HTF HUMAN TECHNOLOGY FOUNDATION

Maîtriser ses dépendances

Le vrai levier de la souveraineté numérique

Mai 2026

Avant-propos

Eric Salobir
Président de la Human Technology Foundation

La souveraineté numérique est un oxymore

La souveraineté numérique porte en elle une contradiction. D'un côté, les tensions géopolitiques croissantes et les risques d'interruptions des chaînes d'approvisionnement poussent les entreprises à privilégier davantage la résilience que l'optimisation. Reprendre le contrôle et maîtriser les risques est devenu nécessaire pour assurer la continuité de l'activité et la pérennité de la structure. Mais le numérique repose précisément sur la connexion et l'interdépendance. Outre la complexité des systèmes, qui révèle un mille-feuille de dépendances (semi-conducteurs, modèles d'IA, constellation de satellites…), la vocation même de ces outils est d'assurer la circulation autant que le traitement de la donnée.

Si la souveraineté, au sens étymologique, consiste à ne dépendre de personne, cette notion est donc, *stricto sensu*, difficilement applicable au domaine du numérique. Au niveau national ou européen, cette souveraineté peut certes prendre la forme d'une interdépendance choisie et assumée : nous avons également des cartes en main et les autres ont collectivement aussi besoin de nous.

Au niveau microéconomique, la chose est plus complexe. Le degré d'autonomie stratégique ne se mesure pas sur une simple échelle allant du moins au plus souverain : se prémunir contre certains risques implique de s'exposer à d'autres. En outre, la maîtrise des risques ne constitue pas le seul objectif. Elle ne peut être atteinte au prix d'une trop forte dégradation des performances ou de coûts exorbitants. Pour reprendre les termes de J. M. Keynes, "La politique visant à renforcer l'autosuffisance nationale ne doit pas être considérée comme un idéal en soi, mais comme un moyen de créer un environnement dans lequel d'autres idéaux peuvent être poursuivis en toute sécurité et sans difficulté.[1]"

Depuis peu, les entreprises disposent de moyens pour évaluer leur résilience numérique, et toutes gagneraient à le faire. A partir de ces données, elles doivent mettre en balance les paramètres de risque, de performance et de coûts. Le présent rapport explore la façon dont cette mise en tension peut faciliter la prise de décision. Il n'a pas vocation à orienter les choix dans une direction : le choix optimal est celui qui place l'entreprise sur la meilleure voie, pour un projet donné et dans un contexte spécifique.

Cette étude a été entreprise par la Human Technology Foundation avec le soutien de ses membres, dont la diversité assure l'indépendance. Qu'ils soient ici remerciés. Elle a été confiée à une équipe dirigée par Josephine Staron, épaulée par Emmanuelle Charghinoff, à qui j'exprime ma gratitude. Ces travaux ont également bénéficié du soutien de nombreux experts, parmi lesquels je tiens à saluer l'apport déterminant de Paul-Henri Charrier.

Les apports théoriques de cette étude pourront trouver place dans des outils d'évaluation développés par nos partenaires. En attendant cette perspective que nous appelons de nos vœux, nous les avons rassemblés au sein d'un petit outil de test, qui vous permettra de mieux les appréhender. Son design a été piloté par Paul Barbaste, chercheur associé à notre fondation. Cette expérience ne se substitue pas à la lecture, mais elle peut utilement la compléter.

Nous espérons que la réflexion présentée dans ce rapport contribuera à faire avancer, même modestement, la recherche dans ce domaine.

Bonne lecture.

Eric Salobir,
Président du Comité exécutif

Eric Salobir

1 "National Self-Sufficiency", John Maynard Keynes, *The Yale Review*, Vol. 22, no. 4 (June 1933)

Introduction

Pendant longtemps, la dépendance technologique a été abordée comme un plus appréciable mais non déterminant de la compétitivité ou, au mieux, de la cybersécurité. Elle est désormais devenue un enjeu stratégique. Ce qui relevait hier de l'optimisation ou du confort d'usage peut aujourd'hui devenir un facteur de paralysie, de renchérissement brutal, de perte de maîtrise ou de vulnérabilité.

Le contexte international impose de regarder cette réalité en face. Dans un monde marqué par le retour de la conflictualité, par une interdépendance économique longtemps pensée comme un facteur de paix, notamment dans le cadre du projet européen, et désormais utilisée comme un instrument de coercition, et par l'affaiblissement des garanties juridiques et institutionnelles qui structuraient jusqu'ici la mondialisation, les entreprises ne peuvent plus considérer l'accès aux infrastructures, aux données ou aux services numériques comme acquis.

Comme l'a souligné le Premier ministre canadien, Mark Carney, lors du Forum de Davos en janvier 2026, nous ne vivons pas une simple transition, mais une rupture : les grandes puissances utilisent désormais les infrastructures, les chaînes d'approvisionnement et les dépendances économiques comme des leviers d'influence et de pression. Dans ce contexte, la question n'est plus seulement celle de la performance technologique, mais celle de la capacité à continuer d'agir.

Le sujet central n'est pas la technologie elle-même, mais les conditions dans lesquelles une organisation peut continuer de fonctionner malgré ses dépendances.

Cette évolution a des implications concrètes. Une entreprise peut avoir externalisé des fonctions critiques auprès de fournisseurs réputés fiables, dans des régions considérées comme stables, et découvrir que cette stabilité est relative. Une dégradation géopolitique, une décision politique extraterritoriale ou une rupture dans une chaîne d'approvisionnement peuvent suffire à remettre en cause l'accès à des ressources essentielles. Dans un environnement dégradé, l'entreprise dépend non seulement de la robustesse technique de ses prestataires, mais aussi de leur exposition géopolitique, de leurs chaînes d'approvisionnement, de leurs conditions contractuelles et, en dernier ressort, des choix souverains des États dont ils relèvent.

C'est à ce point d'articulation entre dépendance, maîtrise et continuité que se situe l'approche de la Human Technology Foundation. Elle ne repose ni sur une souveraineté déclarative, ni sur une indépendance technologique illusoire. **Car l'autonomie stratégique ne doit pas être confondue avec l'autarcie : dans un environnement d'interdépendance, chercher à tout internaliser serait à la fois irréaliste et inefficace.**

D'autant que dans de nombreux domaines critiques, les alternatives intégralement nationales ou européennes n'existent pas encore, ou pas à un coût soutenable. La question n'est donc pas de supprimer les dépendances, mais de retrouver des marges de manœuvre.

La souveraineté numérique ne consiste donc pas à éliminer toutes les dépendances, mais à être en mesure de les comprendre, de les arbitrer et d'en maîtriser les effets.

Elle suppose de réduire les dépendances les plus critiques, de sécuriser celles qui demeurent, et de concentrer les efforts sur les briques réellement décisives. Elle consiste, en pratique, à **rester en mesure de décider et d'agir malgré les contraintes.**

Dans cette perspective, la souveraineté ne se résume pas à un niveau croissant de maîtrise. Elle repose sur une série d'arbitrages entre des objectifs partiellement contradictoires : performance, coût, résilience, simplicité. Renforcer la résilience implique souvent des surcoûts ou une perte d'efficience. À l'inverse, optimiser la performance peut accroître la dépendance. **Se protéger de tous les risques est impossible : toute stratégie suppose de choisir ceux contre lesquels il est pertinent de se prémunir.**

Dans un environnement d'interdépendance, la souveraineté économique ne peut plus être pensée uniquement à l'échelle nationale. Elle se joue, pour l'essentiel, à l'échelle européenne, voire dans des coalitions de pays partageant des intérêts communs, à l'image des "puissances moyennes" évoquées par Mark Carney à Davos.

Le cadre d'analyse et les outils de pilotage évoluent dans ce sens. L'Indice de résilience numérique (IRN) développé en collaboration avec la Caisse des Dépôts, et auquel la Human Technology Foundation est associée constitue à cet égard une contribution essentielle : il permet d'objectiver l'exposition des organisations, de structurer un langage commun et de poser les bases d'un diagnostic partagé de la résilience numérique.

Le présent rapport s'inscrit dans le prolongement de ces démarches. Il ne vise ni à se substituer aux outils existants, ni à produire un nouvel indice, mais à **explorer une étape complémentaire : celle de l'arbitrage.** Une fois les dépendances identifiées et qualifiées, comment choisir entre plusieurs configurations possibles, au regard du coût, de la performance, de la continuité d'activité et du niveau de maîtrise recherchés ?

Cette approche par l'arbitrage s'inscrit aussi dans une logique déjà portée par les méthodes de gestion du risque, notamment EBIOS Risk Manager de l'ANSSI : partir des fonctions critiques et des scénarios redoutés avant de définir les mesures proportionnées.

Le cadre normatif européen s'inscrit également dans cette dynamique : le *Data Act*, entré en application en septembre 2025, vise à faciliter le changement de fournisseurs, à renforcer l'interopérabilité et à réduire certaines asymétries contractuelles. Mais cette approche dépasse une logique de conformité : respecter un cadre réglementaire ne suffit pas à garantir la maîtrise des dépendances en situation de rupture.

Le présent rapport se situe ainsi dans un registre complémentaire aux démarches de mesure et d'évaluation. Le travail de recherche et d'exploration qu'il présente a vocation à être mis à la disposition de la communauté, afin d'enrichir ou de compléter les initiatives existantes.

Il n'existe pas d'architecture optimale en soi, seulement des configurations plus ou moins adaptées à un niveau de risque, à des contraintes de coût et à des exigences de continuité. Les instruments de sécurisation (contrats, certifications, diversification, plans de continuité, assurances) ont chacun leur utilité, mais aucun ne constitue une garantie suffisante à lui seul.

Dans ce contexte, la question centrale n'est plus celle du choix d'une solution, mais celle de l'arbitrage entre plusieurs options imparfaites**. La souveraineté n'est pas un niveau à atteindre, mais une discipline de choix.** C'est pourquoi ce rapport propose de rendre explicites les tensions qui structurent ces décisions, en les représentant sous forme de curseurs sur lesquels chaque organisation doit se positionner. Les choix techniques et organisationnels ne précèdent pas ces arbitrages : ils en sont la conséquence.

Au fond, toute la difficulté tient à un constat : **la dépendance est inévitable. Subie, elle fragilise. Arbitrée, elle devient un levier.**

STRUCTURE DU RAPPORT

Partie 1 • Scénarios de rupture

Le rapport part d'un constat simple : la continuité d'accès aux infrastructures, aux services numériques, aux données ou aux capacités de calcul ne peut plus être tenue pour acquise. Il met en lumière plusieurs scénarios de rupture plausibles — géopolitiques, économiques, techniques ou liés à la chaîne de valeur de l'intelligence artificielle (IA) — afin de montrer en quoi ils transforment les critères de décision.

Partie 2 • Que veut-on maîtriser ? Comparer les configurations de maîtrise

Face à la multiplication des dépendances, l'enjeu n'est pas de tout contrôler, mais d'identifier ce qui doit réellement être maîtrisé. Cette partie propose un cadre pour qualifier les dépendances et comparer différentes configurations de maîtrise en fonction des risques, des coûts et des exigences de continuité.

Partie 3 • Arbitrer en pratique : cas d'usage et configurations

La troisième partie applique cette logique à plusieurs cas d'usage concrets (données sensibles, outils collaboratifs, intelligence artificielle, connectivité) afin d'illustrer comment les arbitrages se traduisent en configurations opérationnelles. Elle met en évidence les compromis associés à chaque choix et propose une méthode pour structurer la décision.

Cinq scénarios de rupture

1

Photo LDD *magnific.com*

Les scénarios présentés dans cette partie ne visent pas à dresser un catalogue exhaustif des risques, ni à documenter des situations avérées. Ils adoptent volontairement un format proche d'un exercice de *red team*, en proposant des récits courts, fictionnels, qui mettent en tension des choix réels.

Chaque scénario décrit une situation plausible, sans référence explicite à des acteurs ou à des contextes géographiques précis, afin de concentrer l'analyse sur les mécanismes à l'œuvre plutôt que sur des cas particuliers.

L'objectif n'est pas de prédire, mais de tester la robustesse des décisions. À travers ces mises en situation, il s'agit de faire apparaître les arbitrages qu'une organisation serait contrainte d'opérer : entre continuité et coût, performance et réversibilité, maîtrise et simplicité, etc.

Chaque scénario est ainsi décrypté selon trois dimensions — sa criticité, sa probabilité et ce qu'il révèle — afin d'éclairer les tensions qu'il met en évidence et les implications concrètes pour la prise de décision.

Scénario 1

La coupure venue d'ailleurs

Il est 8h40 ce lundi matin lorsque, comme à son habitude, Thomas badge à l'entrée de la banque, son café encore à la main. Rien ne distingue ce matin des autres. Les écrans s'allument, les flux se chargent, les premières opérations de la journée commencent.

À 8h47, Thomas tente de valider un virement. Un message d'erreur apparaît. Il recommence. Même message. Il pense à un bug passager.

À 8h52, sa collègue à côté de lui soupire : " Tu arrives à te connecter, toi ? "

Les écrans se figent par intermittence. Les outils internes ralentissent. Certains services ne répondent plus. Les équipes IT sont appelées. Rien d'inquiétant, pense-t-on encore.

À 9h12, une alerte interne circule. Quelques lignes, laconiques : *incident majeur en cours, origine externe probable.*

À 9h18, les téléphones vibrent partout dans l'*open space*. Personne ne parle, mais tout le monde regarde son écran. Les notifications d'actualité pleuvent. Thomas ouvre la première :

une déclaration officielle vient d'être publiée. Les mots sont froids, techniques, presque neutres. Mais leur effet est immédiat : certains services numériques et financiers cessent d'être accessibles, à partir de maintenant. Il n'y a pas de délai. Pas de transition. Juste une coupure.

À 9h25, les effets sont visibles partout. Les paiements ne passent plus. Les cartes sont refusées. Les applications mobiles cessent de fonctionner. Les plateformes de traitement ne répondent plus. Les données clients sont inaccessibles. Elles existent toujours, mais hors de portée. Thomas tente d'accéder à un dossier mais son écran reste vide.

