COHESITY

LIVRE BLANC

Août 2022

Améliorer vos défenses contre les ransomwares : protéger, détecter et récupérer

La gestion des données nouvelle génération protège contre les menaces liées aux ransomware et aux données.

Table des matières

Protéger, Détecter et Récupérer avec Cohesity

La plateforme Cohesity représente un excellent moyen pour les entreprises de protéger et de gérer de vastes magasins de données d'entreprise. Cependant, les cybercriminels ciblent les magasins de données pour différentes activités néfastes, notamment les attaques par ransomware et le vol de données. Les ransomwares restent la principale menace, car ils permettent de gagner facilement de l'argent. Les cybercriminels travaillent donc sans relâche pour compromettre les entreprises.

Les attaques par ransomware ne montrent quant à elles aucun signe de ralentissement. On estime que 714 millions d'attaques ont eu lieu en 2021[1], et qu'une nouvelle entreprise en est victime toutes les 11 secondes[2]. Les cybercriminels sont très organisés et ont créé des outils et des services pour les différentes étapes d'une attaque par ransomware. Un seul clic d'utilisateur erroné, une simple mauvaise configuration du système et l'infiltration d'un nouveau logiciel malveillant indétectable peuvent avoir des conséquences désastreuses pour les entreprises. Les attaques par ransomware peuvent entraîner une méfiance de la part des clients, engendrer des pertes de revenu, et interrompre les activités actuelles et futures.

Parallèlement aux ransomwares, les conflits mondiaux ont augmenté le risque d'attaques commanditées par les états-nations. Plusieurs pays, dont l'agence américaine CISA via son alerte « Shields Up », indiquent que toutes les entreprises doivent prendre des mesures exceptionnelles pour s'assurer que leurs systèmes d'information peuvent résister à des attaques sophistiquées et persistantes.

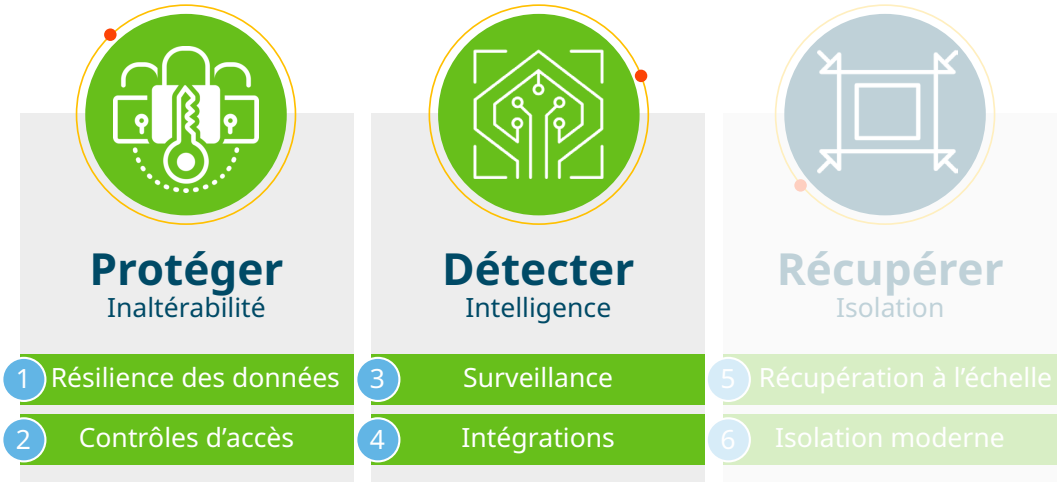
Ces défis imposent de renforcer la sécurité de la gestion des données en permettant à la plateforme de gestion des données de résister et de se défendre activement contre les menaces centrées sur les données. Les capacités de sécurité de base doivent garantir que les données ne peuvent pas être corrompues ou supprimées lors d'attaques par ransomware, qu'elles ne peuvent pas être volées par des pirates informatiques ou des initiés malveillants, et surtout que les entreprises peuvent détecter les attaques en cours.

La dernière ligne de défense contre les ransomwares

Se protéger, détecter les ransomwares, les violations de données ou les menaces internes et récupérer de telles attaques requiert plusieurs capacités et fonctions clés.

