Commvault

GUIDE DE L'ACHETEUR

Aligner les plans de protection et de récupération contre les ransomwares sur les capacités critiques

L’évolution de l’entreprise et la menace des ransomwares

Les organisations sont confrontées à un environnement de données de plus en plus perturbé en raison d’un certain nombre de facteurs allant de l’augmentation des emplois hybrides et distants à la prolifération croissante des données en passant par la montée de cybermenaces sophistiquées. Les dommages causés par la cybercriminalité devraient se chiffrer à 10 500 milliards de dollars par an d’ici 2025.[1] Les entreprises ont besoin de solutions sur mesure qui vont au-delà des sauvegardes et des restaurations traditionnelles pour parvenir à une véritable cyber-résilience dans le monde hybride. Elles permettent aux entreprises non seulement de sécuriser leurs données, mais également d’anticiper de manière proactive les risques potentiels, d’atténuer les préjudices subis et de se rétablir rapidement face aux difficultés. En retour, les organisations peuvent réduire leur exposition globale aux risques et gérer efficacement les coûts.

10 500 MILLIARDS DE DOLLARS

par an d’ici 2025.[1]

Il semble évident que les anciennes méthodes ne font plus leurs preuves. Les organisations s’orientent vers une nouvelle approche de la sécurité des données basée sur des cadres à plusieurs niveaux qui fournissent des défenses actives, ainsi que sur une automatisation qui offre le meilleur modèle de protection et de récupération contre les attaques par ransomwares.

L’OBJECTIF DE CE GUIDE

Utilisez ce guide pour cartographier vos capacités actuelles de protection et de récupération contre les ransomwares et déterminer la meilleure façon d’optimiser votre plan de préparation dans les environnements de charge de travail hybrides, cloud ou SaaS.

1 Cybersecurity Ventures, Steven C. Morgan, Cybercrime to Cost The World 8 Trillion Annually In 2023, octobre 2022

Cadre de cybersécurité du NIST (National Institute of Standards and Technology)

01 **IDENTIFIER :** développer une compréhension de l'organisation pour gérer les risques de cybersécurité pour les systèmes, les personnes, les actifs, les données et les capacités.

02 **PROTÉGER :** assurer la fourniture des services critiques en développant et en mettant en œuvre des garanties appropriées.

03 **SURVEILLER :** définir des procédures continues pour savoir identifier la survenue d'un événement de cybersécurité.

04 **RÉPONDRE :** mettre en œuvre des activités appropriées pour se prémunir contre un incident de cybersécurité connu.

05 **RESTAURER :** élaborer et mettre en œuvre des activités appropriées pour préserver des plans de résilience et restaurer l'ensemble des capacités ou services qui ont été altérés en raison d'un incident de cybersécurité.

Pour contribuer à renforcer la résilience de votre infrastructure de données, la version 1.1 du cadre de cybersécurité du NIST recommande la mise en place de cinq piliers principaux pour instaurer un programme de cybersécurité global performant.

Pour gérer efficacement les risques de cybersécurité dans un paysage en constante évolution, le NIST a rédigé une version mise à jour du cadre : CSF 2.0. Prévue pour une sortie début 2024, cette version mise à jour introduit le sixième pilier, Gouverner, lequel réorganise les éléments de gouvernance des cinq piliers existants et met l'accent sur la cybersécurité comme source majeure de risque pour l'entreprise.

Dans chaque section de ce guide, nous expliquons pourquoi chaque niveau de sécurité est essentiel et passons en revue les fonctionnalités clés à intégrer dans votre solution de protection et de récupération contre les ransomwares.

01 IDENTIFIER

Dans un monde hybride, savoir exactement où et comment les données critiques sont utilisées n'est pas un mince défi. Des outils de sécurité des données efficaces doivent vous procurer une visibilité sur l'ensemble de votre environnement de données afin de mieux identifier les zones de risque et d'éliminer les angles morts. Ils sécurisent à la fois les données et les sauvegardes grâce à une architecture Zero Trust qui comprend des protocoles de sécurité intégrés pour sécuriser les données, empêcher les accès non autorisés et assurer la conformité face à l'évolution des cybermenaces. En cas d'attaque réussie, un contrôle intégral aide les organisations à prendre de meilleures décisions en matière de données avant, pendant et après une cyberattaque.

