COHESITY

GUIDE À L'INTENTION DES DIRIGEANTS

POUR ÉVALUER LES COFFRES-FORTS D'ISOLATION DES DONNÉES

Synthèse : comment l'isolation des données est-elle essentielle à la cyber-résilience ?

Aucune entreprise n'est à l'abri des cyberattaques, c'est pourquoi une réponse et une restauration efficaces sont essentielles pour chaque organisation. Les attaquants iront très loin pour vous forcer à payer une rançon, allant même jusqu'à cibler les systèmes mêmes censés protéger vos données. Les stratégies de sauvegarde traditionnelles, conçues pour protéger contre les pannes matérielles et les catastrophes naturelles, ne font pas grand-chose pour protéger votre entreprise contre des cyberattaques ciblées et à plusieurs étapes. Lorsque des ransomwares frappent, les copies de sauvegarde des données connectées aux réseaux de production peuvent être chiffrées ou supprimées, ce qui rend une restauration propre et rapide presque impossible. Pour les responsables informatiques, la question n'est pas de savoir si une attaque aura lieu, mais quand. Votre entreprise est-elle prête à restaurer en toute confiance lorsque cette attaque survient ?

Alors que les organisations comme la vôtre repensent la façon de protéger et de restaurer les données, l'isolation des données est devenue un élément fondamental d'une stratégie moderne de cyber-résilience. L'isolation des données vous garantit de disposer d'une copie intacte de vos données, que vous pourrez restaurer en cas d'échec. Le coffre-fort numérique fournit la séparation, la vérification et le contrôle nécessaires pour garantir des données propres et récupérables, même face à des cyberattaques destructrices. C'est pourquoi vos pairs adoptent l'isolation des données comme un impératif pour la résilience.

Le défi : la cyber-restauration est beaucoup plus complexe que la reprise après sinistre

Pendant des années, les entreprises ont conçu des systèmes de sauvegarde pour faire face aux défaillances matérielles, aux suppressions accidentelles et aux catastrophes naturelles. Ces systèmes ont souvent bien servi leur objectif. Mais ils ne suffisent pas à sécuriser et à protéger les données contre les cyberattaques destructrices qui dominent aujourd'hui.

Par conséquent, un facteur de risque critique est apparu : les données de sauvegarde peuvent être tout aussi vulnérables que les données de production. Les acteurs malveillants ne se concentrent plus uniquement sur le chiffrement des données de production. Ils infiltrent les référentiels de sauvegarde, désactivent les planifications de snapshots, installent des logiciels malveillants et corrompent les métadonnées afin d'éliminer les possibilités de restauration.

Ces risques existent même si vous disposez d'une plateforme moderne de protection des données.

Pourquoi votre parc de données est en danger

Vous vous demandez peut-être : « J'ai une plateforme de données sécurisée pour toutes mes sauvegardes, avec tous les modules complémentaires de sécurité activés. N'est-ce pas suffisant ? » Réponse courte : non !

Une telle plateforme réduit considérablement vos risques et votre surface d'attaque. Mais à elle seule, elle n'élimine pas l'exposition.

Voici pourquoi :

- **Connectivité partagée** : la plupart des systèmes de sauvegarde restent connectés au réseau de production. Si cet environnement de production est compromis, les attaquants ont déjà un accès aux données de sauvegarde.
- **Chevauchement des identifiants** : les identifiants administratifs sont souvent partagés entre les environnements. Une fois qu'un attaquant obtient un accès privilégié, il peut supprimer ou chiffrer les sauvegardes aussi facilement que les données de production.
- **Fausse immuabilité** : certaines sauvegardes « immuables » ne sont verrouillées que par logiciel. Si le plan de contrôle de stockage ou l'API est compromis, l'indicateur d'immuabilité peut être inversé.
- **Les menaces latentes peuvent subsister** : de nombreuses organisations restaurent à partir de sauvegardes sans valider l'intégrité des données ou rechercher des logiciels malveillants latents, ce qui augmente le risque de réinfection pendant la restauration.

L'impact commercial

Le résultat est un manque de confiance : l'intégrité perçue des données de sauvegarde est bien plus élevée que la réalité. Les conséquences négatives se répercutent :

- **Temps d'arrêt prolongés** : les sauvegardes non vérifiées ou compromises prolongent la restauration de quelques heures à quelques jours ou semaines.
- **Pression d'exploitation** : les équipes passent du temps à recréer des systèmes ou des ensembles de données au lieu d'exécuter des plans de restauration.
- **Coûts cumulés** : chaque heure de temps d'arrêt augmente la perte de revenus, l'exposition réglementaire et les dommages causés à la marque.
- **Érosion de la confiance** : lorsque le service informatique ne peut pas assurer une restauration rapide et propre, la confiance des dirigeants et du conseil d'administration dans la résilience organisationnelle diminue.