Les capacités de protection et de détection assurent la résilience des données pour empêcher la destruction intentionnelle ou accidentelle des données. Des contrôles d'accès stricts protègent les paramètres contre les accès ou les modifications non autorisés. Ils sécurisent et garantissent également la confidentialité des données. En parallèle, la détection et l'analyse permettent d'assurer une surveillance continue afin d'identifier les attaques et les activités inhabituelles. Ces capacités sont soutenues par des intégrations avec les principales applications de sécurité. L'objectif est d'automatiser la réponse aux incidents et d'exploiter les services de sécurité d'entreprise existants, notamment la gestion des clés, la gestion des identités et des accès, l'authentification multifacteur, ainsi que l'analyse des menaces et des vulnérabilités. Ces capacités fonctionnent de concert pour fournir une plateforme de gestion des données renforcée qui empêchera toute attaque d'altérer ou de détruire les données, et qui permettra aux entreprises de mieux détecter les attaques en cours contre leurs données.

En terme de récupération, Cohesity offre une récupération inégalée à l'échelle et une isolation moderne. La récupération à l'échelle permet aux entreprises d'identifier leur meilleur point de récupération, de comprendre l'état de données spécifiques, de fournir immédiatement un accès aux fichiers et aux objets et de restaurer des milliers de VM en quelques minutes. L'isolation moderne assure une récupération fiable pour les scénarios les plus pessimistes, c'est-à-dire lorsque l'emplacement principal de l'entreprise a été complètement désactivé, et qu'il n'est plus disponible ou adapté à la reprise des activités.



Verrouiller les données et la plateforme, surveiller les données et les utilisateurs

La résilience des données se compose de trois fonctions essentielles. Tout d'abord, les données doivent être inaltérables et avoir une persistance configurable. Elles ne peuvent pas être modifiées une fois écrites, et des copies spécifiques seront conservées jusqu'à leur expiration, comme définit par la stratégie de l'entreprise. Ensuite, les données stockées et transmises par la plateforme de gestion des données d'une entreprise doivent utiliser un chiffrement fort pour empêcher qu'elles soient consultées sans autorisation. Les réglementations sectorielles et de protection de la vie privée telles que le RGPD, le PCI et l'HIPAA exigent que les entreprises chiffrent respectivement les informations personnelles identifiables (PII), les données de l'industrie des cartes de paiement (PCI) et les informations de santé protégées (PHI). Et cela ne représente qu'un petit sous-ensemble des lois et réglementations mondiales qui imposent cette protection. Ces capacités protègent les données contre les actions malveillantes engendrées par les ransomwares, et garantissent que les données conservent leur confidentialité et leur intégrité. Enfin, la plateforme de gestion des données doit être tolérante aux pannes et redondante pour éviter tout point de défaillance unique. Cela permet de garantir qu'elle sera disponible pour les sauvegardes planifiées définies dans les objectifs de points de récupération (RPO) de l'entreprise.

Les contrôles d'accès permettent aux entreprises de contrôler précisément qui peut accéder à la plateforme de gestion des données et la modifier, en adhérant aux principes de Zero Trust. Grâce à l'authentification multifacteur (MFA), seuls les utilisateurs vérifiés peuvent se connecter à la plateforme. C'est essentiel pour empêcher que les comptes administratifs soient piratés et que des modifications non autorisées soient apportées aux données et aux paramètres. En y associant des contrôles d'accès granulaires basés sur les rôles (RBAC), les entreprises peuvent contrôler étroitement les capacités auxquelles les utilisateurs peuvent accéder pour respecter le principe du moindre privilège. Le quorum permet quant à lui de contrôler les modifications des paramètres de la plateforme. Il empêche les mises à jour non autorisées en exigeant au moins deux approbations pour modifier les configurations ou les paramètres.

La détection et l'analyse permettent d'analyser et de surveiller les données de la plateforme à la recherche d'indications d'attaques en cours, de charges de travail compromises et de renseignements sur les données afin de garantir que des mesures appropriées soient déployées pour protéger les données sensibles. Parmi les capacités de détection et d'analyse, citons la surveillance des données pour détecter les changements inhabituels susceptibles d'indiquer la présence de ransomware ou d'autres activités malveillantes, ainsi que la surveillance du comportement des utilisateurs pour détecter les accès anormaux aux données. En ajoutant du contexte aux données, notamment l'activité d'accès de l'utilisateur, dans des modèles avancés d'IA/ML, l'analyse comportementale de l'utilisateur peut anticiper une attaque par ransomware ou une menace interne.

