DELL Technologies

Présentation de solution

Cyber Recovery avec les services de données multi-Cloud pour Dell EMC PowerProtect

Service Cyber Recovery optimisé pour le multi-Cloud

Fiable et sécurisé

- Environnement de coffre-fort cloisonné physiquement et logiquement des réseaux d'entreprise par isolation opérationnelle
- Copies immuables des données dans un coffre-fort sécurisé hors site maintenant l'intégrité des données
- L'analytique intelligente assure l'apprentissage automatique et l'indexation de l'ensemble du contenu au sein du coffre-fort

Economique

- Infrastructure de coffre-fort fournie as-a-service
- Connexion directe haut débit à faible latence disponible vers les fournisseurs de Cloud public
- 0 $ en frais de sortie de Microsoft Azure et Oracle Cloud

Commodité sans compromis

- Protéger les données stratégiques qui résident dans le Cloud ou sur site
- Restaurez les données vers n'importe quel fournisseur de cloud public en toute fluidité
- Bénéficiez de la flexibilité et de la commodité du Cloud sans compromettre la sécurité

Cyber Protection pour les déploiements sur site et dans le Cloud

Chaque minute de chaque jour, les rançongiciels et autres cyberattaques évoluées menacent de voler ou de compromettre les ressources les plus stratégiques d'une entreprise : leurs données. Cela peut entraîner une perte de chiffre d'affaires, une atteinte à la réputation et de coûteuses amendes pour infraction. Il est donc impératif de protéger les données stratégiques et, en cas d'attaque, de les récupérer en validant leur intégrité pour pouvoir relancer l'activité de l'entreprise.

Les environnements hybrides et multi-Cloud offrent une flexibilité opérationnelle, une capacité d'évolutivité rapide et un accès à des services et à du matériel innovants. Cependant, l'approche qui consiste à disperser et à dupliquer les données sur plusieurs Clouds peut engendrer de nouveaux risques en matière de sécurité et de conformité, des problèmes de synchronisation potentiels et des coûts de ressources accrus. Cette approche peut également réduire la visibilité sur vos différents environnements, et mener à une protection insuffisante contre les cybermenaces actuelles en évolution constante. Vous avez besoin d'une méthode plus appropriée pour rendre vos données accessibles aux fournisseurs de Cloud public sans compromettre la sécurité, tout en conservant votre liberté de choisir n'importe quel fournisseur de Cloud afin d'éviter toute dépendance envers un seul fournisseur.

À mesure que vous faites passer des charges applicatives et des données dans le Cloud, il est impératif d'investir dans une solution de cyber-protection pour les données stratégiques, quel que soit leur emplacement. Dell Technologies fournit un coffre-fort de données sécurisé avec analytique intelligente qui protège vos données stratégiques contre les cyberattaques, les rançongiciels et les menaces internes.

Cyber Recovery optimisé pour le multi-Cloud

Il est facile de configurer un coffre-fort Cyber Recovery avec des services de données multi-Cloud pour Dell EMC PowerProtect, optimisé par Faction. Ce service sécurisé de mise en coffre-fort des données est un espace isolé reposant sur une infrastructure sécurisée prête pour le multi-Cloud, qui protège vos données stratégiques contre les cyberattaques. Lorsqu'une récupération des données est requise, vous pouvez choisir de restaurer vos données depuis votre coffre-fort vers AWS, Microsoft Azure, Google Cloud, Oracle Cloud, ou à nouveau vers votre environnement sur site.

L'analytique intelligente CyberSense est entièrement intégrée à ce service Cyber Recovery et adopte une approche unique de la détection des cyberattaques, en observant la manière dont les données évoluent au fil du temps et en utilisant l'analytique pour détecter les signes de corruption causés par les rançongiciels. Vous bénéficiez ainsi qu'une couche d'assurance supplémentaire offerte par la validation de l'intégrité des données protégées hors site, dans le coffre-fort Cyber Recovery.

Cyber Recovery avec services de données multi-Cloud pour l'architecture sécurisée Dell EMC PowerProtect

L'environnement du coffre-fort sécurisé inclut un système de services de données multi-Cloud pour Dell EMC PowerProtect qui sert de cible de réplication à votre système Dell EMC PowerProtect DD ou Dell EMC PowerProtect DD Virtual Edition (DDVE). Des ressources de calcul dédiées exécutent les outils de gestion de Cyber Recovery et les outils d'analytique CyberSense éventuels. Combinée à la sécurité physique et à l'isolation du coffre-fort, cette solution comprend une isolation physique opérationnelle : cet espace vide permet juste d'accéder au coffre-fort le temps de répliquer données du système principal, et même ici l'accès est fortement limité. À tout autre moment, le coffre-fort est déconnecté de l'environnement de production du client. Des copies immuables des données sélectionnées par l'utilisateur sont créées dans le coffre-fort Cyber Recovery hébergé dans un datacenter Faction. Une fois qu'une copie des données sélectionnées est sécurisée dans le coffre-fort isolé, les

données ne peuvent plus être modifiées, supprimées ou modifiées pendant une durée déterminée. L'analytique CyberSense, avec ses fonctionnalités d'apprentissage automatique et d'indexation de l'ensemble du contenu, peut analyser chaque jeu de données au sein de la sécurité du coffre-fort.