IDENTIFIER ÉLÉMENTS ESSENTIELS	EXIGENCES PAR RAPPORT AUX RANSOMWARES	CAPACITÉS DE COMMVAULT
Informations sur la protection des données	Analyse et identification automatiques des problèmes avec recommandation d'actions pour traiter les questions de sécurité.	Alertes, résumés et recommandations en temps réel basés sur l'IA dans Commvault® Cloud.
Évaluation de sécurité automatisée	Utilisez des ensembles d'outils interactifs pour évaluer rapidement la posture de sécurité et appliquer des recommandations pour améliorer la sécurité.	Prenez des mesures proactives avant que les attaques ne puissent générer des dommages ou se propager grâce à des tableaux de bord complets qui fournissent des informations détaillées sur tous les aspects de la sécurité des données.
Évaluation automatisée de l'état des sauvegardes	Vérifiez que les sauvegardes s'effectuent correctement.	Les mesures effectuées sur le cloud et sur site fournissent des rapports réguliers à ce sujet.
Rapports et tableaux de bord sur la gestion des données	Visualisez rapidement l'état de préparation à la sauvegarde et à la récupération. Rapports et tableaux de bord personnalisés pour des sujets d'intérêt spécifiques.	Des tableaux de bord unifiés et des rapports étendus permettent de préparer la récupération à l'aide de KPI détaillés.
Audit	Suivi des modifications des données, y compris des personnes les ayant consultées et de leurs dates de modification.	Effectuez un audit des connexions liées à des utilisateurs et des adresses IP spécifiques. Surveillez toutes les modifications de configuration et les événements de sauvegarde et de restauration dans des pistes d'audit détaillées.
Détournement des menaces	Interceptez les attaques avant qu'elles n'atteignent leurs cibles.	Threatwise™ fournit des outils différenciés pour détecter les menaces Zero Day et inconnues dans les environnements de production, et ainsi aider les clients à repérer les cybermenaces sophistiquées avant toute corruption de leurs données.
Analyse des risques	Identifiez et examinez les données sensibles et à risque afin de réduire l'exposition et l'exfiltration des données.	• Identifiez, catégorisez et classifiez les informations sensibles, telles que les données personnelles et financières, pour prioriser les mesures de sécurité et réduire l'exfiltration de données en cas de violation. • Prenez des mesures proactives pour garantir la conformité aux réglementations et réduire les coûts de stockage en archivant les données obsolètes (ROT). • Safe Search & Share exploite l'IA pour identifier rapidement les données et les relations sensibles au sein de vastes ensembles de données, garantissant ainsi que seules les bonnes informations sont partagées avec les bonnes personnes.
Analyse des menaces	Identifiez et examinez les anomalies au niveau des fichiers pour vous assurer de récupérer des données correctes et éviter la réinfection par des logiciels malveillants.	• Identifiez les menaces de logiciels malveillants pour éviter une réinfection pendant la récupération. • Threat Scan analyse les données de sauvegarde pour trouver les fichiers cryptés ou corrompus, garantissant ainsi aux utilisateurs la récupération rapide de versions fiables de leurs données. • Threat Scan Predict ajoute une technologie de prédiction en temps réel axée sur l'IA pour découvrir les menaces exercées par des ransomwares pilotés par l'IA.

02 PROTÉGER

En comprenant bien votre environnement de données, vous pouvez commencer à réduire votre surface d'attaque pour limiter les menaces potentielles et empêcher une propagation systémique. Protégez-vous contre les accès indésirables en préservant les données contre les modifications provenant de l'intérieur et de l'extérieur à l'aide d'une architecture Zero Trust. Vous pouvez isoler et segmenter les réseaux, appliquer une technique d'isolement des données pour confiner et sécuriser des copies de sauvegarde, mais également intégrer une technologie de détournement des cybermenaces pour intercepter ces dernières avant la fuite, le chiffrement et l'exfiltration de données. Des attaques par ransomwares peuvent se produire lorsque des informations d'identification sont compromises ou que les informations d'identification d'un utilisateur autorisent un accès privilégié à des systèmes auxquels il n'aurait normalement pas dû avoir accès. Assurez-vous que des protocoles de sécurité conformes aux normes de l'industrie sont en place pour chiffrer et sécuriser les données afin de réduire l'impact d'une attaque par ransomware.

