Validation technique

Protection des données stratégiques contre les cybermenaces, telles que les rançongiciels, avec une solution complète de coffre-fort numérique

Dell EMC PowerProtect Cyber Recovery avec CyberSense

Par Vinny Choinski, analyste validation senior et Christophe Bertrand, analyste senior

Octobre 2020

Cette validation technique ESG, réalisée à la demande de Dell Technologies, est diffusée sous licence ESG.

© 2020 The Enterprise Strategy Group, Inc. Tous droits réservés.

Sommaire

Introduction 3
Contexte 3
Solution Dell EMC PowerProtect Cyber Recovery 4
Validation technique ESG 5
Coffre-fort PowerProtect Cyber Recovery 5
Vide d'air de Cyber Recovery 8
CyberSense 9
Ce qu'il faut retenir 11

Validations techniques ESG

L'objectif des validations techniques ESG est de sensibiliser les professionnels IT aux solutions de technologies de l'information pour les sociétés de tous types et de toutes tailles. Les validations techniques ESG ne sont pas destinées à remplacer le processus d'évaluation qui doit être mené avant de prendre des décisions d'achat, mais plutôt à fournir des informations sur ces technologies émergentes. Nos objectifs sont d'explorer quelques-unes des principales fonctionnalités et fonctions des solutions IT, de montrer comment elles peuvent être utilisées pour résoudre les problèmes réels des clients et d'identifier les domaines nécessitant des améliorations. Le point de vue d'experts tiers de l'équipe de validation ESG est basé sur nos propres tests pratiques et sur les entretiens avec les clients qui utilisent ces produits dans des environnements de production.

© 2020 The Enterprise Strategy Group, Inc. Tous droits réservés.

Introduction

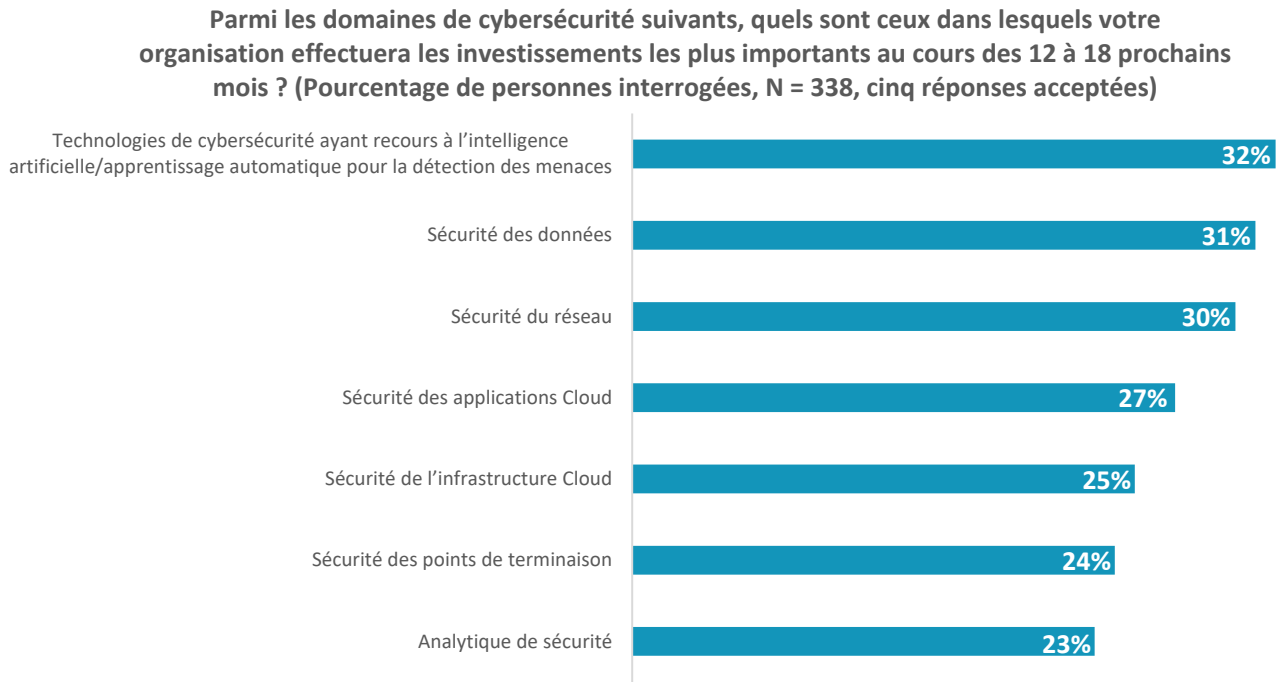
Cette validation technique ESG documente la validation pratique de la solution Dell EMC PowerProtect Cyber Recovery avec CyberSense de Dell Technologies. ESG a réalisé des analyses et des audits des principaux éléments de la solution Cyber Recovery, notamment du coffre-fort Cyber Recovery et de ses multiples couches de sécurité et de protection des données stratégiques, du vide d'air opérationnel et du moteur d'analytique CyberSense.

Contexte

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.