Un élément essentiel de la détection et de l'analyse est l'intelligence des données, qui fournit des détails sur le paysage des données de l'entreprise, notamment l'emplacement, la classification, l'utilisation et le volume. Ces renseignements permettent à l'entreprise de comprendre quelles données elle possède et de s'assurer qu'elle applique les protections et les contrôles appropriés en fonction de leur sensibilité. Les alertes de détection de ransomware peuvent être transmises aux équipes informatiques et de sécurité pour qu'elles puissent prendre en charge l'incident de manière coordonnée, et ainsi accélérer la réponse et la récupération.

Intégrer la sécurité à l'infrastructure de sécurité existante renforce la sécurité et la protection de la plateforme de gestion des données. Les entreprises peuvent identifier les risques et les menaces en intégrant des solutions de gestion des vulnérabilités et de détection des menaces, et optimiser les contrôles d'accès existants en intégrant une gestion des identités et des accès. Les intégrations SIEM et SOAR facilitent la réponse aux incidents et la création de tickets. Cela apporte le soutien environnemental nécessaire pour sécuriser la plateforme et permettre aux opérations de sécurité et informatiques de collaborer en toute transparence.

La plateforme Cohesity utilise les protections de l'architecture Zero Trust, de l'analyse et de la plateforme pour sécuriser et renforcer la plateforme de gestion des données. Cela offre plusieurs avantages essentiels pour réduire les risques et améliorer la cyber-résilience. Parmi ces avantages, citons la sécurité et la résilience des données contre les attaques par ransomware et les violations de données, la protection des données en cas de défaillances opérationnelles et de catastrophes naturelles, ainsi que la sécurité des données archivées et l'intelligence des données pour prendre en charge la gouvernance et la conformité des données.

Explorer en détail

Vous trouverez ci-dessous un examen détaillé des capacités et des fonctions de la plateforme Cohesity. Chaque composant majeur de l'architecture est examiné par catégorie, à savoir :

Résilience des données : chiffrement des données au repos et en mouvement, tolérance aux pannes et stockage de données inaltérable

Contrôles d'accès : authentification multifacteur (MFA), contrôle d'accès basé sur les rôles (RBAC), quorum, audit et surveillance continue

Détection et analyse : détection d'anomalies, détection des menaces en temps quasi réel, classification des données et analyse comportementale adaptative

Intégrations de sécurité : SIEM (gestion des informations et des événements liés à la sécurité), SOAR (orchestration, automatisation et réponse aux incidents de sécurité informatique), gestion des identités, solutions de détection des menaces, gestion des vulnérabilités et API (Interface de programmation d'applications)

Résilience des données : assurer l'intégrité et la disponibilité des données de la plateforme

Chiffrement des données au repos et en mouvement

Cohesity chiffre toutes les données et tous les flux de données sur la plateforme. Le chiffrement empêche les utilisateurs non autorisés de consulter les données en dehors de la plateforme. Les données stockées dans la plateforme ne sont pas compréhensibles, sauf si un utilisateur autorisé y accède et les déchiffre. La plupart des réglementations relatives à la vie privée et à l'industrie, notamment le RGPD, le CCPA, la norme PCI et l'HIPAA, exigent que les entreprises protègent par chiffrement les PII, PCI et PHI. Les données de la plateforme sont chiffrées au repos à l'aide du chiffrement AES-256. La plateforme propose plusieurs options pour gérer les clés de chiffrement en toute sécurité : les entreprises peuvent utiliser le service de gestion de clés (KMS) de Cohesity, ou gérer les clés via le KMS d'Amazon Web Services ou d'autres fournisseurs tiers, notamment Thales, Fortanix et Entrust.

La plateforme de gestion des données de Cohesity utilise la norme TLS pour les données en transit. Le protocole TLS chiffre les données afin de garantir que les écoutes clandestines et les pirates informatiques ne puissent pas les voir entrer et sortir de la plateforme. C'est essentiel pour protéger les données privées et sensibles à des fins de sécurité et de conformité. Cohesity utilise les protocoles TLS 1.2 et mTLS pour la sécurité de la couche de transport, et uniquement des suites de chiffrement approuvées par le FIPS avec une protection PFS (Perfect Forward Secrecy).

Tolérance aux pannes

La plateforme de gestion des données de Cohesity tolère plusieurs défaillances du système pour assurer la haute disponibilité de la plateforme. Cela permet d'éviter les interruptions dues à un point de défaillance unique, et ainsi de répondre aux exigences en matière de SLA et de continuité des activités. Les clusters peuvent continuer à fonctionner malgré plusieurs défaillances de disques durs, de disques SSD, de nœuds, de châssis et de racks. Les clusters peuvent également supporter des pannes d'alimentation, de ventilateurs et de réseaux.