PROTÉGER ÉLÉMENTS ESSENTIELS	EXIGENCES PAR RAPPORT AUX RANSOMWARES	CAPACITÉS DE COMMVAULT
Immuabilité	Protégez les données de sauvegarde des modifications non autorisées.	• Protection anti-ransomware pour les systèmes Windows et Linux. • Appliquez des verrous de stockage sur site et dans le cloud – personnalisez-les pour répondre aux besoins de l'entreprise. • Activez WORM (Write Once, Read Many - écriture unique, lecture multiple) pour empêcher les modifications non autorisées et la technologie d'isolement des données sur le cloud pour mieux vous protéger contre les menaces par ransomware.
Renforcement des infrastructures	Réduisez l'exposition aux menaces sur l'infrastructure de sauvegarde.	Le logiciel Commvault® a été testé et validé comme étant capable de renforcer le niveau 1 du Center for Internet Security (CIS). La conformité aux contrôles de sécurité CIS de niveau 1 est disponible sous forme d'une machine virtuelle CIS pré-renforcée (déployée via OVA) ou sous forme d'une appliance matérielle comme HyperScale X™. Tous les composants secondaires, y compris CommServe, les agents multimédias et les nœuds d'accès, peuvent également être renforcés jusqu'au niveau CIS 1.
Authentification et autorisation	Contrôlez les personnes disposant d'un accès et leur niveau d'accès tout en ajoutant plusieurs niveaux d'autorisation pour garantir une sécurité supplémentaire.	• Les contrôles d'accès basés sur les rôles limitent l'utilisation non autorisée ainsi que les fournisseurs d'identité SAML (Security Assertion Markup Language) et OATH pour fournir une couche de sécurité supplémentaire. • Intégration avec Active Directory et LDAP. • Contrôles d'authentification multifacteur et multipersonne pour les verrous de rétention et autorisation des commandes afin de protéger les données des accidents et d'éviter les actions destructrices. • Intégration avec la gestion des accès privilégiés et des outils améliorés de gestion des identités et des accès tels que CyberArk, Yubikey et la biométrie pour une meilleure authentification et sécurité des utilisateurs (AAL3). • Intégration juste à temps avec CyberArk pour minimiser le risque lié aux informations d'identification stockées. • Chiffrement des données de bout en bout tout en permettant aux plates-formes de gestion de clés externes de gérer et de contrôler les clés, et authentification par certificat, afin de se protéger contre l'accès malveillant aux données. • Logiciel WORM (verrouillage de rétention) • Locations multiples

