Améliorer la cyberrésilience et protéger les données contre les cybermenaces avec un coffre-fort isolé, un logiciel basé sur l'IA/ML ainsi que sur l'analytique et bien plus encore

Avec Dell technologies PowerProtect Cyber Recovery avec CyberSense

À mesure que la fréquence des cybermenaces augmente et que les méthodes d'attaque évoluent, les plans de protection des données doivent sécuriser et analyser tous les composants IT, des plus superficiels aux plus profonds. Dell PowerProtect Cyber Recovery peut vous aider à protéger les données les plus stratégiques et les plus sensibles, tout en garantissant une récupération appropriée face à une cyberattaque ou à un autre événement perturbateur.

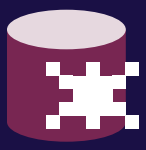
Dell PowerProtect Cyber Recovery est une solution de gestion, de protection et de récupération des données. Les organisations peuvent ainsi protéger leurs données et leurs applications contre les ransomwares, les cyberattaques destructrices et les événements inattendus. La solution utilise une approche multicopie, ce qui signifie qu'après avoir créé des sauvegardes, elle copie ces sauvegardes vers un stockage isolé à des fins de protection et d'analyse. PowerProtect Cyber Recovery comprend de nombreux composants, y compris un ou plusieurs coffres-forts de stockage, qui peuvent être placés sur site dans une appliance PowerProtect DD (anciennement Data Domain) ou dans le Cloud via Dell APEX Protection Storage for Public Cloud (anciennement DD Virtual Edition). Dans les deux cas, le coffre-fort est isolé des opérations, c'est-à-dire séparé de l'environnement de production : isolé physiquement par air gap dans un environnement sur site et logiquement dans un environnement APEX. Par conséquent, il est extrêmement difficile pour les acteurs malveillants ou les utilisateurs non autorisés de se connecter et de compromettre les copies de sauvegarde.

PowerProtect Cyber Recovery inclut également CyberSense, un moteur intelligent, entièrement automatisé et intégré pour l'analyse de la sécurité. Celui-ci parcourt automatiquement les données, les fichiers, les bases de données et les images dans le coffre-fort à la recherche de signes de corruption après une attaque par ransomware. Suite à une analyse complète du contenu, CyberSense utilise les observations des fichiers comme entrées pour son modèle d'apprentissage automatique (ML) basé sur l'intelligence artificielle (IA) et détecte les activités malveillantes, notamment les suppressions massives, le chiffrement et d'autres modifications suspectes dans l'infrastructure principale (y compris Active Directory et DNS), les fichiers utilisateur et les bases de données de production stratégiques susceptibles d'indiquer un ransomware ou une attaque destructrice. Lorsque CyberSense détecte des schémas de corruption, il génère une alerte dans le tableau de bord PowerProtect Cyber Recovery qui fournit des informations supplémentaires sur l'échelle et l'impact de l'attaque.[1]

PowerProtect Cyber Recovery aide les organisations à limiter les cyberattaques, à améliorer la résilience des données avec plusieurs copies de sauvegardes de données à partir de sites distincts, à réduire les interruptions de service et à maintenir la continuité de l'activité. Ce rapport utilise des données accessibles au public pour mettre en évidence les principales fonctionnalités de protection des données et présente les conclusions d'une analyse concurrentielle de CyberSense.

Protection des données sensibles

Chiffrement des données immuables en cours de transfert lors de la réplication de sauvegarde vers des coffres-forts physiquement et logiquement isolés



Détection de la corruption de la page SQL Server

CyberSense a détecté une infection alors qu'une solution concurrente n'est pas parvenue → le faire

Identification des copies de sauvegarde non corrompues

CyberSense a identifié la copie de sauvegarde non infectée la plus récente pour la restauration

Sécurité

Dell PowerProtect Cyber Recovery fournit plusieurs fonctionnalités de sécurité pour protéger les données stratégiques contre les ransomwares et autres menaces sophistiquées, empêcher les utilisateurs non autorisés d'accéder aux informations sensibles et accélérer la récupération afin que les organisations puissent reprendre leurs opérations normales.

Les fonctionnalités des appliances PowerProtect DD sont essentielles aux opérations de sécurité, de maintien de l'intégrité et de récupération proposées par les solutions PowerProtect Cyber Recovery. Ces fonctionnalités sont les suivantes :

1. **Immuabilité**
   Les données immuables ne peuvent pas être modifiées ou supprimées, uniquement écrites. Les systèmes DD peuvent écrire des sauvegardes immuables à la fois sur les systèmes de production et dans le coffre-fort. Autrement dit, si un acteur malveillant accède d'une manière ou d'une autre au système de sauvegarde, il ne peut pas modifier, supprimer ou compromettre les copies protégées existantes.[2] Toute sauvegarde créée par le système DD dans l'environnement de production est immédiatement immuable et disponible pour être copié dans le coffre-fort par le service IT, pour plus de sécurité. La section suivante de ce rapport traite davantage de l'immuabilité.

2. **Retention Lock**
   La fonctionnalité DD Retention Lock rend les données immuables pendant une période prédéterminée. Une fois que la solution place les données sous un verrouillage de rétention, aucun utilisateur ou système ne peut altérer, supprimer ou modifier les données tant que la période de verrouillage n'a pas expiré.[3]

   Retention Lock propose deux modes : gouvernance et conformité. Son mode de conformité peut permettre aux clients de respecter de nombreuses normes réglementaires. Un tiers indépendant a attesté que DD Retention Lock répond aux exigences de stockage spécifiées dans les règles SEC 17a-4(f)(2) et 240.18a-6(e)(2) et la règle FINRA 4511(c).[4] Cette fonctionnalité peut également aider une organisation à se conformer aux normes FDA 21 CFR Part11, Sarbanes-Oxley Act, IRS 98025 et 97-22, ISO Standard 15489-1 et MoREQ2010.[5]

   Étant donné que les personnes mal intentionnées pourraient tenter de contourner Retention Lock en modifiant l'horloge d'un système, ce qui obligerait la solution à supprimer les fichiers plus tôt que prévu, DD dispose d'une horloge de sécurité interne. Le système compare régulièrement les heures des horloges de sécurité et du système. En cas de décalage cumulé de deux semaines entre les deux au cours d'une même année civile, le système désactive automatiquement le système de fichiers DD File System (DDFS) pour empêcher l'accès aux données.[6]

3. **Chiffrement des données en cours de transfert avec DDBoost**
   Les données en cours de transfert peuvent poser un risque de sécurité important. DDBoost limite la quantité de données en cours de transfert. Le serveur de sauvegarde ou le client d'application ne peuvent envoyer à l'appliance DD que des segments de données uniques et non toutes les données via le réseau. En outre, les organisations peuvent utiliser le protocole DDBoost avec ou sans certificats pour l'authentification et le chiffrement des données. Les certificats offrent une capacité de transport des données plus sécurisée. Le chiffrement à la volée permet aux applications de chiffrer directement des données de sauvegarde et de restauration transitant via un réseau local à partir du système. Le client peut utiliser TLS (Transport Layer Services) pour chiffrer la session entre le client et le système.[7]

4. **Sécurité du système d'exploitation DD (DD OS)**
   Les fonctionnalités de sécurité DD s'étendent également au système d'exploitation. À des fins de sécurité, le système d'exploitation DD implémente des contrôles d'accès personnalisés et des restrictions sur le shell Bash. Le shell Bash restreint permet aux utilisateurs d'exécuter uniquement un ensemble de commandes prédéfinies nécessaires à leurs rôles et tâches. Le système d'exploitation DD améliore l'intégrité des données en bloquant les commandes non définies qui apportent des modifications non autorisées ou involontaires au système.[8]

5. **Sécurité des systèmes de fichiers DD (DDFS) et contrôle d'accès basé sur les rôles (RBAC)**
   Les systèmes DD utilisent plusieurs mesures pour protéger les fichiers et les données au sein du système de fichiers. Tout d'abord, les systèmes DD fournissent un RBAC, qui permet aux administrateurs de définir des rôles avec des privilèges spécifiques et d'attribuer des utilisateurs à ces rôles. Seuls les utilisateurs autorisés disposant des privilèges appropriés peuvent accéder à l'appliance et à ses données. Cela garantit que les utilisateurs n'ont accès qu'aux fonctions et aux données dont ils ont besoin pour effectuer leurs tâches, ce qui réduit le risque d'accès non autorisé ou d'exposition accidentelle de certaines données.