L'étude ESG confirme que la plupart des organisations augmenteront leurs dépenses en cybersécurité en 2020, poussées par le désir de protéger leurs processus métiers et de neutraliser les menaces dangereuses. Si la plupart d'entre elles investiront probablement dans l'analytique basée sur l'intelligence artificielle/l'apprentissage automatique, la sécurité des données, du réseau et des applications, les RSSI répartiront les budgets dans de nombreux domaines (voir Figure 1). Les données indiquent que de nombreuses organisations sont en cours de restructuration de l'intégralité de leur infrastructure de cybersécurité afin d'améliorer l'efficacité, de rationaliser les opérations de sécurité et de prendre en charge de nouveaux processus métiers axés sur les technologies[1].

Figure 1 : Les 7 principaux domaines d'investissement en cybersécurité en 2020



Source : Enterprise Strategy Group

Les pirates à l'origine des rançongiciels et les personnes mal intentionnées ont appris qu'ils ont une meilleure chance d'atteindre leur objectif (se faire payer une rançon ou détruire des données), si aucune sauvegarde n'est disponible pour la récupération. Les données et les systèmes de sauvegarde sont ainsi soumis à des attaques directes. Malheureusement, il

[1] Source : étude ESG, *2020 Cybersecurity Spending Trends*, mars 2020.

© 2020 The Enterprise Strategy Group, Inc. Tous droits réservés.

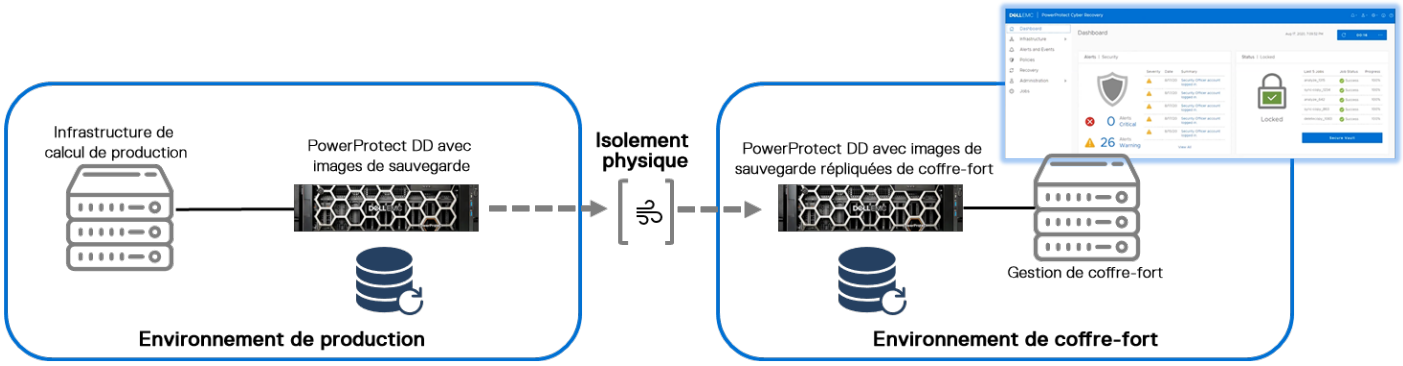
existe plusieurs points vulnérables, car les sauvegardes ont été conçues pour l'accessibilité, et pas nécessairement pour la sécurité. Les systèmes de sauvegarde des données et des applications deviennent des cibles pour les compromissions, car leur accès est basé sur la confiance et peut donc être plus facilement et rapidement infiltré. De plus, les systèmes de sauvegarde contiennent souvent des catalogues de données, et le chiffrement ou la suppression de ces données de catalogue peut rendre la récupération à partir d'une sauvegarde beaucoup plus longue, voire empêcher l'utilisation de la sauvegarde pour la récupération.

Solution Dell EMC PowerProtect Cyber Recovery

La solution Cyber Recovery complète permet de lutter contre les rançongiciels et les cyberattaques destructrices. Cette solution mature, disponible sur le marché depuis 5 ans est utilisée par des centaines de clients. Le logiciel Cyber Recovery automatise la synchronisation des données entre les systèmes de production et le coffre-fort, créant ainsi des copies isolées physiquement et inaltérables avec des règles de conservation avec verrou. En cas de cyberattaque, les utilisateurs peuvent rapidement identifier une copie saine des données, restaurer les systèmes stratégiques et relancer l'activité.

La solution PowerProtect Cyber Recovery s'appuie sur le concept de « coffre-fort » des données qui est souvent isolé physiquement, au sein d'un endroit verrouillé, et toujours isolé logiquement via un vide d'air opérationnel. Le coffre-fort n'est pas un datacenter supplémentaire : il se situe généralement dans le datacenter de production ou d'entreprise, ou parfois chez un fournisseur de solutions tierces. Les composants du coffre-fort ne sont jamais accessibles depuis l'environnement de production. L'accès au coffre-fort s'effectue à travers un « vide d'air opérationnel », comme l'illustre la Figure 2.