02 PROTÉGER

PROTÉGER ÉLÉMENTS ESSENTIELS	EXIGENCES PAR RAPPORT AUX RANSOMWARES	CAPACITÉS DE COMMVAULT
Chiffrement	Mettez en œuvre des normes de chiffrement qui répondent aux directives de l'industrie.	Normes et outils pour gérer efficacement les clés de chiffrement pour la sauvegarde et la restauration dans Commvault : • Module de chiffrement des normes fédérales de traitement de l'information • Gestion des clés intégrée • Intégration avec la gestion des clés tierce • Système de gestion des clés par phrase secrète
Protection du catalogue de sauvegarde	Garantissez une protection immuable dans plusieurs secteurs, qu'il s'agisse de copies locales sur site ou dans le cloud.	• Forte protection contre les ransomwares pour les copies locales. • Sauvegarde sur Air Gap Protect ou sur un cloud tiers.
Isolation/isolation physique	Segmentez et isolez les données des réseaux externes et garantissez une récupération rapide en cas d'attaque.	• Air Gap Protect utilise l'isolation physique pour confiner et protéger les données sensibles. • Les applications HyperScale X sont dotées de commandes intégrées d'isolation physique des données. • Topologies de réseau : utilisez une topologie unidirectionnelle ou proxy.
Protection Active Directory	Créez la possibilité de protéger et de restaurer Active Directory, de sauvegarder les attributs des objets et d'effectuer des sauvegardes complètes, différentielles, incrémentielles et synthétiques.	La plateforme Commvault Cloud offre une protection Active Directory isolée sur site et basée sur le cloud.
Stratégie de sauvegarde 3-2-1	Créez une stratégie de sauvegarde efficace qui garantit la disponibilité constante des données. Disposez d'au moins trois copies des données, dont deux locales mais situées à des endroits différents, et une placée hors site.	• Configurez des copies illimitées de données sur site ou dans plusieurs points terminaux sur le cloud. • Air Gap Protect offre la possibilité d'activer un stockage isolé sur le cloud.
Détournement des menaces	Détectez les attaques par ransomwares le plus tôt possible, avant la fuite, le chiffrement, l'exfiltration ou la destruction de données.	• Couvrez votre surface en déployant en masse des capteurs de menaces (leurres). • Imitez les actifs critiques avec des capteurs préconfigurés. • Émulez des actifs hautement spécialisés uniques à votre environnement.
Contrôles de sécurité à la demande	Veillez à la conformité et au contrôle à l'aide de politiques de rotation des mots de passe qui n'ont aucun impact sur la protection des sauvegardes.	Améliorez votre posture de sécurité avec un contrôle Zero Trust et supprimez les informations d'identification compromises. L'intégration de CyberArk permet la récupération des informations d'identification juste à temps, y compris le stockage et la gestion sécurisés des informations d'identification au sein de CyberArk.

03 SURVEILLER

Les organisations touchées par une menace de sécurité peuvent même ne pas se rendre compte qu'elles ont été attaquées jusqu'à ce qu'il soit trop tard et que la violation devienne hors de contrôle. Il est donc essentiel de veiller à ce que des outils appropriés soient mis en place pour obtenir rapidement des informations sur un événement de cybersécurité afin de contenir une attaque par ransomware avant qu'elle n'affecte plus largement une infrastructure. En mettant en place un système d'alerte précoce de nouvelle génération et une surveillance approfondie, vous pouvez détecter et neutraliser les menaces de type Zero Day et internes afin de défendre vos données. Détectez, détournez et signalez les activités malveillantes le plus tôt possible afin de réduire les efforts de récupération.

SURVEILLER ÉLÉMENTS ESSENTIELS	EXIGENCES PAR RAPPORT AUX RANSOMWARES	CAPACITÉS DE COMMVAULT
Surveillance de la sécurité avec l'IA	Utilisez l'IA pour surveiller les cadres défaillants qui prennent en charge les sauvegardes des machines virtuelles et les applications SaaS. Elle offre une visibilité granulaire sur les activités inhabituelles des fichiers en utilisant une piste d'audit pour identifier les événements de sécurité potentiels.	Exploitez le potentiel de l'IA pour : • Effectuer des récupérations propres, rapides et sécurisées tout en réduisant les faux positifs grâce à l'IA/apprentissage automatique. • Surveiller les sauvegardes et analyser les événements et leur évolution pour déterminer leur statut (réussite, attente ou échec). • Prévoir la future conformité aux SLA grâce à une analyse des tendances en matière de sauvegardes.
Surveillance du système	Surveillance des charges de travail et des infrastructures critiques.	• Identifiez les anomalies liées aux modifications des caractéristiques des fichiers dues à la corruption, au chiffrement ou aux fichiers malveillants dans les données en direct et de sauvegarde. • Découvrez les nouvelles menaces par ransomware de type Zero Day et basées sur l'IA.
Surveillance des journaux	Recherchez des événements de journal spécifiques pour surveiller l'activité de ce dernier dans votre environnement. Recherchez un événement particulier parmi tous les événements du journal indexés sur le tableau de bord. Recherchez les événements de journal associés à un client, un fichier journal, un modèle ou une stratégie de surveillance spécifique.	La plateforme Commvault Cloud vous permet de surveiller les conditions des fichiers journaux et les événements Syslog et Windows de manière granulaire.
Sensibilisation aux menaces	Obtenez de manière proactive un aperçu immédiat des menaces actives et latentes	• N'exposez les capteurs qu'aux acteurs malveillants ; ils restent invisibles pour les utilisateurs et les systèmes autorisés. • Obtenez des informations essentielles sur les activités et les stratégies. • Éliminez les faux positifs et la fatigue liée aux alertes. • Incitez les acteurs malveillants à utiliser de fausses ressources.
Honeypots (leurres informatiques) et activité des fichiers en direct	Surveillez les actifs exposés au risque de ransomware et identifiez les points de récupération propres.	Surveillez les fichiers suspects en direct pour détecter les menaces et protéger les sauvegardes afin de garantir une récupération propre des fichiers et d'éviter leur réinfection.