   DDFS utilise également le hachage pour la vérification de l'intégrité des données. Le hachage transforme une clé ou une chaîne de caractères donnée en une autre valeur. L'appliance stocke des fragments de données uniques dans des conteneurs de stockage logiques, et le système de fichiers hache à la fois les fragments de données et les conteneurs. Lorsque le système récupère des données, il recalcule la valeur de hachage des données pour qu'elle corresponde à la valeur de hachage stockée dans DDFS, ce qui permet de s'assurer que rien n'a altéré ou corrompu les données.[9]

6. **Autorisation à deux rôles**
   Lorsqu'une organisation active le mode de conformité DD Retention Lock, le système DD fournit une sécurité administrative supplémentaire sous la forme d'une double authentification. Cela signifie que l'administrateur système et un deuxième utilisateur autorisé (par exemple, le responsable de la sécurité) doivent se connecter ensemble. Le mécanisme d'authentification double des fonctions du mode de conformité DD Retention Lock sert de protection contre toutes les actions susceptibles de compromettre l'intégrité des fichiers verrouillés avant l'expiration de la période de rétention.[10]

7. **Architecture d'invulnérabilité des données**
   DD OS dispose de fonctionnalités de vérification de bout en bout, de prévention et de confinement des pannes, ainsi que de détection et de réparation en continu des pannes. Cet outil fournit également une capacité de restauration du système de fichiers qui offre une protection contre les problèmes d'intégrité des données imputables à des dysfonctionnements matériels et logiciels. Lorsque le système DD reçoit des requêtes d'écriture du logiciel de sauvegarde, il recherche d'abord une éventuelle redondance d'un segment de données, en calculant l'empreinte de ce segment de données et en la comparant aux empreintes existantes stockées dans le système. Il stocke uniquement les segments de données uniques et leurs empreintes digitales sur disque. DD lit les données du disque en continu, recalcule l'empreinte qu'il lit et s'assure qu'elle correspond à l'empreinte sur le disque. Le système DD effectue un processus d'autoréparation pour reconstruire les données corrompues et restaurer les données à leur état correct si le système détecte une corruption au cours de ce processus (c'est-à-dire, si ce qu'il lit ne correspond pas à ce qui est écrit). En outre, le processus d'autoréparation permet de protéger le système contre d'autres modifications susceptibles d'affecter l'intégrité de la plate-forme.

Immuabilité*

En rendant ses sauvegardes immuables, autrement dit en les basculant en lecture seule, une organisation s'assure de pouvoir faire confiance à ces sauvegardes pour une éventuelle restauration. Sur le plan opérationnel, l'immuabilité permet de préserver l'authenticité et la fiabilité des données.

*Les produits Dell permettent aux clients de sécuriser leurs données stratégiques. Comme pour tout produit électronique, les produits de protection des données, de stockage et d'infrastructure peuvent rencontrer des failles de sécurité. Il est important que les clients installent les mises à jour de sécurité dès qu'elles sont mises à disposition par Dell.

Fonctionnement

Les systèmes DD offrent une immuabilité dans la façon dont ils stockent les données à l'aide des MTree. Les MTree sont des partitions logiques du système de fichiers. Lorsqu'une application écrit des données sur une MTree, le système DD utilise une fonctionnalité appelée Fast Copy pour créer une copie instantanée de la MTree d'origine vers une nouvelle MTree. Dans la nouvelle MTree, DD applique Retention Lock pour s'assurer qu'un utilisateur ou un processus ne peut pas supprimer la nouvelle MTree pendant la durée définie par la période de rétention. La nouvelle structure MTree est une copie immuable des données et est indépendante de la structure MTree d'origine.[11]

Les solutions PowerProtect Cyber Recovery utilisent également la réplication MTree pour copier des copies de données immuables d'un DD de production vers un autre DD dans le coffre-fort via le protocole DDBoost.[12] Lors de la synchronisation initiale entre les deux DD, la solution copie toutes les données sur le DD du coffre-fort. Lors de chaque synchronisation suivante, seuls les segments de données nouveaux et modifiés sont copiés. CyberSense, que nous aborderons plus loin dans ce rapport, analyse toutes les copies immuables du coffre-fort pour détecter toute corruption potentielle.

Approches de l'immuabilité

La suppression des sauvegardes immuables est rare, mais ce scénario peut se produire. Les organisations peuvent rencontrer sur le long terme des problèmes de capacité et de coûts lorsqu'elles accumulent des sauvegardes immuables qu'elles ne peuvent pas supprimer. Le stockage des sauvegardes peut nécessiter une grande capacité, ce qui nécessite des coûts d'exploitation, de gestion et de surveillance continus en plus de l'investissement matériel initial. La suppression périodique de sauvegardes immuables peut vous aider à résoudre ces problèmes.

Comme nous l'avons indiqué, Dell PowerProtect Cyber Recovery offre une immuabilité grâce à Retention Lock et à d'autres outils. Rétention Lock offre une certaine flexibilité, car les deux modes, conformité et gouvernance, offrent de légères différences dans la façon dont les clients peuvent implémenter l'immuabilité. L'immuabilité signifie que les utilisateurs ou les acteurs malveillants ne peuvent pas supprimer les sauvegardes. Toutefois, dans certains cas, par exemple lorsqu'un problème de capacité de stockage survient, PowerProtect Cyber Recovery permet aux clients de les supprimer avec le mode Gouvernance de Retention Lock.

Comparées à PowerProtect Cyber Recovery, comment les autres offres similaires proposées par d'autres entreprises se positionnent-elles ? Nous avons examiné les informations accessibles au public pour Cohesity Cyber Recovery, Veeam, Rubrik et Veritas NetBackup. À l'exception de Cohesity Cyber Recovery, les solutions peuvent résider sur site ou hors site (Cohesity est une solution basée sur le Cloud soutenue par AWS). Les documentations des quatre solutions prétendent que celles-ci offrent une immuabilité, mais Rubrik et NetBackup présentent des différences par rapport à PowerProtect Cyber Recovery.

Pour Rubrik, les administrateurs peuvent supprimer des sauvegardes, mais pas du côté client et uniquement avec certains contrôles en place. En outre, toutes les écritures sont « déplacées », ce qui signifie que les nouvelles écritures ne touchent jamais les données précédemment écrites.[13]

Malgré l'immuabilité promise, les administrateurs ou des acteurs malveillants peuvent supprimer le verrouillage des sauvegardes au sein d'un stockage compatible NetBackup WORM. Ils pourraient ensuite supprimer l'image à l'aide de la commande bpexpdate.[14]

Isolement

L'isolement des données désigne la séparation des données et l'accès restreint à celles-ci via des obstacles ou des limites afin d'empêcher tout accès non autorisé. L'isolement utilise des connexions réseau temporaires au lieu de connexions permanentes.

L'isolement des données déconnecte celles qui sont stratégiques d'un réseau infecté, où un acteur malveillant pourrait modifier des configurations, supprimer des données, modifier des règles ou détecter le trafic réseau pour obtenir les identifiants de l'utilisateur. L'isolation permet également de réduire la surface d'attaque, ce qui limite les opportunités d'accès et de contrôle des acteurs malveillants. De plus, les organisations peuvent restreindre l'accès aux seuls membres autorisés du personnel, ce qui aide à empêcher les utilisateurs non autorisés de supprimer les données.

