Contrez les attaques par ransomware avec Cohesity

Principaux avantages

- Protégez vos données et votre activité grâce à une architecture de défense approfondie
- Identifiez rapidement les attaques potentielles grâce à la détection des anomalies basée sur l'apprentissage automatique
- Réduisez les temps d'arrêt grâce à une récupération rapide à l'échelle

Les données sont un facteur de différenciation dans l'économie numérique. Elles sont donc devenues simultanément la ressource commerciale la plus précieuse et la plus ciblée. Selon Cybersecurity Ventures, les coûts annuels de la cybercriminalité dans le monde devraient atteindre 10 500 milliards USD d'ici 2025, et une entreprise sera victime d'une attaque par ransomware toutes les 2 secondes d'ici 2031[1]. Même si les entreprises sont de plus en plus conscientes des stratagèmes d'extorsion numérique, des attaques plus sophistiquées et plus ciblées visent de plus en plus les données et l'infrastructure de sauvegarde et continuent de menacer les entreprises du monde entier. La perte financière considérable subie par les entreprises compromises est souvent aggravée par la méfiance des clients et, dans le cas de la santé, par un risque pour la vie humaine.

Cohesity contrecarre efficacement les attaques par ransomware et aide votre entreprise à échapper aux rançons. La solution complète de gestion des données next-gen de Cohesity propose une approche multicouche pour protéger les données de sauvegarde contre les ransomware, détecter et récupérer rapidement après une attaque. L'architecture inaltérable unique de Cohesity empêche le chiffrement, la modification et la suppression de vos données de sauvegarde. Grâce à l'apprentissage automatique, elle offre une visibilité et surveille en permanence la présence d'anomalies dans vos données. Et en cas de sinistre, Cohesity vous permet de localiser une copie propre de vos données dans l'ensemble de votre empreinte mondiale, notamment dans les clouds publics, pour les récupérer instantanément et réduire les temps d'arrêt.

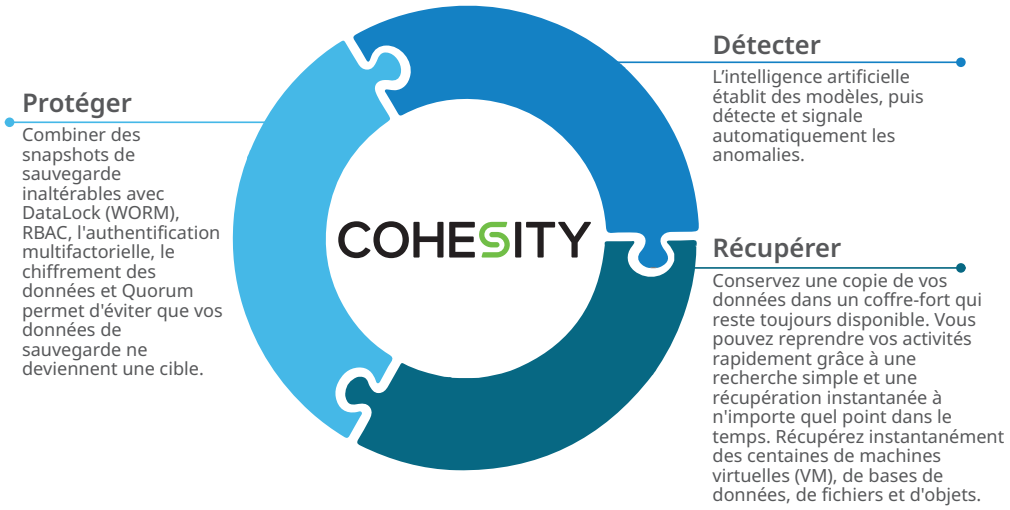

Figure 1 : Cohesity offre des capacités complètes pour protéger, détecter et récupérer d'une attaque par ransomware

1. Cybersecurity Ventures : Top 6 Cybersecurity Predictions And Statistics For 2021 To 2025 (30 décembre 2021)

Protéger

Des ransomwares sophistiqués comme Locky et Crypto ont récemment détruit des clichés instantanés de données et des données de point, transformant l'infrastructure de sauvegarde destinée à défendre l'entreprise en une cible de choix pour les cybercriminels. Cohesity stoppe les intrus en empêchant votre sauvegarde de devenir la cible d'une attaque.

