CYBER RÉSILIENCE MANUEL

Commvault®

APERÇU

À l'ère du numérique, où les cybermenaces sont de plus en plus sophistiquées et omniprésentes, il est essentiel d'être préparé à la reprise après un cyber-événement.

Des stratégies efficaces de reprise après sinistre sont essentielles pour lutter contre ces menaces et permettre à votre entreprise de restaurer rapidement les systèmes et données critiques après un incident informatique, réduisant ainsi les temps d'arrêt et l'impact sur les opérations commerciales. En étant prêtes à affronter la cybersécurité, les entreprises démontrent à leurs clients, à leurs parties prenantes et aux organismes de réglementation qu'elles prennent au sérieux la protection des données sensibles et des systèmes qui respectent leurs engagements envers leurs clients.

De plus, la préparation à la reprise après sinistre est essentielle pour se conformer aux diverses exigences réglementaires qui dictent la manière dont les données doivent être gérées et protégées (notamment le RGPD, la HIPAA, la CCPA et d'autres lois sur la confidentialité propres à chaque État). En outre, de nombreux secteurs sont soumis à des réglementations strictes, telles que DORA pour les organismes de services financiers basés dans l'UE et PCI-DSS pour les détaillants qui acceptent les cartes de paiement, qui les obligent à mettre en place des plans détaillés de cybersécurité, de résilience, de reprise après sinistre et de continuité des activités. Le non-respect de ces règles peut entraîner de lourdes amendes, des répercussions juridiques et la perte des licences d'exploitation.

Au-delà des obligations de conformité, un plan de reprise d'activité bien structuré réduit le risque de perte de données, garantissant que les informations critiques telles que les coordonnées des clients, les données propriétaires et la propriété intellectuelle restent protégées. En cas de compromission des données, un mécanisme de récupération rapide permet de restaurer rapidement l'intégrité des informations et la capacité opérationnelle.

LE COMMVAULT +
LE RAPPORT GIGAOM SOULIGNE
LE BESOIN CRITIQUE DE
CYBER-INFORMATION COMPLÈTE
STRATÉGIES DE RÉCUPÉRATION.

Lisez la suite pour en savoir plus sur le noyau composants nécessaires pour être prêt à faire face à une cyberattaque - et découvrez comment Commvault® Cloud offre la
des outils pour vous aider à réussir.

ÉTAPE #01

IDENTIFIER

Un principe clé de toute stratégie est une visibilité approfondie de l'environnement.

Avec Commvault Cloud, vous avez la possibilité de découvrir, classer et surveiller les données sensibles dans tous vos magasins de données. La classification des données peut ensuite déclencher des politiques de protection et aider les organisations à identifier les éléments les plus critiques et ceux qui nécessitent un niveau de protection différent.

Une fois que vous connaissez les éléments à protéger, vous pouvez équiper l'environnement de mécanismes de détection des menaces, de détection des anomalies et d'alerte précoce pour alerter les équipes de sécurité des menaces dans vos réseaux avant qu'elles ne causent des dommages.

Vous avez également besoin d'une approche à plusieurs niveaux pour rechercher et arrêter les logiciels malveillants, les ransomwares et autres vecteurs de corruption des données.
Les données doivent être inspectées à tous les points de leur cycle de vie pour trouver des données corrompues afin que vous puissiez les restaurer à un moment précis.

PRODUITS CLOUD COMMVAULT
POUR AIDER À IDENTIFIER LES MENACES :

- Analyse des risques pour la découverte et le contrôle des données sensibles
- Threatwise™ pour la détection des menaces et des anomalies et l'alerte précoce
- Analyse des menaces pour identifier les données malveillantes ou corrompues

PLATEFORME CLOUD COMMVAULT
CAPACITÉS :

- Validation du point de nettoyage

ÉTAPE #02

PROTÉGER

Pour être prêt à faire face à une attaque inévitable, vous devez protéger vos données contre les actions des attaquants, des initiés malveillants et même des mauvaises configurations ou des pannes.

Cette protection est multidimensionnelle et doit prendre en compte les données elles-mêmes, l'identité et les configurations. En commençant par les données, les bonnes pratiques imposent aux organisations de suivre la règle 3-2-1 : trois copies des données, sur deux types de supports (ou sur deux plateformes différentes), et une copie impossible à modifier. La duplication des données pour les deux premières étapes est simple, mais la troisième est un peu plus difficile. Il faut un mécanisme pour rendre les données immuables et indélébiles afin de les protéger contre les modifications ou suppressions unilatérales. Cela est particulièrement important pour deux raisons : la majorité des ransomwares disposent de mécanismes pour altérer les sauvegardes, et les menaces internes sont réelles.

Vous devez vérifier que votre infrastructure (cloud et sauvegarde) est configurée selon les principes de la confiance zéro. Des mécanismes doivent être en place pour vérifier les configurations et signaler et alerter sur les changements ou les « dérives ».