En plus des fonctionnalités que nous avons notées, PowerProtect Cyber Recovery peut fournir une isolation physique et logique, sous la forme d'air gaps opérationnels, pour aider à protéger les données. PowerProtect Cyber Recovery peut utiliser à la fois un air gap physique, dans lequel les données de sauvegarde sont physiquement déconnectées du réseau de production et stockées dans un emplacement isolé, et un air gap logique, qui s'appuie sur des contrôles d'accès réseau pour séparer les copies de sauvegarde logiquement déconnectées de l'environnement de production. Le fait de pouvoir disposer des deux types d'air gap est précieux, car un air gap logique seul ne peut empêcher un utilisateur interne disposant d'un accès réseau au coffre-fort d'accéder aux données et de les compromettre.

Un PowerProtect DD physique et isolé sur site pourrait fonctionner comme le coffre-fort, dans lequel les utilisateurs ou les systèmes provenant de l'environnement de production ne peuvent pas accéder aux composants, et le coffre-fort est physiquement déconnecté du réseau de production.[15] En éliminant l'accès à l'environnement de récupération à partir du réseau de production, une organisation peut réduire sa surface d'attaque. Comme indiqué, l'accès aux données isolées nécessite des informations d'identification de sécurité distinctes, ainsi qu'une authentification multifacteur (MFA).[16]

Approches de l'isolement

Selon Gartner, « les environnements de récupération isolés (IREs, Isolated Recovery Environments) avec des coffres-forts de données immuables (IDV) offrent le plus haut niveau de sécurité et de capacité de récupération contre les menaces internes, les rançongiciels et d'autres formes de piratage ».[17] Gartner note également qu'une solution IRE avec IDV ne remplace pas, mais à tout le moins complète, les systèmes de sauvegarde et de reprise après sinistre (DR) traditionnels en fournissant une copie de sauvegarde tertiaire immuable dans une IRE équipée de tous les outils, processus et ressources nécessaires pour restaurer les systèmes affectés.[18]

Lors de l'examen des informations accessibles au public sur les solutions Cohesity, Veeam, Rubrik et Veritas, nous avons constaté que chacune d'elles avait une approche IRE légèrement différente de celle de PowerProtect Cyber Recovery. Avec la solution Dell, les clients peuvent isoler physiquement ou logiquement leurs coffres-forts DD de la production afin de séparer les plans de contrôle et de données de production des coffres-forts. En outre, PowerProtect Cyber Recovery automatise les air gaps, ce que ne font pas toutes les autres solutions.

Conformément à la documentation :

- Cohesity Cyber Recovery offre uniquement un air gap logique dynamique et automatisé pour leur coffre-fort FortKnox basé sur AWS.[19]
- Veeam prend en charge un air gap logique pour les fournisseurs de Cloud public et privé via Veeam Cloud Connect, mais il n'est pas automatisé. Veeam propose également Veeam Hardened Repository, qui fait office de coffre-fort sur site pour la solution et que les organisations peuvent configurer pour disposer d'un air gap physique.[20]
- Rubrik ne propose pas d'air gap automatisé pour Rubrik Cloud Vault, mais les clients peuvent ajouter un air gap logique via un partenariat tiers avec Microsoft.[21]
- Les clients NetBackup doivent activer manuellement un air gap logique et peuvent créer un air gap physique avec une solution sur site ou hors site.[22]

Fonctionnement

La figure 1 illustre les chemins de gestion de réseau du coffre-fort Cyber Recovery isolé. Notez que le coffre-fort ne dispose d'aucun accès de gestion ou de contrôle pour l'environnement de production, ce qui permet de réduire la surface d'attaque.

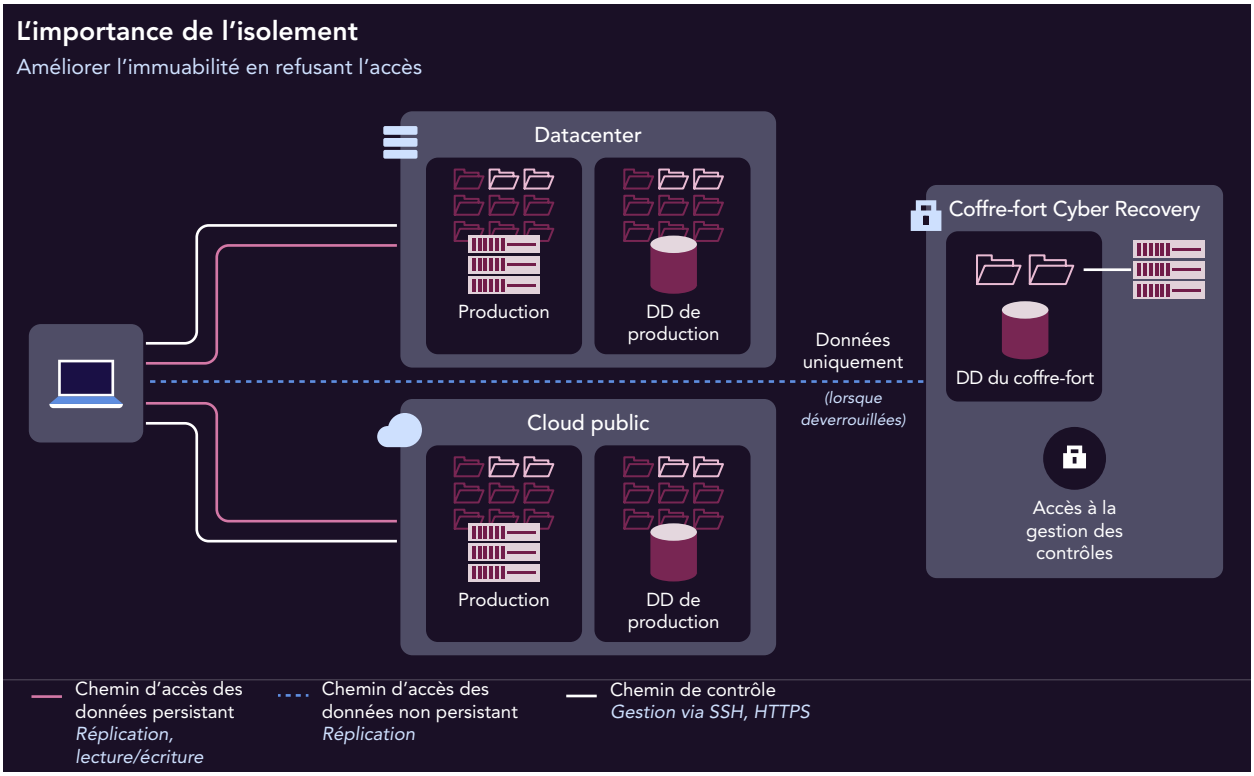


Figure 1 : Données de haut niveau et architecture de chemin de contrôle du coffre-fort Cyber Recovery. Source : Principled Technologies.

La seule connexion requise pour le coffre-fort Cyber Recovery est un chemin de données pour la synchronisation périodique des données. La synchronisation se produit lorsque la solution Cyber Recovery ingère des données à des intervalles courts et dictés par des règles pour la réplication.[23] Le guide de la solution Cyber Recovery de PowerProtect indique que « L'architecture de la solution Cyber Recovery de base se compose d'une paire de systèmes PowerProtect DD et de l'hôte de gestion Cyber Recovery. Dans cette configuration de base, le logiciel Cyber Recovery, qui s'exécute sur l'hôte de gestion, active et désactive l'interface Ethernet de réplication ainsi que les contextes de réplication sur le système PowerProtect DD dans le coffre-fort Cyber Recovery pour contrôler le flux de données de l'environnement de production vers l'environnement de coffre-fort ».[24] Dell suggère d'autres moyens permettant aux organisations de sécuriser et d'isoler les chemins de données. Lors de nos tests, nous avons pu observer que Cyber Recovery déverrouillait le coffre-fort pendant la réplication et le verrouillait ensuite.