03 SURVEILLER

SURVEILLER ÉLÉMENTS ESSENTIELS	EXIGENCES PAR RAPPORT AUX RANSOMWARES	CAPACITÉS DE COMMVAULT
Sensibilisation aux menaces	Obtenez de manière proactive un aperçu immédiat des menaces actives et latentes.	• N'exposez les capteurs qu'aux acteurs malveillants ; ils restent invisibles pour les utilisateurs et les systèmes autorisés. • Obtenez des informations essentielles sur les activités et les stratégies. • Éliminez les faux positifs et la fatigue liée aux alertes. • Incitez les acteurs malveillants à utiliser de fausses ressources.
Surveillance de la sécurité avec l'IA	Utilisez l'intelligence artificielle pour surveiller les cadres défaillants qui prennent en charge les sauvegardes des machines virtuelles et d'autres charges de travail, telles que les applications SaaS.	• Obtenez des informations sur les moments où les sauvegardes subissent des changements anormaux pour permettre une récupération propre, rapide et sécurisée. • Trouvez des versions propres des données pour effectuer une récupération propre, rapide et sécurisée. • Réduisez les faux positifs avec l'IA/apprentissage automatique.
Honeypots (leurres informatiques) et activité des fichiers en direct	Surveillez les actifs exposés au risque de ransomware et identifiez les points de récupération propres.	Surveillez les fichiers suspects en direct pour détecter les menaces et protéger les sauvegardes afin de garantir une récupération propre des fichiers et d'éviter leur réinfection.

04 RÉPONDRE

Une fois le ransomware détecté, vous devez immédiatement réagir. Obtenir des informations grâce à des outils de sécurité et des alertes proactives permet à votre organisation de protéger vos données. Des politiques documentées et un plan de réponse aux incidents aident à déterminer la suite des événements. La réponse doit être à la fois technique et commerciale, et chaque partie prenante doit, dans son propre domaine d'intervention, comprendre son rôle et les actions à entreprendre. La coordination et la communication entre les différentes équipes sont essentielles. L'essentiel est que les équipes de sécurité fassent tout ce qui est possible pour contenir et stopper la propagation tout en mettant en place les outils appropriés pour éviter toute réinfection potentielle.