À 9h40, les chaînes d'information s'emballent. Une allocution présidentielle est annoncée en urgence. Un conseil européen exceptionnel doit se tenir dans la journée. Les responsables politiques parlent de " mesures de rétorsion ", de " riposte coordonnée ", de " solutions en cours d'élaboration ".

Mais dans l'immédiat, rien ne se passe. Alors dans les bureaux, les équipes improvisent. On passe sur des messageries personnelles. On tente de joindre des prestataires. On redémarre des systèmes qui ne répondent plus. Les responsables évoquent des plans de continuité, des bascules possibles. Mais rien n'est prêt pour une rupture aussi brutale. Les systèmes critiques reposaient sur des services désormais inaccessibles et les alternatives, quand elles existent, ne sont ni immédiates, ni compatibles, ni dimensionnées pour absorber le choc.

Le choix de concentrer les infrastructures auprès de quelques fournisseurs globaux s'était imposé progressivement. Il permettait de bénéficier d'économies d'échelle, d'une qualité de service homogène et d'une simplification de la gestion opérationnelle. Des stratégies de diversification avaient été évoquées (multi-cloud, répartition géographique, recours à des acteurs de plusieurs nationalités), mais elles impliquaient une complexité accrue, des coûts supplémentaires et, dans certains cas, une moindre maturité des solutions disponibles.

À 11h15, l'activité est quasiment à l'arrêt. Les opérations sont suspendues. Les clients attendent. Les équipes n'ont plus d'outils. Les décisions politiques s'enchaînent à l'extérieur, mais à l'intérieur, le constat est simple : plus rien ne fonctionne.

Thomas regarde son écran, inquiet. Tout ce qui lui permettait de travailler (accéder aux comptes, valider des opérations, communiquer avec ses collègues) dépend d'infrastructures qu'il ne maîtrise pas.

Il se tourne vers son manager : " On fait quoi ? ". Le silence qui règne est assourdissant.

Degré de criticité du scénario 1 : TRÈS ÉLEVÉ

Le scénario entraîne une interruption immédiate des fonctions critiques : paiements, accès aux données, outils de travail, communication. L'activité peut être paralysée en quelques heures.

Probabilité du scénario 1 : FAIBLE

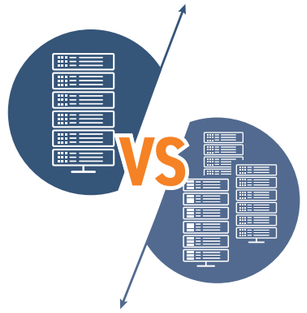
Il s'inscrit dans un contexte de montée des tensions internationales et d'usage croissant des dépendances économiques et technologiques comme instruments de pression.

ce que ce scénario révèle

- Une décision politique externe peut produire des effets immédiats sur la capacité opérationnelle des entreprises.
- Les architectures optimisées pour le coût et la performance sont souvent celles qui maximisent la dépendance.
- La réversibilité est rarement effective dans le temps court : les alternatives existent, mais ne sont ni immédiates ni opérationnelles à grande échelle.
- Les réponses politiques et institutionnelles, même coordonnées, interviennent souvent trop tard pour éviter la paralysie initiale.
- La continuité d'activité dépend de marges de manoeuvre construites en amont, et non de solutions improvisées en situation de crise.

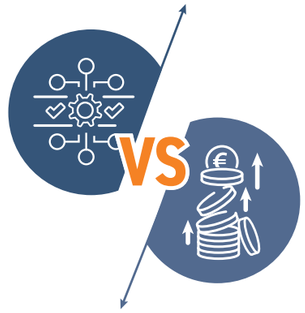
Quelles sont les tensions que ce scénario illustre :

Choix de concentrer les dépendances sur un nombre limité de fournisseurs globaux (acteurs majeurs du cloud, modèles d'IA, des paiements ou des infrastructures, offrant standardisation, qualité de service et économies d'échelle).



Choix de diversifier les fournisseurs (répartition entre plusieurs acteurs et modèles d'IA, multi-cloud, recours à des fournisseurs de tailles ou de juridictions différentes), **au prix d'une complexité accrue et d'une moindre homogénéité des systèmes.**

Choix de l'efficience opérationnelle (mutualisation des ressources, absence de duplication, optimisation des coûts et des performances).



Choix de la redondance pour renforcer la résilience (duplication des infrastructures, réplication des données, environnements de secours, absence de point de défaillance unique), **au prix d'un surcoût et d'une complexité supplémentaire.**

Scénario 2

La juridiction des uns commence là où s'arrête celle des autres

En arrivant au bureau ce matin, Sarah, juriste spécialisée en conformité, relit un contrat signé quelques mois plus tôt avec un fournisseur de services cloud. Ce contrat encadre l'hébergement de données sensibles : informations clients, documents internes, échanges stratégiques. Il a été validé, audité, jugé conforme aux exigences européennes. Tout est en ordre.

Sarah s'apprête alors à archiver le contrat lorsqu'elle reçoit un e-mail d'un collègue : "Peux-tu regarder ça en urgence ?". Un lien vers un texte publié quelques heures plus tôt : une nouvelle loi adoptée en urgence par un État dont relèvent plusieurs fournisseurs critiques de l'entreprise.

Sarah commence à lire, stupéfaite : désormais, et dans certaines situations, les fournisseurs de services numériques relevant de cet État devront permettre l'accès aux données qu'elles hébergent, y compris lorsqu'elles concernent des acteurs situés à l'étranger.

Sarah rouvre le contrat qu'elle s'apprêtait à ranger. Tout y est : confidentialité, sécurité, localisation des données, conformité réglementaire. Mais aucune clause ne peut s'opposer à une obligation légale imposée au fournisseur.

Sarah attrape son téléphone et appelle le DSI : " Marc, on a un problème ".

Une heure plus tard, les associés se réunissent pour décider de la marche à suivre : faut-il migrer ? Isoler certaines données ? Changer de fournisseur ?

Les équipes techniques parlent de délais et de dépendances. Les équipes métiers rappellent que ces systèmes sont au cœur de l'activité. Les équipes juridiques parlent d'amendes massives en cas de refus d'obtempérer.

Les données critiques de l'entreprise (clients, stratégie, opérations) peuvent désormais être consultées dans un cadre qu'elle ne maîtrise pas. Le contrat n'a pas changé. Mais l'entreprise vient de perdre la maîtrise de ses données.

Pourtant, quelques mois plus tôt, le choix du fournisseur avait fait l'objet de discussions approfondies. Plusieurs options avaient été étudiées, y compris des solutions plus cloisonnées ou localisées, des architectures reposant sur du chiffrement avec gestion indépendante des clés, ou encore des environnements plus autonomes, combinant technologies étrangères et opérateurs soumis à des cadres juridiques différents. Mais ces solutions alternatives impliquaient des coûts significativement plus élevés, des délais de déploiement incompatibles avec les besoins métiers et une moindre qualité de service. D'autant que le fournisseur retenu présentait toutes les garanties attendues : certifications, conformité aux standards européens, clauses contractuelles encadrant précisément l'accès et la localisation des données.

Rien n'a été violé. Rien n'a été piraté. Et pourtant, les données ne sont plus sous contrôle. L'entreprise s'était appuyée sur les garanties contractuelles sans mettre en place de mesures techniques complémentaires pour en renforcer la protection. Ce que l'entreprise découvre, ce n'est pas une faille contractuelle, mais une limite structurelle : la maîtrise juridique ne garantit pas la maîtrise réelle.

Degré de criticité du scénario 2 : ↗ ÉLEVÉ

Le scénario expose directement des données sensibles (clients, stratégie, opérations), avec des conséquences potentielles en termes de confidentialité, de concurrence et de responsabilité.

Probabilité du scénario 2 : → MODÉRÉE à ↗ ÉLEVÉE

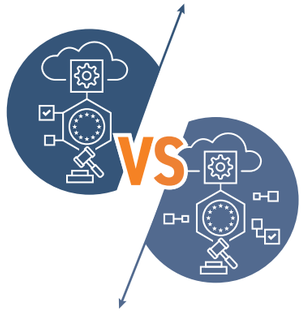
Les mécanismes juridiques permettant ce type d'accès existent déjà et peuvent être étendus ou durcis rapidement.

ce que ce scénario révèle

- La protection contractuelle ne garantit pas la confidentialité réelle des données.
- L'accès aux données peut être imposé par un État tiers, indépendamment de la volonté de l'entreprise.
- Externaliser des données critiques revient à exposer leur accès à des règles juridiques extérieures.
- La fuite de données ne passe pas nécessairement par une faille technique, mais aussi par un cadre légal.
- Les capacités de réaction (migration, isolation, reconfiguration) sont lentes face à un risque immédiat.
- La question n'est donc plus seulement de savoir si les données sont sécurisées, mais de savoir qui, en dernier ressort, peut y accéder.

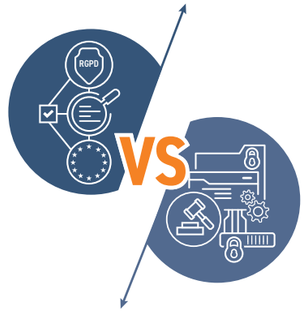
Quelles sont les tensions que ce scénario illustre :

Choix de solutions intégrées, performantes et juridiquement encadrées (services cloud complets, suites collaboratives, plateformes unifiées conformes aux standards européens).



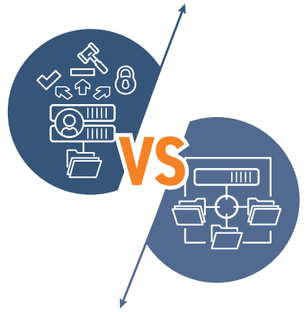
Choix d'une architecture plus fragmentée visant à renforcer la maîtrise (séparation des environnements, cloisonnement des données sensibles, recours à plusieurs prestataires ou infrastructures dédiés), **au prix d'une complexité accrue et d'une moindre fluidité opérationnelle.**

Choix de s'appuyer sur un cadre contractuel et réglementaire robuste (contrats, clauses de confidentialité, conformité RGPD, certifications, audits).



Choix de privilégier des garanties techniques de protection des données (chiffrement avec gestion indépendante des clés, isolation des environnements, contrôle des accès), **sans pouvoir totalement neutraliser les contraintes juridiques externes.**

Choix d'externaliser la gestion des données pour bénéficier d'un haut niveau de service et de conformité (hébergement chez un fournisseur certifié, gestion déléguée de la sécurité et des obligations réglementaires).



Choix de conserver un contrôle accru sur certaines données critiques (hébergement local ou cloud maîtrisé, gestion interne des accès et des clés, limitation des transferts), **au prix d'une perte d'efficience et d'une responsabilité opérationnelle plus forte.**

Scénario 3

Le prix d'entrée n'est jamais le prix de sortie

Avant de terminer sa journée, Julien, directeur des systèmes d'information, jette un dernier coup d'œil au tableau de suivi des coûts de connectivité de l'entreprise. Un chiffre attire son attention. Il actualise la page une fois, deux fois. Mais le chiffre ne bouge pas : les dépenses liées au réseau ont brutalement augmenté. Pas de quelques points, mais de plusieurs dizaines de pourcents.

Julien pense d'abord à une erreur. Il appelle son équipe : " Vous avez vu ça ? ".

Un e-mail envoyé la veille au soir par leur fournisseur confirme l'information : une révision tarifaire s'applique immédiatement à plusieurs usages critiques : bande passante, volumes de données transmis, priorisation du trafic.

Depuis plusieurs années, l'entreprise s'appuie sur une connectivité satellitaire en orbite basse pour opérer dans des zones où les réseaux terrestres sont inexistants ou instables. Toute l'activité en dépend : coordination des équipes sur le terrain, remontée de données en temps réel, supervision des opérations, communications critiques.

Julien ressort le contrat : " Il doit bien y avoir une clause qui protège contre cette hausse soudaine ? ". Mais les conditions sont claires : le fournisseur peut ajuster ses tarifs en fonction de l'évolution du marché et des contraintes opérationnelles.

Le choix initial n'avait rien d'irrationnel. Cette solution offrait une couverture globale, une qualité de service inégalée et une rapidité de déploiement. À l'époque, l'entreprise devait accélérer son développement, étendre ses opérations dans des zones isolées et garantir une connectivité fiable à ses équipes. Aucune alternative ne présentait le même niveau de performance.

D'autres options avaient été étudiées : combiner plusieurs technologies (satellite, radio, réseaux terrestres), maintenir des solutions de secours locales, ou limiter certains usages les plus consommateurs de données. Mais ces choix impliquaient des compromis importants : une dégradation de la qualité de service, des investissements initiaux élevés, une complexité opérationnelle accrue et des délais incompatibles avec les objectifs de croissance. Si la question de la dépendance avait été identifiée, elle n'avait pas été jugée prioritaire à court terme.

Au fil des années, l'entreprise a étendu ses usages : davantage de données transmises, plus d'outils connectés, une dépendance croissante aux flux en temps réel… Chaque évolution répondait à un besoin opérationnel immédiat. Ensemble, elles ont rendu la connectivité indispensable et difficilement substituable.

En début de soirée, une réunion d'urgence est organisée pour poser une question : peut-on changer de fournisseur ? Sur le papier, oui. Mais en pratique, les obstacles apparaissent immédiatement : remplacer les équipements sur le terrain, reconfigurer les réseaux, former les équipes, accepter une couverture dégradée dans certaines zones. Aucun autre opérateur ne propose, à court terme, un service équivalent.

Peut-on réduire les usages ? Cela impliquerait de ralentir les opérations, de perdre en visibilité, voire d'interrompre certaines activités.

Peut-on négocier ? À la marge, peut-être. Mais la position de force est claire.

La conclusion s'impose rapidement : sortir est possible, mais lent, coûteux et risqué. À court terme, l'entreprise n'a pas d'autre choix que de payer la facture.