Pour la mise en œuvre physique du coffre-fort, Dell recommande « d'installer l'équipement de coffre-fort Cyber Recovery dans une salle ou une cage dédiée avec des contrôles d'accès physiques. Cette pièce sécurisée doit avoir une liste d'accès limitée avec signatures pour la restitution des clés ou accès aux clés par deux personnes. Une surveillance vidéo des points d'entrée devrait être installée dans la cage ou la salle et sur l'équipement. Pour une sécurité optimale, le logiciel Cyber Recovery ne doit être accessible que par un accès physique au serveur de gestion Cyber Recovery et via un clavier et une souris associés ».[25]

Avec la séparation des chemins de gestion et de contrôle, les options d'isolation par air gap physique et logique de Cyber Recovery se distinguent des autres solutions. Certaines solutions permettent d'accéder à leurs données de coffre-fort à partir d'une interface d'environnement de production. Cela place les données du coffre-fort sur la même surface d'attaque que les données de production, ce qui permet potentiellement aux acteurs malveillants d'accéder aux copies de sauvegarde à l'aide d'informations d'identification compromises.

CyberSense

Bien protéger vos données nécessite une stratégie complète qui assure la sécurité à tous les niveaux. Malgré toutes les fonctionnalités d'autoréparation, de sécurité, d'immuabilité et d'isolement de Dell PowerProtect Cyber Recovery, les attaques moins évidentes peuvent tout de même pénétrer davantage dans l'infrastructure d'entreprise, par exemple au niveau de la sauvegarde des données, sans être détectées jusqu'à ce que les données de production ou un groupe d'utilisateurs soient compromis. Les solutions Dell PowerProtect Cyber Recovery offrent une dernière ligne de défense contre les cyberattaques et une approche efficace pour accélérer la récupération via CyberSense. CyberSense est un moteur d'analytique qui utilise des algorithmes d'analytique ML basés sur l'IA pour analyser et valider l'intégrité des sauvegardes dans le coffre-fort et le contenu utilisateur des fichiers au sein des sauvegardes.

CyberSense s'exécute dans le coffre-fort, isolé de l'environnement de production. Ce logiciel surveille les images de machines virtuelles, les bases de données et les fichiers répliqués dans le coffre-fort et analyse l'intégrité des données pour déterminer si une cyberattaque s'est produite. Une fois que la solution Cyber Recovery a répliqué les copies de sauvegarde vers le coffre-fort et appliqué la fonctionnalité Retention Lock, CyberSense analyse automatiquement les copies, en créant des observations ponctuelles des fichiers, des bases de données et de l'infrastructure principale. Le moteur d'analytique analyse l'intégralité du contenu des fichiers et de chaque page de base de données, pas seulement les métadonnées. Là où d'autres solutions recherchent des modifications dans les seuils de données ou les métadonnées, CyberSense examine le contenu des fichiers pour valider l'intégrité des données. Ces observations permettent à CyberSense de suivre l'évolution des fichiers et des bases de données au fil du temps et de découvrir de nombreux types d'attaques avancées cachées. CyberSense génère ensuite des analyses qui détectent les schémas de corruption susceptibles d'indiquer une mauvaise activité d'un acteur, y compris le chiffrement, la suppression, la création ou l'obscurcissement de fichiers, etc.[26] D'autres solutions imposent l'analyse dans le Cloud, ce qui est susceptible d'élargir la surface d'attaque, alors qu'avec CyberSense, les organisations peuvent choisir une exécution sur site ou dans l'une des nombreuses options Cloud prises en charge par Cyber Recovery.

CyberSense combine plus de 200 analyses avec des observations de données qui deviennent plus utiles au fil du temps, à mesure que les observations augmentent. L'algorithme d'apprentissage automatique utilise des informations sur des milliers d'infections par logiciels malveillants afin de détecter des schémas de comportement inhabituels et de distinguer l'activité utilisateur légitime de celle des rançongiciels, en réduisant dans le même temps les faux positifs et les faux négatifs. L'algorithme reçoit régulièrement de nouvelles informations sur des éléments tels que les variantes d'attaque, via des recherches continues. En outre, l'algorithme d'apprentissage automatique reçoit des mises à jour basées sur des données réelles des clients CyberSense existants.[27]

CyberSense prend également en charge l'indexation des données dans les formats de sauvegarde de disque courants de Dell, IBM, CommVault et Veritas.[28] En prenant en charge les formats de sauvegarde d'autres fournisseurs, Dell démontre sa volonté d'aller à la rencontre les clients là où ils se trouvent en termes de sauvegardes de données.

Nous avons testé le logiciel d'analytique intelligente basée sur l'apprentissage automatique de deux solutions clé en main de récupération informatique et de protection des données d'entreprise : CyberSense for Dell PowerProtect Cyber Recovery sur un Dell PowerStore™ 7000T et un outil fonctionnant de manière similaire sur la plateforme de gestion des données d'un concurrent (« fournisseur X ») pour une appliance de taille équivalente.

Procédure suivie pour le test

Nous avons exécuté tous les tests à distance et nous avions un contrôle total sur les bancs d'essai; ainsi qu'un accès sans entrave à ces derniers. La solution Dell (incluant CyberSense, l'application de sauvegarde PowerProtect Data Manager, APEX protection Storage (anciennement DD Virtual Edition) et la solution PowerProtect Cyber Recovery) et la solution Vendor X se trouvaient dans un laboratoire de datacenter hors site.

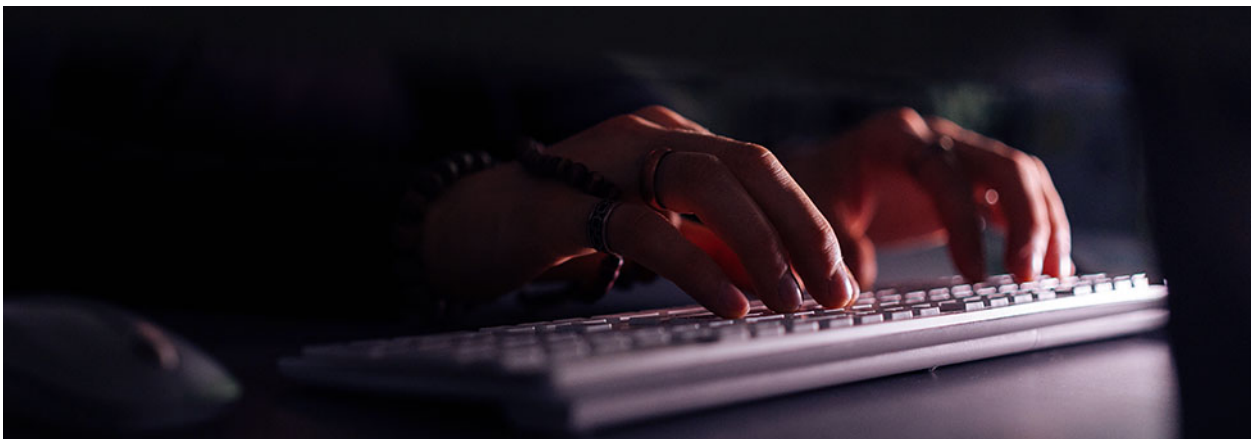
Sur les deux solutions, nous avons exécuté trois scénarios d'événements malveillants basés sur des scripts qui ciblaient les sauvegardes :

Figure 2 : Nos scénarios de test. Source : Principled Technologies.

Pour les deux solutions, les deux premiers scénarios ont suivi la même procédure générale. Tout d'abord, nous avons créé une sauvegarde complète de toutes les machines virtuelles saines sur les appliances de stockage (Dell PowerProtect Data Manager et celle du fournisseur X), créé des sauvegardes incrémentielles pour l'analyse, puis vérifié que la solution cible ne détectait pas de menace. Cela nous a donné un ensemble de sauvegardes de base sur lequel nous pouvions exécuter les scripts d'attaque.

