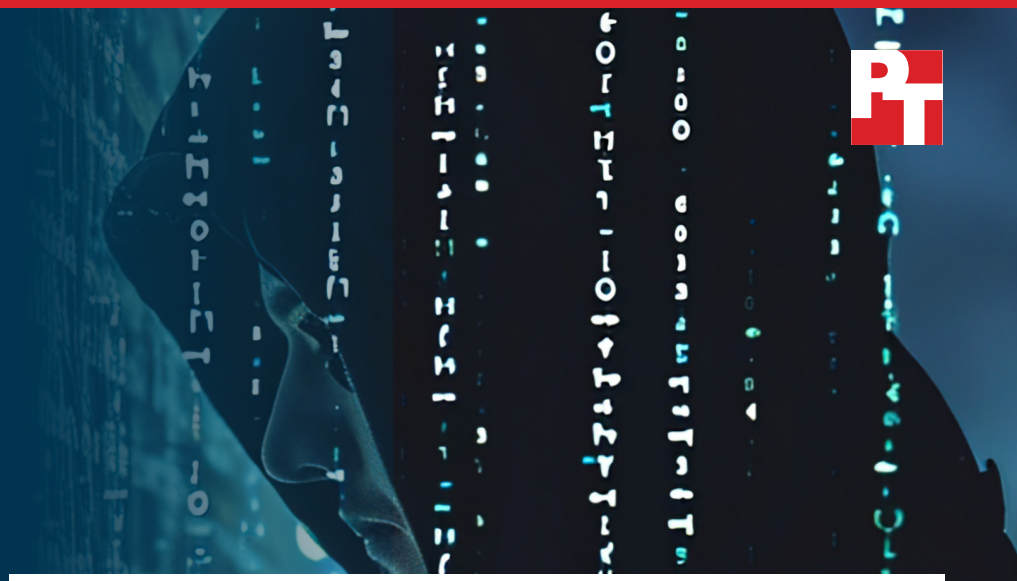

Renforcer votre plan de protection des données avec une solution de cyber-récupération à action rapide et plus robuste

Selon nos recherches, Dell Technologies PowerProtect Cyber Recovery peut fournir un isolement physique pour les coffres-forts de sauvegarde et une analyse plus approfondie des rançongiciels

Isolation par air gap physique pour les coffres-forts de sauvegarde

Création d'une barrière physique que les données ne peuvent pas franchir

Analyse plus approfondie pour détecter les ransomwares

CyberSense examine les contenus des fichiers et les bases de données, pas seulement les métadonnées

Analyse du double de charges applicatives d'anomalies

Recherche des logiciels malveillants dans plus d'endroits avec un seul outil

Le coût moyen d'une attaque par rançongiciel a augmenté de près de 20 % sur deux ans pour atteindre 5,23 millions de dollars.[1] Efficaces, les solutions de cyber-récupération peuvent aider à limiter, voire à éviter ces coûts éventuels en apportant aux organisations des capacités de récupération rapide après un incident, de réduction des interruptions de service et des pertes de données, tout en préservant l'intégrité de leur marque dans le processus. Ces solutions doivent identifier et restaurer les données fiables après une attaque, afin que l'organisation puisse récupérer les données et les systèmes stratégiques, tout en réduisant les risques métier et les interruptions de service.

Dell PowerProtect Cyber Recovery (Cyber Recovery) est une solution de ce type. Elle aide les organisations à protéger leurs données et leurs applications contre les ransomwares, les cyberattaques destructrices et les événements inattendus. Ce rapport utilise des données accessibles au public pour comparer les fonctionnalités fondamentales de protection des données de Cyber Recovery et d'une solution concurrente, Rubrik Security Cloud (RSC). Plus précisément, nous avons examiné les fonctionnalités que les clients des solutions de cyber-récupération peuvent trouver importantes, notamment le coffre-fort de récupération, l'immuabilité, la prise en charge des charges applicatives, la technologie d'analyse, la capacité de récupération et l'isolement.

À la différence de RSC, Cyber Recovery utilise une approche multicopie, ce qui signifie qu'après avoir créé des sauvegardes, il copie ces sauvegardes (ou normalement un sous-ensemble sélectionné) vers un stockage isolé à des fins de sauvegarde et d'analyse. Cyber Recovery comprend plusieurs composants, notamment un ou plusieurs coffres-forts de stockage, situés soit sur site dans une appliance PowerProtect Data Domain, soit software-defined dans le Cloud via Dell APEX protection Storage for Public Cloud. En comparaison, RSC n'offre pas d'options de coffre-fort local. Cyber Recovery comprend également CyberSense, un moteur d'analytique de la sécurité intelligent entièrement automatisé et intégré qui analyse les données, les fichiers, les bases de données et les images du coffre-fort à la recherche de signes de corruption suite à une attaque par rançongiciel. La solution CyberSense peut analyser deux fois plus de charges applicatives d'anomalies que la solution Rubrik, ce qui pourrait permettre au système d'apprentissage automatique (ML) d'analyse CyberSense de repérer les effets des logiciels malveillants ou d'autres menaces dans un plus grand nombre de données. Nous allons découvrir dans quelle mesure PowerProtect Cyber Recovery fonctionne différemment et pourrait être plus avantageux pour votre organisation.