Degré de criticité du scénario 3 : → MODÉRÉ

Le scénario n'entraîne pas nécessairement une interruption immédiate de l'activité, mais il peut dégrader rapidement la rentabilité, contraindre les choix stratégiques et, à terme, fragiliser la viabilité économique de certaines fonctions critiques. Dans les cas les plus extrêmes, l'entreprise peut se retrouver dans l'incapacité d'absorber les coûts, sans alternative opérationnelle à court terme.

Probabilité du scénario 3 : ↗ TRÈS ÉLEVÉE

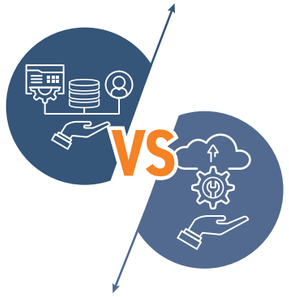
Les évolutions tarifaires, les modifications de conditions commerciales et les mécanismes de dépendance progressive sont fréquents et structurels dans les modèles de services numériques. Le risque ne repose pas sur un événement exceptionnel, mais sur une dynamique normale de marché dans un contexte de forte concentration.

ce que ce scénario révèle

- La dépendance ne se manifeste pas uniquement par une impossibilité d'accès, mais par une incapacité à arbitrer.
- Le verrouillage (*lock-in*) est progressif : technique, contractuel et économique, mais aussi matériel et géographique (équipements, couverture).
- La concurrence existe en théorie, mais devient difficilement mobilisable en pratique en raison des coûts, des délais de bascule ou de l'absence d'alternatives équivalentes à court terme.
- Les choix initiaux d'optimisation (performance, intégration, simplicité) produisent des effets de dépendance différés.
- La réversibilité, souvent prévue en principe, n'est pas toujours activable dans des conditions économiquement soutenables.

Quelles sont les tensions que ce scénario illustre :

Choix de solutions très performantes et fortement intégrées à un fournisseur (services propriétaires, bases de données spécifiques, outils natifs du cloud, automatisation poussée).



Choix d'une architecture plus "transportable" et standardisée (technologies *open source*, conteneurisation type Docker/Kubernetes, formats de données ouverts), **permettant de changer de fournisseur mais avec moins d'optimisation et plus de complexité.**

Choix d'une dépendance assumée à un fournisseur dominant (centralisation des services chez un acteur unique, intégration forte de l'écosystème, simplicité de gestion).

Choix de maintenir une capacité d'arbitrage (multi-cloud, répartition des charges entre fournisseurs, solutions alternatives activables souvent au prix de conditions tarifaires moins favorables, voire sans alternative réelle dans certains cas comme la connectivité satellite).

Choix d'une optimisation des coûts à court terme (mutualisation maximale, absence de duplication, choix des services les plus économiques à l'instant T).

Choix d'un surcoût anticipé pour préserver une capacité de sortie ou de migration (duplication partielle des environnements, maintien d'alternatives, investissements dans la portabilité).

Scénario 4

Prométhée privé de son feu

Ce matin, Paul, chef de projet dans une entreprise de services numériques, arrive tôt au bureau. À quelques jours de livraisons importantes pour plusieurs clients, les équipes sont déjà sous pression. Mais en ouvrant son ordinateur, il comprend immédiatement que quelque chose ne va pas.

Les outils habituels fonctionnent, mais quelque chose manque. Les assistants de développement ne répondent plus, les interfaces d'automatisation sont inactives, les modules d'analyse et de génération de contenu restent bloqués. Les équipes essaient de relancer les systèmes. Rien ne revient. Dans un premier temps, ils pensent à un incident isolé. Mais très vite, le diagnostic tombe : le modèle d'intelligence artificielle sur lequel repose une partie significative de la production est indisponible.

L'origine reste floue. Une panne chez le fournisseur ? Une suspension temporaire du service ? Une dégradation volontaire liée à une mise à jour ou à un incident de sécurité ? Peu importe, à ce stade. Les équipes attendent un rétablissement rapide. Mais les minutes passent, puis les heures.

Très vite, les effets deviennent visibles. Les développeurs perdent leurs outils d'assistance au code. Les équipes métiers ne peuvent plus produire certains livrables générés en grande partie via des modèles. Les processus automatisés (rédaction, synthèse, analyse) ralentissent brutalement, voire s'arrêtent.

Au fil des mois, ces outils s'étaient imposés comme des accélérateurs indispensables. Pris isolément, chaque usage était marginal. Ensemble, ils étaient devenus structurants.

En fin de matinée, une question s'impose : que peut-on maintenir ? Et la réponse inquiète : très peu de choses, car aucun modèle alternatif n'est immédiatement mobilisable. Les outils internes ne permettent pas de compenser, et les équipes n'ont plus les mêmes capacités de production sans ces briques invisibles mais centrales. L'activité ralentit, puis à midi, elle s'arrête.

Dans les jours qui suivent, la situation continue de se dégrader : les délais contractuels ne sont plus tenus, des pénalités s'appliquent, les projets prennent du retard. Certaines tâches doivent être reprises manuellement, avec une productivité fortement dégradée. Les équipes tentent d'adapter leurs méthodes, mais les habitudes ont changé, les dépendances se sont installées.

Dans l'urgence, l'entreprise explore des alternatives : tester d'autres modèles, reconfigurer les outils, internaliser certaines briques. Mais ces solutions prennent du temps, nécessitent des ajustements techniques, et n'offrent pas toujours le même niveau de performance. Les clients s'inquiètent : certains demandent des garanties, d'autres suspendent les projets.

Progressivement, un constat s'impose : l'entreprise n'avait pas réellement anticipé la dépendance à ces modèles. Aucun plan de continuité n'avait été conçu pour fonctionner sans eux. Des alternatives avaient été évoquées, comme le recours à plusieurs fournisseurs, l'intégration de modèles *open source*, ou encore le maintien de capacités internes, mais elles avaient été jugées trop coûteuses, trop complexes ou insuffisamment performantes.

Le choix avait été rationnel : privilégier la performance, la rapidité et la simplicité d'intégration. Mais ces choix ont progressivement déplacé le centre de gravité de la production.

Quelques semaines plus tard, la reprise est partielle. Mais l'essentiel est déjà joué. L'entreprise découvre qu'elle ne dépendait pas seulement d'un outil, mais d'une capacité à produire qu'elle ne maîtrisait plus.

Degré de criticité du scénario 4 : ↗ ÉLEVÉ

Ce scénario entraîne une diminution directe de la capacité de production. Il affecte la continuité d'activité, expose l'entreprise à des pénalités contractuelles, dégrade la relation client et peut avoir des conséquences durables sur sa réputation et sa stabilité opérationnelle.

Probabilité du scénario 4 : → MODÉRÉE

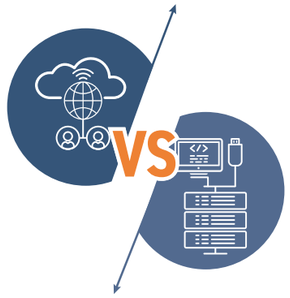
Les incidents techniques majeurs sont rares à l'échelle d'un fournisseur, mais leur occurrence est régulière à l'échelle du marché. Leur impact est d'autant plus important que les infrastructures sont concentrées et mutualisées.

ce que ce scénario révèle

- La dépendance ne réside pas seulement dans l'accès aux services, mais dans la capacité à continuer à produire sans eux.
- Les plans de continuité sont rarement conçus pour intégrer la disparition soudaine de briques d'IA devenues critiques, et s'avèrent difficilement activables en pratique.
- La délégation de capacités de production à des modèles externes entraîne une perte de maîtrise des modes de fonctionnement dégradés.
- Les engagements contractuels vis-à-vis des clients ne sont pas toujours alignés avec le niveau réel de résilience technique.
- La dépendance technologique devient organisationnelle et cognitive : les équipes, habituées à produire avec ces outils, peinent à retrouver des modes de fonctionnement autonomes. Ce phénomène peut être accentué par un décalage entre les outils internes et les solutions accessibles au grand public, favorisant le recours à des usages non encadrés (*shadow AI*) qui échappent aux dispositifs de contrôle de l'entreprise.

Quelles sont les tensions que ce scénario illustre :

Choix d'externaliser les infrastructures critiques pour gagner en efficacité et en qualité de service (cloud public, services managés, dépendance à un fournisseur unique).

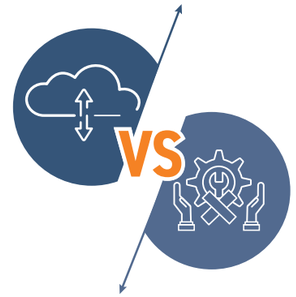


Choix de conserver des capacités internes ou alternatives pour assurer la continuité (infrastructures *on-premises*, second fournisseur, environnement de secours indépendant).

Choix de la simplicité opérationnelle (un seul environnement, architecture centralisée, peu de duplication des systèmes).

Choix de la résilience impliquant duplication et redondance (multi-cloud, réplication des données, environnements miroir, plans de reprise d'activité — PRA/PCA).

Choix d'un système optimisé pour le fonctionnement normal (toute l'activité sur un seul cloud, dépendance à un environnement principal, absence de bascule testée).



Choix d'un système capable de fonctionner en mode dégradé en cas d'incident (mode de secours, bascule vers un environnement alternatif, procédures de crise testées régulièrement, fonctionnement partiel mais maintenu).

Scénario 5

L'effondrement du château de cartes pour une carte parmi cent

Amine, directeur de l'innovation dans une entreprise européenne, prépare le lancement d'un nouveau service basé sur l'intelligence artificielle. Depuis plusieurs mois, ses équipes développent un modèle interne, entraîné sur des données propriétaires, destiné à automatiser une partie critique de l'activité. Le projet est stratégique et repose sur un équilibre fragile : des capacités de calcul louées à l'extérieur, des composants matériels difficiles à obtenir, et des outils logiciels fournis par quelques acteurs dominants.

À quelques jours du lancement, Amine reçoit un message : les conditions d'accès aux ressources de calcul viennent de changer. Les volumes disponibles sont fortement réduits et les prix augmentent.

Amine pense d'abord à un ajustement temporaire. Mais, très vite, les informations se précisent : un État qui contrôle une part essentielle des composants nécessaires à l'intelligence artificielle, fait l'objet d'un blocus. Les effets sont immédiats sur l'ensemble de la chaîne. Si les capacités de calcul sont encore disponibles, la peur de la pénurie engendre une compétition entre utilisateurs : chacun veut sécuriser ses approvisionnements, parfois au-delà du nécessaire. Les délais s'allongent et les coûts explosent.

En quelques jours, le projet est à l'arrêt. Les équipes ne peuvent plus entraîner le modèle, les itérations deviennent impossibles et les délais de mise sur le marché sont compromis.

Alors une alternative est envisagée : utiliser des modèles déjà disponibles, proposés par les grands acteurs du marché. C'est une solution rapide, performante et surtout immédiatement opérationnelle. Mais elle implique de renoncer à une partie de la maîtrise : dépendance à une API, conditions d'usage imposées, évolution des modèles non maîtrisée et incertitude sur les coûts futurs.

Le choix est posé : soit continuer à investir dans une capacité devenue incertaine, lente et coûteuse, soit basculer vers une solution externe, performante mais dépendante.

À court terme, la décision est évidente et l'entreprise s'oriente vers le second choix. Le projet reprend en s'appuyant sur une solution externe et, quelques mois plus tard, le service est lancé. Il fonctionne, il est performant, mais il repose entièrement sur des briques que l'entreprise ne maîtrise pas. Dans un environnement concurrentiel, renoncer à ces solutions aurait signifié accepter un décrochage technologique immédiat.

Chaque usage renforçait progressivement la dépendance, sans qu'il soit possible, à court terme, de reconstruire une chaîne de valeur équivalente. Amine résume, en comité : " On n'a pas perdu l'accès à l'IA, mais on a perdu la capacité de la maîtriser ".

Degré de criticité du scénario 5 : → MODÉRÉ à ↗ ÉLEVÉ

Contrairement au scénario n° 4, qui porte sur l'indisponibilité ponctuelle d'un service ou d'un outil, ce scénario s'intéresse à une rupture plus structurelle, affectant l'ensemble de la chaîne de valeur de l'intelligence artificielle. Il peut entraîner une perte durable de position dans la chaîne de valeur et une dépendance accrue à des solutions externes.

Probabilité du scénario 5 : → MODÉRÉE à ↗ ÉLEVÉE

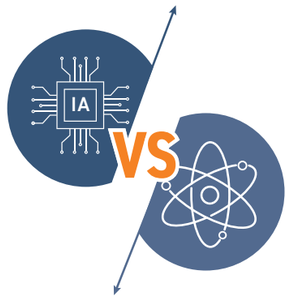
La concentration des ressources critiques (*compute*, composants, modèles) rend ce type de rupture plausible, notamment dans un contexte de tensions géopolitiques et de compétition technologique accrues.

ce que ce scénario révèle

- L'accès à l'IA repose sur une chaîne de valeur complexe, dont chaque maillon peut devenir un point de blocage.
- La dépendance ne porte pas uniquement sur les modèles, mais sur les ressources nécessaires pour les concevoir et les exploiter (*compute*, composants, outils).
- Les alternatives existent, mais elles impliquent souvent un arbitrage entre performance immédiate et maîtrise à long terme.
- La dépendance peut évoluer : d'une dépendance technique (*compute*) à une dépendance fonctionnelle (modèles, API).
- À terme, le risque est un déplacement durable de la valeur vers les acteurs dominants.

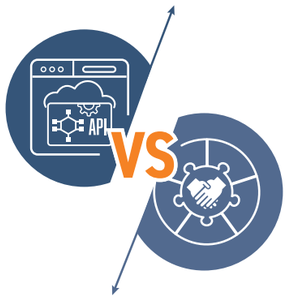
Quelles sont les tensions que ce scénario illustre :

Choix d'accéder aux technologies d'IA les plus performantes, souvent intégrées et propriétaires (modèles fermés, API managées, infrastructures de calcul spécialisées, services cloud intégrés).