Nous avons ensuite exécuté le script de simulation de rançongiciel sur quatre machines virtuelles avec différents systèmes d'exploitation et types d'applications, effectué de nouvelles sauvegardes incrémentielles sur l'appliance cible, puis vérifié si le logiciel d'analytique cible détectait la « menace de chiffrement ».

Pour le troisième scénario (infecter une page SQL Server), nous avons suivi une procédure similaire à celle des deux autres scénarios, mais nous nous sommes concentrés sur les machines virtuelles SQL et avons utilisé un script de corruption de page plutôt qu'un script de chiffrement. Nous avons exécuté le script sur une seule machine virtuelle.



Nos constatations

Scénario 1 : détection des fichiers cryptés avec des noms de fichiers obfusqués

Ce scénario a permis de simuler un événement malveillant de chiffrement des fichiers et de masquage de leur nom, ce qui a pour effet de modifier les métadonnées des fichiers en plus de chiffrer leur contenu. Ce type d'attaque est généralement connu sous le nom de rançongiciel, un événement de sécurité dans lequel un logiciel malveillant bloque l'accès à un système informatique jusqu'à ce que le propriétaire ou l'utilisateur du système paie une somme d'argent prédéterminée. Selon la CISA (US Cybersecurity and Infrastructure Security Agency), « l'impact des rançongiciels et des extorsions de données sur le plan économique et sur la réputation est à la fois complexe à gérer et coûteux pour toute organisation, quelle que soit sa taille, tout au long de la phase de perturbation initiale et, parfois même, pour la période étendue de récupération ».[29] L'utilisation d'un logiciel d'analytique intelligente pour détecter des opérations de chiffrement de sauvegardes moins visibles peut renforcer la stratégie de protection des données de toute organisation, aider à protéger des informations précieuses et sensibles et réduire les risques d'interruptions de service coûteuses imputables aux cyberattaques.

Lors de nos tests, les deux applications d'analytique intelligente ont découvert les fichiers chiffrés avec des noms de fichiers modifiés. La solution du fournisseur X a eu besoin d'une base de référence de 15 sauvegardes avant de détecter les infections (une sauvegarde complète et 14 sauvegardes incrémentielles), tandis que CyberSense a détecté les infections après une seule sauvegarde complète. Autrement dit, la solution du fournisseur X a nécessité14 sauvegardes de plus que CyberSense.

Lorsque la solution du fournisseur X nous a alertés d'une activité suspecte, elle a uniquement indiqué que quelque chose avait supprimé de nombreux fichiers et ajouté un nombre égal de fichiers, ce qui représente une activité suspecte si on considère le taux d'entropie de la sauvegarde.[30] La solution du fournisseur X n'a pas indiqué que les fichiers avaient été chiffrés ou que les noms de fichiers avaient changé. En revanche, la solution Cyber Recovery avec CyberSense nous a clairement indiqué que quelque chose avait chiffré des fichiers et masqué leurs noms.

Les résultats pour le fournisseur X peuvent correspondre à un faux positif. En d'autres termes, si nous supposons qu'une organisation exécute des sauvegardes quotidiennes avec la solution du fournisseur X, elle aurait pu ingérer 14 jours de fichiers infectés avant qu'une anomalie ne soit détectée. A contrario, CyberSense n'a eu besoin que d'une seule sauvegarde de référence pour générer une alerte avec des détails sur l'infection. À ce stade de notre exemple, la restauration avec Cyber Recovery se produit à partir du coffre-fort isolé, ce qui garantit à l'organisation qu'elle n'a pas exposé le réseau de production aux 14 sauvegardes infectées, comme l'aurait fait la solution du fournisseur X.

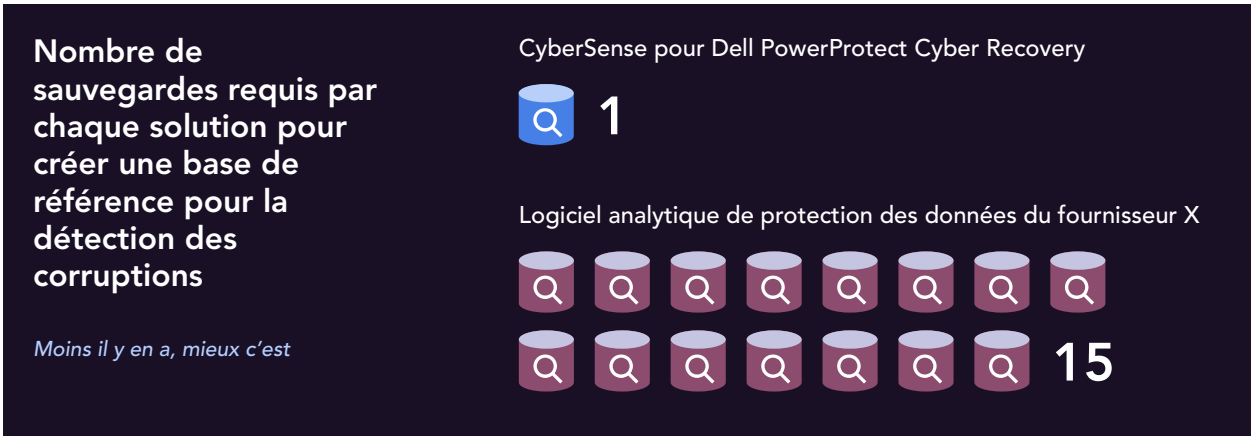


Figure 3 : Nombre de sauvegardes requises par chaque solution pour créer une ligne de base de détection de la corruption.
Source : Principled Technologies.

Scénario 2 : détection de fichiers chiffrés avec des noms de fichiers d'origine

Ce scénario était similaire au premier scénario, mais le script conservait les noms de fichiers d'origine des fichiers chiffrés. Cette modification n'a pas affecté les métadonnées des fichiers, uniquement les fichiers eux-mêmes. Cela peut s'apparenter à une attaque à retardement par un rançongiciel, lequel reste en sommeil pendant un certain temps avant de s'activer. L'attaque à retardement par un rançongiciel peut échapper à la détection et cibler les sauvegardes, rendant les sauvegardes infectées inutiles lorsque l'organisation en a besoin.[31] Sans modification des métadonnées, le fichier peut sembler non infecté en surface, ce qui permet de masquer l'attaque en sommeil.

Lors de nos tests, les deux applications d'analytique intelligente ont découvert les fichiers chiffrés. Encore une fois, la solution du fournisseur X a eu besoin d'une référence de 15 sauvegardes, dont 14 sauvegardes incrémentielles, avant de pouvoir détecter une anomalie. CyberSense n'a eu besoin d'utiliser comme référence qu'une seule sauvegarde complète avant de détecter une anomalie.

Comme dans le premier scénario, la solution du fournisseur X nous a uniquement signalé que quelque chose avait modifié de nombreux fichiers, ce qui représente une activité suspecte si on considère le taux d'entropie de la sauvegarde. Elle ne nous a pas indiqué que quelque chose avait chiffré les fichiers, tandis que Cyber Recovery avec CyberSense l'a fait. Détecter la corruption de cette manière signifie que CyberSense examine le contenu des fichiers et pas seulement les métadonnées au niveau de la surface. Ce type d'analyse ajoute une autre couche de sécurité à vos sauvegardes, et donc à votre infrastructure numérique ou votre environnement dans son ensemble. On pourrait suggérer que CyberSense est une « véritable » application d'analytique intelligente. En outre, les organisations peuvent détecter une corruption de données plus rapidement avec CyberSense, car cette solution a besoin de beaucoup moins de sauvegardes pour créer une base de référence. Selon le planning de sauvegarde adopté par l'organisation concernée, la différence peut être de plusieurs jours.