Figure 2 : Présentation de la solution Dell EMC PowerProtect Cyber Recovery



Source : Enterprise Strategy Group

Éléments clés de la solution Cyber Recovery :

- Seule la solution PowerProtect Cyber Recovery est dotée d'un vide d'air logique automatisé et orchestré destiné à protéger les données. D'autres solutions revendiquent un « vide d'air », car les données peuvent être séparées du réseau de production (par exemple, copie des données stockée dans le Cloud). Cependant, avec cette approche, les données restent accessibles aux personnes mal intentionnées, et une copie hors site seule n'assure pas un isolement physique complet.

- Le coffre-fort proprement dit de la solution Cyber Recovery est isolé physiquement et logiquement. Il ne peut pas être ouvert ni contrôlé à partir de l'environnement de production et il n'est pas non plus accessible, à moins que la personne ne se trouve physiquement dans le coffre-fort.

© 2020 The Enterprise Strategy Group, Inc. Tous droits réservés.

- La fonctionnalité PowerProtect DD Compliance Retention Lock est conforme à la norme 17a-4(f)(ii). Elle ne peut être désactivée qu'avec un mot de passe distinct du responsable de la sécurité, et uniquement pour les données nouvellement stockées. Cette fonctionnalité a été renforcée pour assurer une meilleure protection contre les attaques encore plus avancées, telles que la manipulation du protocole NTP.

- La solution Cyber Recovery protège le système et permet la récupération des jeux de sauvegardes d'un fournisseur pouvant être écrits sur l'appliance PowerProtect.

- En août 2020, la solution PowerProtect Cyber Recovery est devenue la première, et au moment de la publication de ce document, la seule à avoir été approuvée comme répondant à toutes les exigences de mise en coffre-fort des données de la norme Sheltered Harbor.

En tant qu'élément de PowerProtect Data Manager et pour les utilisateurs exécutant Dell EMC NetWorker, PowerProtect Cyber Recovery permet d'effectuer des récupérations automatisées depuis le coffre-fort. Dell et ses partenaires de l'écosystème fournissent une méthodologie complète pour assurer la protection des données, ainsi que pour effectuer les évaluations et les investigations des dommages afin de restaurer les systèmes ou de corriger et de supprimer les logiciels malveillants incriminés.

Validation technique ESG

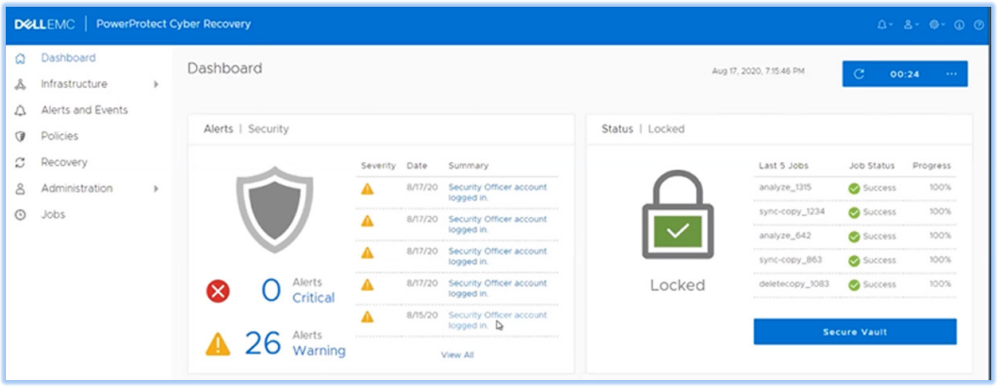
ESG a procédé à la validation et aux tests de la solution PowerProtect Cyber Recovery dans le laboratoire Dell Proof of Concept Engineering Lab. Les tests ont été conçus pour valider l'ensemble des principaux éléments de la solution Cyber Recovery, notamment le coffre-fort Cyber Recovery, le vide d'air opérationnel et le moteur d'analytique CyberSense.

Coffre-fort PowerProtect Cyber Recovery

La solution PowerProtect Cyber Recovery s'appuie sur le déploiement et le fonctionnement d'un « coffre-fort » Cyber Recovery comme élément de base. Le coffre-fort offre plusieurs couches de protection pour assurer la résilience contre les cyberattaques, même en cas de menace interne. Il éloigne les données stratégiques de la surface d'attaque en les isolant physiquement dans une partie protégée du datacenter. De plus, son accès exige des informations d'identification de sécurité distinctes ainsi qu'une authentification multifacteur. Les mesures de protection supplémentaires comportent un vide d'air opérationnel automatisé destiné à assurer l'isolement du réseau, ainsi que l'élimination des interfaces de gestion accessibles à la production qui peuvent être compromises. Comme l'illustre la Figure 3, la solution Cyber Recovery est gérée via une interface intuitive, accessible uniquement à partir du coffre-fort, avec des tableaux de bord complets d'état de la solution. Une interface CLI et des API sont également disponibles pour la gestion. Le logiciel Cyber Recovery déployé dans le cadre de la sécurité de l'environnement du coffre-fort automatise la synchronisation des données entre les systèmes de production et le coffre-fort, puis crée des copies inaltérables à l'aide de règles de conservation avec verrou. En cas de cyberattaque, une copie saine des données peut être rapidement identifiée, et les systèmes métiers stratégiques restaurés.

© 2020 The Enterprise Strategy Group, Inc. Tous droits réservés.