Données inaltérables

Les données sauvegardées par Cohesity ne changeront jamais de leur état sauvegardé jusqu'à ce qu'elles expirent. Cohesity SpanFS™ fournit des snapshots de sauvegarde inaltérables pour empêcher la modification ou la suppression des données. Grâce à son architecture hyperscale, Cohesity SpanFS peut stocker les données sauvegardées dans des snapshots inaltérables sur son système de fichiers sécurisé. Ces snapshots ne sont pas directement accessibles, et ne peuvent pas être montés depuis l'extérieur d'un cluster Cohesity. Les snapshots de sauvegarde sont stockés en mode lecture seule. Ainsi, aucune application externe ou utilisateur non autorisé ne peut les modifier.

Toute tentative d'écriture sur un snapshot de sauvegarde inaltérable est écrite sur des clones (gratuits), lesquels sont également mis en lecture seule à la fin de chaque cycle de protection. Lorsque le processus de restauration massive instantanée de Cohesity utilise une restauration basée sur un montage, la vue interne est d'abord clonée, puis exposée à l'environnement externe. La vue interne reste quant à elle inaccessible de l'extérieur. Lors de la sauvegarde, les écritures dans les vues internes ne sont autorisées que via des services internes de confiance et des API authentifiés. DataLock, la fonctionnalité WORM (Write Once Read Many) de Cohesity, peut être appliquée aux snapshots de Cohesity pour davantage de sécurité. Si DataLock est activé, personne, pas même les administrateurs, ne peut supprimer le snapshot de sauvegarde avant l'expiration de DataLock.

Contrôle d'accès : architecture Zero Trust

Voici la définition du Zero Trust donnée par le NIST (National Institute of Standards and Technology) : « Zero Trust (ZT) désigne un ensemble évolutif de paradigmes de cybersécurité qui déplacent les défenses des périmètres statiques basés sur le réseau pour se concentrer sur les utilisateurs et les ressources. » L'objectif du Zero Trust est de valider l'authenticité et l'autorisation des utilisateurs pour tout accès ou modification de la plateforme.

Authentification multifacteur (MFA)

L'authentification multifacteur (MFA) fournit une authentification forte des utilisateurs pour empêcher les modifications non autorisées des paramètres ou des données de la plateforme. Elle améliore la sécurité de la plateforme en obligeant les utilisateurs à utiliser plus qu'un nom d'utilisateur et un mot de passe pour s'identifier. Les mots de passe et les noms d'utilisateur sont sensibles aux attaques par force brute et peuvent être volés. L'authentification multifacteur oblige l'utilisateur à authentifier ses demandes de connexion à l'aide d'une réponse qu'il est le seul à pouvoir fournir (par exemple, une vérification par téléphone portable), ou d'un TOTP (mot de passe à usage unique basé sur le temps). Cohesity prend en charge l'authentification multifacteur (MFA) native ou celle de fournisseurs tiers, notamment Ping, Duo, Okta etc.

Contrôles d'accès basé sur les rôles (RBAC)

Le contrôle d'accès granulaire basé sur les rôles permet à une entreprise d'accorder aux utilisateurs le moindre privilège nécessaire pour qu'ils puissent satisfaire aux exigences de leur travail, ce qui minimise les risques et rend les zones hors de leurs responsabilités inaccessibles. Les entreprises peuvent restreindre les rôles d'un utilisateur de Cohesity à des applications, des capacités ou des flux de travail spécifiques dans la plateforme, limitant ainsi ses actions en fonction de son rôle et de ses responsabilités. Les entreprises peuvent, par exemple, restreindre certains utilisateurs à faire des sauvegardes ou de la recherche de données.

Quorum

Cohesity exploite le quorum (disponible dans la version 6.8) pour permettre aux entreprises d'empêcher les comptes administratifs de faire des modifications unilatérales de la plateforme, un contrôle crucial pour se protéger contre les erreurs involontaires des utilisateurs, les administrateurs malhonnêtes, ou les comptes compromis. Avec un quorum, plusieurs approbations sont nécessaires pour que les demandes des utilisateurs visant à modifier les paramètres ou les fonctions administratives soient autorisées.