RÉPONDRE ÉLÉMENTS ESSENTIELS	EXIGENCES PAR RAPPORT AUX RANSOMWARES	CAPACITÉS DE COMMVAULT
Intégration des approches SIEM (Security Information and Event Management) et SOAR (Security Orchestration Automation and Response)	Réalisez une intégration fluide avec vos plateformes SIEM et SOAR existantes pour surveiller, gérer et orchestrer les actions et les événements depuis un emplacement central. Exportez les pistes d'audit et les événements et enregistrez-les en toute sécurité dans vos plateformes SIEM et SOAR à des fins de conservation et d'orchestration des événements. Grâce à la surveillance en temps réel, vous pouvez réagir rapidement à toute menace détectée et protéger vos actifs de sauvegarde en prenant des mesures appropriées.	Les intégrations de Commvault permettent l'interopérabilité avec diverses plates-formes d'orchestration telles que Microsoft Sentinel, Palo Alto Networks XSOAR, Splunk et ServiceNow. Nos intégrations fournissent : • Visibilité en temps réel sur les événements et incidents de sécurité. • Capacités améliorées d'automatisation et d'orchestration. • Réduction des temps de réponse aux incidents et des interventions manuelles. • Amélioration de la collaboration interne et de la posture de sécurité générale.
Alertes	Envoyez des notifications automatiques sur les opérations, telles que les tâches ayant échoué. Les alertes sont affichées sur la page Alertes déclenchées et des utilisateurs définis reçoivent une notification par e-mail.	Recevez des alertes exploitables sous diverses formes : e-mail, SCOM (Systems Center Operations Manager), SNMP, webhooks, etc.
Tableaux de bord	Affichez un aperçu des informations les plus critiques collectées sur tous les ordinateurs CommServe de votre organisation, comme le pourcentage de SLA, l'utilisation de la capacité et les avertissements de sauvegarde.	La plateforme Commvault Cloud offre un moyen unifié de visualiser et de gérer votre cyber-résilience sur site et via une application SaaS. Elle fournit des tableaux de bord généraux sur la sécurité, les capacités et l'utilisation, avec notamment des informations supplémentaires sur l'évaluation de l'état de la sécurité et les activités inhabituelles des fichiers.
Outils d'orchestration	Créez des workflows orchestrés pour répondre rapidement aux événements générés par des ransomwares. Vous pouvez même procéder à des intégrations avec des fournisseurs tiers.	• Créez facilement des flux de travail pour les commandes pré/post-sauvegarde. • Flux de travail via l'interface de ligne de commande, les API REST, les modules PowerShell et le SDK Python. • Effectuez l'intégration de Splunk, ServiceNow, Ansible ou Terraform.
Réponse proactive aux menaces	Défendez activement la récupération des données en alertant les services de sécurité dès que l'attaquant agit.	• Des capteurs de menaces sont déployés autour des actifs de valeur (tels que les serveurs de fichiers, les bases de données, les machines virtuelles, etc.) pour créer des leurres au sein de vos environnements. • Prodigue des conseils judicieux sur le placement des leurres en analysant les charges de travail dans les environnements de sauvegarde. • Recevez des alertes très précises dès le début d'une attaque.

05 RÉCUPÉRER

Le processus de récupération commence dès que les menaces sont identifiées et qu'une réponse appropriée à l'incident permet d'isoler et de supprimer le logiciel malveillant. Il est essentiel de veiller à ce que toutes les données concernées retrouvent des conditions de fonctionnement normales depuis le moment exact où l'incident de cybersécurité s'est produit. Des outils et des options de récupération proactifs et fiables, couvrant un très large éventail de charges de travail, ont prouvé qu'ils réduisaient les temps d'arrêt, empêchaient la perte de données et accéléraient les temps de réponse pour assurer une continuité d'activité inégalée. Le plan de récupération commence une fois la cause première identifiée et les fichiers sont restaurés avec pour objectif d'atténuer tout impact potentiel futur à l'aide d'outils de sécurité appropriés. Pendant les phases de récupération, il est essentiel de ne récupérer que les fichiers propres de l'ensemble des technologies touchées par l'attaque.

RÉCUPÉRER ÉLÉMENTS ESSENTIELS	EXIGENCES PAR RAPPORT AUX RANSOMWARES	CAPACITÉS DE COMMVAULT
Récupération hybride multi-cloud	Récupérez rapidement vos données où que vous soyez, tant sur site que dans le cloud.	Effectuez vos opérations d'automatisation et de récupération sur différents hyperviseurs, hyperscalers ou autres plateformes.
Haute disponibilité	Grâce à la fonctionnalité CommServe LiveSync, le serveur CommServe est prêt pour la récupération après sinistre et permet de basculer rapidement vers un hôte de secours désigné en cas de sinistre.	La fonctionnalité Commvault LiveSync permet la sauvegarde des catalogues et autres charges de travail critiques.
Récupération en réponse aux incidents	Permettez aux équipes de réponse aux incidents de récupérer en toute sécurité des données à des fins d'analyses criminalistiques.	• Orchestrez des restaurations hors site dans un environnement isolé de type salle blanche. • Exécutez des pré/post-scripts et des flux de travail pour valider et analyser les données clés.
Analyse des logiciels malveillants	Vérifiez que les données de sauvegarde sont récupérables et que leur contenu ne comporte aucune menace.	• Montez des machines virtuelles en direct en utilisant la validation des applications pour exécuter des scripts en toute sécurité et analyser les machines virtuelles à la recherche de logiciels malveillants. • Recherchez les menaces avant qu'elles ne se propagent grâce à l'IA/apprentissage automatique, la détection des anomalies et l'analyse des signatures de logiciels malveillants.
Récupération et assainissement organisés	Réduisez les pertes de données en effectuant une récupération cohérente et assainie. Pour ce faire, supprimez les fichiers suspects et sachez exactement à partir de quel moment il convient de procéder à la récupération saine des fichiers.	Supprimez, isolez et mettez en quarantaine les fichiers suspects grâce à la détection des anomalies. Assainissez par ailleurs le contenu des sauvegardes en parcourant et en supprimant les menaces.
Récupération proactive	Détectez les menaces et corrigez-les avant qu'elles n'atteignent leur cible.	Avec Threatwise™, trompez les acteurs malveillants, détournez leurs attaques vers de faux actifs, obtenez une visibilité immédiate sur les attaques et remédiez rapidement aux menaces, avant qu'elles n'atteignent vos données.