Isolation des données : votre dernière ligne de défense lorsque tout le reste échoue

Un coffre-fort numérique comble ce manque de confiance. Un coffre-fort numérique est un référentiel sécurisé, isolé et immuable qui stocke des copies propres de données critiques. Le coffre-fort numérique est délibérément déconnecté des réseaux de production et des principaux systèmes de sauvegarde.

L'adoption d'un coffre-fort numérique actualise la règle de sauvegarde 3-2-1 : conserver trois copies de données sur deux types de supports différents, avec une copie hors site isolée et immuable.

En pratique, les organisations mettent en œuvre cette règle de sauvegarde moderne comme suit :

- **3 copies de données doivent être immuables :** les copies doivent être protégées à l'aide d'un verrouillage en écriture unique, lecture multiple (WORM) ou d'un verrouillage au niveau de l'objet, et validées en continu à l'aide d'une détection d'anomalies basée sur l'IA et d'analyses régulières des menaces afin de confirmer que les données sont propres.
- **2 supports différents signifie stocker des données sur deux plateformes différentes ou selon deux périmètres de confiance :** les copies doivent résider sur des systèmes distincts qui ne partagent pas le même plan de contrôle ni la même surface d'attaque. Cela peut inclure des combinaisons de stockage cloud, sur disque ou sur bande conçues pour l'isolation des données.
- **1 copie hors site doit être isolée :** la copie finale doit être séparée par un air gap logique ou physique et protégée par un modèle de sécurité isolé et une garde par un tiers. Cette copie doit également être protégée par une authentification multifacteur (MFA), un quorum et des contrôles d'intégrité des données.

Ensemble, ces avancées transforment la règle 3-2-1 en un pilier fondamental de la cyber-résilience. Le coffre-fort cyber sert de point de restauration final et propre pour les données critiques. En combinant immuabilité, isolation, domaines de stockage diversifiés et validation rigoureuse de l'intégrité, le coffre-fort numérique permet aux organisations de restaurer en toute sécurité en cas de cyberattaque destructrice, même dans le pire des cas où votre parc de sauvegarde a été compromis.

Évaluation des solutions d'isolation des données

Lors de la sélection d'une solution d'isolation des données, les responsables informatiques doivent évaluer à la fois l'architecture de sécurité et la préparation opérationnelle. Sur la base des commentaires de centaines de responsables informatiques, les cinq piliers suivants sont des capacités essentielles :

1. **Isolation et contrôle d'accès :** les données du coffre-fort ne doivent pas être accessibles depuis les réseaux de production. Recherchez des air gaps imposés, des domaines d'identité indépendants, la MFA et des approbations administratives basées sur le quorum.
2. **Immuabilité et intégrité :** les données doivent être inviolables, avec un stockage WORM et des politiques de verrouillage de conservation qui empêchent la modification ou la suppression, même par les administrateurs.
3. **Automatisation et orchestration :** la réplication, la validation et la restauration du coffre-fort doivent être automatisées. L'orchestration basée sur des stratégies réduit les erreurs humaines et accélère la restauration.
4. **Protection contre les menaces :** la détection d'anomalies basée sur l'IA et l'analyse des logiciels malveillants signalent les menaces potentielles dans les instantanés afin de garantir que seules les données propres et sans compromis sont stockées et restaurées.
5. **Conformité et création de rapports :** les journaux d'audit immuables, le chiffrement et la gestion de la conservation doivent s'aligner sur des cadres tels que NIST SP 800-209, ISO 27040 et DORA, pour prouver la capacité de récupération et la préparation à la résilience.

Fiche d'évaluation - Utilisez cette fiche d'évaluation pendant vos conversations avec les fournisseurs.

Instructions :

1. Pour chaque catégorie, attribuez une note de 1 à 5 pour chaque fournisseur, où 1 ne répond pas à l'exigence et 5 répond entièrement à l'exigence.
2. Multipliez le score de chaque fournisseur par le **pondérateur** pour cette catégorie, et enregistrez le résultat dans la cellule Note pondérée correspondante.
3. Pour chaque fournisseur, additionnez toutes les **notes pondérées** de la colonne et enregistrez le total sur la ligne **Total pondéré** en bas du tableau.
4. Utilisez le **total pondéré** pour comparer les fournisseurs dans leur ensemble et saisir séparément les observations qualitatives ou les risques.