Audit

La plateforme Cohesity conserve une piste d'audit utilisateur pour toutes les actions effectuées sur le cluster Cohesity. Ces enregistrements prouvent la conformité et l'intégrité opérationnelle. Les pistes d'audit peuvent également identifier les zones non conformes en fournissant des informations pour les enquêtes d'audit. Les journaux d'audit enregistrent les activités de connexion/déconnexion des utilisateurs, les modifications apportées aux données ou à leurs propriétés, et la planification des tâches. La plateforme organise les journaux par catégories, notamment Active Directory ou Cluster, pour les analyser rapidement.

Surveillance continue

La plateforme Cohesity permet de surveiller l'environnement afin de réduire le risque d'erreurs humaines et de mauvaises configurations. La surveillance fournit des analyses de l'environnement Cohesity, notamment un éventail de configurations de sécurité, et prend en compte une foule de facteurs comme le contrôle d'accès, les journaux d'audit et le cadre de chiffrement, qui jouent un rôle essentiel dans la protection de la sécurité du cluster de données.

Détection et analyse : l'IA et le ML pour détecter les activités malveillantes

Détection d'anomalies

La plateforme Cohesity analyse immédiatement les données provenant des environnements de production à chaque sauvegarde, pour détecter les signes révélateurs d'une activité inhabituelle ou de modifications des données. Une telle activité peut indiquer une attaque par ransomware. Un tableau de bord central signale les anomalies d'après le moment et la fréquence des lectures et des écritures de données, le caractère aléatoire des données et la façon dont les fichiers changent, notamment ceux qui sont ajoutés, supprimés et modifiés. La fonctionnalité de détection des anomalies de Cohesity permet aux entreprises de définir des alertes pour les conditions susceptibles d'indiquer un ransomware ou toute autre activité malveillante.

Détection des menaces en temps quasi réel

Les menaces visant la protection et la sécurité des données peuvent prendre la forme de différentes classes de logiciels malveillants. Les entreprises peuvent compléter leurs contrôles de sécurité par une analyse supplémentaire des données pour détecter les virus, les chevaux de Troie et autres logiciels malveillants afin de réduire les risques. Cohesity prend en charge l'analyse des données non structurées, ce qui permet aux entreprises d'effectuer de nombreuses analyses pour affiner la détection sans surcharger la production et les autres services en temps réel.

Classification des données

La prolifération des données désigne la multiplication des emplacements, ainsi que l'augmentation du volume et de la diversité des données dans les entreprises. Elle est également connue sous le nom de « fragmentation massive des données ». Face à cette prolifération, les entreprises ont besoin d'automatisation pour suivre les sources croissantes de données critiques et sensibles, afin de s'assurer que la couverture de la protection des données, de la sécurité, de l'analyse, de la gouvernance et de la confidentialité ne présente pas de lacunes.

Depuis le 2ème semestre 2022, la plateforme de données Cohesity permet aux entreprises de classer automatiquement leurs données afin qu'elles puissent découvrir, classer et étiqueter les informations sensibles, et s'assurer que les protections et les sauvegardes répondent aux exigences de conformité et de SLA. La classification basée sur l'IA met en lumière les données sensibles dans l'ensemble de l'entreprise pour créer des cartes de privilèges de données qui détaillent l'emplacement et la classification des données sensibles.

Ces stratégies prédéfinies permettent aux entreprises de répondre à leurs exigences mondiales et régionales en matière de RGPD, de CCPA, d'HIPAA et d'autres réglementations. Les entreprises peuvent en outre tirer parti de plus de 100 modèles prédéfinis pour créer des stratégies adaptées à leurs défis et besoins spécifiques.

Analyses comportementales adaptatives

Le comportement anormal d'un utilisateur et le paramétrage inapproprié de données peuvent augmenter le risque de fuite de données. La plateforme, qui devrait être opérationnelle au cours du premier semestre 2022, surveillera l'accès aux données et les journaux pour détecter toute activité ou utilisation inhabituelle des données susceptible d'indiquer des actions malveillantes. Par ailleurs, les données potentiellement surexposées peuvent être identifiées en analysant les ACL (listes de contrôle d'accès), dans lesquelles les données sensibles, notamment les PII, n'ont pas de restrictions d'accès appropriées. Cela permet aux équipes de protection et de sécurité d'être rapidement alertées en cas de comportement révélateur d'une attaque par ransomware ou d'une autre activité malveillante, et d'atténuer de manière proactive les risques pour les données causés par des paramètres d'accès faibles.

