DELL Technologies

Présentation de solution

Dell EMC PowerProtect Cyber Recovery

Une protection moderne et éprouvée des données stratégiques face aux rançongiciels et aux cyberattaques les plus destructrices

POURQUOI CHOISIR CYBER RECOVERY ?

Les cyberattaques ont pour objectif de détruire, voler ou compromettre d'une manière ou d'une autre vos données les plus précieuses, et notamment vos sauvegardes. Il est donc impératif de protéger les données stratégiques et, en cas d'attaque, de les récupérer en assurant leur intégrité pour pouvoir relancer l'activité de l'entreprise. Dans le cas contraire, votre entreprise peut-elle survivre ? Voici les cinq principes fondamentaux d'une solution Cyber Recovery moderne et éprouvée :

Isolation et gouvernance des données Un environnement de datacenter isolé, déconnecté des réseaux d'entreprise et de sauvegarde, et interdit aux autres utilisateurs que ceux qui disposent des autorisations appropriées.

Copie automatisée des données et isolation physique Créez des copies des données immuables et stockez-les dans un coffre numérique sécurisé, et élaborez des processus capables de générer une isolation physique opérationnelle entre l'environnement de sauvegarde/de production et le coffre-fort.

Analytique intelligente et outils Apprentissage automatique et l'indexation de l'ensemble du contenu avec analytique avancée au sein de la sécurité du coffre-fort. Vérifiez l'intégrité de manière automatisée pour déterminer si les données ont été affectées par des logiciels malveillants et autres outils, afin de prendre en charge des mesures correctives, le cas échéant.

Récupération et mesures correctives Utilisez des workflows et des outils pour gérer la récupération après un incident via des processus de restauration dynamiques, en tirant parti de procédures de reprise après sinistre existantes.

Planification et conception de la solution

Des conseils d'experts vous aideront à sélectionner les jeux de données, applications et autres ressources stratégiques pour déterminer les objectifs de délai de récupération (RTO) et RPO et rationaliser la récupération.

Le défi : les cyberattaques sont l'ennemi numéro un des entreprises fonctionnant sur l'exploitation des données

Les données, devise principale d'une économie axée sur Internet, sont une ressource critique qui doit rester confidentielle et efficacement protégée, tout en étant accessible à l'utilisateur immédiatement. Le marché mondial s'appuie actuellement sur le flux constant des données transitant d'un réseau interconnecté à l'autre, et les efforts en matière de transformation numérique risquent de compromettre toujours plus de données sensibles.

Pour cette raison, les informations de votre organisation sont une proie désirable et très rentable pour les cybercriminels.

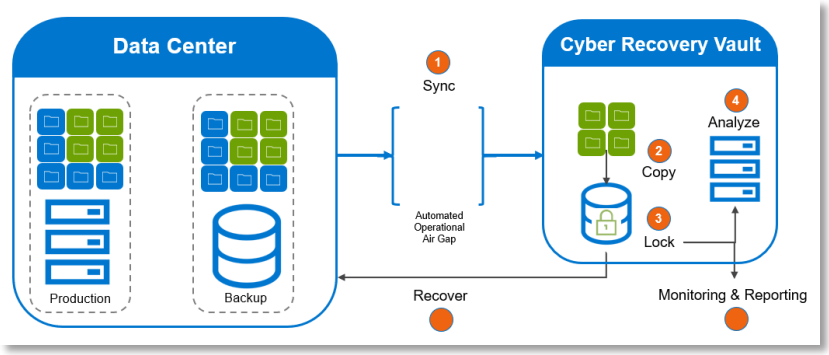
Le cybercrime est le grand vainqueur du transfert des richesses et cela, en exploitant les données. D'après Accenture, 5,2 trillions de dollars de ressources mondiales risquent d'être à la merci des cybercriminels au cours des cinq prochaines années.[i]

Quels que soient le secteur d'activité ou la taille des organisations, les entreprises et administrations s'exposent à des risques de violation de données, de perte de chiffre d'affaires causée par les interruptions de service, d'atteinte à la réputation, ainsi qu'à des amendes élevées en cas de cyberattaque. Le coût annuel moyen du cybercrime par société est monté à 13 millions de dollars USD en 2018, soit une augmentation de 72 % au cours des cinq dernières années.[ii]

Les administrations et entreprises se doivent donc de disposer d'une stratégie Cyber Recovery efficace. D'après une étude de Marsh et Microsoft, menée en 2019, 79 % des responsables mondiaux considèrent les cyberattaques comme l'une des priorités absolues de l'organisation en matière de gestion des risques.[iii]

Dans ce contexte, que pouvez-vous faire pour protéger l'organisation et ses données les plus précieuses ?