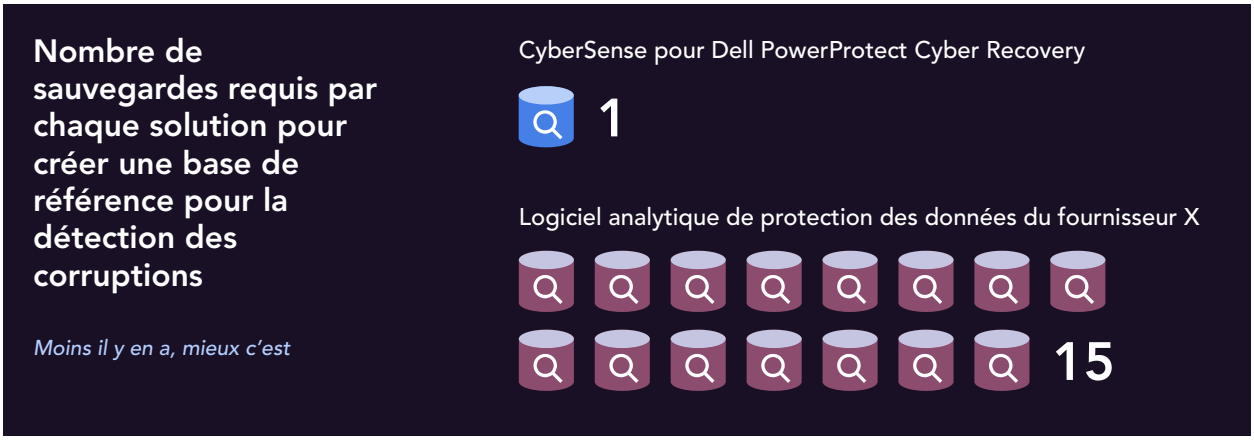


Figure 4 : Nombre de sauvegardes requises par chaque solution pour détecter la corruption. Source : Principled Technologies.

Scénario 3 : détection de corruption d'une page SQL Server

Ce scénario a simulé un événement malveillant qui corrompt une page SQL Server. Dans SQL Server, l'unité fondamentale de stockage des données est la page, et la base de données lit ou écrit des pages de données entières.[32] Cette modification n'a pas affecté les métadonnées, mais uniquement les fichiers eux-mêmes. Ce type d'attaque est communément appelé injection SQL, dans laquelle les pirates ciblent des applications basées sur des données SQL en injectant du code malveillant dans des instructions SQL via une entrée de page Web.[33] Même si elles sont infectées, les bases de données peuvent continuer à s'exécuter. En plus du vol de données, la corruption des pages SQL Server peut entraîner des problèmes d'intégrité des données, des pertes de données et des interruptions des fonctionnalités de base de données. Ces conséquences peuvent nuire à la réputation d'une organisation, perturber les workflows opérationnels, entraîner des pertes pécuniaires et même engager une responsabilité légale.

Même si CyberSense et la solution du fournisseur X ont tous deux détecté le chiffrement dans les deux premiers scénarios, seul CyberSense a pu effectuer une analyse suffisamment approfondie pour détecter la corruption dans la page SQL Server dans ce troisième scénario. Cela montre que, même si les deux solutions offrent des capacités de détection équivalentes à certains niveaux, CyberSense fournit une analyse plus approfondie des sauvegardes pour les applications basées sur SQL Server qui peuvent être stratégiques. Ainsi, CyberSense ajoute une couche de résilience de sécurité avec des analyses plus approfondies et une protection plus complète.

SQL Server alimente de nombreuses applications dans les secteurs de la finance, de la vente au détail, de la santé et autres. Étant donné que SQL Server peut fonctionner comme back-end de l'architecture de développement, une attaque SQL Server peut entraîner des arrêts de service, interrompre les opérations et potentiellement menacer le chiffre d'affaires généré par ces applications.

Restauration et récupération avec Dell PowerProtect Cyber Recovery

La stratégie de cyberrésilience Dell fournit un large éventail de fonctionnalités de récupération. Ces options de récupération incluent des fonctionnalités courantes du secteur, telles que l'accès instantané ou la récupération traditionnelle à partir des sauvegardes immuables conservées en production. En outre, Dell offre des fonctionnalités de récupération uniques à partir de la solution PowerProtect Cyber Recovery. Étant donné que PowerProtect Cyber Recovery conserve les copies de façon isolée et analyse leur intégrité avec CyberSense, les organisations peuvent accéder aux copies immédiatement après une attaque et les utiliser pour lancer des procédures de récupération, ou des restaurations immédiates vers d'autres plates-formes de récupération comme des salles blanches.

Comparez cette utilisation immédiate à un organisme qui ne peut accéder aux données qu'en production ou dans le Cloud public. L'organisation ne peut pas accéder en toute sécurité aux données stockées dans la zone compromise tant qu'elle n'a pas déterminé et corrigé la cause première, qu'elle n'a pas mis fin à la persistance de l'accès des acteurs malveillants, qu'elle n'a pas capturé d'images d'analyse d'investigation pour les assureurs et leur service juridique, qu'elle n'a pas analysé à nouveau les données et qu'elle ne dispose pas des éléments d'infrastructure suffisants (AD, DNS) pour accéder à l'infrastructure de sauvegarde. Ce processus peut prendre des jours ou des semaines en fonction de la portée et de la sophistication de l'attaque.

Fonctionnement

En production normale, PowerProtect Cyber Recovery crée automatiquement des points de restauration pour la récupération et l'analyse de la sécurité. En cas de cyberattaque, Cyber Recovery utilise ses procédures de restauration et de récupération automatisées et ces points de restauration pour remettre en ligne les systèmes stratégiques. Les rapports CyberSense et d'analyse d'investigation aident les équipes de cybersécurité et de récupération à diagnostiquer l'impact de l'attaque. Une fois que l'environnement de production est propre et prêt pour la récupération, Cyber Recovery fournit les outils et la technologie pour procéder à la récupération des données.

Après une cyberattaque, plusieurs métriques de protection des données entrent en jeu pour déterminer la vitesse de récupération (le temps de cyber-récupération ou CRT) et le moment auquel les utilisateurs peuvent revenir à un état antérieur après une attaque destructrice (le point de récupération cybernétique ou CRP). Pour une solution Cyber Recovery, ces indicateurs incluent les éléments suivants :

- **Objectif de détection de destruction (DDO) :** il s'agit d'une fenêtre évolutive basée sur le temps écoulé entre une attaque et la détection de l'attaque. L'analytique et les autres mécanismes de Cyber Recovery doivent opérer pendant cette période.
- **Objectif d'évaluation de destruction (DAO) :** il s'agit du temps alloué à l'équipe de cybersécurité à la suite d'une incursion pour déterminer l'étendue des dommages et les réponses potentielles.
- **Intervalle de synchronisation Cyber Recovery :** fréquence à laquelle la solution Cyber Recovery copie les données de l'environnement de production vers le coffre-fort. Le calendrier est basé sur un objectif de point de restauration (RPO) précédemment établi pour la solution. La période de rétention des copies dépend de la solution, mais varie généralement d'une semaine à un mois.
- **Nombre de copies de données Cyber Recovery :** il s'agit du nombre de copies de données conservées dans le coffre-fort Cyber Recovery. Associée à l'intervalle de synchronisation, cette métrique fournit une mesure approximative de l'ancienneté des données qu'une organisation peut récupérer. Par exemple, sept copies associées à un intervalle de 24 heures permettent de restaurer des données pouvant remonter à une semaine.