Cohesity SpanFS™, un système de fichiers distribué de troisième génération, offre une protection multicouche unique contre une attaque par ransomware. Cohesity offre, entre autres, le plus haut niveau de protection contre les attaques par ransomware, car elle repose sur l'immuabilité.

- **Des snapshots inaltérables** – Tous les snapshots de sauvegarde stockés dans Cohesity sont par défaut inaltérables. Le snapshot original (aussi appelé « gold copy ») n'est jamais monté ou exposé à un système ou une application externe. La seule façon d'écrire de nouvelles données ou de monter la sauvegarde en mode lecture-écriture pour récupérer des données est de créer un clone sans impact sur le stockage de la sauvegarde originale, ce qui est effectué automatiquement par le système.
- **DataLock** – la capacité WORM de la sauvegarde permet de créer et d'appliquer une stratégie DataLock basée sur les rôles à des snapshots de sauvegarde spécifiques. Le responsable de la sécurité de votre entreprise peut utiliser cette fonctionnalité pour stocker les snapshots au format WORM. Les paramètres temporels imposant des intervalles ne peuvent pas être supprimés, même par le rôle d'administrateur ou de responsable de la sécurité, ce qui offre une couche supplémentaire de protection contre les attaques par ransomware.
- **Contrôle d'accès basé sur les rôles (RBAC)** – Cohesity permet à votre personnel informatique d'accorder à chaque personne un niveau d'accès minimum à ce dont elle a besoin pour effectuer une tâche particulière, et ce afin de réduire le risque d'accès non autorisé aux données et aux systèmes.
- **Authentification multifactorielle (MFA)** – Si un criminel avait accès au mot de passe de votre système, il ne pourrait pas accéder à la sauvegarde de Cohesity sans passer par une couche de sécurité supplémentaire de type MFA ou vérification en plusieurs étapes. Cohesity prend en charge diverses capacités d'authentification et d'autorisation, notamment une intégration forte de l'Active Directory, de la MFA, des listes de contrôle d'accès, un contrôle d'accès basé sur les rôles (RBAC) en mode mixte et un audit complet au niveau du système et du produit.
- **Chiffrement des données** – Cohesity dispose d'une fonctionnalité de chiffrement basée sur la norme AES-256, validée par la FIPS et reposant sur une méthode logicielle, pour vos données en transit et au repos. Ce module cryptographique validé par le National Institute of Standards and Technology (NIST) des États-Unis selon la norme 140-2 niveau 1 des Federal Information Processing Standards (FIPS) est reconnu dans le monde entier.
- **Quorum** – Pour protéger vos données et vos systèmes contre les menaces internes et les vols d'identifiants, Cohesity exige que toute modification de niveau racine ou de système critique qu'un membre de votre entreprise souhaite effectuer soit autorisée par plusieurs personnes.

La plateforme de gestion des données next-gen Cohesity Helios offre une combinaison unique de snapshots de sauvegarde inaltérables, de capacités DataLock, de RBAC, de MFA et de Quorum (alias la règle des quatre yeux), afin d'empêcher que les données de sauvegarde ne soient la cible d'une attaque par ransomware.

Détecter

Alors que les cybercriminels continuent de renforcer et de modifier leurs approches, Cohesity permet à votre entreprise de détecter plus facilement les intrusions grâce à une solution de gestion SaaS globale pour les entreprises. Les clients de Cohesity disposent d'un tableau de bord unique pour visualiser, gérer et agir rapidement sur l'ensemble de leurs données et applications. Dans le cadre de la lutte contre les ransomwares, l'apprentissage automatique de Cohesity Helios fournit des informations susceptibles d'échapper à l'homme, car il effectue une surveillance automatique et continue, et vous avertit s'il détecte une anomalie.

Les algorithmes d'apprentissage automatique de pointe évaluent vos besoins informatiques de manière proactive et automatisent régulièrement les ressources de votre infrastructure. Si le taux de modification des données de votre entreprise, notamment l'ingestion de données, sort de la plage normale (sur la base des taux de modification quotidiens des données logiques, des données stockées après déduplication globale ou de l'ingestion de données historiques), la détection d'anomalies pilotée Cohesity Helios envoie une notification à vos administrateurs informatiques. Le service informatique est alors instantanément informé que les modifications de données ne sont pas conformes aux schémas normaux.