Figure 3 : Tableaux de bord de l'interface de gestion de PowerProtect Cyber Recovery



Source : Enterprise Strategy Group

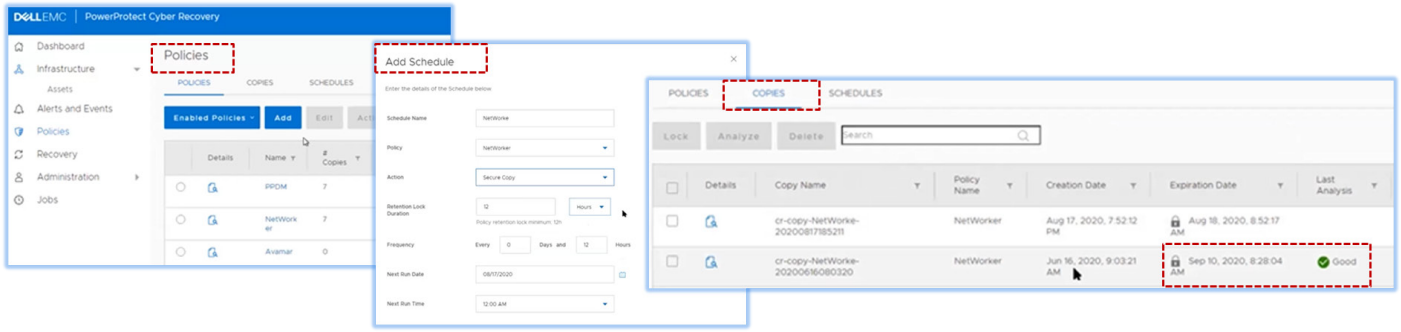
ESG a testé et validé les flux de données opérationnels standard et les performances d'application des systèmes liés à la solution Cyber Recovery, ainsi que ceux qui se trouvent dans le coffre-fort. Les utilisateurs peuvent sauvegarder les applications et les données de production dans une solution telle que l'environnement NetWorker et PowerProtect DD illustré dans l'architecture de référence, même si la solution Cyber Recovery peut s'interfacer avec de nombreuses applications de sauvegarde de fournisseurs différents.

La fonctionnalité de vide d'air est examinée plus en détail dans la section suivante de ce rapport, mais pour l'essentiel, voici ce dont il s'agit : un ou plusieurs ports préconfigurés spécifiques dans le pare-feu du coffre-fort sont destinés à l'ingestion des données, puis le logiciel Cyber Recovery active le port à des intervalles courts en suivant des règles prédéfinies. Les données sont « extraites » par les systèmes du coffre-fort à partir de la solution de sauvegarde, à travers le vide d'air, et dans la cible PowerProtect DD du coffre-fort. Une fois la copie de données ingérée, le port spécifié est désactivé, ce qui permet de reverrouiller efficacement le coffre-fort. En utilisant l'immuabilité WORM et un verrou de conservation conforme à la norme SEC 17a-4(f)(ii), et nécessitant des informations distinctes d'identification d'accès multifacteur et d'un responsable de la sécurité, la conception de la solution Cyber Recovery empêche le piratage du coffre-fort. ESG a vérifié que la solution Cyber Recovery incorpore plusieurs couches de sécurité pour protéger le système des intrus, y compris les utilisateurs internes. Le coffre-fort ne peut pas être ouvert ni contrôlé depuis la production. Les déploiements de coffre-fort utilisent à la fois l'isolement physique et logique : les systèmes de coffre-fort correctement déployés ne sont accessibles que si la personne se trouve physiquement dans le coffre-fort. Les verrous de rétention de données ne peuvent pas être désactivés sans mot de passe distinct d'un responsable de la sécurité distinct.

Comme illustré sur la Figure 4, ESG a utilisé l'interface utilisateur de gestion pour créer facilement des règles Cyber Recovery automatisées. Une fois que la cible PowerProtect DD a ingéré les données, et que le vide d'air a été créé, la solution Cyber Recovery rend la copie et le catalogue connexe inaltérables en plaçant un verrou de conservation suivant des règles prédéfinies sur les fichiers afin de les protéger des suppressions accidentelles ou intentionnelles. Comme indiqué, la conservation en coffre-fort est configurable, mais la plupart des utilisateurs conservent environ un mois de copies.

© 2020 The Enterprise Strategy Group, Inc. Tous droits réservés.

Figure 4 : Gestion des règles de la solution PowerProtect Cyber Recovery



Source : Enterprise Strategy Group

Une fois les données sécurisées, le moteur d'analytique CyberSense intégré peut les analyser pour y détecter des anomalies. ESG a vérifié que CyberSense utilise l'analytique complète du contenu des fichiers et l'apprentissage automatique formé à de nombreux vecteurs d'attaque afin d'identifier les éventuelles compromissions de données. Il fonctionne en toute sécurité dans le coffre-fort, où il évalue les données qui y sont stockées, en effectuant quotidiennement plus de 100 observations par fichier. Ces données sont ensuite évaluées au sein du coffre-fort par un moteur d'apprentissage automatique/intelligence artificielle qui génère un verdict sur leur validité. Tout comme pour la fonctionnalité de vide d'air, les fonctionnalités d'analytique de CyberSense sont étudiées plus en détail plus loin dans ce rapport.