		Fournisseur 1		Fournisseur 2		Fournisseur 3		Fournisseur 4	
Categorie	**Pondérateur**	**Note**	**Note pondérée**	**Note**	**Note pondérée**	**Note**	**Note pondérée**	**Note**	**Note pondérée**
Isolation / air gap	10								
Immuabilité / WORM	10								
Séparation des contrôles d'accès	10								
Authentification forte (MFA / quorum)	8								
Détection des menaces / anomalies	8								
Bloquer la restauration de snapshots infectés	8								
Orchestration de la restauration	8								
Salle blanche / validation	8								
Conformité / auditabilité	8								
Simplicité SaaS / TTV	7								
Flexibilité hybride/multi-cloud	8								
TCO / Frais généraux opérationnels	7								
Total pondéré									

Une isolation des données moderne fournit des résultats commerciaux mesurables :

- **Résilience** : une copie de restauration physiquement ou logiquement isolée qui reste intacte même lorsque les plateformes de sauvegarde sont compromises.
- **Continuité** : les sauvegardes mises en coffre-fort garantissent aux organisations une copie des données à restaurer, quelle que soit la portée de l'attaque.
- **Conformité** : le stockage immuable et l'application de la rétention fournissent des preuves vérifiables de la protection des données et de la préparation à la restauration.
- **Confiance** : les points de récupération sont préservés en dehors du rayon d'impact opérationnel et peuvent être validés avant utilisation, garantissant que les données restaurées sont propres et non compromises.

L'isolation des données connecte les opérations informatiques, la sécurité et la conformité, de sorte qu'en cas de crise, une restauration propre est garantie, et non pas laissée au hasard.

De la dépendance aux sauvegardes à la restauration résiliente : Bethany Children's Health Center

De nombreuses organisations intègrent l'isolation des données comme composant standard de leur stratégie de protection des données. Par exemple, le Bethany Children's Health Center de l'Oklahoma, qui fournit des soins aux enfants ayant des besoins médicaux complexes. Pour prendre en charge des soins ininterrompus, le centre doit protéger les données de santé sensibles et les restaurer rapidement en cas de cyberattaque ou de catastrophe. Bethany satisfait à ces exigences en stockant des sauvegardes immuables en local et dans Cohesity FortKnox, un coffre-fort dans le cloud isolé.

Pour renforcer la résilience, Bethany suit le principe 3-2-1, qui consiste à conserver trois copies de données sur deux supports différents, dont une hors site. Deux sauvegardes immuables sont conservées en local, la troisième étant stockée dans Cohesity FortKnox.

Cohesity FortKnox fournit un service géré d'isolation des données disponible pour les environnements DataProtect et NetBackup, fourni sur AWS, Azure et GCP, et en tant que solutions en local pour les environnements les plus sécurisés. FortKnox combine isolation, immuabilité et automatisation pour fournir une restauration rapide, propre et vérifiée à l'échelle de l'entreprise.

FortKnox ajoute une nouvelle couche de défense : un coffre-fort sécurisé, en air-gapping, qui garantit que les données critiques restent sûres, conformes et récupérables.

Prochaines étapes pour évaluer votre cyber-résilience

Votre plan de résilience ne peut pas reposer sur des hypothèses qui ne s'appliquent plus. Alors que les cyberattaques deviennent de plus en plus agressives, la continuité des activités dépend de plus en plus de la solidité de votre dernière copie de données, la plus sécurisée. L'isolation des données représente une approche proactive qui renforce la restauration cyber et réduit les temps d'arrêt.

Commencez par vous poser les questions suivantes :

- **Sauvegardez-vous les données SaaS, en local et dans le cloud de toutes vos sources de données sur une plateforme moderne unique ?**
- **Avez-vous renforcé votre plateforme avec la MFA, l'immuabilité et le contrôle d'accès basé sur les rôles ?**
- **Respectez-vous la règle de sauvegarde 3-2-1 ?**
- **Quelles mesures d'isolation séparent vos données de sauvegarde des réseaux de production ?**
- **À quelle fréquence analysez-vous vos sauvegardes pour détecter les menaces ?**
- **À quelle fréquence testez-vous votre plan de réponse cyber ?**
- **Au cours de votre dernier test de réponse aux cyber incidents, à quelle vitesse avez-vous restauré ?**

C'est le moment de faire passer la cyber-résilience d'un objectif technique à un impératif stratégique. La préparation, et non les suppositions, est l'avantage concurrentiel ultime.

Découvrez comment une isolation des données moderne peut protéger vos données, renforcer votre posture de restauration et vous donner la confiance nécessaire pour fonctionner en toute sécurité, quelle que soit la menace. Pour en savoir plus, rendez-vous sur https://www.cohesity.com/fr-fr/platform/fortknox/

COHESITY

https://www.cohesity.com/fr-fr/
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

4500065-001-FR 2-2026