OBJECT FIRST

Liste de vérification

Liste de vérification pour la résilience aux ransomwares

Identifiez un stockage de sauvegarde doté d'une immuabilité absolue

Les attaques par ransomware sont devenues plus sophistiquées que jamais. Au cours des deux dernières années, 66% des organisations ont subi au moins une attaque, et 96% d'entre elles visaient les données de sauvegarde.*

C'est pourquoi, lorsque, et non si, une violation survenant et mettant en jeu votre entreprise, votre réputation et vos opérations se produit, un stockage de sauvegarde immuable constitue votre meilleure et ultime ligne de défense.

Cependant, si les données immuables peuvent être modifiées ou supprimées par un administrateur de sauvegarde ou de stockage, par un fournisseur ou par un attaquant, cela signifie que votre solution de stockage n'est pas absolument immuable.

Utilisez cette liste de vérification en trois étapes pour déterminer si votre solution de sauvegarde actuelle (ou envisagée) est résiliente aux ransomwares.

* Étude ESG 2025

Préparez-vous

Étape 1. Utilisez le Stockage objet S3

- ☐ Votre solution de stockage utilise-t-elle les fonctions S3 Object Lock et le versionnage S3 pour garantir l'immuabilité et préserver l'historique des sauvegardes ?
- ☐ Applique-t-elle le mode Conformité (et non le mode Gouvernance) et prend-elle en charge le chiffrement de bout en bout dès la création des données ?
- ☐ L'immuabilité peut-elle être vérifiée de manière indépendante grâce à des normes ouvertes et à des tests d'intrusion réalisés par des tiers indépendants ?

Seul le stockage d'objets S3 offre une sécurité intrinsèque, avec une immuabilité native intégrée directement à son protocole et à ses API. Cette conception fondamentale garantit qu'une fois les données écrites, elles ne peuvent ni être modifiées ni supprimées. Le stockage d'objets S3 repose sur une architecture ouverte conforme aux normes de l'industrie, alignée sur les meilleures pratiques de sécurité informatique et permettant la vérification par des tiers.

Étape 2. Garantissez une immuabilité instantanée

- ☐ Votre solution rend-elle les données de sauvegarde immuables dès leur écriture, sans aucun délai ni « zone de transit » ?
- ☐ Évite-t-elle l'immutabilité basée sur les instantanés ou la couche de déduplication, qui n'applique les protections qu'une fois la tâche terminée ?
- ☐ Les données de sauvegarde sont-elles écrites directement dans le stockage d'objets avec S3 Object Lock activé ?

Garantir que les données de sauvegarde sont immuables dès leur écriture est essentiel pour prévenir toute modification non autorisée, maintenir l'intégrité des données et se protéger contre les ransomwares. La méthode éprouvée et la plus sécurisée pour y parvenir consiste à utiliser le versionnage S3 combiné à Object Lock, qui garantit l'immuabilité lorsqu'un objet est créé dans le système de stockage.

Étape 3. Utilisez un appareil cible conçu sur mesure

- ☐ Votre configuration sépare-t-elle strictement le logiciel de sauvegarde du stockage de sauvegarde, afin de limiter l'impact en cas de violation ?
- ☐ Utilisez-vous un appareil cible dédié, géré par le fournisseur, plutôt qu'une solution de stockage bricolée (DIY) nécessitant des mises à jour, des correctifs et une surveillance manuels ?
- ☐ La sécurité de votre solution est-elle vérifiable, ou repose-t-elle sur un système de fichiers propriétaire du fournisseur qui empêche les tests indépendants et masque la manière dont l'immuabilité est appliquée ?

Un stockage de sauvegarde conçu sur mesure désigne un appareil de stockage autonome, configuré et optimisé pour conserver les données de sauvegarde. Il en existe deux types : les appareils intégrés qui combinent le logiciel de sauvegarde et le stockage dans un même système, et les appareils cibles qui offrent un appareil de stockage clé en main destiné à un logiciel de sauvegarde externe, comme Veeam. Seul un appareil cible S3 de sauvegarde conçu sur mesure et clé en main offre une résilience des données en mode Zero Trust, en séparant correctement le logiciel et le stockage et en permettant des tests de sécurité indépendants.

Immuabilité absolue : la défense ultime contre les ransomwares

Si vous ne pouvez pas cocher toutes les cases, vos sauvegardes risquent d'être vulnérables aux attaques par ransomware. L'immuabilité absolue signifie aucun accès aux actions destructrices. Personne, ni l'administrateur le plus privilégié, ni un attaquant ayant accès au stockage de sauvegarde, ne peut modifier ou supprimer les données.

Atteindre l'immuabilité absolue grâce au Zero Access nécessite le respect **de trois principes fondamentaux :**

1. **Stockage objet S3:** Une norme ouverte entièrement documentée avec une immuabilité native intégrée, permettant une vérification et des tests d'intrusion indépendants.
2. **Immuabilité instantanée:** Les données de sauvegarde doivent être immuables dès leur écriture.
3. **Appareil de stockage cible:** Un appareil de stockage cible dédié sépare le stockage du logiciel de sauvegarde et élimine les risques liés au stockage de sauvegarde auto-géré (DIY) lors des opérations.

Téléchargez notre livre blanc pour comprendre en quoi une **immuabilité absolue** représente le niveau de résilience le plus avancé contre les ransomwares.

Lire le livre blanc ↗

À propos d'Object First

Object First fournit un stockage de sauvegarde sécurisé, simple et performant, conçu sur mesure pour Veeam et entièrement immuable. Avec une protection de niveau ultime contre les ransomwares, votre organisation devient tout simplement résiliente.

Demander une démonstration ↗