La restauration des données du coffre-fort en cas de cyberattaque ou simplement pour des procédures de test de récupération est stratégique. ESG a vérifié que la solution Cyber Recovery fournit plusieurs méthodes de récupération. La solution comprend des outils d'intelligence en coffre-fort destinés à accélérer la récupération des copies « saines ». CyberSense rend un verdict sur chaque jeu de données afin de déterminer s'il est « OK » ou « suspect ». Les données étiquetées « suspectes » comprennent des informations sur un contenu à risque, de sorte que les autres données « saines » peuvent être utilisées à des fins de récupération. Ainsi, la récupération est la plus rapide et la plus sûre possible, et cela contribue potentiellement à suivre la source de l'attaque. Dell affirme qu'aucune solution concurrente ne fournit de détails, lors d'une première analyse, sur des portions du jeu de données susceptibles d'avoir été affectées. De plus, plusieurs solutions concurrentes s'appuient sur l'envoi ou l'extraction d'informations vers et depuis un plan SaaS dans le Cloud public qui ne sont probablement pas disponibles depuis l'environnement de production, qui est normalement arrêté après les attaques.

En quoi est-ce important ?

De nombreuses organisations conviennent qu'elles subiront une cyberattaque réussie dans un avenir pas si lointain. Leurs réflexions sont passées de la prévention à la résilience : elles souhaitent restaurer leurs systèmes stratégiques aussi rapidement et efficacement que possible après une cyberattaque.

La solution PowerProtect Cyber Recovery facilite une approche de type « coffre-fort » en matière de cyber-résilience. ESG a confirmé que le déploiement et le fonctionnement de la solution de coffre-fort et de ses différents composants sont relativement simples, notamment avec l'aide de Dell EMC Advisory Services.

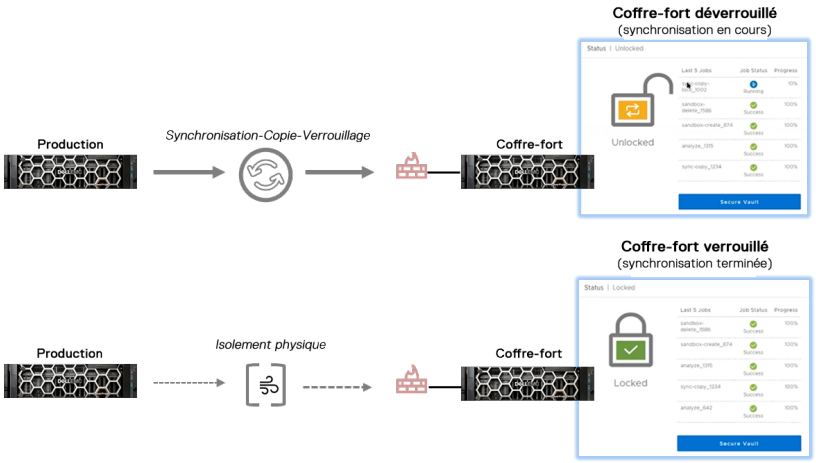
© 2020 The Enterprise Strategy Group, Inc. Tous droits réservés.

Vide d'air de Cyber Recovery

Le concept de « vide d'air » est crucial pour l'approche de type « coffre-fort » utilisée par la solution PowerProtect Cyber Recovery. La création d'un vide d'air qui isole véritablement l'environnement du coffre-fort des systèmes externes et de la connectivité nécessite une ingénierie minutieuse et une conception de solution innovante. Dell qualifie sa mise en œuvre de « vide d'air opérationnel » pour la différencier de l'ancienne définition de « vide d'air », qui identifie un réseau qui n'est jamais connecté en externe. Le vide d'air de Cyber Recovery est également « opérationnel », car l'ingestion des données et la gestion du processus sont automatisées et suivent des règles prédéfinies. De plus, elles ne nécessitent aucune intervention manuelle.

Comme illustrés en Figure 5 et vérifiés par ESG, le coffre-fort ainsi que ses systèmes et données sont isolés physiquement et logiquement, sauf pendant le processus réel d'ingestion des données. Du point de vue de la sécurité du coffre-fort, le logiciel PowerProtect Cyber Recovery lance un transfert de données planifié en désignant, configurant et activant brièvement un port réseau unique sur une interface dédiée à cet effet. Dans le laboratoire Dell Proof-of-Concept Engineering Lab, les données ont été transférées entre un système PowerProtect DD 9900 utilisé comme périphérique de sauvegarde côté production, sur une connexion réseau brièvement activée, vers un système cible PowerProtect DD 9900 dans le coffre-fort. Les données ont été « extraites » du système de sauvegarde côté production, de sorte qu'elles n'ont pas participé à la gestion ni au fonctionnement de la connexion réseau. Dès la fin du transfert de données, la connexion réseau n'a pas seulement été interrompue, mais l'interface elle-même a été désactivée, permettant ainsi de rétablir l'isolement complet du coffre-fort via un vide d'air opérationnel. La gestion du vide d'air a été entièrement contrôlée par le logiciel Cyber Recovery depuis le coffre-fort. Et même lorsque l'isolement par vide d'air a été brièvement déverrouillé, l'accès était extrêmement limité : seule la destination de la réplication est toujours accessible, pour accepter les données mises à jour. Les composants du coffre-fort, y compris les copies de données antérieures, ne sont jamais accessibles.