L'authentification doit également suivre les principes de confiance zéro et inclure une autorisation multifacteur et multi-personnes, en fonction des niveaux d'accès et des actions effectuées.

En plus de cela, tout mécanisme que vous avez mis en place pour valider l'identité, tel qu'Active Directory ou Entra ID, doit également être configuré, sauvegardé et surveillé pour détecter les modifications telles que les ajouts, les suppressions ou l'élévation des privilèges.

Toutes les données, configurations ou plans de contrôle doivent être sauvegardés pour permettre leur restauration en cas d'incident de sécurité, et les sauvegardes doivent être isolées et isolées pour aider à réduire la probabilité que des attaquants trouvent les sauvegardes lors d'une reconnaissance ou qu'elles soient supprimées ou cryptées par un logiciel malveillant ou un ransomware.

PRODUITS CLOUD COMMVAULT QUI VOUS AIDENT À PROTÉGER VOS DONNÉES :

- Sauvegarde et récupération dans le cloud, sur site et Charges de travail SaaS
- Sauvegarde et enregistrement Active Directory Récupération pour protéger l'actif Répertoire et identifiant Entra
- Air Gap Protect pour un stockage immuable, indélébile et déconnecté
- Analyse des menaces pour identifier et mettre en quarantaine les données malveillantes ou corrompues

PLATEFORME CLOUD COMMVAULT CAPACITÉS :

- Security IQ pour la gestion de la posture de sécurité de votre environnement de sauvegarde
- Contrôle d'accès basé sur les rôles (RBAC) et autorisation multi-personnes

ÉTAPE #03

RÉPONDRE

Aucune technologie ne vous sera utile dans un espace isolé.

C'est pourquoi Commvault Cloud s'intègre aux logiciels de gestion des informations et des événements de sécurité (SIEM) et aux plateformes d'orchestration, d'automatisation et de correction de la sécurité (SOAR).

Cela permet le partage de contexte entre Commvault Cloud et d'autres outils de sécurité pour mieux détecter les événements de sécurité, les problèmes d'intégrité des données et les activités anormales.

Que vous utilisiez la plateforme Palo Alto Networks XSOAR, Splunk SIEM, Microsoft Sentinel ou un autre outil, la détection des menaces et des anomalies de Commvault Cloud est un multiplicateur de force pour renforcer la cyber-résilience et améliorer la réponse aux incidents.

Lorsque Commvault Cloud détecte des fichiers suspects ou reçoit une alerte d'anomalie d'une intégration, ce fichier peut être automatiquement mis en quarantaine à partir de vos données de production et une copie peut être envoyée à un Sandbox pour détonation et analyse afin de déterminer s'il est malveillant.

PLATEFORME CLOUD COMMVAULT
DES CAPACITÉS QUI VOUS AIDENT
RÉAGISSEZ PLUS RAPIDEMENT AUX MENACES :

- Intégrations de l'écosystème de sécurité avec SIEM et Technologies SOAR
- Intégrations de renseignements sur les menaces pour une couverture plus large des menaces
- Intégrations Sandbox pour permettre l'inspection et la détection de fichiers suspects

ÉTAPE #04

RÉCUPÉRER

Lorsqu'il s'agit de récupérer des données, que ce soit à la suite d'une catastrophe ou d'une cyberattaque, vous avez besoin d'un plan qui a été mis en pratique et documenté, de données propres et complètes, d'une flexibilité des cibles de restauration, de la capacité de tout restaurer, des données à l'application qui les utilise, et de la rapidité.

Le pire moment pour se rendre compte que votre plan de reprise ne fonctionnera pas est lorsque vous êtes confronté à une attaque. Il est essentiel de réaliser régulièrement des tests de plans de reprise complets pour savoir si vous pouvez effectuer la reprise en cas de besoin et pour aider les équipes chargées de la reprise à savoir ce qui leur est demandé.
Ces tests ou pratiques du processus de récupération doivent vérifier l'intégrité des données et être capables de restaurer les données et de reconstruire les applications dans un nouvel environnement.

La portabilité est importante pour les tests et la récupération, car une attaque ou une panne peut vous obliger à déplacer des charges de travail entières vers un environnement nouveau et différent.
Cela peut impliquer un simple changement de compte ou être aussi radical que le passage d'un environnement sur site au cloud, voire à un autre cloud. Votre récupération doit donc être hybride et flexible.

Nous avons déjà évoqué la nécessité d'analyser et de surveiller les données pour détecter les anomalies, les logiciels malveillants et autres défauts. Au moment de la restauration, il est important d'effectuer une dernière vérification des données pour valider qu'elles sont propres, prêtes à être restaurées et qu'elles ne vont pas simplement réinfecter votre environnement.