En plus des exigences de récupération, le type de données que la solution protège peut vous aider à déterminer l'intervalle de synchronisation des données et le temps de rétention. Selon le guide de la solution Cyber Recovery, pour une flexibilité de restauration optimale, les utilisateurs peuvent classer les données protégées par la solution dans l'un des flux de sauvegarde suivants :[34]

- Sauvegardes binaires et exécutables, y compris les distributions du système d'exploitation de base et les builds d'applications
- Sauvegardes complètes d'applications et de systèmes de fichiers, y compris des images et des données spécifiques aux applications

Ces flux de sauvegarde distincts induisent deux stratégies de restauration différentes :

1. **Restaurer les données et les données binaires d'application dans le coffre-fort Cyber Recovery :** La solution identifie les points de restauration utilisables, ainsi que le logiciel malveillant et l'emplacement où il persiste, et décide si le logiciel malveillant doit être nettoyé à partir de l'image de sauvegarde ou si une reconstruction à l'aide des copies du coffre-fort Cyber Recovery est nécessaire. Après avoir appliqué les correctifs de sécurité, la solution restaure les données sur un hôte de récupération à l'aide du guide d'exploitatio de reprise après sinistre de l'application, puis détermine si le processus de récupération a éliminé les effets du logiciel malveillant. Elle effectue ensuite une exécution de test sur l'application à l'aide du calcul de coffre-fort et nettoie ou recrée l'environnement de production. Finalement, Cyber Recovery connecte l'hôte de récupération dans la production et copie l'application et les données dans l'environnement de production. La Figure 5 illustre ce processus.

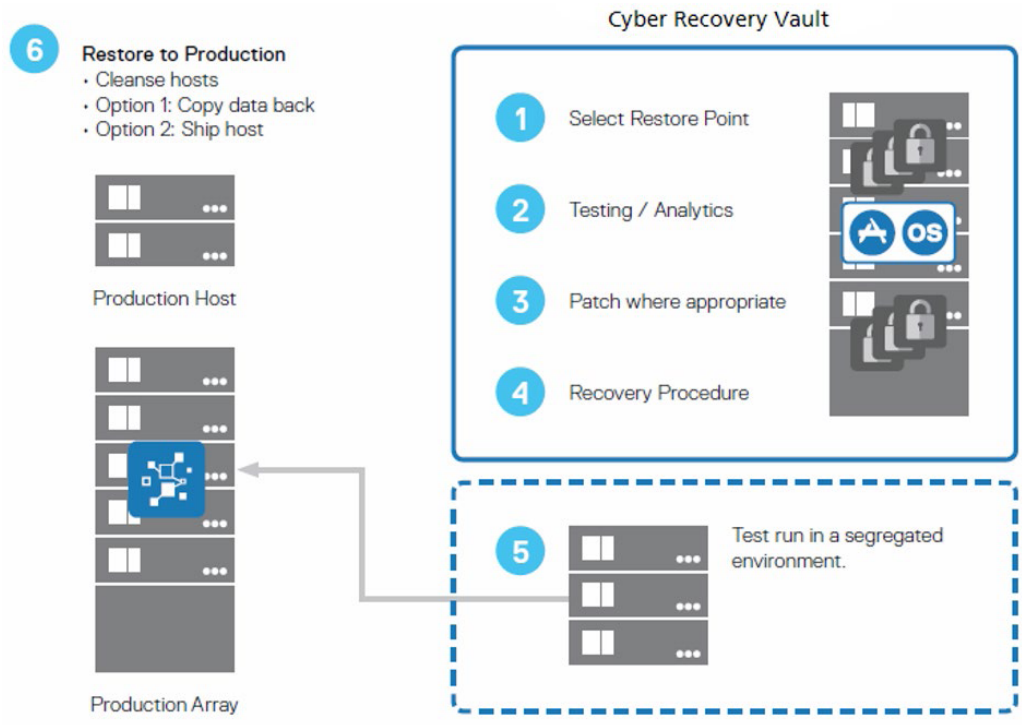


Figure 5 : Processus de restauration des fichiers binaires des données et des applications. Source : Dell Technologies[35]

2. **Reconstruction complète à partir du coffre-fort Cyber Recovery :**
   Dans cette approche, la solution Cyber Recovery reformate les systèmes de production en fonction du niveau de dommages déterminé par l'évaluation d'investigation lors de la réponse à l'incident. La solution reconstruit ensuite les données binaires via des copies dans le coffre-fort Cyber Recovery et applique les correctifs de sécurité disponibles. En dernier, elle restaure les copies appropriées des applications, des données et des fichiers de configuration dans l'environnement de production à l'aide des guide d'exploitation de reprise après sinistre associés à l'application. La Figure 6 illustre ce processus.

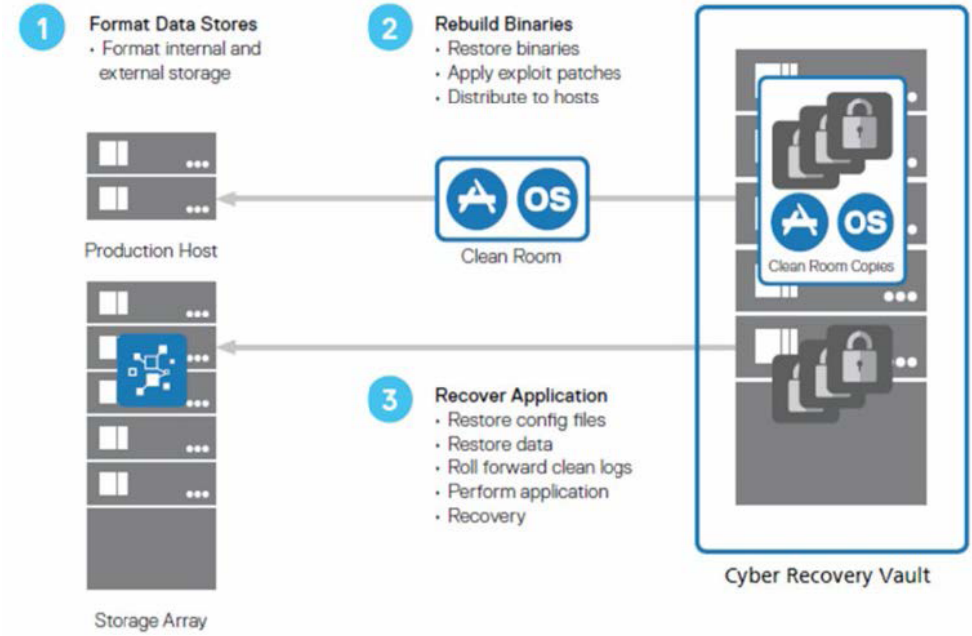


Figure 6 : Processus de reconstruction complète à partir du coffre-fort Cyber Recovery. Source : Dell Technologies[36]

Les solutions Cyber Recovery incluent des hôtes de récupération physiques ou virtuels (ou les deux) que le logiciel Cyber Recovery peut utiliser pour la récupération. Ces hôtes incluent à la fois un serveur de récupération d'applications de sauvegarde, qui est un serveur désigné sur lequel l'application de sauvegarde et le catalogue d'applications de sauvegarde sont restaurés, et un serveur de récupération d'applications. Les organisations peuvent déployer plusieurs serveurs en fonction des exigences de récupération de la solution. Le logiciel Cyber Recovery peut exposer des copies de données en sandbox (un environnement de test pour l'exécution sécurisée de logiciels nouveaux ou non testés) à n'importe quel hôte pour l'exécution des restaurations de données présentes dans le coffre-fort (données de système de fichiers, données de sauvegarde IBM, CommVault et Veritas, ou encore données protégées par Dell NetWorker, Dell Avamar, une appliance Dell PowerProtect série DP ou le logiciel Dell PowerProtect Data Manager). Après la restauration d'une application de sauvegarde dans le coffre-fort, la solution peut restaurer ces données sur des hôtes de récupération supplémentaires dans le coffre-fort.

Les organisations dimensionnent le serveur de récupération des applications de sauvegarde à l'avance afin que les utilisateurs puissent restaurer toutes les applications de sauvegarde protégées par la solution Cyber Recovery. De même, le serveur de récupération d'applications est un serveur désigné sur lequel la solution restaure les applications. Certaines applications peuvent nécessiter que les clients restaurent d'abord d'autres applications dépendantes. L'infrastructure au sein du coffre-fort peut prendre en charge la récupération de la plus grande application de production protégée par la solution.

