Amorcer sa sortie de la dépendance numérique : de l'audit à l'infrastructure

Amorcer sa sortie de la dépendance numérique : de l'audit à l'infrastructure

 Bernard Sfez - 2026-03-15 20:19

De quoi dépendez-vous vraiment ? Quels équipements, quels serveurs, quels services cloud échappent à votre contrôle, et sous quelle juridiction opèrent-ils ? Savez-vous ce que vos collaborateurs utilisent en dehors des outils officiels ? Ce troisième volet de notre série sur la souveraineté numérique vous donne une méthode concrète pour auditer vos dépendances, évaluer votre exposition et identifier les premières briques à reprendre en main.

Car les alternatives souveraines existent, elles sont matures et les premières étapes sont accessibles sans tout bouleverser. Du matériel réseau au serveur, de l'hébergement à la cybersécurité, nous détaillons comment poser un socle d'infrastructure solide, étape par étape, sans paralyser votre activité. Après la prise de la Bastille, il faut bâtir les fondations de votre citadelle.

Dans un premier article, nous avons cartographié l'étendue de la dépendance numérique aux technologies américaines : du matériel aux applications, en passant par le cloud et l'intelligence artificielle, nous avons montré où se cache, ou s'affiche sans complexe, la suprématie technologique américaine. Dans un deuxième article, nous avons examiné les stratégies en place, les avancées concrètes et les contradictions qui freinent encore la reconquête de notre souveraineté numérique.

Ce troisième volet change de perspective. Nous parlons de ce que vous pouvez faire, dès maintenant. Si vous êtes dirigeant ou responsable informatique, vous devez agir. Si vous êtes utilisateur, vous devez comprendre, alerter et faciliter la transition. Quelle que soit la taille de votre organisation, cet article vous donne de nombreuses clés pour auditer votre situation, identifier vos marges de manœuvre et engager une migration progressive, en douceur et en évitant les heurts.

Car le constat est clair : chacun est concerné. Et c'est à chacun d'opérer sa transition, de la soutenir, voire de l'exiger avant de confier des informations sensibles à un prestataire. Les bonnes pratiques sont connues. Les outils, les méthodes et les compétences existent et ils sont matures.

Et cette démarche n'est pas uniquement défensive. Pouvoir démontrer à vos partenaires et clients que vous maîtrisez vos données, que votre hébergement est souverain et que vos

pratiques sont auditables n'est pas un investissement à perte. C'est une carte à jouer pour remporter un contrat, rassurer un donneur d'ordres ou satisfaire une exigence de conformité. La souveraineté numérique devient un avantage concurrentiel.

Étape 1 : Savoir d'où l'on part : l'audit de dépendance

Avant de migrer quoi que ce soit, il faut comprendre précisément où vous en êtes. Pas besoin d'un audit à cinq ou six chiffres pour cela, mais il faut de la méthode.

Prenez une feuille, un tableur (mais pas sur le cloud) ou créez un diagramme directement dans Tiki Wiki qui intègre nativement draw.io (open source, allemand), sans rien installer ni envoyer de données à l'extérieur et listez méthodiquement chaque couche de votre infrastructure. Pour les structures de moins de vingt postes, c'est un exercice d'une journée et si vous n'avez jamais fait, faites pièce par pièce, étage par étage. Pour les plus grandes, votre responsable informatique a probablement déjà une partie de cet inventaire : l'enjeu est de le compléter avec les questions qu'on ne pose jamais.

Le matériel : serveurs, postes de travail, routeurs, switchs, pare-feu, bornes Wi-Fi. L'objectif n'est pas de dresser un inventaire de numéros de série mais de répondre à une question simple, "qui fabrique ces équipements, et sous quelle juridiction opèrent-ils ?" Comme nous l'avons détaillé dans notre précédent article, la nouvelle définition du RISAA américain étend potentiellement l'obligation de communication des données à tout fournisseur ayant accès à un équipement transmettant ou stockant des communications électroniques. Cela inclut désormais les équipementiers réseau, les fournisseurs de services managés, et même dans certains cas les prestataires de maintenance ayant un accès physique ou logique à vos machines.

