



L'infrastructure en détail

Document technique

DOCUMENT TECHNIQUE · PROPOSITION

VERSION 0.3 · 2026-07-23

DOCUMENT III

Sommaire

Les entrées et les numéros de page sont cliquables.

Le principe d'ensemble	2
Le modèle de menace, en clair	2
Le site	2
Les noms de domaine	3
Le DNS	4
La recherche	4
La chaîne éditoriale	5
La transcription	6
Les comptes, abonnements et paiements	6
Le podcast	7
La vidéo	7
La newsletter	8
La garde des clés	8
La supervision et les sauvegardes	9

Version 0.3 — 2026-07-23. Troisième étage du dispositif : après l'histoire (le plan de l'hacienda) et le résumé pratique (l'infrastructure en clair), voici le détail technique — les outils nommés, et pourquoi eux. Tout terme technique est expliqué au premier passage. Les outils et les politiques des prestataires évoluent : ce document porte une version et une date, et se relit périodiquement.

Statut des choix. Pour distinguer la vision du réel : **Déployé** — installé et utilisé dans la maison témoin · **Validé** — testé techniquement, pas encore en production · **Retenu** — choix arrêté, mise en œuvre à venir · **Candidat** — pressenti, à démontrer avant engagement · **Option ultérieure** — prévu dans l'architecture, sans engagement de calendrier. Sauf mention contraire, tout outil cité ici est au statut **Retenu** ; les autres statuts sont indiqués entre parenthèses. Les statuts **Déployé** et **Validé** seront attribués au fur et à mesure de la construction de la maison témoin.

SECTION 01

Le principe d'ensemble

L'architecture suit une règle simple : static-first. Un site « statique » est un site dont les pages sont fabriquées à l'avance, à chaque publication, puis servies telles quelles — par opposition à un site « dynamique » qui recalcule chaque page à chaque visite. Concrètement : tout ce qui est public (catalogue, pages d'épisodes, transcriptions publiques) est un jeu de fichiers pré-construits, donc très rapide, très difficile à faire tomber, et hébergeable n'importe où. Seul un petit noyau reste dynamique : les comptes, les droits des abonnés et le contenu premium. Ce noyau est volontairement minuscule — moins il y a de pièces en mouvement, moins il y a de pannes possibles.

Deuxième règle : le contenu premium n'entre jamais dans la partie publique. Ce n'est pas une politique, c'est une architecture : le pipeline qui construit le site public n'a jamais accès aux fichiers premium — les sources sont séparées à la racine. Une seconde ceinture automatique vérifie à chaque construction qu'aucun fichier ni artefact issu des sources premium n'a atterri dans le résultat, et bloque la publication sinon.

SECTION 02

Le modèle de menace, en clair

Ce contre quoi l'architecture protège : la fermeture d'un compte chez un prestataire, la défaillance d'un hébergeur, la suspension d'un domaine, la coupure d'un moyen de paiement, l'erreur humaine, la perte du technicien principal. Ce qu'elle ne prétend pas neutraliser : une décision de justice exécutoire, une panne générale d'Internet, l'absence totale d'entretien. La cible n'est pas l'invulnérabilité — c'est qu'aucun acteur unique, nulle part, ne détienne un interrupteur général.

SECTION 03

Le site

Astro ([site officiel](#) · [dépôt source](#)) — le générateur du site. Un générateur de site statique est un outil qui prend le contenu (textes, métadonnées) et fabrique les pages finales. Astro est choisi parce qu'il produit des pages très légères et se prête bien à l'ajout d'une PWA (Progressive Web App : un site qui s'installe sur le téléphone comme une application — icône sur l'écran d'accueil, lancement plein écran — sans passer par l'App Store ni le Play Store). La couche PWA (installation, icône, cache hors ligne) s'ajoute séparément, sans validation préalable d'une boutique d'applications — et sans qu'une boutique puisse la retirer.

Caddy ([site officiel et documentation](#) · [dépôt source](#)) — le serveur web (le logiciel qui répond aux visiteurs et leur envoie les pages). Choisi pour sa simplicité et parce qu'il gère automatiquement les certificats HTTPS (le cadenas du navigateur).

