DELL Technologies

Présentation de solution

Dell PowerProtect Cyber Recovery

Protection moderne et résiliente des données stratégiques contre les attaques de rançongiciels et les cyberattaques destructrices.

POURQUOI CHOISIR CYBER RECOVERY ?

Les cyberattaques ont pour objectif de détruire, voler ou compromettre vos données les plus précieuses, d'une manière ou d'une autre. Cela inclut 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 composants d'une solution cyberrésiliente :

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 axées sur les données

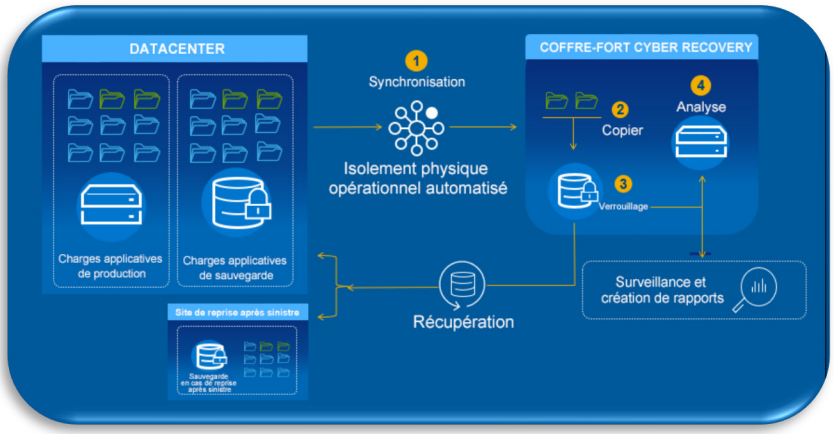
Les données, devise principale d'une économie axée sur Internet, sont une ressource critique qui doit rester confidentielle et efficacement protégée, tout en étant accessible à l'utilisateur immédiatement. Le marché mondial s'appuie actuellement sur le flux constant des données transitant d'un réseau 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. Quel que soit leur secteur d'activité ou leur taille, 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.

Les responsables d'entreprises et d'administrations se doivent de disposer d'une stratégie de cyberrésilience. Pourtant, de nombreuses organisations n'ont pas confiance en leurs solutions de protection des données. Selon le Global Data Protection Index, 79 % des décideurs informatiques craignent de subir un événement perturbateur au cours des 12 prochains mois, et 75 % craignent que les mesures de protection des données en place dans leur organisation ne soient pas suffisantes pour faire face aux logiciels malveillants et aux attaques par rançongiciel[1].

Dans ce contexte, que pouvez-vous faire pour protéger votre organisation, vos clients, vos collaborateurs et ses données les plus précieuses ?

La solution : Dell PowerProtect Cyber Recovery



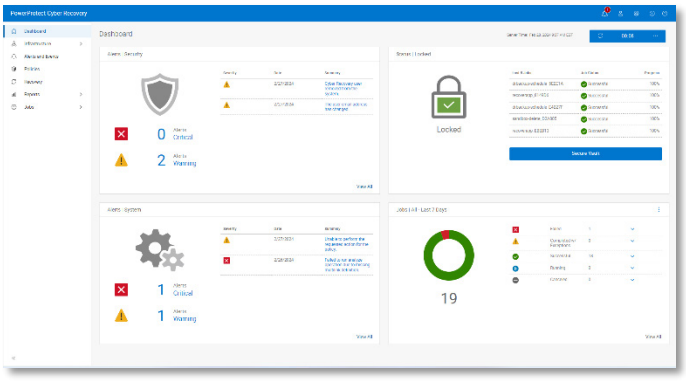
Pour réduire les risques métier entraînés par les cyberattaques et mettre au point une approche de protection des données offrant davantage de cyberrésilience, modernisez et automatisez les stratégies relatives à la continuité d'activité et à la récupération des données, et utilisez les tout derniers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

Dell 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 : immuabilité, isolement et intelligence

Coffre Cyber Recovery

Le coffre-fort PowerProtect Cyber Recovery offre 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. Parmi les protections supplémentaires, citons un air gap opérationnel automatisé pour assurer l'isolation du réseau et éliminer les interfaces de gestion qui pourraient être compromises. PowerProtect Cyber Recovery automatise la synchronisation des données entre les systèmes de production (y compris les mainframe et systèmes ouverts) et le coffre-fort, créant des copies immuables associées à des politiques de conservation verrouillées. En cas de cyberattaque, vous pouvez rapidement identifier une copie adéquate des données, récupérer les systèmes critiques 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 (ML) basé sur l'IA pour analyser plus de 200 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. La récupération est intégrée à votre processus de réponse aux incidents. À l'issue d'un événement, l'équipe chargée de répondre aux incidents analyse l'environnement de production pour déterminer la cause première de l'événement. CyberSense fournit également des rapports d'investigation après cyberattaque pour comprendre la profondeur et l'étendue de l'attaque, ainsi qu'une liste des derniers jeux de sauvegardes fiables avant corruption. Ensuite, lorsque la production est prête pour la récupération, Cyber Recovery fournit les outils de gestion et la technologie pour effectuer la récupération réelle des données. Cette solution automatise la création de points de restauration utilisés pour la récupération ou l'analytique de sécurité.

Planification et conception de la solution

Les services de conseil Dell, proposés en option, vous aident à identifier les systèmes métier 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.

Vous avez besoin de solutions éprouvées, modernes et résilientes pour protéger vos données essentielles contre les cyberattaques. 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.

[1] D'après l'étude « Global Data Protection Index 2023 Snapshot », réalisée par Vanson Bourne à la demande de Dell Technologies, octobre 2023.

En savoir plus sur Dell PowerProtect Cyber Recovery	Contacter un expert Dell Technologies	Afficher plus de ressources	Prenez part à la conversation avec #PowerProtect