Les systèmes d'exploitation : Windows, macOS, Linux ? Sur les postes, sur les serveurs ? Quelles versions, quelles licences, quelles échéances de renouvellement ? C'est généralement la couche la mieux documentée dans les organisations qui ont un minimum de gestion IT. Profitez-en pour noter précisément les numéros de version : une version obsolète ou non maintenue est une porte ouverte aux vulnérabilités connues et activement exploitées.

Les applications : Bureautique, messagerie, visioconférence, stockage de fichiers, CRM, comptabilité, gestion de projet... Pour chaque outil, les questions à poser sont précises. Qui est l'éditeur ? S'agit-il d'une utilisation locale ou en ligne, et où sont hébergées les données ? Sous quelle juridiction l'entreprise opère-t-elle ? Dans quel format pouvez-vous exporter vos données ? Vos utilisateurs ont-ils la possibilité d'installer ou d'utiliser ce qu'ils veulent ? Et surtout : que disent les contrats ? Existe-t-il une clause de réversibilité ? Quelles sont les conditions de résiliation ? Ce volet contractuel est souvent négligé alors qu'il recèle les verrous les plus tenaces. Nous y revenons en détail plus loin.

Les services cloud : Hébergement web, sauvegardes, bases de données, analytics, etc. Même grille de lecture : qui opère, où, sous quel droit ? Mais aussi, concrètement : où sont stockées vos données et celles de vos clients à cet instant précis ? Lorsque vous faites une sauvegarde, est-elle sur un stockage local ou distant ? Pouvez-vous répondre à cette question pour chaque service ?

Le shadow IT C'est le point aveugle de la plupart des organisations et souvent le plus dangereux. Vos collaborateurs utilisent-ils WhatsApp pour échanger des documents internes ? Google Drive à

titre personnel pour stocker des fichiers professionnels ? ChatGPT pour rédiger des propositions commerciales contenant des données clients ? WeTransfer pour envoyer des fichiers volumineux ? Un portable personnel avec des copies de vos fichiers ? Un gestionnaire de mots de passe en ligne dont personne ne connaît les conditions d'hébergement ?

Ces usages « officieux » représentent souvent les fuites de données les plus critiques et les plus ignorées. Et la collecte ne se limite pas aux outils professionnels. L'affaire Pokémon Go, révélée en mars 2026, en est l'illustration la plus spectaculaire : 30 milliards d'images géolocalisées collectées via les smartphones des joueurs, sans que la plupart en aient conscience, pour construire une carte du monde d'une précision centimétrique. Le jeu a depuis été revendu à un fonds d'investissement saoudien, données incluses. Si un jeu mobile gratuit peut cartographier la planète à l'insu de ses utilisateurs, imaginez ce que collectent les applications professionnelles que vos collaborateurs installent sans validation.

Le shadow IT ne concerne pas que les applications : il concerne tout ce que vos équipes utilisent en pensant que « ça ne compte pas ». Y compris les conversations tenues à portée de Siri ou d'Alexa, dont l'écoute passive commence à se banaliser.

Ce que révèle l'audit : le même schéma partout

Le secteur d'activité et la taille varient. Le constat, rarement. Voici ce que révèle la plupart des audits, que l'on parle d'une PME, d'une collectivité, d'une association ou d'un établissement scolaire :
Les documents se rédigent dans Word ou Google Docs. Les tableurs passent par Excel ou Google Sheets. Les fichiers sont stockés sur OneDrive, SharePoint ou Google Drive. Les emails transitent par Outlook ou Gmail. Les réunions se font sur Teams ou Zoom. Le site web utilise un CDN, des vidéos hébergées sur YouTube et Google Analytics pour mesurer le trafic. La comptabilité tourne sur un logiciel en ligne dont l'hébergeur final est rarement connu du client. Et en coulisses, plusieurs collaborateurs utilisent ChatGPT pour tout et n'importe quoi, avec des données professionnelles en pâture.

La question n'est pas de savoir si ces outils sont bons. Ils le sont, c'est d'ailleurs pour ça qu'ils dominent. La question est de savoir à quelle juridiction ils vous exposent, et si vous en êtes conscient. Sur une quinzaine de briques technologiques du quotidien, la majorité dépend d'entreprises soumises au Cloud Act. Vos données clients, vos propositions commerciales, votre comptabilité, vos communications internes : tout est potentiellement accessible à une juridiction étrangère. Que vous le sachiez ou non.

