IT (technologies, fournisseurs, prestataires) a suffisamment mûri pour soutenir cette quête de résilience et la considérer comme un levier à part entière de la modernisation des systèmes d'information. Et c'est cette quête que SFEIR propose à ses clients d'engager et de co-construire. Avec à la clé, une réelle autonomie et liberté gagnées pour rester maître du devenir de son système d'information.

À propos du Groupe SFEIR

Pour accompagner votre trajectoire vers une souveraineté agile, le groupe SFEIR, entreprise française, avec des capitaux français, opérant en France et dont la valeur est reconnue à l'échelle européenne, propose les 3 grandes compétences requises et des accélérateurs.

Des compétences d'ingénierie logicielle de haut niveau

Qu'il s'agisse de renforcer vos talents, de prendre en charge un projet ou encore de développer et maintenir vos solutions avec une efficacité et une qualité optimales, les équipes SFEIR sont au rendez-vous. Adossés à une culture du Software Craftsmanship, les 850 ingénieurs, architectes et experts du groupe se démarquent par leur capacité à contribuer de manière tangible à la modernisation de votre système d'information.

Des compétences de... transmission de compétences

La souveraineté technologique est un concept inopérant sans souveraineté des compétences. Avec 5 700 personnes formées en 2025, le titre de Google Cloud Training Partner of the Year EMEA pour la deuxième année consécutive et plus de 60 formateurs, SFEIR Institute, le pôle formations du groupe, dispose de toutes les ressources pour accompagner la montée en compétences des équipes de nos clients.

Des compétences de conseil

La souveraineté est d'abord une question de stratégie. L'entité conseil de SFEIR, WEnvision, joue un rôle pivot pour baliser vos trajectoires. Au croisement de la technologie, de l'organisation et de la culture, WEnvision déploie une approche holistique pour définir VOTRE souveraineté.

Des accélérateurs

Pour faciliter l'innovation, SFEIR propose plusieurs produits clés en main. Supervisés par la SFEIR Factory pour assurer leur maintenance et évolution continue, ces produits sont issus de l'expertise terrain de SFEIR, et pré-packagés pour un ROI rapide. Parmi eux, 3 produits phares qui, chacun, peuvent contribuer à votre souveraineté :

- **Cloud Foundation Platform** : accélère et sécurise la stratégie Cloud avec une fondation robuste et gouvernée.
- **MADS** : plateforme analytique moderne et modulaire, déployable en quelques semaines.
- **RAISE AI Semantic Engine** : exploite l'IA générative sur les données internes, en toute sécurité.