Choix de solutions plus ouvertes et maîtrisées, permettant de préserver une autonomie technologique (modèles *open source*, déploiement local ou cloud maîtrisé, architectures modulaires, gestion interne des données et du calcul), **au prix d'une moindre performance immédiate.**

Choix d'accélérer rapidement l'innovation en s'appuyant sur des acteurs dominants (accès immédiat à des modèles avancés, APIs prêtes à l'emploi, infrastructures de calcul mutualisées, intégration rapide dans les produits).



Choix d'un développement plus progressif mais soutenable et maîtrisé (développement interne ou hybride, adaptation de modèles *open source*, montée en compétence des équipes, construction d'infrastructures ou de partenariats maîtrisés).

Conclusion

Photos LDD *magnific.com* – Montage AVDB

Les dépendances numériques auxquelles sont aujourd'hui confrontées les entreprises recouvrent plusieurs dimensions complémentaires :

Cloud : stockage des données, capacité de calcul (*compute*), plateformes et services critiques sur lesquels reposent les systèmes d'information.

Intelligence artificielle : modèles, API et briques avancées qui introduisent des dépendances fonctionnelles et cognitives dans les processus de production, ainsi qu'une dépendance à l'accès aux données indispensables à leur entraînement, à leur fonctionnement et à leur amélioration.

Connectivité : infrastructures réseau, y compris satellitaires, qui conditionnent l'accès auxsystèmes et la continuité des opérations.

Cadres juridiques : exposition à des droits étrangers et à des mécanismes d'extraterritorialité pouvant affecter l'accès, l'usage ou le contrôle des ressources.

L'enjeu ne réside pas dans chacune de ces dépendances prises isolément, mais dans leur imbrication, qui crée des vulnérabilités à la fois techniques, économiques, opérationnelles et juridiques.

Si ces cinq scénarios ne visent pas à dresser un inventaire supplémentaire des risques, ils permettent de déplacer les critères de décision. Tous les chocs ne produisent pas les mêmes effets, n'affectent pas les mêmes actifs et n'exigent pas le même niveau de préparation. Une interruption brutale, une contrainte juridique, une hausse tarifaire ou une rupture dans la chaîne de valeur de l'IA ne se traitent pas de la même manière.

Dès lors, la question centrale n'est plus seulement d'identifier les vulnérabilités, mais de déterminer dans quelles conditions l'entreprise souhaite rester capable d'agir.

Cela suppose de hiérarchiser les dépendances, puis d'arbitrer entre des objectifs difficilement conciliables : performance, maîtrise, coût et continuité.

L'enjeu n'est pas de supprimer ces tensions, mais de les rendre explicites pour éclairer la décision.

Que veut-on maîtriser ?

Comparer les configurations de maîtrise

Les scénarios précédents ont mis en évidence la diversité des dépendances numériques et les effets qu'elles peuvent produire en situation de rupture. Ils montrent que toutes les dépendances ne présentent ni le même niveau de criticité, ni les mêmes implications opérationnelles.

L'enjeu de cette seconde partie est de passer de l'illustration à la structuration. Il ne s'agit plus seulement d'identifier des vulnérabilités, mais de qualifier les dépendances, de rendre visibles les arbitrages qu'elles impliquent et de fournir un cadre permettant de comparer différentes configurations de maîtrise.

Cette approche repose sur une idée centrale : la souveraineté numérique ne se décrète pas, elle se construit par des arbitrages explicites entre dépendance, coût et performance.

1 Hiérarchisation des dépendances

Face à des situations de dépendance de gravité différente, l'enjeu n'est pas d'éliminer toutes les vulnérabilités mais de les qualifier selon leur criticité réelle et leur probabilité d'occurrence, c'est-à-dire selon leur effet sur la continuité d'activité, en situation spécifique.

Avant d'aller plus loin, il convient d'expliciter ce que recouvre la notion de dépendance numérique. En 2026, le Club des Experts de la Sécurité de l'Information et du Numérique (CESIN) en donne la définition suivante :

> **« La dépendance numérique est la situation dans laquelle une organisation, une collectivité ou un État ne peut plus assurer ses missions essentielles sans recourir à des technologies, des plateformes ou des services numériques sur lesquels elle n'a ni la maîtrise suffisante, ni la capacité réaliste d'arbitrage ou de substitution. »**

Cette définition met en lumière deux dimensions essentielles : d'une part, la perte de maîtrise, d'autre part, l'impossibilité pratique d'arbitrer ou de remplacer. C'est précisément cette combinaison qui transforme une dépendance en vulnérabilité stratégique.

Des outils existent déjà pour objectiver ces enjeux, notamment l'Indice de Résilience Numérique (IRN) qui constitue désormais un point d'appui de référence pour objectiver l'exposition d'une organisation et structurer un premier diagnostic de résilience.

Une fois le niveau de résilience évalué, il faut le placer en regard d'autres facteurs clés comme la performance et le coût, afin d'orienter des arbitrages opérationnels. L'objet de notre rapport est précisément d'explorer des pistes en ce sens.

Sur cette base, l'analyse doit être approfondie : toutes les dépendances ne justifient pas le même niveau de maîtrise, ni les mêmes investissements. Il convient donc de les hiérarchiser, puis d'identifier les configurations de maîtrise pertinentes pour chacune d'elles.

Commençons par distinguer quatre niveaux de dépendances :

Dépendances supportables
L'activité peut se poursuivre sans impact significatif ou avec des dégradations marginales (perte de confort ou d'un élément négligeable, baisse d'efficacité limitée). Ces dépendances ne nécessitent pas de maîtrise spécifique à court terme.

Dépendances gênantes
Une rupture entraîne des perturbations visibles, mais des alternatives existent et sont mobilisables dans des délais raisonnables. L'organisation peut continuer à fonctionner au prix d'une baisse temporaire de performance ou d'un surcoût.

Dépendances critiques

Il s'agit de dépendances essentielles pour lesquelles des alternatives existent théoriquement, mais sont difficilement accessibles (coût, délais, maturité technique, dette technologique). La continuité d'activité est fortement contrainte : certaines fonctions deviennent indisponibles ou dégradées de manière prolongée.

Dépendances inacceptables
L'absence de solution de substitution rend la continuité impossible. La rupture entraîne une cessation d'activité totale ou une incapacité à redémarrer dans des conditions viables.

Tableau de référence pour la qualification des risques liés aux dépendances

	Très peu probable Aucune fois	Probable Peut-être une fois	Très probable Une fois	Fréquent Plus d'une fois
Dépendance inacceptable Cessation d'activité totale			INACCEPTABLE	
Dépendance critique Activité fortement contrainte				
Dépendance gênante Perturbations visibles				
Dépendance supportable Dégradations marginales	ACCEPTABLE			

CRITICITÉ ↑ — PROBABILITÉ →

Ce tableau propose une lecture volontairement simplifiée et théorique des niveaux de dépendance afin d'offrir un repère dans la grande majorité des situations. Il ne prétend toutefois pas refléter la complexité de la réalité, car son interprétation dépend étroitement des cas d'usage, de l'existence (ou non) d'alternatives crédibles et du coût que représente leur mise en œuvre.

En pratique, le niveau de dépendance est contextuel. Une dépendance initialement jugée inacceptable, par exemple vis-à-vis d'un fournisseur étranger, peut devenir critique mais nécessaire en l'absence d'alternatives viables ou lorsque les solutions de substitution impliquent des coûts prohibitifs susceptibles de fragiliser l'entreprise. Dans ce type de situation, l'organisation peut être contrainte d'accepter une dépendance théoriquement inacceptable, faute de meilleure option.

2 Trois variables de décision : dépendance, coût et performance

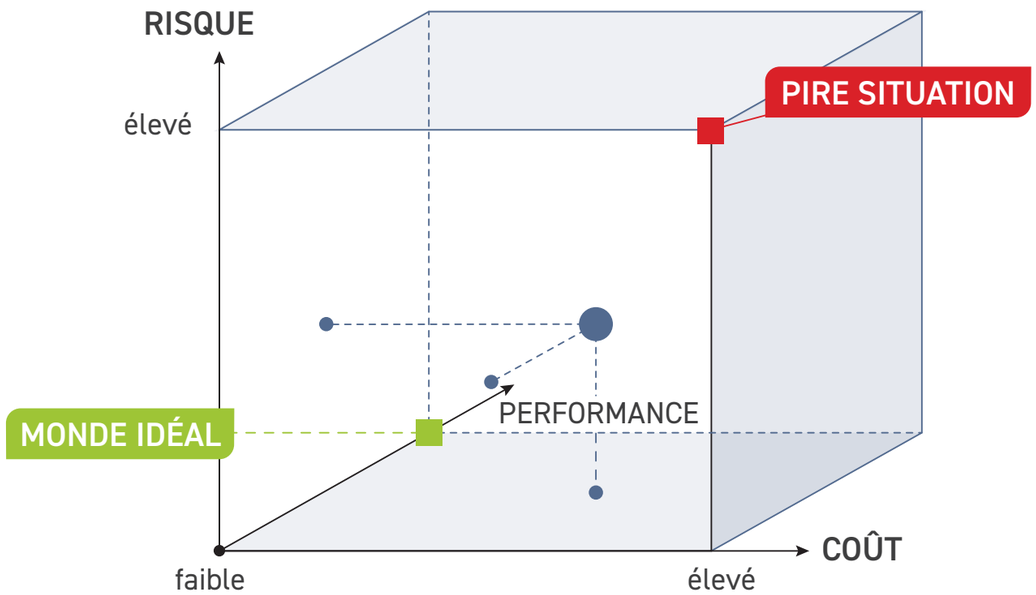
La hiérarchisation ne suffit donc pas, à elle seule, à orienter la décision. Savoir qu'une dépendance est critique n'indique pas automatiquement comment la traiter. Toute stratégie de maîtrise se heurte ainsi à des tensions structurantes : renforcer la résilience a un coût, améliorer la réversibilité peut dégrader la performance, accroître la maîtrise complexifie les opérations.

La souveraineté, entendue ici comme la capacité à maîtriser les risques pesant sur la continuité et la pérennité de l'activité, ne constitue donc pas un objectif autonome. Elle doit se penser au regard de deux contraintes structurantes : le coût et la performance.

Car réduire une dépendance implique implique presque toujours :

- Des investissements supplémentaires (duplication des infrastructures, diversification des fournisseurs, adoption de solutions alternatives).
- Une complexité accrue, parfois au détriment de la performance.

Autrement dit, **toute stratégie de souveraineté opérationnelle repose sur un compromis entre niveau de dépendance accepté, coût soutenable et efficacité recherchée.** Ces trois dimensions ne peuvent être optimisées simultanément.



- Monde idéal > faible coût, faible risque, performance maximale
- Pire situation > coût maximal, risque maximal, faible performance
- Exemple de dépendance positionnée dans le cube

Pour représenter ces arbitrages, il est possible de se référer à un espace à trois dimensions structuré autour du coût, du niveau de risque lié à la dépendance (cf. Tableau de référence pour la qualification des risques liés aux dépendances) et de la performance.

Chaque configuration de maîtrise peut ainsi être positionnée dans ce volume. Le point qui se situe à l'intersection de ces trois variables pourrait matérialiser les arbitrages retenus par l'organisation.

Deux repères théoriques en dessinent les limites :

- d'un côté, un "monde idéal" combinant faible coût, faible risque et performance maximale ;
- de l'autre, la "pire situation" pour l'entreprise où coût et risque sont élevés pour une performance faible.

Ces deux extrêmes n'ont pas vocation à être atteints ; ils permettent uniquement de situer les configurations réelles.

Toute décision consiste donc à déplacer sa position dans cet espace. Réduire une dépendance (plus particulièrement le risque qu'elle entraîne) implique le plus souvent une augmentation des coûts ou une dégradation de la performance. Inversement, optimiser la performance ou les coûts peut dans plusieurs cas accroître l'exposition au risque. Toutefois, certaines configurations permettent des gains simultanés sur plusieurs dimensions au prix de conditions spécifiques rarement généralisables.

L'intérêt de cette représentation est précisément de rendre visibles ces effets de déplacement. En effet, elle permet de situer une configuration existante, d'anticiper les conséquences d'un choix et d'identifier les zones de fragilité, ou au contraire, les marges de manœuvre encore disponibles. L'arbitrage porte ainsi également sur la trajectoire que l'on accepte de suivre entre ces trois variables.

Pour rendre ces arbitrages opérationnels, il est nécessaire de les matérialiser sous une forme lisible et manipulable : c'est le rôle des curseurs présentés ci-après.

3 Comparer les configurations de maîtrise à partir de curseurs

Les curseurs ne décrivent pas des solutions, mais les tensions au sein desquelles toute décision doit se situer. Ils permettent de rendre explicites des arbitrages souvent implicites, et d'éviter une approche binaire opposant "bonne" et "mauvaise" solution.

Chacun des curseurs ci-dessous représente ainsi une tension structurante entre deux objectifs légitimes mais difficilement conciliables : résilience et coût, maîtrise et simplicité, performance et réversibilité, ou encore autonomie et accès aux technologies les plus avancées.

La souveraineté, dans cette perspective, ne se résume pas à un niveau à atteindre : elle résulte d'une combinaison d'arbitrages, nécessairement imparfaite, qui reflète les priorités, les contraintes et les risques propres à chaque organisation.

D'autre part, les curseurs ne doivent pas être appréhendés de manière indépendante. En pratique, toute décision prise sur l'un d'entre eux a des effets sur les autres. Choisir une solution externalisée, par exemple, peut simultanément améliorer la performance, réduire la maîtrise opérationnelle, accroître la dépendance contractuelle et réduire le coût. À l'inverse, renforcer l'autonomie peut dégrader la performance ou augmenter significativement les coûts.

