Se défendre contre les ransomwares et les menaces internes grâce à l'isolation des données

Principaux avantages

- Renforcer la stratégie de sécurité des données
- Protéger les données contre les cybermenaces et les menaces internes
- Respecter les SLA et réduire les risques commerciaux
- Réduire les temps d'arrêt grâce à une restauration instantanée à l'échelle

Selon une récente étude de Cybersecurity Ventures, d'ici 2031, les entreprises subiront une attaque par ransomware toutes les deux secondes, pour un préjudice de plus de 265 milliards de dollars. Par ailleurs, d'après Tech Jury, plus de 34 % des entreprises dans le monde seront confrontées à une attaque d'initié, soit une augmentation de 47 % au cours des deux dernières années. La multiplication et la gravité croissante des cyberattaques et des menaces d'initiés poussent les entreprises à renforcer leurs systèmes informatiques et leurs données. Pour ce faire, nombre d'entre elles suivent les conseils du NIST Cybersecurity Framework afin d'adopter une stratégie de défense à plusieurs niveaux.

Les entreprises qui investissent dans la gestion des données de nouvelle génération de Cohesity ont une longueur d'avance. Cohesity est conçu pour offrir des capacités de défense approfondies, notamment :

- **Des snapshots immuables** : une « gold copy » des données de sauvegarde qui n'est jamais exposée ni montée à l'extérieur
- **DataLock** : un verrouillage WORM limité dans le temps sur le snapshot de sauvegarde qui ne peut pas être modifié
- **Le chiffrement** : les données sont chiffrées au repos et en vol
- **Le contrôle d'accès basé sur les rôles (RBAC)** : l'accès granulaire de l'administrateur et de l'utilisateur peut être mis en œuvre selon les principes du moindre privilège et du besoin d'en connaître
- **Pas de porte dérobée** : seuls les utilisateurs autorisés du client prennent en charge l'activation des comptes
- **Un accès SSH sécurisé** : un chemin d'accès sécurisé sur un réseau non sécurisé
- **L'isolation des données** : les données sont isolées pour les protéger des cybermenaces et des menaces internes

L'isolation des données ne remplace pas les solutions existantes de sauvegarde et de récupération ou de reprise après sinistre (DR), mais fournit une couche supplémentaire de protection. L'objectif : renforcer la stratégie globale de sécurité des données.

L'isolation moderne des données avec Cohesity

Le « air gapping » défini par le NIST requiert que les entreprises conservent au moins une copie de leurs données isolée physiquement et électroniquement pour plus de sécurité. Cette approche, bien que très sécurisée, ne permet pas d'atteindre les objectifs de RTO et de RPO des entreprises modernes. L'isolement des données est donc apparu comme une alternative permettant de mieux répondre aux exigences modernes en matière de RTO et de RPO. Les données de sauvegarde sont stockées dans le cloud ou dans un autre endroit avec une connexion temporaire extrêmement sécurisée. Cela permet de disposer d'un environnement inviolable qui protège contre les ransomwares et les menaces d'initiés, tout en respectant les accords de niveau de service (SLA) de l'entreprise.

Grâce à Cohesity, les entreprises ne sacrifient jamais les SLA ou la tolérance au risque. Elles disposent d'un choix et d'une flexibilité maximum pour isoler et protéger les données de leur entreprise contre les acteurs malveillants. Cohesity prend en charge un déploiement flexible avec une isolation vers :