Conclusion

Les organisations doivent prendre en compte de nombreux vecteurs d'attaque lors de l'élaboration d'un plan de protection des données. Cela implique de protéger toutes les données, mais surtout, les données essentielles pour les opérations. PowerProtect Cyber Recovery isole les données stratégiques et aide à garantir une récupération correcte des données en cas de cyberattaque. Dans CyberSense, Cyber Recovery utilise l'analytique basée sur le ML pour évaluer l'intégrité des données présentes dans le coffre-fort et identifier les données de sauvegarde saines pour la restauration. Lors de nos tests, nous avons constaté que PowerProtect Cyber Recovery est parvenu à détecter une infection dans les pages de base de données SQL, ce que la solution concurrente n'a pas réussi à faire. PowerProtect Cyber Recovery a également nécessité moins de sauvegardes que la solution concurrente pour déterminer qu'une corruption des données s'était produite. En plus de tout cela et bien plus encore, la solution Cyber Recovery offre de nombreuses options de récupération, s'appuyant sur des données non compromises provenant du coffre-fort pour un retour efficace et fluide aux opérations.

---

1. Dell, « CyberSense® pour Dell PowerProtect Cyber Recovery », consulté le 8 septembre 2023, https://www.delltechnologies.com/asset/en-in/products/data-protection/briefs-summaries/h18214-cybersense-for-dellemc-powerprotect-cyber-recovery-solution-brief.pdf.
2. Dell, « Guide de solutions Dell PowerProtect Cyber Recovery », consulté le 23 août 2023, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf.
3. Dell, « Guide de solutions Dell PowerProtect Cyber Recovery ».
4. Cohasset Associates, Inc, « Dell Technologies PowerProtect DD and DDVE – Compliance Assessment: SEC 17a-4(f), SEC 18a-6(e) and FINRA 4511(c) », consulté le 27 octobre 2023, https://infohub.delltechnologies.com/section-assets/cohasset-dell-powerprotect-dd-compliance-assessment.
5. Dell, « Data Domain : questions fréquentes sur Retention Lock », consulté le 12 septembre 2023, https://www.dell.com/support/kbdoc/en-us/000079803/data-domain-retention-lock-frequently-asked-questions-faq.
6. Dell, « Data Domain : questions fréquentes sur Retention Lock ».
7. Dell, « Encryption types offered by DD series encryption appliance », consulté le 8 septembre 2023, https://infohub.delltechnologies.com/l/powerprotect-dd-series-appliances-encryption-software-1/encryption-types-offered-by-dd-series-encryption-appliance.
8. Dell, « Guide de configuration de la sécurité Dell EMC Data Domain », consulté le 11 septembre 2023, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/docu91808.pdf.
9. Dell, « Role based access control (RBAC) in Data Domain », consulté le 11 septembre 2023, https://www.dell.com/community/en/conversations/data-domain/role-based-access-control-rbac-in-data-domain/647f70a9f4ccf8a8dee30f99.
10. Dell, « Guide de configuration de la sécurité de Dell EMC Data Domain ».
11. Dell, « MTree replication », consulté le 11 septembre 2023, https://infohub.delltechnologies.com/l/dell-powerprotect-cyber-recovery-reference-architecture/mtree-replication-3.

12. Veeam, « Dell EMC Data Domain - DataDomain MTree overview and limits », consulté le 11 septembre 2023, https://bp.veeam.com/vbr/2_Design_Structures/D_Veeam_Components/D_backup_repositories/datadomain.html
13. Chris Wahl, « Recover Fast from Ransomware Attacks: The Magic of an immutable Backup architecture », consulté le 13 décembre 2023, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/rwp-recovering-fast-from-ransomware-attacks.pdf.
14. Veritas, « NetBackup™ Security and Encryption Guide », consulté le 13 décembre 2023, https://www.veritas.com/support/en_US/doc/21733320-149123528-0/v143394540-149123528.
15. Principled Technologies, « Dell EMC Cyber Recovery protected our test data from a cyber attack », consulté le 21 août 2023, http://facts.pt/rkew01n.
16. Dell, « Dell PowerProtect Cyber Recovery », consulté le 12 septembre 2023, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf.
17. Jerry Rozeman et Michael Hoeck, « Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults to Protect and Recover From Ransomware », consulté le 14 décembre 2023, https://www.gartner.com/doc/reprints?id=1-27MOHCBD&ct=211011&st=sb.
18. Jerry Rozeman et Michael Hoeck, « Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults to Protect and Recover From Ransomware ».
19. Nikitha Okmar, « Going Beyond the Air Gap - Data Isolation and Recovery for the Modern Era », consulté le 13 décembre 2023, https://www.cohesity.com/blogs/going-beyond-the-air-gap-data-isolation-and-recovery-for-the-modern-era/.
20. Marco Horstmann, « How to protect your data from ransomware and encryption Trojans », consulté le 13 décembre 2023, https://www.veeam.com/blog/how-to-protect-against-ransomware-data-loss-and-encryption-trojans.html.
21. Rubrik, « Rest easy with immutable, off-site data storage », consulté le 13 décembre 2023, https://www.rubrik.com/products/rubrik-cloud-vault.
22. Veritas, « NetBackup Isolated Recovery Environment », consulté le 13 décembre 2023, https://www.veritas.com/content/dam/www/en_us/documents/solution-overview/SO_flex_appliance_netbackup_ire_solution_V1543.pdf.
23. CSI Group, « Dell Cyber Recovery Vault (overview by CSI) », consulté le 23 août 2023, https://youtu.be/ej5nZzWNRM0.
24. Dell, « Guide de solutions Dell PowerProtect Cyber Recovery ».
25. Dell, « Guide de solutions Dell PowerProtect Cyber Recovery ».
26. Dell, « CyberSense® for PowerProtect Cyber Recovery ».
27. Dell, « CyberSense® for Dell PowerProtect Cyber Recovery – Powered by Index Engines », consulté le 13 septembre 2023, https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/cybersense-for-dell-powerprotect-cyber-recovery-whitepaper.pdf.
28. Index Engines, « CyberSense for Dell Cyber Recovery », consulté le 25 septembre 2023, https://indexengines.com/csmatrix.
29. CISA, « #StopRansomware Guide », consulté le 1er août 2023, https://www.cisa.gov/stopransomware/ransomware-guide.
30. « En matière de sécurité, la plupart des utilisateurs utilisent l'entropie Shannon, un algorithme spécifique qui renvoie une valeur comprise entre 0 et 8. Plus le nombre est élevé, plus les données sont aléatoires. Souvent, une valeur élevée signifie que les données sont compressées ou chiffrées ». Mueller, Clint, « How to Use Entropy Analysis in Penetration Testing », 28 août 2023, https://www.schellman.com/blog/cybersecurity/penetration-testing-methods-entropy.
31. Cooper, Steven, « How to Protect your Backups from Ransomware in 2023 », 1er août 2023, https://www.comparitech.com/net-admin/protect-backups-from-ransomware/.
32. Microsoft, « Guide d'architecture des pages et des étendues », consulté le 3 août 2023, https://learn.microsoft.com/en-us/sql/relational-databases/pages-and-extents-architecture-guide?view=sql-server-ver16.
33. W3 Schools, « SQL Injection », consulté le 3 août 2023, https://www.w3schools.com/sql/sql_injection.asp.
34. Dell, « Guide de solutions Dell PowerProtect Cyber Recovery ».
35. Dell, « Guide de solutions Dell PowerProtect Cyber Recovery ».
36. Dell, « Guide de solutions Dell PowerProtect Cyber Recovery ».

Consultez les données scientifiques qui sous-tendent ce rapport ▶

▶ Consultez la version d'origine de ce rapport (en anglais) à l'adresse https://facts.pt/64FU3b2

Principled Technologies®

Facts matter.®

Ce projet a été réalisé à la demande de Dell Technologies.