Figure 5 : Vide d'air opérationnel de PowerProtect Cyber Recovery



Source : Enterprise Strategy Group

© 2020 The Enterprise Strategy Group, Inc. Tous droits réservés.

En quoi est-ce important ?

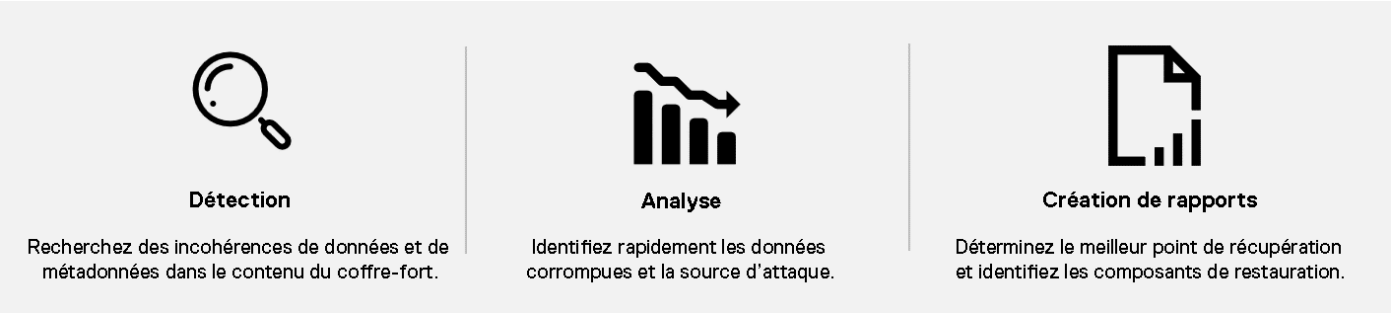
Le coffre-fort Cyber Recovery est une solution puissante qui améliore la cyber-résilience organisationnelle. Cependant, elle n'est pas aussi efficace que l'approche et la technologie de vide d'air utilisées pour établir et maintenir l'isolement. ESG a confirmé que la solution de vide d'air opérationnel utilisée par Cyber Recovery est une solution de pointe, qu'elle exécute la fonction prévue et qu'elle constitue une solution sécurisée pour protéger les données stratégiques contre les cyberattaques, les rançongiciels, les logiciels malveillants et les autres menaces observées par ESG sur le marché.

Pour toutes les organisations et tous les décideurs informatiques qui évaluent différentes solutions de cyber-résilience, avoir confiance en la capacité à isoler les données des cyber-intrusions continues est un élément clé d'une solution de cyber-résilience fructueuse.

CyberSense

ESG a validé la configuration et le fonctionnement de base du moteur d'analytique CyberSense et de ses fonctionnalités au sein de l'environnement de la solution PowerProtect Cyber Recovery implémenté dans le laboratoire Dell Proof-of-Concept Engineering Lab. CyberSense est intégré à la solution Cyber Recovery globale et ajoute une couche de protection intelligente pour détecter la corruption des données en cas de cyberattaque sur les environnements de sauvegarde et de production du datacenter. Le moteur d'analytique CyberSense fournit une indexation complète du contenu et utilise l'apprentissage automatique pour analyser plus de 100 statistiques basées sur le contenu afin de détecter des signes de corruption due aux cyber-intrusions. Dell affirme que CyberSense détecte les corruptions avec jusqu'à 99,5 % de confiance, ce qui permet aux utilisateurs d'identifier les menaces et de diagnostiquer les vecteurs d'attaque tout en protégeant les contenus stratégiques, le tout dans la sécurité du coffre-fort. La Figure 6 illustre les étapes de base du processus d'analytique et de création de rapport CyberSense.

Figure 6 : Processus d'analytique et de création de rapport CyberSense



Source : Enterprise Strategy Group

- Les données sont numérisées dans leur format de stockage dans le coffre-fort (par exemple, les sauvegardes restent au format de sauvegarde).
- L'analytique effectue plus de 100 observations par fichier, notamment des mesures telles que l'entropie et la similarité.
- Ces observations sont collectées et évaluées par un outil d'apprentissage automatique qui a identifié des schémas indiquant que des données ont été corrompues. Comme elle recherche des schémas, et pas des signatures, l'analyse est plus efficace et n'a pas besoin d'être mise à jour aussi fréquemment. Le processus est répété à chaque insertion d'un nouveau jeu de données dans le coffre-fort.

© 2020 The Enterprise Strategy Group, Inc. Tous droits réservés.

- Les outils d'analytique et de création de rapport contribuent à identifier rapidement les données corrompues et la source d'une attaque, ce qui permet une récupération plus rapide et plus sûre.