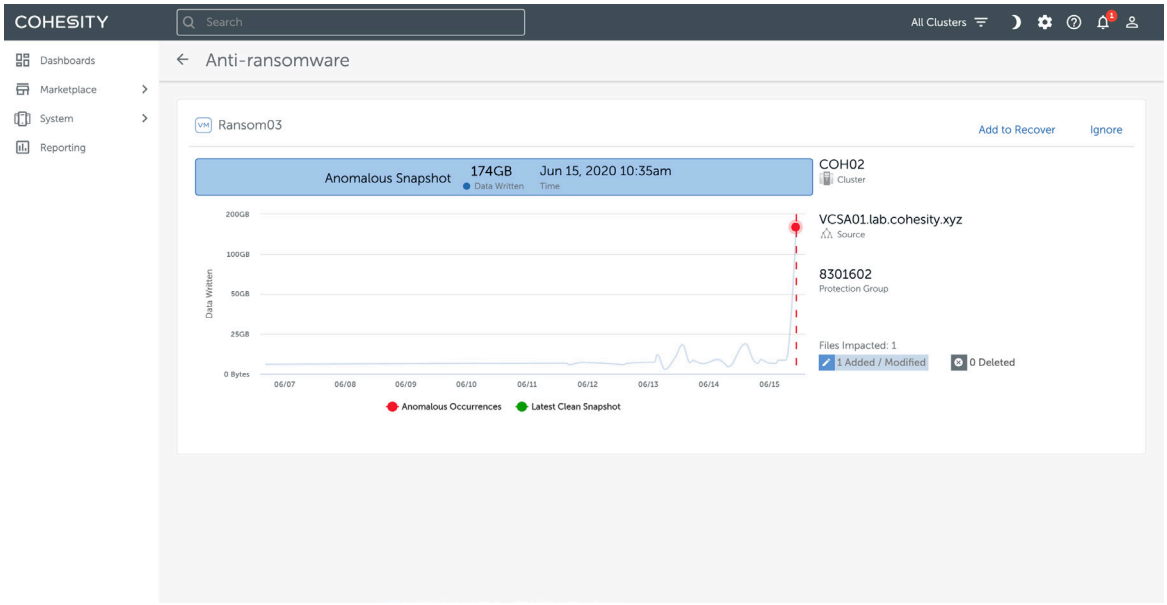

Figure 2 : Cohesity Helios permet aux entreprises de détecter les intrusions de ransomware

L'apprentissage automatique d'Helios établit des modèles et recherche automatiquement les anomalies d'acquisition ou de modification des données, ce qui lui permet de détecter une potentielle attaque par ransomware. En cas d'anomalie, la plateforme alerte simultanément l'équipe informatique de votre entreprise et l'équipe d'assistance de Cohesity pour accélérer la prise en charge et la correction du problème.

Non seulement Cohesity surveille le taux de modification des données de sauvegarde pour détecter une éventuelle attaque par ransomware, mais elle est également la seule à détecter et à signaler les anomalies au niveau des fichiers dans les fichiers non structurés et les données d'objet. Cela inclut, entre autres, l'analyse de la fréquence d'accès aux fichiers, et du nombre de fichiers modifiés, ajoutés ou supprimés par un utilisateur spécifique ou une application, pour garantir la détection rapide d'une attaque par ransomware.

Récupérer

Les menaces de cybersécurité, internes et externes, sont bien réelles, et elles arrivent vite. C'est pourquoi la récupération doit être prévisible et rapide. Cohesity accélère le processus de récupération des données et des applications d'entreprise victimes d'une attaque par ransomware, et ce à grande échelle. Outre les sauvegardes inaltérables, Cohesity offre plusieurs méthodes basées sur des stratégies pour isoler vos données stratégiques et sécuriser la dernière bonne copie. Pour répondre à vos exigences uniques en matière de récupération et de sécurité, vous pouvez isoler vos données dans Cohesity FortKnox, le coffre-fort cloud géré par Cohesity, les répliquer sur un autre cluster immuable, ou les enregistrer sur bande et les stocker sur un site distant, comme Iron Mountain.