05 RÉCUPÉRER

RÉCUPÉRER ÉLÉMENTS ESSENTIELS	EXIGENCES PAR RAPPORT AUX RANSOMWARES	CAPACITÉS DE COMMVAULT
Validation de la récupération	Planifiez, mettez en œuvre, validez et démontrez votre préparation à la récupération.	• Validez les sauvegardes en continu ou périodiquement pour détecter les sauvegardes corrompues en début de cycle. • Apportez des preuves de votre degré de préparation à la récupération sans perturbation des opérations. • Réduisez la complexité des tests de récupération en éliminant les étapes manuelles.
Analyses criminalistiques au service de la récupération	Effectuez des analyses criminalistiques sur des réseaux isolés, en toute sécurité pour éviter une propagation des violations.	• Analysez les données des fichiers pour détecter les fichiers susceptibles d'être chiffrés ou corrompus par des logiciels malveillants, afin de vous assurer que vous ne sauvegardez pas de fichiers infectés. • Intégrez une analyse des menaces pour détecter les contenus malveillants dans les données sauvegardées au moment de la restauration. Vous éviterez ainsi de corrompre à nouveau les systèmes de production lorsque vous restaurerez la dernière sauvegarde avant infection des données.
Orchestration de la récupération	Orchestration de la récupération après sinistre et de la cyber-récupération avec rapports de conformité automatisés.	• Récupérez en un clic des copies propres des charges de travail pour les remettre en production après avoir validé et nettoyé les points de récupération.
Récupération rapide des infrastructures	Restauration rapide à l'échelle du cloud sans limitations des emplacements de récupération.	• Associe des tests continus, l'infrastructure en tant que code et la mise à l'échelle du cloud pour automatiser une cyber-récupération rapide, prévisible et fiable des charges de travail hybrides vers le cloud, au coût total de possession le plus bas. • Portabilité totale qui permet une récupération depuis et vers n'importe quel endroit.

Une véritable cyber-résilience, au coût total de possession le plus bas.

Commvault Cloud fournit une défense multiniveaux, réduisant l'impact des cyberattaques via des alertes précoces et des leurres, tout en accélérant la récupération avec une analyse complète des menaces, des corrections, une mise en quarantaine intelligente, la validation de récupérations sans défaut et des vitesses de récupération inégalées.

Démarrez votre stratégie de cyber-résilience avec la meilleure solution qui soit pour vous aider à anticiper, combattre de manière proactive et accélérer la récupération après les cybermenaces.

Trouvez la solution correspondant le mieux à vos besoins.

INTÉGRATIONS DE SÉCURITÉ COMMVAULT

Commvault offre des intégrations transparentes avec des partenaires de sécurité de premier plan pour s'appuyer sur les capacités existantes de Commvault et proposer diverses options de cyber-résilience pour un environnement hybride intégré.

En savoir plus sur la cyber-résilience
commvault.com/platform

Commvault®

commvault.fr | 01 73 13 00 23 | talktous@commvault.com

© 2023 Commvault. Cliquez ici pour obtenir plus d'informations sur nos marques et brevets. 12_23