Hetzner ([site officiel](#) — [Cloud](#) · [documentation](#)) — l'hébergeur, sous forme de VPS (serveur privé virtuel : une machine louée dans un centre de données, dont on a le contrôle complet). Hetzner est allemand, solide et bon marché ; surtout, on ne lui confie que les machines — ni les domaines, ni l'annuaire, ni les paiements, ni l'identité des abonnés. Tout y tourne dans des conteneurs Docker ([site officiel](#) · [dépôt du moteur open source Moby](#)) (une technologie qui emballe chaque logiciel avec tout ce qu'il lui faut pour fonctionner). L'intérêt réel : les logiciels se reproduisent à l'identique chez n'importe quel autre hébergeur ; les données, secrets et réglages, eux, voyagent séparément, par les sauvegardes — la fin du document y revient.

Coolify ([site officiel](#) · [dépôt source](#)) — le panneau d'administration (une interface graphique pour gérer les services du serveur sans taper de commandes). Règle maison : le panneau est un confort, jamais une nécessité — tout est reconstituible sans lui.

SECTION 04

Les noms de domaine

Un registraire (ou registrar — le « bureau d'enregistrement » du guide pratique) est la plateforme où l'on enregistre un nom de domaine — l'adresse du site, comme amazon.fr. C'est un maillon sensible : un registraire qui suspend un domaine rend le site introuvable, même si le serveur tourne parfaitement.

La parade : trois domaines, chez trois registraires différents — et, autant que possible, sous trois registres distincts. La nuance compte : au-dessus du registraire se trouve le registre, l'organisme qui opère l'extension elle-même et qui peut, lui aussi, bloquer un domaine (.ch est opéré par SWITCH en Suisse, .cc par Verisign aux États-Unis — le même registre que .com). Trois registraires adossés au même registre ne font donc pas trois chaînes indépendantes ; la répartition définitive des noms entre extensions est arrêtée avec cette contrainte.

Porkbun ([site officiel](#)) (États-Unis) — le principal : registraire accrédité ICANN, politique d'abus publiée, sécurité de compte sérieuse, transfert sans friction. Ces critères sont réévalués périodiquement, comme pour tout prestataire.

Infomaniak ([site officiel](#) — [domaines](#)) (Suisse) — hébergeur-registraire suisse, juridiction stable et hors Union européenne.

easyDNS ([site officiel](#)) (Canada) — politique de retrait publiquement documentée : titre juridique exécutoire dans sa juridiction, obligation ICANN/CIRA, ou abus réseau manifeste.

Sont écartées des fonctions critiques les extensions relevant du registre français, .fr en tête : le droit positif y permet la suppression ou le transfert d'un domaine sur injonction administrative, sans décision judiciaire préalable (art. L.45-2 du Code des postes et des communications électroniques), et le Conseil constitutionnel a lui-même censuré en 2010 l'encadrement antérieur pour insuffisance de garanties. Les extensions étrangères ne rendent pas intouchable ; elles imposent une procédure internationale et interdisent qu'une seule autorité nationale atteigne toutes les adresses à la fois.

Et une règle de propriété non négociable : les domaines appartiennent à la structure de Papacito dès le premier jour — jamais à un prestataire, jamais à un intermédiaire.

SECTION 05

Le DNS

Le DNS est l'annuaire du web. Un annuaire classique vous dit qu'à telle adresse habite telle personne ; l'annuaire du web fait la correspondance entre les noms et les machines : il indique quelle adresse IP (le numéro unique d'un serveur sur le réseau) se cache derrière tel nom de domaine. Quand quelqu'un tape l'adresse du site, c'est le DNS qui le dirige vers le bon serveur.

Deux ceintures de protection, distinctes et complémentaires. Première ceinture : l'annuaire n'est jamais tenu par le registraire. L'annuaire (les serveurs DNS) est confié à un prestataire distinct — Cloudflare ([site officiel](#) — [DNS](#)) pour la performance, complété par des acteurs européens comme Bunny ([site officiel](#) — [Bunny DNS](#)) ou deSEC ([site officiel](#) · [dépôt source principal](#) — [desec-stack](#)). Cette séparation a sa valeur propre : une panne, un piratage ou une fermeture de compte chez le teneur d'annuaire ne touche pas le domaine lui-même, et le repointage vers un autre annuaire prend des minutes. Elle ne neutralise pas, en revanche, le pouvoir du registraire sur son propre domaine — c'est structurel, aucun montage DNS n'y change rien. D'où la seconde ceinture : trois domaines indépendants, chacun chez son registraire, chacun avec son annuaire. Si un domaine entier était suspendu à la source, les deux autres ne partagent avec lui ni bureau d'enregistrement, ni annuaire — et, autant que possible, ni registre. C'est la protection de dernier ressort, et c'est pour elle que les adresses de secours sont annoncées d'avance.