Dès lors, la valeur de cette approche ne réside pas uniquement dans l'identification de ces tensions, mais dans la compréhension de leur articulation. L'enjeu est moins de positionner chaque curseur isolément que de comprendre les déplacements dans l'ensemble du système qu'implique toute décision.

Les curseurs qui suivent ne décrivent donc pas des solutions, mais une cartographie des tensions à partir de laquelle les choix techniques et organisationnels peuvent ensuite être éclairés. Tous les curseurs présentés traduisent une même logique : il ne s'agit pas de supprimer le risque, mais de le déplacer en fonction des priorités de l'organisation.

Les deux premiers curseurs présentent un caractère plus théorique que les suivants ; à ce titre, ils peuvent être envisagés comme des curseurs fondamentaux, dans la mesure où ils conditionnent en partie le positionnement sur l'ensemble des autres curseurs.

EXIGENCE DE CONTINUITÉ

1

Ce curseur fixe la cible de disponibilité pour chaque usage, exprimée en termes de RTO (*Recovery Time Objective* : durée maximale d'indisponibilité acceptable) et de RPO (*Recovery Point Objective* : perte de données maximale acceptable). Il est le point de départ de tout arbitrage d'architecture : c'est lui qui justifie (ou non) les investissements en redondance, en réplication et en planification de continuité.

Interruption tolérable
RTO > 72h, RPO > 24h. Systèmes non critiques : outils de *reporting*, archivage, services administratifs non urgents. Interruption acceptable sans impact métier immédiat.

Reprise différée
RTO 24–72h, RPO 4–24h. Systèmes importants mais substituables temporairement par des processus manuels : ERP secondaire, outils collaboratifs non vitaux.

Reprise rapide
RTO 4–24h, RPO 1–4h. Systèmes critiques dont l'interruption dégrade significativement l'activité : ERP principal, plateforme de paiement B2B, outils de supervision.

Haute disponibilité
RTO 15min–4h, RPO < 1h. Systèmes vitaux pour la continuité commerciale, ex : plateforme e-commerce, *core banking*, infrastructure de *trading*. Redondance active-passive requise.

Continuité absolue
RTO < 15min, RPO ≈ 0. Systèmes à mission critique absolue, ex : *clearings* financiers, SCADA industriels, systèmes de défense. Redondance active-active, multi-sites, sans interruption perceptible.

SOUVERAINETÉ JURIDIQUE ET LOCALISATION DES DONNÉES

2

Ce curseur mesure le degré d'exposition de l'organisation à des mécanismes de droit extraterritorial (CLOUD Act américain, FISA 702, législations similaires d'autres États). Il ne porte pas sur la localisation physique des données — qui est une mesure insuffisante à elle seule — mais sur la chaîne complète : juridiction de l'opérateur, localisation des données, contrôle des clés de chiffrement, et immunité contractuelle face à des injonctions étrangères.

Exposition maximale
Fournisseur soumis à une juridiction étrangère contraignante (ex. droit américain), données non localisées, aucun mécanisme de chiffrement indépendant. CLOUD Act, *FISA* 702 pleinement applicables.

Exposition contractuelle
Localisation contractuelle des données en UE, clauses RGPD, mais fournisseur toujours soumis à extraterritorialité étrangère. La protection est contractuelle, non structurelle.

Protection qualifiante
Fournisseur certifié SecNumCloud ou EUCS Haute, opérateur de droit européen sans dépendance capitalistique à une entité non-européenne. Exposition résiduelle possible sur les composants sous-jacents.

Maîtrise structurelle
BYOK (*Bring Your Own Key*) ou *HYOK* (*Hold Your Own Key*) : clés de chiffrement gérées en interne, fournisseur incapable techniquement de déchiffrer les données. Opérateur qualifié. Données et métadonnées protégées.

Immunité totale
On-premises ou cloud souverain certifié avec contrôle total des données, des clés et des traitements. Aucune dépendance à un acteur soumis à une juridiction étrangère sur toute la chaîne. Applicable aux données classifiées ou à très haute sensibilité stratégique.

PROFONDEUR D'INTERNALISATION (*MAKE OR BUY*)

3

Ce curseur mesure la profondeur de l'internalisation technique et opérationnelle, de la couche infrastructure jusqu'à la couche applicative. Il détermine qui conçoit, qui opère et qui décide des évolutions. C'est un curseur de contrôle opérationnel, pas seulement économique : si l'internalisation donne de la maîtrise, elle crée une responsabilité directe sur la sécurité, la maintenance et la dette technique. Ce curseur est fortement conditionné par les ressources humaines disponibles.

SaaS pur
L'organisation consomme des applications entièrement gérées par le fournisseur (couches infrastructure, plateforme et application). Aucun contrôle opérationnel.

PaaS
Contrôle de la couche applicative, infrastructure et *middleware* gérés par le fournisseur. L'organisation déploie et maintient ses applications, pas l'infra.

IaaS + applicatif interne
Infrastructure cloud externalisée, mais systèmes d'exploitation, *middleware* et applications gérés en interne. Niveau standard du cloud "*lift-and-shift*" avec équipes DevOps.

***On-premises* géré**
Infrastructure physique propre (datacenter propre ou co-location), toute la *stack* logicielle gérée en interne. Forte dépendance aux équipes internes. Investissements CAPEX significatifs.

Internalisation totale
Maîtrise de l'ensemble de la chaîne : matériel, firmware, OS, *middleware*, applications, sécurité. Uniquement accessible à de très grands acteurs (opérateurs critiques, État, banques systémiques). Coût et complexité maximaux.

PORTABILITÉ ET RÉVERSIBILITÉ

4

La réversibilité est multidimensionnelle : une solution peut être techniquement réversible (standards ouverts) mais économiquement verrouillée (remises tarifaires conditionnées à des engagements pluriannuels), ou opérationnellement irréversible (migration de 18 mois incompatible avec un besoin de bascule en 48h). Ce curseur évalue la réversibilité effective, c'est-à-dire activable dans des conditions opérationnellement et économiquement soutenables, selon quatre sous-dimensions indépendantes.

***Lock-in* total**
Standards propriétaires non documentés, engagement pluriannuel avec pénalités élevées, migration estimée > 18 mois, aucune clause de sortie opérationnelle. Changement techniquement, économiquement et contractuellement verrouillé.

Réversibilité théorique
Données exportables en formats standards, mais coût de migration entre 15–30 % du budget annuel, délai > 12 mois, intégrations nombreuses à reconstruire. *Exit* possible mais déstabilisant.

Réversibilité planifiable
Standards ouverts sur les données et API, engagement 1–3 ans, coût de migration 5–15 % du budget annuel, délai 3–12 mois. La sortie est faisable avec une planification anticipée de 6–12 mois.

Réversibilité opérationnelle
Interopérabilité native, clauses de sortie sans pénalité, coût de migration < 5 % annuel, délai < 3 mois. Bascule fournisseur activable dans le cadre d'un cycle budgétaire normal.

Portabilité complète
Architecture fournisseur-agnostique (*Infrastructure-as -Code*, standards CNCF, données en formats ouverts), bascule activable en < 4 semaines, coût marginal.
Fournisseur interchangeable sans impact opérationnel majeur.

5 NIVEAU D'ISOLATION DES ENVIRONNEMENTS

Ce curseur porte sur l'architecture physique et logique de l'environnement. Il ne réduit pas le risque mais le transforme : la mutualisation expose à des risques systémiques (cyber, défaillance en cascade, concentration), tandis que l'isolation expose à des risques physiques et opérationnels (panne locale, erreur humaine, absence de redondance). Le choix optimal dépend donc du profil de risque dominant pour chaque usage.

Cloud public mutualisé
Ressources computationnelles partagées entre tous les clients du fournisseur. Isolation logique uniquement (hyperviseur). Niveau standard des offres IaaS/PaaS/SaaS publiques.
Risque de side-channel, d'erreur de configuration exposant des données.

Tenant isolé logiquement
VPC dédié, réseau privé virtuel, isolation logique renforcée mais infrastructure physique partagée.

Dédié physiquement
Serveurs physiques dédiés à l'organisation (*bare metal* dédié), infrastructure physique non partagée mais *datacenter* et opérateur communs.

***On-premises* / cloud privé**
Infrastructure physique appartenant à l'organisation ou en co-location dédiée, opérée en interne. Aucun partage de ressources physiques. Risques physiques directs (incendie, accès, SPOF).

***Air-gap* complet**
Déconnexion physique totale du réseau public, accès physique contrôlé et tracé. Réservé aux données les plus sensibles : défense nationale, R&D stratégique, systèmes industriels critiques. Complexité opérationnelle et coût maximaux.

6 CONCENTRATION FOURNISSEUR

Ce curseur mesure le degré de concentration des dépendances sur un nombre restreint d'acteurs. Un fournisseur unique constitue un point de défaillance unique sur les dimensions technique, commerciale et géopolitique. La diversification réduit ce risque mais engendre une complexité opérationnelle et des coûts d'intégration croissants. Il faut distinguer la diversification nominale (plusieurs contrats) de la diversification effective (fournisseurs réellement indépendants, technologiquement et capitalistiquement).

Mono-fournisseur
Un seul fournisseur pour une fonction critique donnée, sans solution de secours activable. Dépendance totale sur les dimensions technique, contractuelle, commerciale et géopolitique. SPOF (Single Point of Failure) assumé.

Fournisseur principal + secours passif
Un fournisseur principal actif et un secondaire en mode veille (*cold standby*). La bascule est possible mais non testée régulièrement, et le délai d'activation peut dépasser 48h. Réduction partielle du risque.

Multi-fournisseur actif
Charge répartie entre 2–3 fournisseurs indépendants, chacun actif en production. Bascule automatique ou semi-automatique en cas de défaillance. Complexité opérationnelle significative.

Diversification technologique
Mix de technologies distinctes (cloud public + *on-premises*, satellite + terrestre, SaaS + *open source*). Indépendance non seulement contractuelle mais aussi technologique entre fournisseurs.
Gouvernance multi-cloud mature.

Architecture fournisseur-agnostique
Architecture conçue dès l'origine pour être indépendante de tout fournisseur spécifique. Abstraction via des couches d'interopérabilité. Substitution de fournisseur sans refonte architecturale.

7 DÉPENDANCE À L'INNOVATION EXTERNE

Ce curseur mesure la dépendance de l'organisation à l'innovation produite par des tiers pour maintenir sa compétitivité. Il n'est pas identique au curseur n°3 (qui mesure le degré d'internalisation et qui conçoit ou opère les systèmes) : une organisation peut opérer ses propres systèmes (C3 élevé) tout en les construisant sur des technologies tierces à forte dépendance à l'innovation externe. L'enjeu est ici la capacité à innover indépendamment, et le coût d'opportunité associé à chaque posture.

***Best-of-breed* pur**
Adoption intégrale des solutions du marché telles que proposées par les fournisseurs (SaaS, modèles IA propriétaires, services managés). *Roadmap* entièrement subie. Accès immédiat aux dernières innovations, mais aucune différenciation technologique propre.

Intégration sélective
Adoption de solutions tierces avec personnalisation et intégration interne. L'organisation adapte mais ne crée pas les briques fondamentales. Dépendance forte aux décisions de mise à jour des fournisseurs.

Hybride (modèle dominant)
Mix entre adoption externe et R&D interne sur les composants les plus critiques ou différenciants. *Open source* activement utilisé et contribué. Modèle économiquement réaliste pour la majorité des organisations.

R&D interne dominante
L'essentiel de la différenciation technologique est produit en interne. Recours à des composants externes uniquement pour les fonctions standardisées. Implique des équipes R&D importantes et des cycles d'innovation longs.

Autonomie technologique totale
Innovation entièrement produite en interne, y compris sur les couches fondamentales (algorithmes, modèles, protocoles). Réservé aux très grands acteurs (États, opérateurs stratégiques, acteurs technologiques majeurs). Risque d'isolement technologique et de sur-investissement.

4 Grille d'arbitrage

Les curseurs ci-dessus permettent de structurer les tensions, mais ne suffisent pas à orienter une décision concrète.

Le passage à l'opérationnel suppose de confronter ces tensions à un nombre limité de critères structurants, qui déterminent les arbitrages possibles au sein de chaque organisation.

Ces critères ne constituent pas de simples variables contextuelles, mais les principaux paramètres de décision, à partir desquels une stratégie de maîtrise peut être définie :

- Le stade de développement de l'entreprise (phase de croissance rapide, stabilisation, transformation)
- Sa taille et la complexité de sa structure
- Le volume de données à traiter, stocker ou faire circuler
- La criticité des données et des fonctions concernées (données sensibles, stratégiques ou encore remplaçables)
- Les exigences de continuité d'activité (tolérance à l'interruption, délais de reprise acceptables)
- Les contraintes réglementaires et juridiques (localisation des données, extraterritorialité, conformité sectorielle)
- Les ressources internes disponibles (niveau de compétences techniques, capacité à opérer et maintenir les systèmes)
- Les contraintes budgétaires et la capacité d'investissement dans la durée
- Le degré de dépendance existant et la maturité des alternatives disponibles (coût, délai, faisabilité de substitution)

Ces critères pourraient être affinés ou complétés selon les contextes, mais au prix d'une perte de lisibilité. Leur rôle est précisément de fournir un cadre de décision suffisamment structurant pour être opérationnel, tout en restant applicable à une grande diversité de situations.

La grille d'arbitrage vise ainsi à opérer ce passage, en transformant ces tensions en critères de décision concrets et comparables.

Face à des dépendances de nature et d'intensité variables, nous l'avons vu, l'enjeu n'est pas de rechercher une maîtrise absolue, mais de disposer d'un cadre permettant d'éclairer les arbitrages entre risque, performance et coût. Une fois les risques identifiés, encore faut-il être en mesure d'en apprécier les implications concrètes : que se passe-t-il en cas de rupture, dans quels délais une alternative peut être activée, à quel coût, et avec quel niveau de perte de contrôle ?