Intégrations de la sécurité : exploiter les outils existants pour détecter, répondre et corriger les problèmes

Il faut être nombreux pour garder les acteurs malveillants à distance. Presque toutes les entreprises possèdent des ensembles d'outils pour détecter les logiciels malveillants, les virus et les vulnérabilités, et ont créé des pratiques et des stratégies étendues pour valider que les ressources d'information peuvent être utilisées en toute sécurité. La plateforme Cohesity est donc conçue pour s'intégrer dans la stratégie de sécurité existante d'une entreprise. Elle permet par exemple d'assurer que l'authentification des utilisateurs et du chiffrement des données est mis en œuvre de façon cohérente, de compléter les solutions et processus de réponse et de gestion des incidents existants, et d'exploiter les solutions de détection des menaces et des vulnérabilités déjà en place. La plateforme de gestion des données de Cohesity peut ainsi prendre en charge et amplifier les stratégies et processus de sécurité de l'entreprise. Les intégrations englobent plusieurs catégories de sécurité, notamment SIEM et SOAR, la gestion des identités, la gestion des vulnérabilités et la détection des menaces, comme indiqué ci-après :

SIEM (gestion des informations et des événements liés à la sécurité)

Les entreprises utilisent le système SIEM pour obtenir une analyse en temps réel des alertes de sécurité générées par les applications et le matériel réseau. La plateforme de gestion des données de Cohesity génère des alertes en cas d'attaque par ransomware ou d'autres activités malveillantes. L'intégration de Cohesity et de Cisco SecureX permet aux entreprises d'automatiser leur réponse à ces alertes. Cela permet aux entreprises de regrouper sur une plateforme unique les informations sur les données compromises ainsi que d'autres renseignements généraux et informations contextuelles, de les mettre en corrélation, et donc d'accélérer les enquêtes et la réponse aux menaces de ransomware.

SOAR (orchestration, automatisation et réponse aux incidents de sécurité informatique)

Les technologies SOAR permettent aux entreprises de gérer la sécurité, d'automatiser les opérations de sécurité et de répondre aux incidents de sécurité. Les entreprises peuvent ainsi réagir rapidement et efficacement aux incidents, notamment lorsque la plateforme de gestion des données de Cohesity suspecte la présence d'un ransomware. Cohesity s'intègre à la solution Cortex XSOAR de Palo Alto Networks. Cette intégration permet aux équipes de sécurité et informatiques de détecter les attaques par ransomware et de prendre les mesures nécessaires pour rétablir la situation. La plateforme de gestion des données de Cohesity détecte les anomalies de données et les achemine vers XSOAR, qui traite et gère les incidents de manière automatisée, fournit des renseignements sur les menaces et détecte les logiciels malveillants.

Solutions de gestion des identités

De nombreuses entreprises utilisent couramment des solutions de gestion des identités pour authentifier les utilisateurs de façon très sécurisée. La plateforme de gestion des données de Cohesity prend en charge l'authentification multifacteur (MFA) native ou celle de fournisseurs tiers, notamment Ping, Duo, Okta etc.

Solutions de détection des menaces

La détection des menaces permet d'identifier les logiciels malveillants susceptibles d'être utilisés par des attaquants pour lancer des attaques par ransomware ou des cyberattaques, voler des données, ou prendre le contrôle des systèmes d'une entreprise. Cohesity exploite la détection des menaces pour analyser la plateforme avant ou après l'ingestion de données afin de détecter les logiciels malveillants. Cohesity a une prise en charge native via sa solution ClamAV.