L'audit contractuel : le verrou invisible

L'audit technique ne suffit pas. Le verrouillage le plus pernicieux est souvent contractuel.

Vérifiez systématiquement, pour chaque prestataire :

La clause de réversibilité. Avez-vous le droit d'exporter toutes vos données dans un format standard et exploitable ? Sous quel délai ? À quel coût ? Beaucoup de contrats cloud prévoient un export... en format propriétaire, rendant la migration techniquement possible mais pratiquement inutilisable sans outils de conversion coûteux.

La propriété des données. Le contrat stipule-t-il explicitement que vos données vous appartiennent ? Que le prestataire n'a aucun droit d'usage, d'analyse ou de revente ? Attention

aux clauses d'« amélioration du service » qui permettent de facto l'exploitation de vos données à des fins de machine learning.

La juridiction applicable. Quel tribunal est compétent en cas de litige ? Si la réponse est « l'État de Californie » ou « l'État de Washington », vous avez un problème. Et si votre prestataire est une filiale européenne d'un groupe américain, le Cloud Act s'applique quand même à la maison mère.

Les conditions de résiliation. Quel est le préavis ? Y a-t-il des pénalités ? Le service continue-t-il de fonctionner pendant la période de transition ? Certains contrats prévoient la suppression automatique des données 30 jours après résiliation — sans possibilité de récupération.

La conformité RGPD réelle. "Nous sommes conformes au RGPD" est devenu un mantra marketing. Exigez le détail : où sont les données ? Qui y a accès ? Le sous-traitant a-t-il des sous-traitants (et où sont-ils) ? Le DPA (Data Processing Agreement) mentionne-t-il les transferts hors UE ? Rappelez-vous : comme l'a reconnu le directeur technique de Microsoft France devant le Sénat en juin 2025, même un hébergement en France ne garantit pas l'immunité face aux injonctions américaines.

Ce travail est fastidieux mais indispensable. Il constitue la base de toute stratégie de sortie crédible. Et il révèle souvent des surprises désagréables que les directions générales préfèrent ignorer — jusqu'au jour où elles ne peuvent plus.

Étape 2 : La matrice de remplacement — quoi migrer, vers quoi

Une fois l'audit réalisé, la question devient concrète : par quoi remplacer chaque brique ? Voici les alternatives souveraines éprouvées en 2026, couche par couche, avec un avis honnête sur leurs forces et leurs limites. D'autres solutions émergeront, le paysage évolue vite, mais celles-ci ont déjà fait leurs preuves en production.

Le matériel réseau et les objets connectés : segmenter et isoler

C'est la couche où il faut être le plus pragmatique. Remplacer l'intégralité de vos équipements réseau par des alternatives européennes n'est pas toujours possible ni même nécessaire. Côté pare-feu, Stormshield (filiale d'Airbus CyberSecurity, R&D intégralement en France) reste à ce jour le seul qualifié au niveau Standard par l'ANSSI. Le choix est donc encore limité sur le haut du spectre, mais l'entrée en vigueur de la directive NIS2 et la prise de conscience croissante des enjeux de souveraineté devraient accélérer l'arrivée de nouvelles offres européennes. Pour les routeurs, MikroTik (letton) propose des équipements professionnels à des tarifs accessibles, et des firmwares Open Source comme OPNsense ou pfSense permettent de transformer du matériel standard en pare-feu performant et auditable.

Pour le reste, imprimantes, caméras, téléviseurs en salle de réunion, bornes Wi-Fi, objets connectés divers, le remplacement n'est pas toujours l'enjeu. L'enjeu, c'est l'isolation. Un téléviseur connecté dans une salle de réunion n'a pas besoin d'être sur le même réseau que vos fichiers clients. Une caméra de surveillance IP n'a pas à communiquer avec Internet sans contrôle. La segmentation réseau, c'est-à-dire la séparation de vos équipements en sous-réseaux étanches selon leur niveau de sensibilité, est une mesure simple, peu coûteuse et redoutablement efficace. Elle limite la propagation en cas de compromission et réduit la surface d'attaque sans rien changer aux usages quotidiens.