La grille d'arbitrage proposée vise précisément à structurer cette analyse. Elle permet d'objectiver une dépendance à partir de critères opérationnels (comme l'exposition, la réversibilité, la portabilité, la continuité), puis de comparer différentes configurations de maîtrise en fonction de ce qu'elles protègent, de ce qu'elles exposent et des compromis qu'elles impliquent.

Elle ne fournit pas de réponse unique, mais un cadre de décision. Son objectif n'est pas d'éliminer toute dépendance, mais de s'assurer que celle-ci reste choisie, comprise et supportable, au regard des priorités de l'organisation.

La grille d'arbitrage se déploie en trois étapes complémentaires : qualifier la dépendance (A), vérifier la réalité des garanties (B), puis comparer les configurations de maîtrise envisageables (C).

A • Qualifier son niveau de dépendance

Dimension	Question clé	Niveau faible	Niveau élevé
Exposition à la rupture	Que se passe-t-il si la solution devient indisponible ?	Impact limité, contournable	Paralysie immédiate de l'activité
Perte d'accès unilatérale	Existe-t-il un risque de type *kill switch* ?	Contrôle conservé	Accès dépendant d'un tiers
Capacité d'alternative	Une alternative existe-t-elle et est-elle activable ?	Substitution rapide possible	Aucune alternative réaliste à court terme
Coût de sortie	Quel est le coût réel d'un changement ?	Faible, anticipé	Très élevé, voire prohibitif
Portabilité	Les données / systèmes sont-ils transférables ?	Standards ouverts, facilement migrables	Formats propriétaires, migration complexe

Une fois la dépendance qualifiée, il convient d'évaluer la réalité des garanties associées. Au-delà des engagements affichés, l'enjeu est d'identifier ce qui est effectivement maîtrisable en situation de rupture.

B • Réalité des garanties

Dimension	Question clé	Faible maîtrise	Forte maîtrise
Contrat	Les clauses de sortie sont-elles activables ?	Théoriques	Opérationnelles et testées
Technique	Des mécanismes de réversibilité existent-ils ?	Absents ou partiels	Structurés et testés
Gouvernance	Qui contrôle les accès et les clés ?	Solutions par défaut du fournisseur	Contrôle interne ou partagé
Identité du fournisseur	Quelles garanties apporte le fournisseur ?	Fournisseur soumis à une juridiction étrangère contraignante	Fournisseur disposant d'une autonomie réelle, gouvernance claire, exposition juridique maîtrisée
Continuité (PCA/PRA)	Les plans sont-ils testés ?	Non testés	Testés régulièrement
Assurance	Le risque est-il couvert ?	Couverture partielle	Couverture adaptée aux scénarios

Sur cette base, différentes configurations de maîtrise peuvent être envisagées. Leur comparaison permet d'identifier les compromis qu'elles impliquent et d'éclairer la décision.

C • Comparer les configurations de maîtrise

Critère	Question clé	Risque associé
Ce que je protège	Quel objectif est prioritaire ?	Surprotéger un aspect au détriment des autres
Ce que j'expose	Quelle vulnérabilité est créée ?	Angle mort stratégique
Coût réel	Quel est le coût total ?	Sous-estimation des coûts cachés
Dépendance (*lock-in*)	Suis-je lié techniquement, contractuellement ou économiquement ?	Perte de capacité d'arbitrage
Réversibilité	Puis-je réellement sortir ou migrer ?	Réversibilité théorique mais inapplicable

Ces trois niveaux d'analyse doivent être lus conjointement : une dépendance peut apparaître maîtrisée en théorie, mais se révéler critique en pratique si les garanties ne sont pas opérationnelles ou si les configurations alternatives ne sont pas soutenables.

Ce travail a aussi pour vocation d'aider le dirigeant à évaluer la vulnérabilité de leurs distributeurs, leurs fournisseurs, et leurs prestataires aussi.

5 Traduction des arbitrages sur des technologies clés

Les arbitrages présentés jusqu'ici ne portent pas sur des solutions en tant que telles, mais sur la nature des risques que l'on accepte de porter — en interne ou en externe, de manière localisée ou systémique.

Ils traduisent moins un choix technologique qu'un positionnement stratégique : où se situe le risque, sous quelle forme il se manifeste, et dans quelle mesure il reste maîtrisable.

Toutefois, ces arbitrages prennent une forme concrète dans un nombre limité de briques technologiques structurantes, qui concentrent aujourd'hui une part importante des dépendances numériques. Parmi elles : les infrastructures (cloud), les modèles et systèmes d'intelligence artificielle, les réseaux de connectivité, les systèmes d'identité et de gestion des accès, ou encore les mécanismes de chiffrement.

Chacune de ces briques ne crée pas les mêmes types de dépendances, ni les mêmes effets en cas de rupture. Certaines relèvent principalement d'une dépendance infrastructurelle (accès aux ressources, continuité technique), d'autres d'une dépendance fonctionnelle ou décisionnelle (production, automatisation, traitement de l'information), d'autres encore d'une dépendance transversale qui conditionne l'accès à l'ensemble du système (connectivité, identité).

Dans tous les cas, l'enjeu n'est pas de supprimer le risque, mais de le déplacer. Externaliser, internaliser, mutualiser ou isoler revient à transformer la nature du risque, plus qu'à le réduire.

Les développements qui suivent visent à illustrer ces arbitrages à travers plusieurs briques technologiques clés. Ils ne constituent pas un inventaire exhaustif, mais des points d'appui pour comprendre comment les choix opérés se traduisent concrètement, et quelles dépendances ils créent ou renforcent.

8 PROFIL DE RISQUE INFRASTRUCTURE (NUMÉRIQUE *VS* PHYSIQUE)

Ce curseur formalise un *trade-off* fondamental : déplacer les données vers le cloud réduit les risques physiques (redondance, supervision 24h/24, protection contre les sinistres locaux) mais augmente les risques numériques (ingérences extérieures, injonctions, surface d'attaque étendue). Et inversement, l'hébergement physique propre et l'isolement réduisent les risques numériques mais exposent à des risques physiques et opérationnels qui doivent être compensés par des investissements importants.

Cloud souverain
Fournisseur cloud dont le capital est détenu majoritairement par une entité nationale souveraine. Réduction partielle de l'exposition aux ingérences étrangères. Infrastructure physique restant mutualisée — la souveraineté du capital ne garantit pas une immunité juridique complète si des sous-traitants non-européens sont impliqués.

***On-premises* connecté**
Datacenter propre, connecté à internet. Protection accrue contre les ingérences extérieures et les injonctions : l'organisation est l'opérateur de son infrastructure. Exposition aux risques physiques directs (SPOF local, sinistre, erreurs humaines internes) à compenser par des PCA/PRA dédiés et des tests réguliers.

Cloud public total
Architecture entièrement dépendante des *hyperscalers*. Résilience physique maximisée par la redondance native du fournisseur. Perméabilité maximale aux risques numériques : ingérences étrangères, injonctions (CLOUD Act), cyberattaques sur infrastructure partagée, dépendance à la disponibilité du fournisseur.

Cloud privé (*hardware* externalisé, *software* maîtrisé)
Infrastructure physique hébergée chez un tiers (co-location, *bare metal* dédié), mais systèmes d'exploitation, *middleware* et applications gérés en interne. Compromis équilibré : réduction du risque numérique par la maîtrise logicielle, maintien d'une résilience physique via l'opérateur d'hébergement.

***Air-gap* total**
Isolation physique complète du réseau public. Immunité aux risques numériques d'origine externe. Exposition maximale aux risques physiques et opérationnels : toute interruption physique (panne matérielle, sinistre, erreur humaine) est absorbée sans filet de sécurité externe. Réservé aux données et traitements les plus sensibles.

9 DÉLÉGATION DÉCISIONNELLE À L'IA

Ce curseur mesure le degré de délégation décisionnelle à des systèmes d'intelligence artificielle, et corrélativement le niveau de supervision humaine explicite sur les décisions et traitements. Il ne porte pas sur la source des modèles (curseur n°7), ni sur qui les opère (curseur n°3), mais sur la gouvernance algorithmique : qui décide *in fine*, à quelle fréquence l'humain intervient dans la boucle, et dans quelle mesure les décisions de l'IA sont auditables et réversibles. Cet enjeu est directement lié aux réglementations sur l'IA (*EU AI Act*, entré en application en 2025) qui imposent des niveaux de supervision humaine distincts selon la criticité des usages.

Automatisation totale
L'IA décide et agit sans validation humaine systématique. *Workflows* entièrement automatisés : *scoring* de risque, modération de contenu, *trading* algorithmique, génération de documents diffusés sans revue. Aucune boucle de contrôle humain sur les décisions individuelles. Risque réglementaire élevé (*EU AI Act*, systèmes à haut risque).

Automatisation supervisée
Décisions IA soumises à validation humaine a posteriori ou sur échantillon statistique. L'humain peut intervenir mais pas en temps réel sur chaque décision. Alertes automatiques sur les cas limites ou les anomalies. Ex : *scoring* de crédit avec revue manuelle des dossiers atypiques, détection de fraude avec investigation humaine déclenchée.

Assistance décisionnelle active
L'IA produit des recommandations que l'humain valide systématiquement avant exécution. Boucle humaine obligatoire sur les décisions importantes. L'IA peut agir de manière autonome sur les tâches non critiques uniquement. Ex : aide à la rédaction avec revue, diagnostic assisté validé par un médecin, recommandation RH validée par un manager.

IA consultative
L'IA fournit des analyses, synthèses et options comme outil d'aide à la réflexion. Toutes les décisions sont prises par des humains. L'IA n'a pas accès en écriture aux systèmes de production. Traçabilité complète des recommandations IA et des décisions humaines effectives.

Contrôle humain souverain
Absence d'IA dans les processus décisionnels critiques. Outils algorithmiques limités à des règles déterministes, auditables et entièrement explicables. Applicable aux processus à très haute sensibilité réglementaire, souveraine ou éthique : justice, défense, applications nucléaires, décisions à impact vital.

10 RÉSILIENCE DE LA CONNECTIVITÉ

La connectivité est la couche invisible qui conditionne l'accès à toutes les autres : cloud, données, identité, IA. Par exemple, une architecture cloud de niveau 5 sur tous les autres curseurs devient inopérante si la connectivité repose sur un lien unique. Ce curseur évalue ainsi la diversification effective de la connectivité selon trois dimensions indépendantes : opérateur, technologie (câble, fibre, satellite, radio) et route physique (câble sous-marin, point d'échange).

Lien unique
Un seul opérateur, un seul câble, une seule technologie. SPOF réseau absolu. Une interruption chez l'opérateur ou une coupure physique (câble tranché, avarie satellite) paralyse immédiatement l'accès à tous les services dépendants.

Redondance simple
Deux liens distincts du même opérateur, ou deux liens de technologies identiques. Protège contre la panne de lien unique, pas contre une défaillance de l'opérateur ou une coupure sur un câble partagé.

Diversification opérateurs
Deux opérateurs indépendants (vérification de l'absence de points de mutualisation sur les routes physiques), même technologie. Protège contre la défaillance d'un opérateur, pas contre une coupure de type géographique ou géopolitique.

Diversification technologique
Mix de technologies distinctes : fibre terrestre + liaison satellitaire LEO ou GEO, ou fibre + radio. Protège contre les pannes liées à une technologie spécifique. Particulièrement pertinent pour les opérations en zones isolées ou en situation de crise.

Diversification complète
Multi-opérateur, multi-technologie, multi-route physique documentée et vérifiée (câbles sous-marins distincts, points d'échange indépendants). Bascule automatique entre chemins. Gouvernance des flux avec détection proactive de dégradation.

MAÎTRISE DE L'IDENTITÉ ET DES ACCÈS (IAM)

11 L'IAM (*Identity and Access Management*) est la couche fondatrice de tout système d'information : elle détermine qui peut accéder à quoi, dans quelles conditions. Un IAM externalisé crée une dépendance sur la couche la plus basse du SI, qui amplifie mécaniquement toutes les autres dépendances. C'est un curseur multiplicateur : un IAM faiblement maîtrisé réduit l'efficacité des protections mises en place sur les autres curseurs, car une injonction sur le fournisseur d'identité suffit à bloquer l'accès à l'ensemble du SI.

Fédération sans maîtrise des clés
IdP (*Identity Provide*r) interne fédéré avec les solutions fournisseur, mais clés de chiffrement et PKI gérées par le fournisseur. L'organisation contrôle les politiques d'accès mais pas les mécanismes cryptographiques sous-jacents.

IAM hybride maîtrisé
Infrastructure d'identité interne (LDAP/*Active Directory* interne, PKI propre, MFA interne), intégrations externes contrôlées par l'organisation. Les fournisseurs tiers sont des consommateurs de l'IAM interne, pas l'inverse.

IAM fournisseur pur
L'organisation utilise intégralement les solutions d'identité du fournisseur. Annuaires, politiques d'authentification et clés gérés par le fournisseur. Risque de blocage total en cas d'injonction ou de défaillance du fournisseur.

BYOK / BYOI
Bring Your Own Key ou Bring Your Own Identity : l'organisation gère ses clés de chiffrement et son IdP principal, mais s'appuie sur des solutions tierces pour les intégrations applicatives.

IAM souverain
Annuaire, PKI, HSM, politiques d'authentification et de droits 100% internalisés, sans dépendance à un tiers pour aucun composant de la chaîne d'identité. Audit complet et contrôle total des accès. Réservé aux environnements à très haute sensibilité.

HORIZON DE PROTECTION CRYPTOGRAPHIQUE

12 Ce curseur introduit une dimension temporelle absente des autres : la durabilité de la protection cryptographique face à l'évolution des capacités de décryptage, notamment liées à l'informatique quantique. Le principe du "*harvest now, decrypt later*" — collecter aujourd'hui des données chiffrées pour les déchiffrer lorsque les capacités de calcul le permettront — transforme cet enjeu futur en décision immédiate pour les données à longue durée de vie. Les standards NIST post-quantiques (FIPS 203 ML-KEM, FIPS 204 ML-DSA, FIPS 205 SLH-DSA), publiés en 2024, constituent la référence de transition.