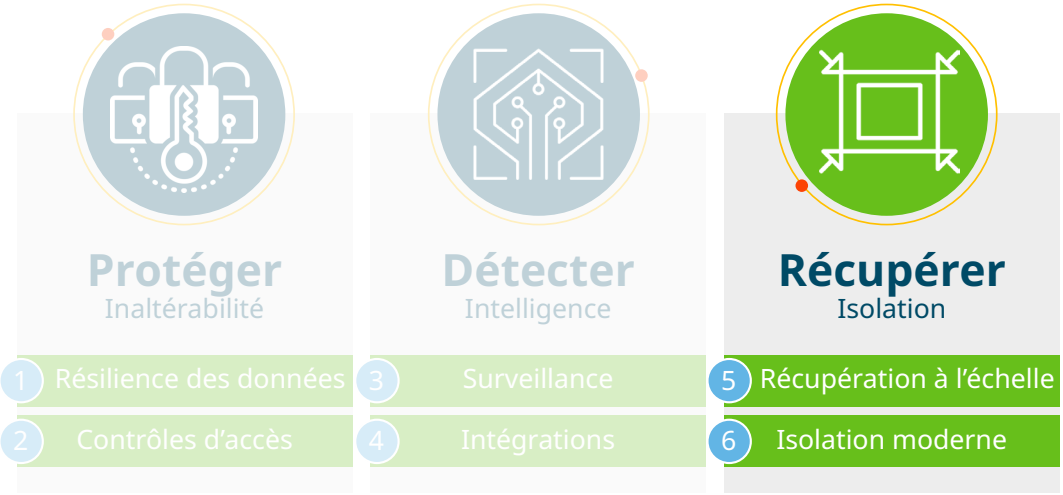
Gestion des vulnérabilités

La gestion des vulnérabilités donne un aperçu des risques potentiels posés par les applications, les navigateurs et les services logiciels. Les solutions classent ces vulnérabilités par catégories et par ordre de priorité pour permettre aux entreprises de réduire les risques de violations de données et de logiciels malveillants de type ransomware. Les entreprises peuvent s'appuyer sur la technologie de gestion des vulnérabilités de Tenable pour identifier les vulnérabilités des données et des environnements gérés par la plateforme de gestion des données de Cohesity. La solution Cohesity CyberScan optimisée par Tenable propose un tableau de bord détaillé qui donne une vue d'ensemble de toutes les cyber-expositions dans votre environnement de production et permet de réduire les risques. Comprendre les lacunes existant dans leur infrastructure permet aux entreprises de s'attaquer aux cyber-expositions et aux vulnérabilités critiques avant qu'elles ne soient exploitées.

API (Interface de programmation d'applications)

Outre les intégrations préconstruites mentionnées ci-dessus, la plateforme de gestion des données de Cohesity peut s'intégrer à toute solution de sécurité grâce à une API sécurisée mais ouverte. Les alertes, informations d'état et autres renseignements provenant de la plateforme Cohesity peuvent être exploités par des applications de sécurité tierces afin de répondre aux besoins spécifiques et aux défis opérationnels des entreprises. La liste des intégrations prêtes à l'emploi devrait donc évoluer au fil du temps en fonction de la demande des clients, mais sachez qu'il est possible de créer dès aujourd'hui des intégrations sur mesure pour répondre à vos besoins.

Récupération : récupérer instantanément les processus et fichiers essentiels de l'entreprise



Récupération à l'échelle : accélérer la récupération, soutenir les opérations 24 h/24, 7 jours sur 7, et respecter les SLA

Récupérer à l'échelle permet aux entreprises d'accéder immédiatement aux processus et données métier critiques pour atteindre leurs objectifs exigeants de délai de récupération (RTO). Tout d'abord, les modèles de ML (apprentissage automatique) de la plateforme permettent aux entreprises de trouver le dernier bon point de récupération connu et de lancer des recherches puissantes pour vérifier l'état de certaines instances de données. Ensuite, des snapshots entièrement hydratés permettent aux entreprises de récupérer instantanément des centaines de VM, des fichiers ou des bases de données de toute taille. Ce processus permet au personnel informatique de respecter les SLA de l'entreprise tout en économisant du temps et des ressources.

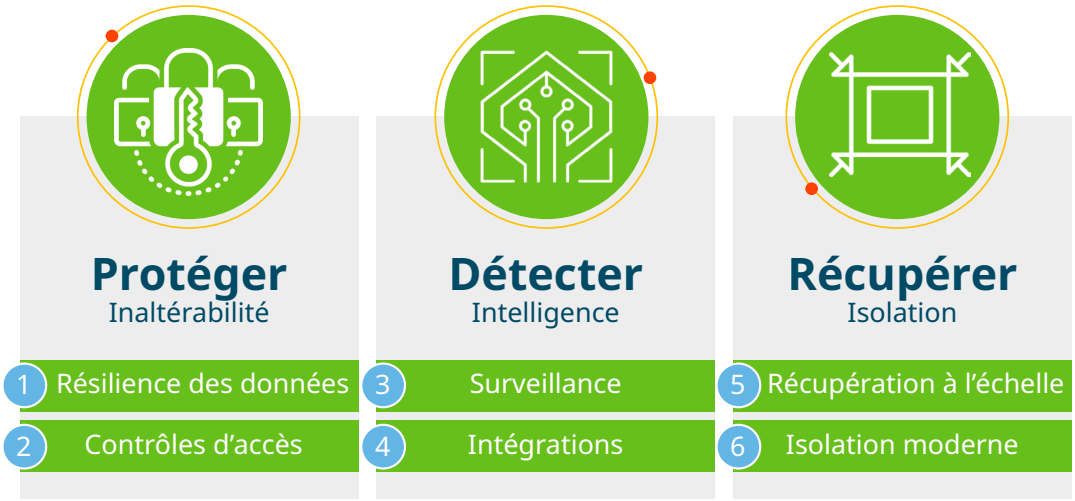
Et les entreprises peuvent accéder immédiatement aux fichiers et aux objets. Les entreprises peuvent accéder rapidement aux fichiers et aux objets avec Cohesity Smartfiles. Elles peuvent instantanément cloner la dernière bonne sauvegarde de leurs partages NAS et servir ces fichiers directement à partir du cluster Cohesity, ce qui permet de rétablir le service aux utilisateurs sans avoir à déplacer les données. Si les listes de contrôle d'accès ont été affectées, les entreprises peuvent également récupérer leurs données critiques à partir d'Active Directory (AD).