L'hébergement et l'infrastructure : la fondation

Si vos serveurs sont chez AWS, Azure ou Google Cloud, rien de ce que vous construisez dessus n'est souverain — quels que soient les logiciels utilisés.

De plus, chez ces hyperscalers, la facture est un assemblage de bande passante sortante au gigaoctet, de requêtes API à l'unité, de coûts de transfert entre services et de paliers de stockage dont la logique échappe à la plupart des directions financières. Ainsi, beaucoup d'organisations découvrent le vrai coût de leur cloud après quelques mois d'utilisation réelle. Mais le piège ne s'arrête pas là : Cette incertitude tarifaire se poursuit mois après mois, et les factures arrivent toujours avec juste le retard qu'il faut pour qu'il soit devenu trop coûteux de partir. Réinvestir le temps, les ressources et l'argent pour déménager ailleurs ? C'est précisément ce sur quoi ces fournisseurs comptent pour vous retenir.

Les alternatives existent. OVHcloud et Scaleway en France, Hetzner en Allemagne, Infomaniak en Suisse proposent des infrastructures performantes. Leur avantage le plus concret n'est d'ailleurs pas forcément le prix au centime : c'est la lisibilité tarifaire. Un serveur dédié chez un hébergeur européen, c'est généralement un tarif mensuel fixe. Pour les données sensibles, une dizaine de prestataires sont déjà qualifiés SecNumCloud par l'ANSSI, garantissant l'immunité aux lois extraterritoriales.

Mais il y a une option que beaucoup d'organisations négligent : le serveur local. Les niveaux de qualité et les débits réseau disponibles aujourd'hui pour les entreprises, y compris en fibre professionnelle, permettent parfaitement d'héberger en interne un serveur dont le coût sera vite amorti face à des abonnements cloud mensuels qui ne cessent d'augmenter. Vous êtes propriétaire du matériel, les données ne quittent jamais vos locaux, et vous éliminez d'un coup la question de la juridiction. Pour les structures qui n'ont pas de salle serveur, un simple serveur dédié chez un hébergeur européen offre le même bénéfice.

La gestion de ces serveurs repose sur des outils Open Source matures comme Virtualmin et

Webmin permettent d'administrer depuis une interface unifiée l'hébergement web, les comptes email, les bases de données, les certificats SSL et les sauvegardes, le tout en Open Source, sans licence et sans dépendance à un éditeur. Et les coûts matériels ont considérablement baissé. Un serveur silencieux, performant et adapté à une PME se monte aujourd'hui pour moins de 1 500 euros. Amorti en quelques mois face à un abonnement cloud, il vous appartient ensuite pour des années. La souveraineté, en ce domaine, n'est plus une question de budget, c'est une question de volonté.

Reste la question que tout le monde pose. Qui s'en occupe ? Deux options selon vos ressources. Si vous avez un profil technique en interne, ces outils permettent de prendre en main la gestion courante comme créer un compte email, ajouter un site ou vérifier l'état des sauvegardes. Mais ne nous voilons pas la face. La sécurité, la maintenance système, la gestion des mises à jour critiques et la supervision restent des compétences qui s'acquièrent sur la durée. Ce peut être l'amorce d'un poste à part entière dans votre organisation, accompagné dans sa montée en compétence par un prestataire expérimenté. Si vous n'avez pas cette ressource, ou si vous préférez concentrer vos équipes sur votre cœur de métier, la gestion peut être entièrement externalisée. C'est une part importante de notre activité. Nous déployons, maintenons et supervisons des serveurs pour des organisations qui veulent la souveraineté sans recruter un administrateur système à temps plein.

Cybersécurité et supervision : protéger ce qu'on a repris

C'est le sujet le plus sous-estimé, et de loin. La plupart des petites et moyennes organisations raisonnent ainsi : « Nous n'avons rien d'intéressant, qui voudrait nous attaquer ? » Les chiffres disent le contraire. Selon l'ANSSI, les TPE, PME et ETI concentrent 34 % des cyberattaques en France, et les collectivités locales 24 %. Le baromètre 2025 de Cybermalveillance.gouv.fr confirme que 16 % des TPE-PME ont subi au moins un incident dans l'année, et que 80 % reconnaissent ne pas être préparées. Plus brutal encore : 60 % des PME victimes d'une cyberattaque ferment dans les 18 mois.