Chiffrement renforcé
Algorithmes à longue clé (RSA-4096, courbes elliptiques 521 bits), durée de rotation des clés réduite, audit cryptographique régulier. Adapté aux données de sensibilité 2–5 ans. Mesure transitoire, non pérenne face à la menace quantique.

Post-quantique (standards NIST)
Adoption des algorithmes post-quantiques standardisés par le NIST (ML-KEM / FIPS 203, ML-DSA / FIPS 204, SLH-DSA / FIPS 205). Protection sur 10–25 ans selon l'évolution des capacités de calcul. Recommandé pour les données stratégiques à longue durée de vie.

Protection standard
Algorithmes actuels (AES-256, RSA-2048, TLS 1.3, ECDSA). Adapté aux données dont la durée de sensibilité est inférieure à 2 ans. Cible à risque pour des données collectées aujourd'hui dans une logique *harvest now, decrypt later* si les capacités quantiques progressent.

Transition hybride
Combinaison d'algorithmes classiques et post-quantiques (ex. X25519Kyber768). Approche recommandée pendant la période de transition, permettant une compatibilité ascendante tout en commençant la migration. Applicable aux données 5–10 ans.

Protection souveraine certifiée
Algorithmes post-quantiques sur HSM qualifiés, certifiés ANSSI (ou équivalent national), clés maîtresses en interne, protocoles conformes aux exigences gouvernementales ou de défense. Applicable aux données classifiées, à très haute sensibilité stratégique ou à durée de conservation > 25 ans.

Conclusion

Les éléments présentés dans cette seconde partie montrent que la souveraineté numérique ne repose ni sur l'élimination des dépendances, ni sur des choix technologiques isolés, mais sur la capacité à structurer et à arbitrer des tensions multiples, entre maîtrise, performance et coût.

Les outils proposés (hiérarchisation, curseurs, grille d'arbitrage) permettent de rendre ces arbitrages explicites et comparables. Ils constituent un cadre pour passer d'une lecture des risques à une prise de décision éclairée.

Reste à en éprouver la mise en œuvre concrète. La partie suivante propose d'illustrer ces arbitrages à travers plusieurs cas d'usage, afin de montrer comment ils se traduisent dans des situations opérationnelles.

Arbitrer en pratique :
cas d'usage et configurations

3

1 5 cas d'usages

Les cas d'usage suivants illustrent concrètement la manière dont les arbitrages précédemment décrits se traduisent en configurations de maîtrise. Ils ne constituent pas des modèles à reproduire, mais des exemples de positionnement en fonction d'objectifs et de contraintes spécifiques.

Cas d'usage 1 > Données clients sensibles

Les données clients (personnelles, contractuelles, financières) constituent un actif critique. Leur compromission ou leur indisponibilité expose l'entreprise à des risques juridiques, réputationnels et opérationnels majeurs.

OBJECTIF

Garantir la confidentialité, l'intégrité et la disponibilité des données critiques, en toutes circonstances, y compris en cas de rupture externe.

SOLUTIONS TECHNIQUES :

> Hébergement des données critiques sur des infrastructures dédiées (*on-premises* ou cloud privé)
> Mise en place de chiffrement systématique (au repos et en transit), avec gestion interne des clés
> Architecture segmentée et cloisonnée (réseaux isolés, environnements séparés)
> Déploiement de mécanismes de redondance et de sauvegardes hors ligne (*air gap* partiel)
> Contrôle strict des accès (IAM avancé, journalisation, supervision continue)

ARBITRAGES :

CURSEUR

Exigence de continuité :	Interruption tolérable	Continuité absolue
Souveraineté juridique :	Exposition extraterritoriale	Immunité totale
Internalisation (*Make or Buy*) :	SaaS pur	Internalisation totale
Réversibilité :	*Lock-in*	Portabilité complète
Isolation des environnements :	Mutualisation totale	Isolation complète
Concentration fournisseur :	Mono-fournisseur	Diversification totale
Dépendance à l'innovation externe :	*Best-of-breed*	Autonomie
Maîtrise de l'identité (IAM) :	IAM externalisé	IAM souverain
Profil de risque infrastructure : (cloud vs physique)	Cloud total (risque numérique)	Air-gap (risque physique)

Ce positionnement traduit un arbitrage clairement orienté vers la maîtrise et la continuité, avec une très faible tolérance au risque et une acceptation explicite du surcoût et de la complexité opérationnelle.

CE QUE L'ENTREPRISE PRIVILÉGIE :

> Priorité à la protection, à la maîtrise et à la continuité
> Recours à des environnements isolés, chiffrés et fortement contrôlés
> Acceptation d'un surcoût et d'une complexité accrue
> Faible tolérance au risque : l'interruption ou la fuite ne sont pas acceptables

CONTREPARTIES :

> Coûts élevés (infrastructures redondantes, chiffrement, gouvernance renforcée)
> Complexité opérationnelle accrue (gestion des accès, des environnements, des architectures hybrides)
> Moindre agilité dans le déploiement de nouveaux services
> Difficulté à bénéficier des solutions les plus innovantes ou intégrées

À noter que l'isolation, si elle réduit certaines dépendances logiques, ne protège pas contre des événements physiques affectant les infrastructures.

Cas d'usage 2 > Outils collaboratifs pour les fonctions support

Les outils collaboratifs (messagerie, gestion de projet, visioconférence) soutiennent l'activité quotidienne mais, selon les métiers, ne conditionnent pas directement la continuité de production/d'activité.

OBJECTIF

Maximiser l'efficacité opérationnelle et la fluidité des usages, tout en maintenant un niveau de risque acceptable et maîtrisé.

SOLUTIONS TECHNIQUES :

> Recours à des solutions SaaS mutualisées (messagerie, collaboration, visioconférence)
> Centralisation des usages autour d'une suite intégrée de communication, de collaboration et de gestion documentaire (messagerie, partage de fichiers, visioconférence, outils bureautiques)
> Paramétrage standard de sécurité, complété par des politiques d'accès et d'authentification renforcées
> Sauvegardes externalisées ou outils tiers pour limiter le risque de perte de données
> Mise en place de mesures de réversibilité minimales (export des données, documentation)

ARBITRAGES :

CURSEUR

Exigence de continuité :	Interruption tolérable	Continuité absolue
Souveraineté juridique :	Exposition extraterritoriale	Immunité totale
Internalisation (*Make or Buy*) :	SaaS pur	Internalisation totale
Réversibilité :	*Lock-in*	Portabilité complète
Isolation des environnements :	Isolation complète	Mutualisation totale
Concentration fournisseur :	Mono-fournisseur	Diversification totale
Dépendance à l'innovation externe :	Autonomie totale	*Best-of-breed*
Maîtrise de l'identité (IAM) :	IAM souverain	IAM externalisé

Ce positionnement traduit un arbitrage en faveur de la simplicité, du coût et de la performance, avec une dépendance assumée et une tolérance à un niveau de risque jugé acceptable au regard des impacts limités d'une rupture.

CE QUE L'ENTREPRISE PRIVILÉGIE :

> La priorité à la simplicité d'usage, à la rapidité de déploiement et à l'efficience économique
> Le recours à des solutions mutualisées et standardisées (SaaS)
> La dépendance assumée, car les impacts d'une rupture restent limités et temporaires
> L'acceptation d'un certain niveau de risque en échange de gains opérationnels

CONTREPARTIES :

> Dépendance forte à un fournisseur unique ou dominant
> Maîtrise limitée des données et des flux
> Réversibilité théorique mais difficile à activer en pratique
> Exposition à des ruptures unilatérales (techniques, juridiques, tarifaires)
> Restriction potentielle des usages afin d'éviter l'exposition de données de clients

Cas d'usage 3 > IA intégrée à une fonction métier critique

Un modèle d'IA est utilisé dans un processus central (analyse, production, décision). Il permet des gains significatifs de productivité ou de qualité, mais crée une dépendance à des briques externes (modèles, API, *compute*).

OBJECTIF

Exploiter des capacités d'IA performantes pour rester compétitif, tout en conservant une marge de manœuvre face aux dépendances technologiques.

SOLUTIONS TECHNIQUES :

> Architecture hybride combinant modèles externes et briques internes
> Mise en place de multi-modèles ou multi-fournisseurs pour éviter une dépendance unique)
> Développement de couches d'abstraction (API internes) pour limiter le couplage aux fournisseurs
> Conservation locale ou maîtrisée des données critiques d'entraînement et d'inférence
> Mise en place de mécanismes de secours (solutions dégradées, règles métiers)

ARBITRAGES :

CURSEUR

Exigence de continuité :	Interruption tolérable	Continuité absolue
Souveraineté juridique :	Exposition extraterritoriale	Immunité totale
Internalisation (*Make or Buy*) :	SaaS pur	Internalisation totale
Réversibilité :	*Lock-in*	Portabilité complète
Isolation des environnements :	Isolation complète	Mutualisation totale
Concentration fournisseur :	Mono-fournisseur	Diversification totale
Dépendance à l'innovation externe :	Autonomie totale	*Best-of-breed*
Délégation décisionnelle à l'IA :	Automatisation totale	Contrôle humain

Ce positionnement traduit un arbitrage en faveur de la simplicité, du coût et de la performance, avec une dépendance assumée et une tolérance à un niveau de risque jugé acceptable au regard des impacts limités d'une rupture.

CE QUE L'ENTREPRISE PRIVILÉGIE :

> Une recherche d'équilibre entre performance et maîtrise
> Une dépendance partielle à des solutions externes pour rester compétitif
> Une mise en place de mesures de limitation du risque (multi-modèles, solutions hybrides, capacité de repli)
> Un arbitrage permanent entre rapidité d'innovation et capacité à conserver une autonomie minimale

CONTREPARTIES :

> Compromis sur la performance si diversification ou solutions alternatives
> Coûts supplémentaires liés à la mise en place d'architectures hybrides ou multi-modèles
> Complexité technique accrue (orchestration, supervision, interopérabilité)
> Difficulté à maintenir un équilibre stable entre innovation rapide et maîtrise

Cas d'usage 4 > IA générative pour l'usage quotidien des collaborateurs

Des outils d'IA générative sont déployés à grande échelle auprès des collaborateurs (rédaction, analyse, développement, support).

OBJECTIF

Maximiser les gains de productivité et l'accès aux technologies les plus avancées, en privilégiant des solutions simples, mutualisées et économiquement efficientes.

SOLUTIONS TECHNIQUES :

> Déploiement d'outils d'IA générative via API ou plateformes SaaS mutualisées
> Intégration dans les outils existants (bureautique, code, support)
> Mise en place de politiques d'usage (types de données autorisées, sensibilisation)
> Cloisonnement partiel via comptes entreprise / instances dédiées lorsque possible
> Surveillance des usages (*logs*, audit), sans contrôle exhaustif

Ce positionnement traduit un arbitrage fortement orienté vers la performance et l'innovation, avec une dépendance élevée acceptée en contrepartie de gains immédiats de productivité et de simplicité d'usage.

ARBITRAGES :

CURSEUR

Exigence de continuité :	Interruption tolérable	Continuité absolue
Souveraineté juridique :	Exposition extraterritoriale	Immunité totale
Internalisation (*Make or Buy*) :	SaaS pur	Internalisation totale
Réversibilité :	*Lock-in*	Portabilité complète
Isolation des environnements :	Isolation complète	Mutualisation totale
Concentration fournisseur :	Mono-fournisseur	Diversification totale
Dépendance à l'innovation externe :	Autonomie totale	*Best-of-breed*
Délégation décisionnelle à l'IA :	Automatisation totale	Contrôle humain
Maîtrise de l'identité (IAM) :	IAM souverain	IAM externalisé

CE QUE L'ENTREPRISE PRIVILÉGIE :

> Une priorité assumée au coût, à la simplicité et à la rapidité de déploiement
> Un recours à des solutions mutualisées et standardisées (APIs, SaaS)
> Un accès privilégié aux modèles les plus performants, permettant une innovation continue
> Une dépendance élevée, mais jugée acceptable car : • usage non critique individuellement
• gains immédiats importants

CONTREPARTIES :

> Une faible maîtrise des données partagées avec les outils
> Un risque de fuite ou d'exposition d'informations sensibles
> Une dépendance forte aux APIs et aux modèles externes
> Une difficulté à encadrer des usages diffus et non homogènes dans l'organisation

Cas d'usage 5 > Connectivité critique via satellites

Une entreprise dépend de solutions de connectivité par satellites en orbite basse pour ses opérations (sites isolés, mobilité, continuité réseau, logistique, énergie, défense, etc.). Ces solutions offrent une couverture et une performance difficiles à substituer.

OBJECTIF

Assurer la continuité des communications critiques, tout en limitant l'exposition à une dépendance unique en matière de connectivité.

SOLUTIONS TECHNIQUES :

> Recours à un opérateur principal de connectivité satellite (LEO) pour assurer la couverture
> Mise en place d'une architecture hybride combinant satellite et réseaux terrestres (4G/5G, fibre)
> Déploiement de solutions de bascule automatique (*failover*) entre réseaux
> Redondance partielle via plusieurs terminaux ou opérateurs lorsque possible
> Priorisation des flux critiques (QoS, segmentation des usages)

ARBITRAGES :

CURSEUR

Exigence de continuité :	Interruption tolérable	Continuité absolue
Souveraineté juridique :	Exposition extraterritoriale	Immunité totale
Internalisation (*Make or Buy*) :	SaaS pur	Internalisation totale
Réversibilité :	*Lock-in*	Portabilité complète
Isolation des environnements :	Isolation complète	Mutualisation totale
Concentration fournisseur :	Mono-fournisseur	Diversification totale
Résilience de la connectivité :	Voie unique	Connectivité totalement diversifiée
Profil de risque infrastructure :	Cloud total (risque numérique)	Air-gap (risque physique)

Ce positionnement traduit un arbitrage sous contraintes dans lequel la continuité prime, mais où les marges de manœuvre restent limitées en raison d'une dépendance structurelle à une infrastructure critique et à un marché concentré.