L'assistance basée sur l'apprentissage automatique de Cohesity Helios permet d'accélérer la récupération en recommandant une copie propre des données à restaurer. Vous pouvez également tirer parti des capacités de recherche globale de la plateforme pour localiser vos données et y accéder rapidement dans tous vos environnements.

Cohesity CyberScan offre une visibilité approfondie de l'état des sauvegardes et du potentiel de récupération des snapshots protégés afin de garantir une restauration propre et d'éviter de réinjecter une cybermenace ou une vulnérabilité logicielle dans votre environnement de production. CyberScan affiche l'indice de vulnérabilité de chaque snapshot et fait des recommandations exploitables pour remédier aux vulnérabilités des logiciels. Cela vous permet de récupérer proprement et de manière prévisible suite à une attaque par ransomware.

En combinant des snapshots entièrement hydratés avec l'architecture propriétaire SnapTree B+Tree de Cohesity, MegaFile et le montage instantané, vous pouvez réduire considérablement vos temps d'arrêt en restaurant instantanément des centaines de machines virtuelles (VM), de fichiers, d'objets et de larges bases de données.

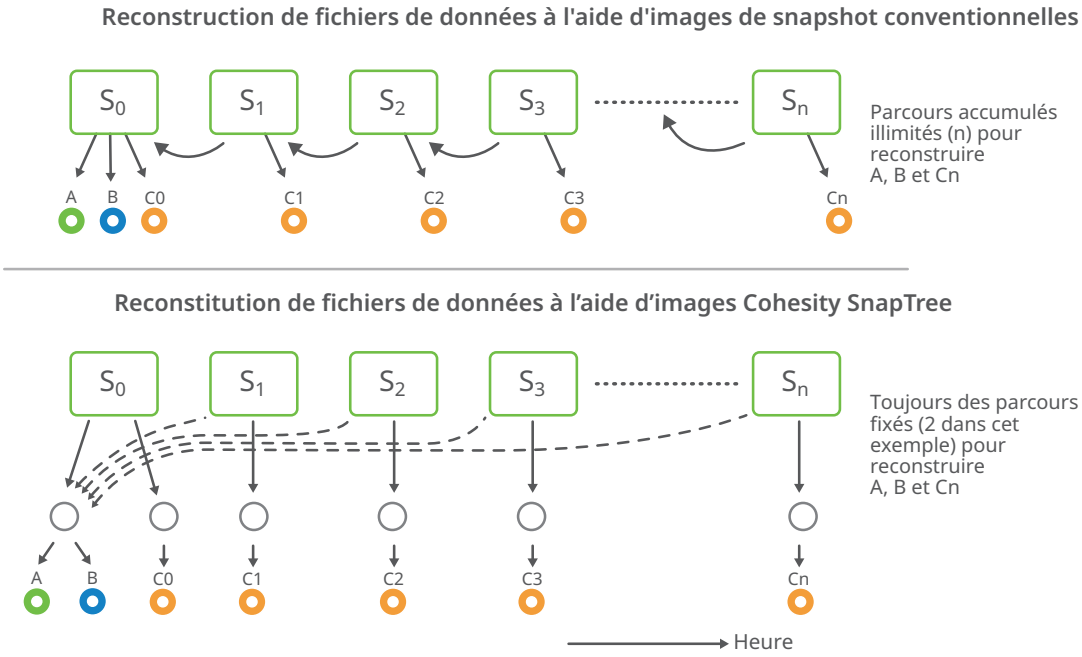

Figure 3 : la technologie SnapTree brevetée de Cohesity fournit un nombre illimité de snaps sans frais généraux, pour une récupération instantanée à l'échelle

Contrez les attaques par ransomware avec Cohesity

La sauvegarde est votre dernière ligne de défense contre les attaques sophistiquées et paralysantes par ransomware. La solution anti-ransomware complète de Cohesity permet de protéger, de détecter et surtout de récupérer rapidement ce dont vous avez besoin pour réduire les temps d'arrêt et assurer la continuité des activités.

Pour en savoir plus, consultez www.cohesity.com/fr/solutions/ransomware

COHESITY