Toute la configuration est gérée en DNS as Code avec l'outil DNSControl ([site officiel et documentation](#) · [dépôt source](#)) : au lieu de cliquer dans les interfaces de chaque fournisseur, la configuration est un fichier texte versionné, poussé vers les fournisseurs d'un coup. Ce qui est garanti dès aujourd'hui : la configuration est un fichier, donc reproductible chez un fournisseur de secours en quelques minutes — puis le temps que le réseau propage le changement. Ce qui reste à valider ([Candidat](#)) : faire tenir la même zone par plusieurs annuaires simultanément suppose que les fournisseurs sachent se synchroniser, et tous ne le savent pas ; s'y ajoutent DNSSEC et la propagation des délégations. DNSControl sait piloter plusieurs fournisseurs ; il ne les rend pas compatibles entre eux. C'est un point que la maison témoin doit trancher.

Dernier filet : un manifeste signé des domaines officiels (signature cryptographique Minisign ([site officiel](#) · [dépôt source](#)) : un procédé qui prouve qu'un fichier vient bien du détenteur d'une clé et n'a pas été modifié). Diffusé par la newsletter, il permet à la communauté de vérifier qu'une adresse est authentique — et de retrouver les adresses de secours si la principale tombe. La clé publique qui permet cette vérification est diffusée dès le départ, par les canaux existants — newsletter, podcast, réseaux — avant tout incident : la confiance s'amorce quand tout va bien. Reste une condition sans laquelle le dispositif ne sert à rien : que la vérification soit à la portée du public. Personne n'ouvrira une ligne de commande un jour de crise ; la maison témoin doit donc démontrer au moins une méthode simple (page de vérification, instructions en trois lignes, empreinte de clé affichable). À terme, des preuves d'identité croisées type Keyoxide ([site officiel](#) · [dépôt source](#) — [Codeberg](#)) ([Option ultérieure](#)) pourront compléter le dispositif.

SECTION 06

La recherche

C'est le cœur de la promesse : tout retrouver. L'outil : Meilisearch ([site officiel](#) · [dépôt source](#)), un moteur de recherche interne auto-hébergé (il tourne sur le serveur, aucune donnée ne part chez un tiers). Un moteur de recherche interne indexe tout le contenu du site — y compris l'intégralité des transcriptions — et répond instantanément, en tolérant les fautes de frappe.

Concrètement : un auditeur tape « souffle du vivant », et le moteur lui sort directement les deux épisodes de podcast et le live qui en parlent, avec le minutage exact du passage — plus besoin de réécouter trois heures pour retrouver une anecdote.

Détail d'architecture qui compte : deux index séparés. L'index public ne contient que le contenu public. L'administration de l'index premium n'est pas exposée au public ; seule l'API de recherche répond, à des jetons courts (une clé d'accès temporaire, générée pour un abonné connecté, limitée à ses droits, qui expire d'elle-même). Sans droits valides, aucune requête vers l'index premium n'est autorisée.

SECTION 07

La chaîne éditoriale

Le circuit de publication, du clic à la mise en ligne :

Baserow ([site officiel](#) · [dépôt source](#)) — le cockpit éditorial (un tableur en ligne auto-hébergé, dans l'esprit d'Airtable). C'est là que l'équipe prépare et valide : titres, descriptions, statuts. Interface simple, zéro manipulation technique.

n8n ([site officiel](#) · [dépôt source](#) — [fair-code](#)) — l'orchestrateur (un outil d'automatisation auto-hébergé, l'équivalent libre de Zapier ou Make). Quand un contenu est validé dans Baserow, n8n transporte l'information et déclenche la suite. Règle stricte : l'orchestrateur transporte, il ne décide rien.

Git ([site officiel](#) · [dépôt source officiel](#)) — la mémoire de tout. Git est un système de versionnage : chaque modification produit un commit (un instantané du contenu, identifié par son empreinte et accompagné de son auteur et de sa date), et l'historique complet est conservé dans les dépôts et leurs sauvegardes. Le contenu du site (textes, transcriptions, métadonnées) vit dans des dépôts Git : c'est la source de vérité, récupérable et rejouable à tout moment.