Protection des services de données multi-Cloud existants pour les déploiements Dell EMC PowerProtect

Dans le cas d'une combinaison avec les services de données multi-Cloud pour Dell EMC PowerProtect, les clients bénéficient d'une protection souveraine des données sur tous les Clouds (AWS, Google Cloud, Oracle et Azure) et sont alors en mesure de protéger leurs données stratégiques dans un coffre-fort Cyber Recovery.
Les services de données multi-Cloud pour Dell EMC PowerProtect peuvent être utilisés en tant que système polyvalent : une cible de sauvegarde pour les données d'applications Cloud natives ou une cible de réplication pour les systèmes PowerProtect existants. Le coffre-fort Cyber Recovery est une option supplémentaire qui peut facilement être ajoutée pour assurer l'isolation des données stratégiques contre les cyberattaques et la validation de l'intégrité des données.

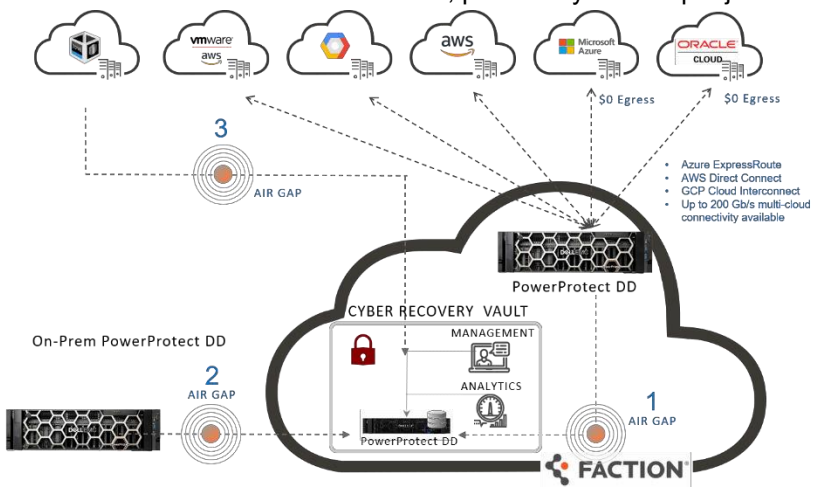

Figure 1 : Cas d'utilisation des services de données multi-Cloud pour Dell EMC PowerProtect

1. Protection des services de données multi-Cloud existants pour les déploiements Dell EMC PowerProtect

2. Protection des données sur le site du client

3. Protection des données dans le Cloud public

Protection des données sur le site du client

Les clients peuvent répliquer des données à partir d'un système PowerProtect DD sur site vers un coffre-fort Cyber Recovery dans l'un des datacenters de Faction. Cela offre ainsi aux entreprises la meilleure chance possible de récupération lorsque leurs sauvegardes principales ou de production ont été compromises ou que leur site de reprise après sinistre a été piraté ou infecté. En cas de cyberattaque, ils peuvent rapidement identifier la copie intacte la plus récente des données dans le coffre-fort Cyber Recovery et restaurer leurs systèmes stratégiques sur site ou choisir de les récupérer dans le Cloud si leur service a été conçu selon ce principe de récupération.

Protection des données dans le Cloud public

Pour les applications Cloud natives qui utilisent déjà PowerProtect DDVE (une cible de sauvegarde virtuelle dans le Cloud prise en charge dans AWS, Google Cloud et Azure), le coffre-fort Cyber Recovery est un service en option qui permet aux clients de répliquer les données stratégiques vers un coffre-fort sécurisé.

Dell EMC PowerProtect Cyber Recovery avec CyberSense

PowerProtect Cyber Recovery est la première solution capable d'intégrer pleinement CyberSense, mécanisme ajoutant une couche de protection intelligente qui permet de rechercher les cas de corruption des données lorsqu'un attaquant parvient à pénétrer dans le datacenter. Avec cette approche innovante, vous pouvez indexer l'ensemble du contenu et tirer parti de l'apprentissage automatique pour analyser plus de 100 statistiques basées sur le contenu, mais aussi détecter toute manifestation d'une corruption des données suite à l'action d'un rançongiciel. La fonction de détection de la corruption de CyberSense est fiable à 99,5 %. Ainsi, vous pouvez rapidement identifier les menaces et diagnostiquer les vecteurs d'attaque, tout en protégeant efficacement le contenu essentiel au sein d'un coffre sécurisé.

Solutions de protection des données Dell Technologies : votre accompagnement vers le Cloud

Vous pouvez protéger les données stratégiques dans le Cloud sans compromettre l'intégrité, la confidentialité ou la disponibilité. La solution Cyber Recovery avec les services de données multi-Cloud pour Dell EMC PowerProtect protège vos données stratégiques en toute confiance, qu'elles soient hébergées dans le Cloud ou sur site à partir d'une destination unique. Pour plus d'informations, commencez ici :

En savoir plus sur Cyber Recovery avec les services de données multi-Cloud pour Dell EMC PowerProtect	Contacter un expert de Dell Technologies	En savoir plus sur les solutions de protection des données et de sauvegarde dans le Cloud	