La solution : PowerProtect Cyber Recovery

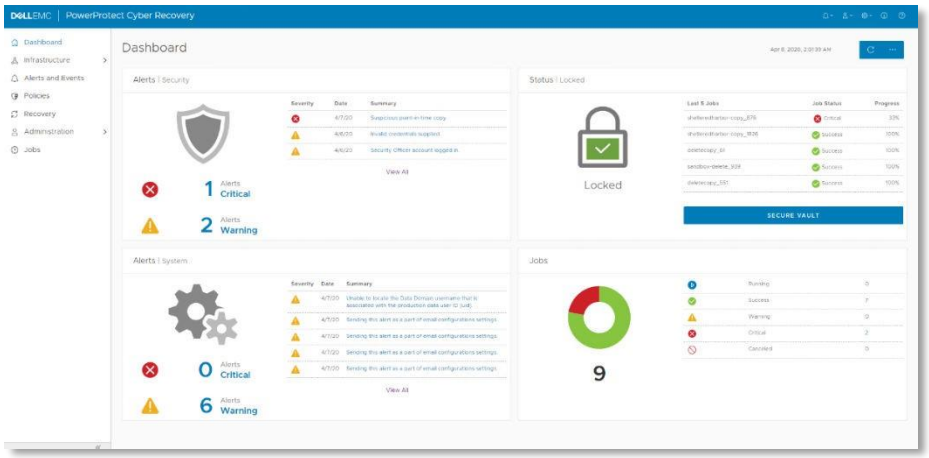


Pour réduire les risques métier entraînés par les cyberattaques et mettre au point une approche de protection des données offrant davantage de cyber-résilience, modernisez et automatisez les stratégies relatives à la continuité d'activité et à la récupération des données, et utilisez les tout derniers outils intelligents pour détecter et vous défendre face aux cybermenaces.

Dell EMC PowerProtect Cyber Recovery offre une protection éprouvée, moderne et intelligente visant à isoler les données stratégiques, à identifier les activités sujettes à caution et à rétablir rapidement le fonctionnement normal des opérations métier.

PowerProtect Cyber Recovery offre une protection éprouvée, moderne et intelligente, qui réduit les risques métier causés par les cybermenaces

- **Coffre Cyber Recovery :** le coffre PowerProtect Cyber Recovery propose plusieurs couches de protection, qui optimisent la résilience de l'infrastructure face aux cyberattaques, même internes. Cette solution déplace les données stratégiques hors de la surface d'attaque, les isolant physiquement dans un espace protégé du datacenter. Pour accéder à cet espace, il vous faut des informations d'identification de sécurité distinctes et une authentification multifacteur.
  Elle propose des protections supplémentaires, par exemple un mécanisme opérationnel automatisé assurant l'isolation du réseau et éliminant les interfaces de gestion susceptibles d'être compromises.
  PowerProtect Cyber Recovery automatise la synchronisation des données entre les systèmes de production et le coffre, créant des copies immuables associées à des politiques de conservation verrouillées. En cas de cyberattaque, vous pouvez rapidement identifier une copie intacte des données, récupérer les systèmes stratégiques et rétablir leur bon fonctionnement.



- **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.
- **Récupération et mesures correctives :** PowerProtect Cyber Recovery comprend des procédures de récupération et de restauration automatisées. Cela permet de remettre rapidement en ligne les systèmes stratégiques, en toute confiance. Pour les clients exécutant Dell EMC NetWorker, via PowerProtect Data Manager, Cyber Recovery propose une fonction de récupération automatisée depuis le coffre. Dell EMC et les partenaires de son écosystème mettent à votre disposition une méthodologie de protection complète des données, effectuent l'analyse forensique et évaluent des dégâts en cas d'attaque, afin de récupérer les systèmes ou d'appliquer des mesures correctives pour supprimer les logiciels malveillants.
- **Planification et conception de la solution :** les services de conseil Dell EMC, proposés en option, vous aident à identifier les systèmes stratégiques à protéger et peuvent élaborer des plans de dépendance pour les applications et services associés, ainsi que l'infrastructure requise pour les restaurer. Ces services génèrent également des exigences en matière de récupération, ainsi que d'autres options de conception possibles. Ils identifient les technologies pour analyser, héberger et protéger vos données, ainsi qu'un dossier commercial et une chronologie pour l'implémentation.

Pour protéger les données critiques des cyberattaques, il vous faut des solutions modernes et éprouvées. Avec PowerProtect Cyber Recovery, vous savez que vous pouvez rapidement identifier et restaurer les données reconnues comme intègres, puis rétablir le fonctionnement normal des opérations métier après une cyberattaque.

En savoir plus sur Dell EMC PowerProtect Cyber Recovery

Contacter un expert Dell EMC

[Source : Étude Accenture The Cost of Cybercrime 2019]
[Source : Étude Accenture The Cost of Cybercrime 2019]
[Source : Enquête de Marsh et Microsoft sur les perceptions en matière de cyber-risques, 2019]