Forgejo ([site officiel](#) · [dépôt source](#) — [Codeberg](#)) — la forge auto-hébergée qui abrite ces dépôts (l'équivalent d'un GitHub qu'on possède, sur son propre serveur, avec sa chaîne de construction intégrée). Un miroir GitHub ([site officiel](#)) existe pour le code — mais jamais pour le contenu : les transcriptions premium ne dorment pas chez Microsoft.

Répartition nette des rôles : Baserow tient l'état opérationnel (préparation, statuts, feu vert) ; Git tient le contenu publié canonique. La logique de transformation vit dans des programmes versionnés, rejouables depuis Git — n8n ne fait que les déclencher.

Releases versionnées et signées — publier, c'est produire une version complète du site : identifiée par son empreinte, signée, conservée à part et reliée au commit qui l'a produite ; toute modification ultérieure invaliderait sa signature. Mettre en ligne = basculer un lien vers la nouvelle version. En cas de problème, le retour arrière (le rollback) consiste à re-basculer le lien vers la version précédente : quelques secondes, tant qu'aucune migration irréversible de base de données n'est en jeu — cas rares et traités comme tels.

SECTION 08

La transcription

Whisper ([présentation officielle](#) · [dépôt source](#)) — le modèle de reconnaissance vocale (il transforme l'audio en texte). Exécuté en local, sur des machines qu'on contrôle, jamais via une API cloud : le contenu ne transite par aucun prestataire extérieur, et rien n'est facturé à la minute — le coût marginal se limite aux ressources de calcul, sur des machines contrôlées par la maison.

Le texte sort au format WebVTT (le format standard des sous-titres, où chaque segment porte son minutage) — c'est ce minutage qui permet la recherche à la seconde près et les chapitres cliquables.

Les transcriptions sont publiées en sortie machine, signalées comme telles, pour l'ensemble du catalogue. C'est un choix assumé : rendre tout le fonds cherchable tout de suite, plutôt que le retenir derrière une relecture intégrale préalable — la qualité se gagne ensuite, par passes d'amélioration successives.

Cette montée en qualité passe par la chaîne autour du modèle : un lexique maison (noms propres, vocabulaire de l'émission) guide la transcription et alimente des corrections automatiques ; chaque correction humaine, faite au fil de l'eau en priorité sur les passages signalés et les plus consultés, l'enrichit pour tous les épisodes suivants.

Le feu vert de publication reste humain : la machine transcrit, un humain décide de publier.

À la publication, chaque fichier reçoit deux sceaux complémentaires. L'horodatage OpenTimestamps ([site officiel](#) · [dépôt source du client](#)) : une preuve, à coût quasi nul, que ce contenu existait déjà, tel quel, avant une date donnée — elle complète l'historique Git ; elle n'établit ni l'auteur ni les circonstances, et ne prétend pas le faire. Et la signature de la maison (même procédé Minisign que le manifeste des domaines) : elle établit la provenance officielle — ce fichier a bien été validé et signé par la clé de publication de la maison. Le jour où les voix synthétiques seront indiscernables des vraies, la question ne sera plus « est-ce sa voix ? » mais « où est la signature ? » : un enregistrement non signé qui prétend venir d'ici n'apporte aucune preuve de provenance.

SECTION 09

Les comptes, abonnements et paiements

L'asymétrie fondatrice de toute l'architecture : le paiement est plural et remplaçable ; les droits sont uniques et chez nous. Dit simplement : qui a payé quoi, c'est l'affaire du prestataire de paiement ; qui a accès à quoi, c'est l'affaire de la maison — et ces deux registres sont volontairement séparés.

Authentik ([site officiel et documentation](#) · [dépôt source](#)) — le service d'identité auto-hébergé (il gère les comptes et les connexions, via le standard OIDC — le protocole derrière les boutons « se connecter avec », sauf qu'ici le fournisseur d'identité, c'est la maison). Un seul compte pour tout : site, recherche premium, flux podcast, vidéo.