Isolation moderne : en cas de perte catastrophique des données de sauvegarde locales

Les entreprises devraient appliquer la règle du 3-2-1 recommandée par « Shields Up » pour les données de sauvegarde : 3 copies de données de sauvegarde complètes, 2 locales et 1 isolée. La copie isolée fournit une autre copie hors site des données de sauvegarde au cas où un événement catastrophique désactiverait les copies locales des données.

Il existe plusieurs façons d'isoler : l'isolation sur bande, l'isolation dans le cloud gérée par le client, ou l'isolation fournie par SaaS. Lorsque les exigences en matière de RTO et de RPO sont élevées, la plupart des entreprises ont recours à l'isolation dans le cloud ou via SaaS. Ces options offrent le meilleur équilibre entre récupération et isolation. Il n'est cependant pas question de choisir un seul mode d'isolation parmi les options disponibles. Il est possible d'en sélectionner plusieurs pour prendre en charge différents types de données, notamment les données de transaction ou la propriété intellectuelle essentiellement statique, le code source ou les secrets industriels.

Conclusion : ça n'est pas une option



Les capacités de Cohesity à protéger l'entreprise, détecter les actes malveillants et récupérer d'une attaque par ransomware forment une approche en couches pour sécuriser et augmenter la résilience des données et assurer une récupération rapide. Le chiffrement, l'inaltérabilité et les capacités WORM permettent de protéger les données de sauvegarde contre les modifications non autorisées. Les principes de Zero Trust permettent de contrôler et de gérer l'accès des utilisateurs de la plateforme grâce à un RBAC granulaire, à l'authentification multifacteur (MFA) et à une sécurité de niveau bancaire avec Quorum. L'outil de détection fournit des informations exploitables grâce à l'analyse des anomalies de données et du comportement des utilisateurs, ainsi qu'à la détection des menaces en temps quasi réel. Il est intégré aux contrôles existants afin de renforcer les défenses existantes contre les attaques par ransomware. La phase finale, la récupération, utilise une puissante récupération massive instantanée et un accès aux fichiers pour rétablir les processus métier et les données critiques.

La plateforme est pilotée par l'IA et le ML pour suivre l'évolution constante des menaces. Ces technologies fournissent des capacités essentielles pour garder une longueur d'avance sur les nouvelles menaces de sécurité, ce qui est impossible à faire avec des processus manuels.

Les ransomware et autres menaces ont placé la gestion des données au premier plan de la sécurité et de la cyber-résilience. Les entreprises qui ne disposent pas d'une plateforme de gestion des données renforcée, intelligente et intégrée pour résister aux cyberattaques, les déjouer et reprendre leurs activités, risquent de subir des pertes de données catastrophiques et des interruptions d'activité.

Sources :

1 https://blog.sonicwall.com/en-us/2021/10/cyber-threat-alert-ransomware-breaks-another-record/

2 https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

À propos de Cohesity

Cohesity simplifie radicalement la gestion des données. Nous simplifions la protection, la gestion et la valorisation des données dans les centres de données, à la périphérie et dans le cloud. Nous offrons une suite complète de services consolidés sur une plateforme de données multicloud : sauvegarde et récupération, reprise après sinistre, services de fichiers et d'objets, dev/test, conformité, sécurité et analyse des données. Cela permet de réduire la complexité et d'éliminer la fragmentation massive des données. Cohesity est disponible en tant que service, en mode autogéré, ou peut être fourni par un partenaire utilisant Cohesity.

Visitez notre site Web et notre blog, suivez-nous sur Twitter et LinkedIn, et abonnez-vous à notre page Facebook.

2000044-002-FR 8-2022