Une fois que les données sont répliquées vers le coffre-fort Cyber Recovery et qu'un verrou de conservation est appliqué, CyberSense analyse les données de sauvegarde, en créant des observations ponctuelles de fichiers et de bases de données. L'analytique des données du coffre-fort est un élément important pour maintenir l'intégrité de ces données et permettre une récupération rapide après une attaque. L'analytique contribue à déterminer si un jeu de données est valide et utilisable pour la récupération ou s'il a été corrompu ou altéré de façon incorrecte, de sorte qu'il est « suspect » et potentiellement inutilisable.

CyberSense détecte les suppressions groupées, les chiffrements et d'autres types de modifications des fichiers et des bases de données qui résultent de cyberattaques courantes. Cette détection s'effectue directement sur les données de l'image de sauvegarde sans besoin du logiciel de sauvegarde d'origine. L'analytique générée inclut les incompatibilités de types de fichiers, les corruptions, les extensions de rançongiciels connus, les suppressions, l'entropie, la similarité, etc. Les résultats d'analytique sont ensuite utilisés par les algorithmes d'apprentissage automatique pour prendre une décision déterministe sur la corruption des données, révélatrice d'une cyberattaque. Les algorithmes d'apprentissage automatique ont été formés par l'ensemble des derniers chevaux de Troie et rançongiciels et peuvent être mis à jour à mesure que de nouveaux vecteurs d'attaque sont détectés. L'analytique CyberSense est particulièrement puissante, car (a) elle peut lire le format de sauvegarde de sorte qu'il n'est pas nécessaire de restaurer les données, ce qui est difficile à automatiser et peut exposer le coffre-fort à un risque potentiel ; et (b) elle évalue l'intégralité du contenu du fichier, et pas seulement ses métadonnées, pour fournir des connaissances améliorées.

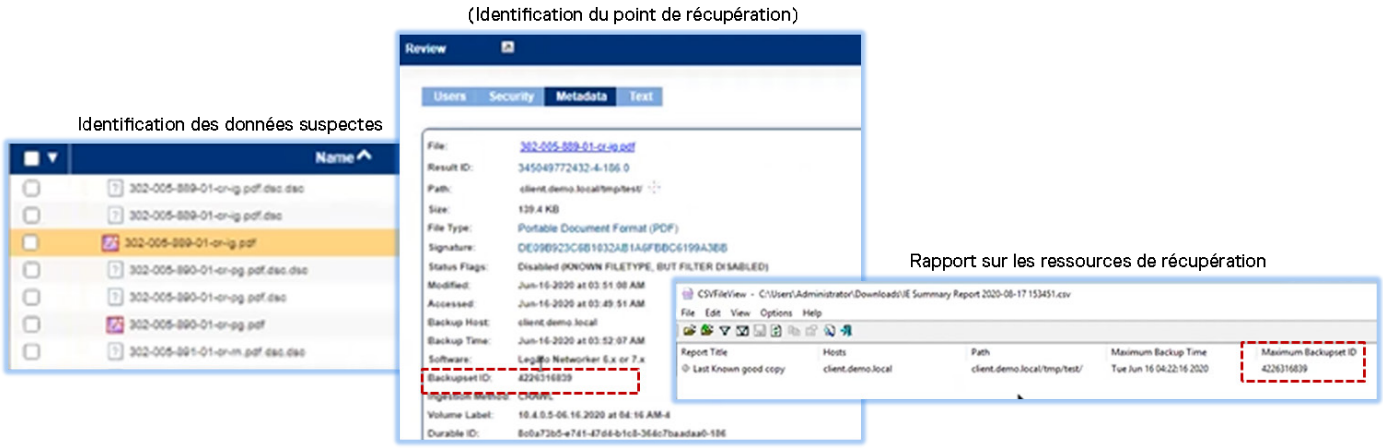
La solution CyberSense va bien au-delà des solutions de métadonnées uniquement, car elle est basée sur l'analytique du contenu complet des fichiers mis en coffre-fort, ce qui fournit un degré élevé de confiance dans la détection de la corruption des données. Elle vérifie les fichiers et les bases de données pour y détecter les attaques qui comportent une corruption de la structure de fichiers basée sur le contenu uniquement ou un chiffrement partiel dans un document ou une page d'une base de données. Ces attaques sont indétectables sans l'analytique interne du fichier pour comparer son évolution dans le temps. Sans analytique complète du contenu, le nombre de faux négatifs est significatif, donnant un faux sentiment de confiance en l'intégrité et la sécurité des données.

Les observations en continu des données permettent à CyberSense de suivre l'évolution du contenu des fichiers au fil du temps. CyberSense génère des résultats d'analytique à partir d'une gamme complète de types de données : infrastructure centrale (par exemple DNS, LDAP et Active Directory), fichiers de données non structurées (documents, contrats et accords), propriété intellectuelle et bases de données (Oracle, DB2, SQL, Epic Caché, etc.).