Le service de droits (entitlements — littéralement « ce à quoi chacun a droit ») — le seul composant développé sur mesure, volontairement réduit à une fonction simple et testable : associer un compte à des droits d'accès. Il s'adosse à PostgreSQL ([site officiel et documentation](#) · [dépôt source officiel](#)) (le système de base de données libre de référence). Concrètement : quand un paiement réussit chez un prestataire, celui-ci prévient le service, qui allume le droit correspondant ; quand un abonnement s'arrête, le droit s'éteint. Mais le droit lui-même vit ici, pas chez le prestataire. C'est ce qui permet d'offrir un mois premium sans qu'un paiement existe (récompense communautaire, geste commercial) — et de changer de prestataire de paiement sans toucher aux

comptes. Les événements de paiement sont traités de façon idempotente (un même événement reçu deux fois ne produit qu'un seul effet), journalisés et rapprochés régulièrement avec les prestataires ; toute modification manuelle d'un droit laisse une trace d'audit. La difficulté réelle du composant n'est pas l'association compte-droit : ce sont les délais de grâce, les paiements en échec, les remboursements et les contestations — traités en V1 de façon délibérément pauvre et explicite plutôt qu'automatique et opaque.

Deux rails de paiement, deux réseaux : Stripe ([site officiel](#)) (le standard des cartes bancaires) et GoCardless ([site officiel](#)) (prélèvement SEPA — le prélèvement bancaire européen, qui passe directement de banque à banque, sans le réseau Visa/Mastercard). L'expérience du secteur l'a montré : quand une pression s'exerce, elle s'exerce sur le circuit de paiement bien plus souvent que sur le site lui-même. Si l'un coupe, l'autre continue d'accepter les paiements et de rétablir les abonnements ; la base interne conserve comptes, droits et historique — la migration des autorisations de paiement existantes dépend des procédures du prestataire et peut demander, au pire, une confirmation de l'abonné. Des remplaçants sont déjà instruits sur dossier, prêts à être branchés.

SECTION 10

Le podcast

Castopod ([site officiel](#) · [dépôt source officiel](#)) — la plateforme podcast auto-hébergée. Elle publie un flux RSS (le format standard et ouvert des podcasts : un fichier que n'importe quelle application — Apple Podcasts, Pocket Casts, AntennaPod — sait lire et suivre). Personne n'est obligé d'installer quoi que ce soit : chacun écoute dans son application habituelle.

Pour les abonnés : des flux privés à jeton — chaque abonné reçoit son lien d'écoute personnel, qui fonctionne aussi dans son application habituelle, et qui est révoqué individuellement. Un lien qui fuit se coupe sans toucher aux autres. Castopod gère nativement les abonnés premium et leurs flux ; le pilotage de ces droits depuis le service de droits maison est à démontrer en maison témoin ([Candidat](#)).

Les chapitres suivent le standard Podcasting 2.0 (chapitres horodatés lisibles par les applications modernes).

SECTION 11

La vidéo

Phase ultérieure, à la carte — rien n'oblige à migrer la vidéo en même temps que le reste. Le pressenti : PeerTube ([site officiel](#) · [dépôt source officiel](#) — [Framagit](#)) ([Candidat](#) — plateforme vidéo auto-hébergée, l'équivalent libre d'un YouTube qu'on possède), en instance fermée : inscriptions désactivées, connexion uniquement via le compte maison, vidéos premium lisibles seulement dans les pages du site par les abonnés connectés. PeerTube y est un moteur, pas une destination. Précision de vocabulaire : il s'agit de contrôle d'accès, pas de protection anti-copie — l'objectif est qu'une adresse partagée cesse de fonctionner, pas d'empêcher un abonné d'enregistrer son écran. Point de vigilance assumé : la vidéo est le poste le plus coûteux (le transcodage — la conversion des vidéos dans plusieurs qualités — est vorace en machine), d'où la décision de ne l'engager que quand ça se justifie.

SECTION 12

La newsletter

Le canal de repli ultime : si tout brûle, la liste reste.

Listmonk ([site officiel](#) · [dépôt source](#)) — le gestionnaire de newsletter auto-hébergé. La liste des abonnés vit sur le serveur — adresses, consentements, préférences, désabonnements — exportable à tout moment : c'est un actif qu'on possède, pas un service qu'on loue.

Le domaine d'envoi est séparé du domaine principal. Pourquoi : les boîtes mail (Gmail, Outlook...) notent chaque expéditeur — c'est la « réputation d'envoi », et c'est elle qui décide si un message arrive en boîte de réception ou en spam. Un domaine dédié à l'envoi fait vivre cette note à part : un incident d'envoi n'éclabousse pas le site, un souci du site ne dégrade pas la délivrabilité des emails.