Vous n'avez peut-être pas de secrets industriels. Mais vous avez des noms, des adresses, des emails, des historiques de facturation, des coordonnées bancaires de fournisseurs, des échanges contractuels. Tout cela a une valeur marchande. Sur les marchés noirs du web, un fichier clients qualifié se vend, une base d'emails vérifiés se vend, des données de facturation permettent des fraudes au virement et de l'usurpation d'identité. Pour donner un ordre de grandeur : chaque donnée personnelle compromise coûte en moyenne 150 à 200 € à l'organisation responsable en France, en cumulant les frais de notification, de remédiation, les conséquences juridiques et les sanctions. Une base de 1 000 clients qui fuite, c'est potentiellement 150 000 à 200 000 euros de préjudice.

Et les attaquants ne passent plus des heures ni des jours à préparer une attaque ciblée ou à chercher des failles manuellement. Désormais, des fermes de bots dopés à l'intelligence artificielle scannent, testent et exploitent les vulnérabilités en continu, sans coût marginal et sans consommation de temps ni de ressources humaines. Ils ratissent large, automatiquement, et ce sont les organisations les moins protégées qui tombent en premier. Un ransomware ne vérifie pas votre chiffre d'affaires avant de chiffrer vos fichiers.

Les conséquences dépassent votre propre périmètre. L'accès à vos données peut provoquer un effet cascade : c'est un de vos clients ou partenaires qui se retrouve exposé. Des messages confidentiels contenant des accès, des rendez-vous ou des informations stratégiques se

retrouvent dans la nature. Au mieux, votre réputation est dégradée : 47 % des entreprises déclarent perdre des prospects et 43 % des clients après un incident. Au pire, les assurances chercheront à déterminer qui est responsable du préjudice, sachant que seules 3 % des PME sont aujourd'hui assurées contre le risque cyber. Et le RGPD prévoit des sanctions pouvant atteindre 4 % du chiffre d'affaires annuel.

Reprendre le contrôle de son infrastructure sans la protéger, c'est déménager dans une maison neuve en laissant la porte ouverte. La souveraineté exige de la rigueur.

La supervision en temps réel est la première ligne de défense. Zabbix permet de surveiller en continu l'état de vos serveurs, services et équipements réseau : charge processeur, espace disque, disponibilité des services, tentatives de connexion suspectes. Vous êtes alerté avant que le problème ne devienne visible pour vos utilisateurs, et surtout avant qu'un incident ne devienne une crise.

Le filtrage géographique des accès est une couche de protection souvent ignorée et pourtant redoutablement efficace. Notre suite GeoIP de cybersécurité, développée en interne, permet de restreindre l'accès à vos serveurs en fonction de la provenance géographique des connexions. Si votre activité est en France et en Europe, pourquoi accepter des connexions entrantes depuis des plages IP situées à l'autre bout du monde ? Les tentatives d'intrusion automatisées, les scans de ports, les attaques par force brute proviennent massivement de certaines régions. Les bloquer en amont, c'est éliminer le bruit avant même qu'il n'atteigne vos défenses.

Les sauvegardes offsite sont le filet de sécurité ultime. Sans sauvegarde externe, un ransomware, un incendie ou une simple erreur humaine peut signifier une perte définitive. La règle de base est le 3-2-1 : trois copies de vos données, sur deux supports différents, dont une hors site sur une infrastructure souveraine. Et surtout, une sauvegarde qui n'a jamais été testée en restauration n'est pas une sauvegarde, c'est un espoir. Notre service de sauvegarde offsite repose sur une infrastructure privée en France, avec transferts chiffrés, zéro accès tiers et des tests de restauration documentés.

Supervision, filtrage et alertes forment un ensemble cohérent : vous savez en permanence ce qui se passe sur votre infrastructure, qui tente d'y accéder, et vous êtes en mesure de réagir immédiatement.

Votre socle est posé : un réseau segmenté, un serveur que vous maîtrisez, une infrastructure supervisée et protégée. Reste à voir ce qu'on fait tourner dessus. Dans notre prochain article, nous aborderons les briques applicatives : emails, bureautique, collaboration, gestion, et le sujet qui fâche, le poste de travail. C'est là que la souveraineté cesse d'être un sujet technique pour devenir un sujet humain.