Enfin, après une récupération, vous devrez conserver une copie des données et des systèmes affectés par l'attaque afin de la fournir aux équipes d'enquête et de réponse aux incidents de tiers, aux forces de l'ordre, aux cyberassureurs ou à d'autres parties intéressées. Cette copie médico-légale doit être conservée séparément de votre environnement de production et conservée telle quelle pour vos enquêtes. Cela peut aider à la rétro-ingénierie des logiciels malveillants, à l'identification de l'attaquant et à l'identification des techniques et procédures à affronter à l'avenir.

PRODUITS CLOUD COMMVAULT
QUI VOUS AIDENT À RÉCUPÉRER :

- Récupération en salle blanche pour les tests de récupération, la validation et l'analyse médico-légale
- Analyse des menaces pour valider cela les fichiers récupérés sont propres et exempts de logiciels malveillants, de ransomwares et de corruption
- Cloud Rewind pour reconstruire applications sur différents clouds, du code aux données
- Récupération d'Active Directory pour la continuité de l'identité même face à une cyberattaque

PLATEFORME CLOUD COMMVAULT
CAPACITÉS :

- Cloudburst Recovery pour une récupération rapide à l'échelle du cloud, disponible lorsque vous en avez besoin
- Validation du point de nettoyage pour fournir un point de nettoyage connu dans le temps pour vous permettre de restaurer

ÉTAPE #05

MONITEUR

Toute votre planification et votre préparation ne fonctionnent que si vous avez instrumenté votre environnement pour alerter les opérations de sécurité et les équipes informatiques des anomalies ou des événements survenant dans votre infrastructure.

La surveillance des menaces qui ont infiltré votre organisation et tentent d'échapper à la détection est essentielle pour minimiser les dommages qu'elles peuvent causer. Plus tôt vous en serez informé, plus tôt vous pourrez les éliminer et restaurer les données affectées.

Le problème de la surveillance est que de nombreux outils informatiques déclenchent des centaines ou des milliers d'alertes, ce qui génère beaucoup de bruit à partir de faux positifs. Cela conduit les équipes d'opérations de sécurité à s'engager dans des enquêtes qui ne mènent à rien, ce qui provoque un épuisement et une lassitude face aux alertes, et fait perdre du temps aux enquêtes sur les menaces réelles. Il est essentiel de régler les systèmes pour qu'ils n'alertent que pour les véritables attaques afin d'aider les équipes à se concentrer et à trouver les véritables menaces.

Les données de production et de sauvegarde doivent être surveillées en permanence pour détecter les modifications, les anomalies et les programmes malveillants afin de détecter les menaces plus tôt, de minimiser le risque d'infection supplémentaire et de restaurer les données vers des données connues comme propres. Cela inclut la possibilité d'examiner les comportements des fichiers, pas seulement le contenu, afin de pouvoir détecter des attaques jamais vues auparavant.

Vous pouvez également bénéficier de la consolidation de toute la surveillance sur une seule plateforme – dans la plupart des cas, un outil SIEM ou SOAR qui est surveillé en permanence par le personnel des opérations de sécurité et utilisé pour coordonner les enquêtes et les réponses.

PRODUITS CLOUD COMMVAULT QUI PERMETTENT UNE CONTINUITÉ SURVEILLANCE:

- Threatwise™ pour la détection des attaquants effectuant des reconnaissances et des pièges qui fournissent des alertes de haute fidélité en cas de violation
- Analyse des menaces en continu analyse des données et des fichiers de sauvegarde à la recherche de logiciels malveillants
- Analyse des menaces Prédire pour découvrir les menaces zero-day ou Attaques polymorphes pilotées par l'IA

PLATEFORME CLOUD COMMVAULT CAPACITÉS :

- Intégrations de l'écosystème de sécurité pour ajouter des niveaux encore plus élevés de renseignements sur les menaces provenant de fournisseurs tiers

RÉSUMÉ

En résumé, vous devez être conscient des risques que vos données présentent pour votre organisation.

1. Investissez dans une protection, une détection et une surveillance avancées des outils pour améliorer la capacité de votre organisation à détecter et à répondre rapidement aux cybermenaces.

2. Élaborer et maintenir à jour un plan de réponse aux incidents, décrivant clairement les rôles, les responsabilités et les procédures à suivre en cas de violation.

3. Exécutez des tests complets pour valider que vous avez couvert plusieurs scénarios et que vous pouvez récupérer complètement.

4. Surveillez vos systèmes et vos sauvegardes afin d'être sûr qu'ils sont propres et prêts lorsqu'ils sont nécessaires.

Pour découvrir comment Commvault Cloud peut vous aider avec la partie technologique du puzzle de la cyberpréparation, demandez une démonstration et une consultation avec nos experts en préparation et en récupération.