L'envoi passe par deux prestataires SMTP (le protocole d'acheminement des emails) : Amazon SES ([site officiel](#)) en principal (le service d'envoi d'AWS — délivrabilité de référence, coût dérisoire), Brevio ([site officiel](#)) en secondaire. Les deux sont authentifiés et testés dès le départ (DKIM : le cachet cryptographique qui prouve aux boîtes mail que l'expéditeur est légitime). Si l'un bloque, le second s'active sans reconstruire la chaîne d'envoi. Chaque prestataire apporte sa propre infrastructure et sa propre réputation technique ; la réputation du domaine d'envoi, elle, reste commune aux deux — raison de plus pour la protéger des deux côtés, et pour l'isoler du domaine principal.

SECTION 13

La garde des clés

Toute cette architecture repose en dernier ressort sur quelques trousseaux — et trois registraires ne servent à rien s'ils tombent ensemble avec le même mot de passe. Les secrets d'exploitation (mots de passe de services, clés d'API) sont conservés dans des fichiers chiffrés par un outil dédié à la gestion de secrets (SOPS ([site officiel et documentation](#) · [dépôt source](#)) associé à age ([site officiel / spécification](#) · [dépôt source](#))), versionnés avec l'infrastructure sans jamais exposer leur contenu en clair ; les identifiants humains vivent dans un gestionnaire de mots de passe dédié, et les accès d'administration sont protégés par double authentification — de préférence par clé matérielle (un petit boîtier qu'on branche et sur lequel on appuie : la clé cryptographique ne sort jamais du boîtier, et rien ne s'ouvre sans lui). Les comptes chez les registraires, les fournisseurs d'annuaire et l'hébergeur ont chacun leurs propres contacts de récupération.

Deux clés font exception : celle qui déchiffre les sauvegardes et celle qui signe les publications. Elles ne vivent pas dans le système — support hors ligne vérifié et impression encodée, répartis entre deux lieux physiques distincts — parce que ce sont les seules dont la perte serait irrattrapable. La signature des publications pose un arbitrage assumé : une clé strictement hors ligne rendrait chaque publication manuelle. La piste retenue est la clé matérielle, éventuellement doublée d'une clé de publication révocable pour les signatures courantes, la clé maîtresse restant hors ligne ; le montage exact sera arrêté en maison témoin.

Enfin, un trousseau ne suffit pas à reprendre une maison. Il s'accompagne d'un inventaire d'exploitation tenu à jour : liste des services, propriétaire de chaque compte, échéances de renouvellement, chemins de sauvegarde, procédures de récupération, contacts utiles. C'est lui, autant que les clés, qui permet à un second technicien de reprendre la main sans dépendre du premier.

SECTION 14

La supervision et les sauvegardes

Uptime Kuma ([site officiel](#) · [dépôt source](#)) (surveillance de disponibilité — il vérifie en permanence que tout répond) doublé d'une sonde externe chez un fournisseur tiers : le surveillant ne dort pas dans la maison qu'il surveille. GlitchTip ([site officiel](#) · [dépôts source](#) : [backend](#) / [frontend](#)) capte les erreurs techniques ; Plausible ([site officiel](#) · [dépôt source](#)) fournit les statistiques de fréquentation sans cookies ni Google.

Restic ([site officiel et documentation](#) · [dépôt source](#)) — l'outil de sauvegarde chiffrée. Stratégie 3-2-1 : la production, plus une copie chiffrée hors site (chez un fournisseur distinct de l'hébergeur, dans un autre pays), plus une copie froide locale. Le dépôt distant est configuré en append-only (« ajout seulement ») : les identifiants dont dispose le serveur de production lui permettent d'ajouter de nouvelles sauvegardes, jamais de supprimer ni d'écraser les anciennes ; le nettoyage se fait depuis un autre poste, avec d'autres identifiants, conservés ailleurs. Conséquence : avec les identifiants de production, un attaquant maître du serveur ne peut ni supprimer ni écraser les sauvegardes antérieures à sa compromission. C'est une protection majeure, pas une invulnérabilité — d'où les contrôles d'intégrité réguliers et les restaurations d'épreuve.

Et le test-roi, régulier et chronométré : reconstruire la plateforme complète sur un serveur vierge, à partir des seules sauvegardes et d'un manuel écrit (runbook : la procédure pas à pas), exécutable par un technicien compétent muni du manuel, des sauvegardes et des clés — sans rien demander à l'ancien hébergeur. Une sauvegarde qui n'a jamais été restaurée est une hypothèse ; ici, c'est un exercice.

Tout cela s'entretient — mises à jour, renouvellement des domaines, contrôle des sauvegardes : posséder la maison évite le propriétaire, pas la toiture.