Cette configuration s'inscrit dans un contexte fortement contraint, où la dépendance ne résulte pas uniquement de choix techniques, mais des caractéristiques mêmes du marché et des infrastructures :

> Une dépendance à une infrastructure critique difficilement substituable, avec des coûts très élevés de duplication
> Un marché souvent très concentré (donc faibles marges de manoeuvre)
> Un arbitrage entre : • performance et couverture immédiate
• diversification ou solutions hybrides (terrestre + satellite)

CONTREPARTIES :

Cette configuration expose l'entreprise à des risques spécifiques, moins liés à ses choix internes qu'à son environnement :

> Dépendance structurelle à un nombre limité d'acteurs
> Faible capacité de substitution à court terme
> Exposition à des évolutions tarifaires ou stratégiques unilatérales
> Risque géopolitique et opérationnel (accès, couverture, priorisation des usages)

Dans ce cas, la dépendance n'est pas seulement technologique mais structurelle : elle résulte d'un écosystème concentré et de barrières à l'entrée élevées, ce qui limite fortement la capacité d'arbitrage de l'entreprise.

—

Ces cas d'usage montrent que les arbitrages ne peuvent être ni standardisés ni implicites. Ils doivent être construits, comparés et pilotés dans le temps.

2 Méthode d'arbitrage

1 Partir d'un cas d'usage critique

L'analyse doit être ancrée dans une réalité opérationnelle. Il s'agit d'identifier une fonction, un processus ou un actif dont la continuité conditionne directement l'activité (données clients, outil métier, IA, connectivité, etc.).
Ce point de départ est essentiel : une même technologie peut relever d'arbitrages très différents selon l'usage qui en est fait.

2 Qualifier la dépendance

La dépendance doit être objectivée à partir de critères concrets. À ce titre, des outils existants comme l'Indice de Résilience Numérique (IRN) constituent un point d'entrée utile pour identifier et cartographier les dépendances d'une organisation, et amorcer un premier niveau de diagnostic.

La grille d'arbitrage proposée ici s'inscrit dans cette continuité, en permettant d'approfondir cette analyse autour de trois dimensions complémentaires :

> la nature de l'exposition (impact en cas de rupture, perte d'accès, capacité d'alternative)
> la réalité des garanties (contractuelles, techniques, organisationnelles)
> les contraintes de sortie et de réversibilité (coût, délai, faisabilité)
> L'enjeu est de dépasser une lecture théorique de la dépendance pour en apprécier les implications réelles en situation de rupture, et ainsi éclairer des arbitrages opérationnels.

3 Positionner les curseurs

Les curseurs permettent de rendre visibles les arbitrages implicites de l'organisation. Ils traduisent un positionnement sur plusieurs tensions structurantes (voir partie II et cas d'usage) :

N° 01 — Exigence de continuité (Interruption tolérable / Continuité absolue)
N° 02 — Souveraineté juridique et exposition extraterritoriale (Exposition extraterritoriale / Immunité totale)
N° 03 — Profondeur d'internalisation (*Make or Buy*) (SaaS pur / Internalisation totale)
N° 04 — Portabilité et réversibilité (*Lock-in* / Portabilité complète)
N° 05 — Niveau d'isolement des environnements (Mutualisation totale / Isolation complète)
N° 06 — Concentration fournisseur (Mono-fournisseur / Diversification totale)
N° 07 — Dépendance à l'innovation externe (Autonomie totale / *Best-of-breed*)

À ces curseurs s'ajoutent des tensions spécifiques, propres à certaines briques technologiques, comme par exemple :

N° 08 — Profil de risque infrastructure (numérique *vs* physique) Cloud total (risque numérique) / *Air-gap* (risque physique)
N° 09 — Délégation décisionnelle à l'IA (Automatisation totale / Contrôle humain)
N° 10 — Résilience de la connectivité (Voie unique / Connectivité totalement diversifiée)
N° 11 — Maîtrise de l'identité et des accès (IAM) (IAM externalisé / IAM souverain)
N° 12 — Horizon de protection cryptographique (Protection standard / Protection post-quantique souveraine)

Ce positionnement ne décrit pas seulement une situation technique : il reflète des choix stratégiques, souvent non formalisés.

4 Comparer les configurations de maîtrise

À partir de ce positionnement, différentes configurations peuvent être envisagées. Leur analyse consiste à expliciter les compromis qu'elles impliquent :

> ce que la configuration protège (performance, continuité, maîtrise, simplicité)
> ce qu'elle expose (risques juridiques, techniques, opérationnels)
> son coût réel, y compris dans la durée
> son niveau de dépendance et sa capacité de sortie effective

Cette étape permet de comparer des options qui, en apparence, répondent au même besoin, mais n'engagent pas les mêmes risques.

5 Mettre en évidence les écarts critiques

L'analyse met souvent en évidence des désalignements entre :

> le niveau de risque réellement porté
> et le niveau de maîtrise supposé

Par exemple :

> une dépendance critique non explicitement assumée
> une réversibilité prévue en théorie mais inopérante en pratique
> une performance optimisée au prix d'une exposition mal maîtrisée

Ces écarts ne sont pas nécessairement visibles sans un travail préalable de qualification. Ils constituent les principaux points d'attention pour la décision.

6 Arbitrer et définir une trajectoire

La décision ne consiste pas à éliminer la dépendance, mais à choisir la forme de dépendance la plus compatible avec les contraintes de l'organisation.

Elle repose sur un arbitrage entre :

> le niveau de risque acceptable
> les coûts soutenables
> les exigences de performance et de compétitivité

Ces arbitrages ne sont pas figés. Ils s'inscrivent dans une trajectoire, qui doit être réévaluée à mesure que les usages évoluent et que les dépendances se renforcent.

Ainsi, ces choix ne relèvent pas uniquement de décisions techniques. Ils engagent la stratégie de l'entreprise, son organisation et son modèle économique. À ce titre, ils doivent être portés au niveau de la direction générale.

Arbitrer, c'est donc accepter que toute solution déplace le risque, qui peut être celui d'une dépendance, mais aussi d'un manque de performance, et choisir en connaissance de cause où celui-ci doit se situer.

CONCLUSION

Ces cas d'usage montrent que la question n'est pas d'échapper aux dépendances, mais de les minimiser et de les arbitrer. Ils illustrent la diversité des configurations possibles, ainsi que les compromis qu'elles impliquent.

Sans cadre structuré, ces arbitrages restent implicites et se construisent au fil des contraintes. Les rendre explicites et pilotables constitue la condition d'une maîtrise réelle des dépendances numériques.

Conclusion

Les travaux présentés dans ce rapport reposent sur une conviction simple : la souveraineté numérique ne se définit ni par l'indépendance, ni par l'absence de dépendance. Elle se définit par la capacité à les comprendre, à les arbitrer et à en maîtriser les effets.

Dans un environnement technologique marqué par l'interdépendance, la complexité et la concentration des acteurs, toute organisation est nécessairement dépendante. La question n'est donc pas de savoir comment supprimer ces dépendances, mais comment éviter qu'elles ne deviennent subies, invisibles ou incontrôlables.

La souveraineté numérique doit ainsi être entendue comme une capacité opérationnelle : celle de qualifier ses dépendances, d'en mesurer les implications réelles, et d'arbitrer entre différentes configurations en connaissance de cause, au regard de ses priorités, de ses contraintes et de son exposition aux risques.

Cette capacité repose sur trois conditions : rendre les dépendances visibles, expliciter les arbitrages qu'elles impliquent, et se doter des moyens de les piloter dans le temps. Elle ne relève pas uniquement de choix techniques, mais engage la stratégie, l'organisation et le modèle économique des acteurs.

En ce sens, la souveraineté numérique n'est pas un état à atteindre, mais une dynamique à construire. Elle ne se décrète pas : elle se pratique par des arbitrages continus entre maîtrise, performance et coût.

Ainsi, la souveraineté commence là où la dépendance cesse d'être subie. Rendre visibles, arbitrer, piloter : telle est la condition d'une souveraineté numérique effective.

Photo LDD *magnific.com*

Glossaire

Photo LDD *magnific.com*

Air gap

Architecture ou système totalement isolé d'un réseau externe (notamment d'Internet). L'objectif est de réduire le plus possible les risques d'intrusion ou d'exfiltration de données. Utilisé pour les environnements les plus sensibles (défense, infrastructures critiques, données stratégiques).

API (*Application Programming Interface*)

Interface de programmation d'application permettant à différents logiciels ou services de communiquer entre eux automatiquement. Les API sont largement utilisées pour connecter des applications à des services cloud ou à des modèles d'IA.

Best-of-breed

Approche consistant à choisir les solutions considérées comme les plus performantes dans chaque domaine, même si elles proviennent de fournisseurs différents. Cette stratégie maximise souvent la performance mais peut accroître la complexité et les dépendances.

Cloud

Ensemble de services informatiques accessibles à distance via internet : stockage de données, puissance de calcul, hébergement d'applications ou logiciels. Le cloud permet de mutualiser les infrastructures plutôt que de les héberger localement.

Compute

Capacité de calcul informatique mobilisée pour exécuter des traitements numériques, notamment l'entraînement ou l'utilisation de modèles d'intelligence artificielle.

Conteneurisation

Méthode permettant d'exécuter des applications dans des environnements isolés et standardisés appelés conteneurs (ex. Docker). Elle facilite la portabilité et la réversibilité des systèmes.

Docker et Kubernetes

Docker est une technologie de conteneurisation permettant d'isoler des applications. Kubernetes est un outil d'orchestration qui permet de gérer automatiquement plusieurs conteneurs à grande échelle.

Hardware* et *Software

Le *hardware* désigne les composants matériels d'un système informatique (serveurs, processeurs, disques, équipements réseau).

Le *software* désigne les composants logiciels (systèmes d'exploitation, applications, programmes).

Hyperscaler

Très grand fournisseur mondial de services cloud disposant d'infrastructures massivement distribuées et mutualisées. Les principaux *hyperscalers* sont par exemple Amazon Web Services, Microsoft Azure et Google Cloud.

IAM (*Identity and Access Management*)

Ensemble des outils et règles permettant de gérer les identités numériques et les droits d'accès aux systèmes d'information. L'IAM détermine qui peut accéder à quelles ressources et dans quelles conditions.

***Lock-in* (verrouillage technologique)**

Situation dans laquelle une organisation devient fortement dépendante d'un fournisseur ou d'une technologie, rendant un changement de solution difficile, coûteux ou risqué.

Middleware

Couche logicielle intermédiaire reliant différentes applications ou systèmes entre eux. Le *middleware* facilite les échanges de données et le fonctionnement coordonné des services.

Multi-cloud

Stratégie consistant à utiliser plusieurs fournisseurs cloud simultanément afin de limiter la dépendance à un acteur unique et d'améliorer la résilience.

On-premises

Infrastructure informatique hébergée directement dans les locaux de l'organisation ou dans un environnement qu'elle contrôle physiquement, par opposition au cloud public.

Open source

Logiciel dont le code source est accessible, modifiable et réutilisable librement. Les solutions *open source* favorisent généralement l'interopérabilité et la réversibilité.

PCA et PRA

PCA (Plan de continuité d'activité) : ensemble des mesures permettant de maintenir les activités essentielles en cas d'incident majeur.

PRA (Plan de reprise d'activité) : procédures permettant de restaurer les systèmes et les opérations après une interruption.

Red team

Méthode consistant à charger une équipe de simuler des scénarios de crise, d'attaque ou de rupture afin de tester la robustesse d'une organisation, de ses systèmes ou de ses décisions.

RPO (*Recovery Point Objective*)

Volume maximal de données qu'une organisation accepte de perdre après un incident. Il correspond au point de restauration visé.

RTO (*Recovery Time Objective*)

Durée maximale d'interruption acceptable d'un service ou d'un système après un incident.

SaaS (*Software as a Service*)

Modèle dans lequel un logiciel est accessible directement via internet, sans installation locale. Le fournisseur gère l'infrastructure, la maintenance et les mises à jour.

SecNumCloud

Qualification délivrée pour la France par l'Agence nationale de la sécurité des systèmes d'information (Anssi) aux fournisseurs cloud respectant un haut niveau d'exigence en matière de cybersécurité et de protection contre certaines formes d'extraterritorialité.

Shadow AI

Usage non encadré d'outils d'intelligence artificielle par des collaborateurs en dehors des règles ou des outils validés par l'organisation.

SPOF (*Single Point of Failure*)

Point de défaillance unique dont l'indisponibilité peut entraîner l'arrêt d'un système ou d'une activité entière.

Workflow

Enchaînement structuré d'étapes ou de tâches permettant d'automatiser ou d'organiser un processus métier ou technique.

Principaux contributeurs

Paul Barbaste
Senior AI Applied Engineer
Wavestone / Inclusive Brains

Emmanuelle Charghinoff
Chargée de mission études
Human Technology Foundation

Paul-Henri Charrier
Director of Public Affairs
Upsun

Benjamin Ducos
Responsable Groupe de la Gestion des risques de l'information / Head of Group Information Risk Management
GIE AXA

Jean-Baptiste Fourmont
Head of Solution Architecture
Scaleway

Frederic Geraud de Lescazes
Government Affairs & Public Policy
Google Cloud

Joshua Henry
Analyst
Accuracy

Arnaud Merveille
Directeur des Relations Institutionnelles
ME Group

Cédric Mora
Policy Manager (France) – Public Policy Cyber/AI/Health
AWS

Eric Salobir
Président
Human Technology Foundation

Christoph Siegelin
Vice-President
Thales Digital Factory

Joséphine Staron
Directrice de la présente étude
Human Technology Foundation

Robert Wrigley
Co-fondateur
Kwantai

Maquette & Graphisme
Anne Vanden-Borre - *Comtactic*

Relecture
Odile Landreau-Jacquemin

Photo LDD midjourney.com

HUMAN TECHNOLOGY
FOUNDATION