Si CyberSense détecte des signes de corruption, il génère une alerte qui inclut le vecteur d'attaque et la liste des fichiers concernés. Une alerte critique s'affiche dans le tableau de bord Cyber Recovery, puis les rapports d'investigation CyberSense post-attaques sont disponibles pour diagnostiquer et restaurer rapidement les données à partir de l'attaque par rançongiciel. Comme illustré en Figure 7, avec CyberSense, les organisations peuvent vérifier proactivement leurs fichiers et bases de données pour déterminer le début d'une attaque, puis les restaurer rapidement avec la dernière version des données correcte, peut-être même avant qu'il n'y ait une interruption de l'activité.

© 2020 The Enterprise Strategy Group, Inc. Tous droits réservés.

Figure 7 : Mesure corrective de CyberSense



Source : Enterprise Strategy Group

En quoi est-ce important ?

Isoler des copies des données cruciales du reste du datacenter est une chose, avoir la certitude que ces copies peuvent être utilisées pour restaurer les opérations métiers en toute sécurité en est une autre. Ce qui compte le plus pour les organisations qui déploient des solutions de cyber-résilience telles que PowerProtect Cyber Recovery, c'est d'avoir la certitude que certains jeux de données peuvent réellement être utilisés pour restaurer des systèmes stratégiques.

L'analytique CyberSense complète le processus de Cyber Recovery en offrant aux utilisateurs l'assurance que les données contenues dans le coffre-fort Cyber Recovery sont « saines » et utilisables à des fins de récupération effective. L'analytique du contenu complet et des données orientées apprentissage automatique est à la pointe pour ce type d'opérations. Ainsi, les organisations qui dépendent de PowerProtect Cyber Recovery ont la certitude qu'elles font tout ce qu'elles peuvent pour accroître leur cyber-résilience et réduire les risques et les coûts liés aux cyberattaques et aux intrusions.

Ce qu'il faut retenir

Les organisations s'éloignent de la cybersécurité pour se tourner vers une approche plus globale appelée cyber-résilience. Plutôt que d'espérer pouvoir vaincre les cybermenaces à 100 %, elles partent du principe qu'une cyberattaque finira par réussir, et qu'elles devront se remettre de l'attaque et reprendre leurs activités aussi rapidement et économiquement que possible.

Pour réussir à restaurer les données et systèmes stratégiques après une cyberattaque, des copies d'applications et de jeux de données non affectées ou « saines » doivent être disponibles. Le défi est de savoir comment une organisation s'assure de l'existence de données saines et d'applications non affectées. Pour de nombreuses organisations, la réponse consiste à isoler physiquement et logiquement les copies de données de tous les systèmes de production et de sauvegarde normaux, puis à analyser ces données à l'intérieur de l'environnement de type « coffre-fort » sécurisé afin de détecter toute corruption et d'identifier les copies saines pouvant être utilisées en toute confiance pour la reprise des opérations.

La solution PowerProtect Cyber Recovery de Dell Technologies répond à une exigence importante du marché de la cyber-résilience en pleine expansion en fournissant une solution complète de coffre-fort numérique, d'analyse des données et de cyber-récupération. La solution Cyber Recovery intègre des éléments clés d'une solution globale, notamment une

© 2020 The Enterprise Strategy Group, Inc. Tous droits réservés.

protection automatisée de pointe par « vide d'air », ainsi qu'un moteur d'analytique éprouvé basé sur l'intelligence artificielle qui fonctionne à partir de la sécurité de l'environnement de coffre-fort.

Les stratégies de cyber-résilience utilisent souvent des termes tels que « confiance » et « assurance » pour décrire les niveaux d'efficacité fournis par telle ou telle solution. L'évaluation pratique d'ESG a confirmé que les organisations qui déploient la solution PowerProtect Cyber Recovery peuvent en effet indiquer aux actionnaires qu'elles possèdent un niveau de confiance élevé en matière de récupération des systèmes après une cyberattaque et que l'entreprise sera à nouveau opérationnelle et rentable avec le moins d'interruptions possible.

La confiance est cruciale sur le marché. La solution PowerProtect Cyber Recovery offre une protection des données éprouvée et moderne qui améliore la cyber-résilience. C'est exactement ce que recherchent nombre d'organisations.

Tous les noms de marques sont la propriété de leurs sociétés respectives. The Enterprise Strategy Group (ESG) considère que les informations contenues dans cette publication proviennent de sources connues comme fiables, mais ne garantit pas leur exactitude. Cette publication peut comporter des informations reflétant des opinions propres à ESG et qui sont susceptibles de changer. Cette publication a fait l'objet d'un dépôt légal par The Enterprise Strategy Group, Inc. Toute reproduction ou redistribution partielle ou totale de cette publication, au format papier, électronique ou autre, à des personnes non autorisées à la recevoir, sans le consentement exprès de The Enterprise Strategy Group, Inc., constitue une violation de la loi américaine relative aux droits d'auteur et entraînera une action civile et, le cas échéant, des poursuites judiciaires. Pour toute question, veuillez contacter le service client d'ESG au 508.482.0188.

Enterprise Strategy Group est une entreprise de recherche, de validation, de stratégie et d'analyse IT qui fournit des perspectives interactives et intelligentes à la grande communauté des technologies de l'information.

© 2020 The Enterprise Strategy Group, Inc. Tous droits réservés.

www.esg-global.com contact@esg-global.com 508.482.0188