Synthèse

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.

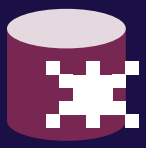
Dell PowerProtect Cyber Recovery est une solution de gestion, de protection et de récupération des données. Les organisations peuvent ainsi protéger leurs données et leurs applications contre les ransomwares, les cyberattaques destructrices et les événements inattendus. La solution utilise une approche 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 peuvent être essentielles à la sécurité, à l'intégrité et à la récupération offertes par les solutions PowerProtect Cyber Recovery. Ces fonctionnalités incluent Retention Lock, DDBoost, le contrôle d'accès basé sur les rôles (RBAC), la double autorisation et bien plus encore.

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 souvent 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, pour aider à protéger les données. 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.[2] En éliminant l'accès à l'environnement de récupération à partir du réseau de production, une organisation pourrait réduire sa surface d'attaque.

Immuabilité*

Rendre les sauvegardes immuables, c'est-à-dire les basculer en lecture seule, permet à une organisation de faire confiance à ces sauvegardes pour la restauration. Sur le plan opérationnel, l'immuabilité permet de préserver l'authenticité et la fiabilité des données. Les systèmes DD, y compris ceux des solutions PowerProtect Cyber Recovery, peuvent fournir une immuabilité dans la façon dont ils stockent les données à l'aide de partitions logiques du système de fichiers appelées MTrees. Les solutions 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.[3]

*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.

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 et un outil fonctionnant de manière similaire à partir de la plateforme de gestion des données d'un concurrent (que nous appelons « fournisseur X ») pour une appliance de taille similaire. Lors de nos tests, nous avons constaté que PowerProtect Cyber Recovery détectait une infection dans les pages de base de données SQL, ce que la solution du fournisseur X n'a pas réussi à faire. PowerProtect Cyber Recovery a également nécessité moins de sauvegardes que la solution du fournisseur X pour déterminer la corruption des données.

1. Dell, « CyberSense® for 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, « MTree replication », consulté le 11 septembre 2023, https://infohub.delltechnologies.com/l/dell-powerprotect-cyber-recovery-reference-architecture/mtree-replication-3.
3. Principled Technologies, « Dell EMC Cyber Recovery protected our test data from a cyber attack », consulté le 21 août 2023, http://facts.pt/rkew01n.

▶ Consultez la version en anglais d'origine de ce résumé

Lire le rapport ▶

Principled Technologies®

Facts matter.®