- **Cohesity FortKnox** : une solution SaaS d'isolation et de restauration des données qui améliore la cyber-résilience en fournissant une copie immuable des données isolée dans une chambre forte gérée par Cohesity dans le cloud via un air-gap virtuel. La solution assure la sécurité de vos données grâce à des fonctionnalités de détection des ransomwares, de quorum et de Zero Trust. Combiner FortKnox à une séparation physique et à une isolation du réseau et de la gestion permet de fournir la protection optimale et la facilité d'utilisation nécessaires contre les ransomwares et les autres menaces de cybersécurité.
- **Cluster Cohesity distant** : les clients peuvent répliquer d'un cluster Cohesity immuable vers un autre cluster distant fonctionnant sur site ou comme cluster virtuel dans un cloud public. Comparée à l'ancienne approche d'isolation des données qui nécessitait d'expédier des bandes hors site, cette nouvelle méthode permet de rendre les données sur le cluster distant immédiatement disponibles, et donc de réduire le RTO et le RPO.
- **Cible NAS** : Cohesity archive les données sur une cible de stockage externe NAS qui prend en charge le WORM pour isoler les données avec des RTO et RPO plus faibles.
- **Cloud** : Les entreprises tirent parti de l'évolutivité et de l'élasticité du cloud public en l'utilisant comme l'un des moyens modernes d'assurer l'isolation des données. Cohesity prend en charge l'archivage vers le cloud ou tout stockage compatible S3 qui prend en charge Object Lock et Object Versioning afin d'isoler les données, de réduire le RTO et le RPO, et de diminuer le TCO.
- **Bande (air gap)** : Cohesity permet d'archiver les données sur bande à partir de la sauvegarde afin que service informatique puisse envoyer les bandes vers un stockage hors site, ce qui garantit un accès uniquement par engagement physique.

Récompenses risque-SLA optimales avec l'isolation sur un cluster Cohesity

Répliquer les données de sauvegarde sur un cluster Cohesity distant permet aux clients de Cohesity de gagner en résilience des données, de respecter des SLA exigeants et de réduire les risques. Conformément au modèle de défense approfondie du NIST Cybersecurity Framework, Cohesity permet aux équipes de répliquer leurs données vers un autre cluster Cohesity immuable sur un site isolé. Les données sont ainsi conservées dans un coffre-fort moderne situé sur un réseau isolé et prenant en charge le WORM.

La figure 1 illustre la flexibilité du déploiement de Fort Knox et la possibilité de restaurer vers plusieurs destinations en cas de reprise après sinistre. Seul l'administrateur de l'entreprise ouvre et ferme les ports nécessaires et ce, uniquement pendant le transfert de données afin d'en assurer la sécurité.

Répliquer vers un cluster Cohesity isolé permet aux entreprises de moderniser leurs centres de données, de renforcer leur cyberdéfense, d'accélérer la restauration (grâce à une restauration instantanée à l'échelle), de raccourcir leurs RTO/RPO et de réduire les besoins en bande passante du réseau. Protégez votre entreprise contre l'augmentation des ransomwares et des menaces d'initiés en fortifiant vos systèmes informatiques avec la protection air-gap de Cohesity.

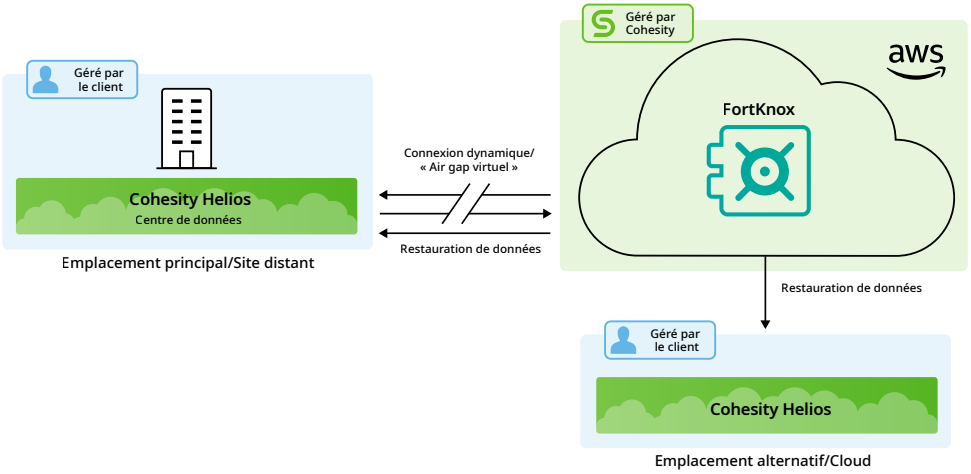

Figure 1 : Flexibilité de la restauration de FortKnox

Pour en savoir plus, rendez-vous sur www.cohesity.com/fr/

COHESITY