Présentation du produit

Présentation de Dell PowerProtect Cyber Recovery

Dell PowerProtect Cyber Recovery comprend une appliance de stockage qui héberge les données de production et une appliance de stockage cible dans le coffre-fort pour la réplication. Elle comprend également le logiciel Cyber Recovery, qui coordonne la synchronisation, gère plusieurs copies de données sur le système PowerProtect Data Domain (PPDD) dans le coffre-fort Cyber Recovery, supervise le processus de récupération et supervise le processus d'analytique avec CyberSense.

La solution permet de transférer des données uniques de la structure MTree de production vers la structure homologue du coffre-fort via la réplication de structure MTree et permet l'immuabilité des données* pendant une durée définie. Le coffre-fort est doté d'un serveur qui contient le logiciel Cyber Recovery et d'un composant dans lequel la solution restaure les applications et les données de sauvegarde. Chaque coffre-fort Cyber Recovery héberge généralement de nombreux composants de ce type. Le coffre-fort contient également un hôte d'analytique/d'indexation équipé d'un logiciel d'analyse des données, ce qui permet une intégration directe entre le logiciel Cyber Recovery et CyberSense.

*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.

La Figure 1 présente la solution Dell Cyber Recovery.

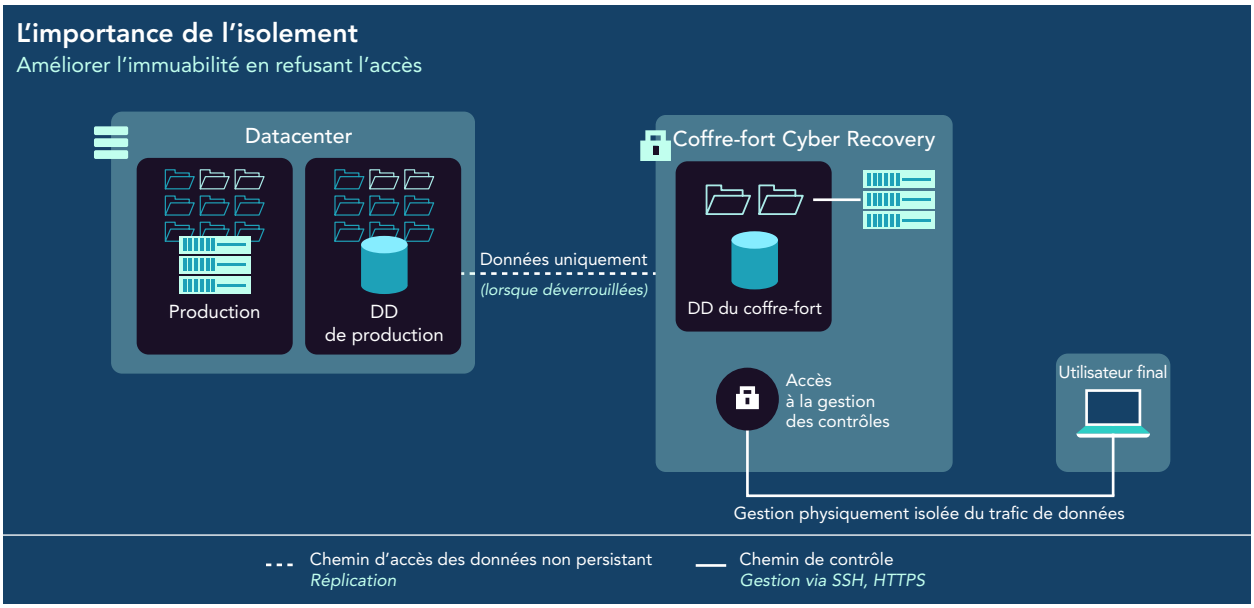

Figure 1 : Données de haut niveau et architecture de chemin de contrôle du coffre-fort Cyber Recovery.
Source : Principled Technologies.

Pour en savoir plus sur les composants clés de la solution Dell PowerProtect Cyber Recovery, lisez le Guide de solutions Dell PowerProtect Cyber Recovery.

Présentation de Rubrik Security Cloud

Rubrik décrit Rubrik Security Cloud comme une plateforme SaaS (Software-as-a-service) qui permet aux clients de « sécuriser [leurs] données, de surveiller les risques liés aux données et de restaurer rapidement [leurs] données, où qu'elles se trouvent, dans l'entreprise, dans le Cloud et dans les applications SaaS ».[4] L'entreprise Rubrik déclare avoir créé la solution sur une « architecture de microservices sécurisée utilisant des services haute disponibilité et une infrastructure s'exécutant dans Google Cloud Platform (GCP) ».[5] La Figure 2 illustre la structure générale de Rubrik Security Cloud.

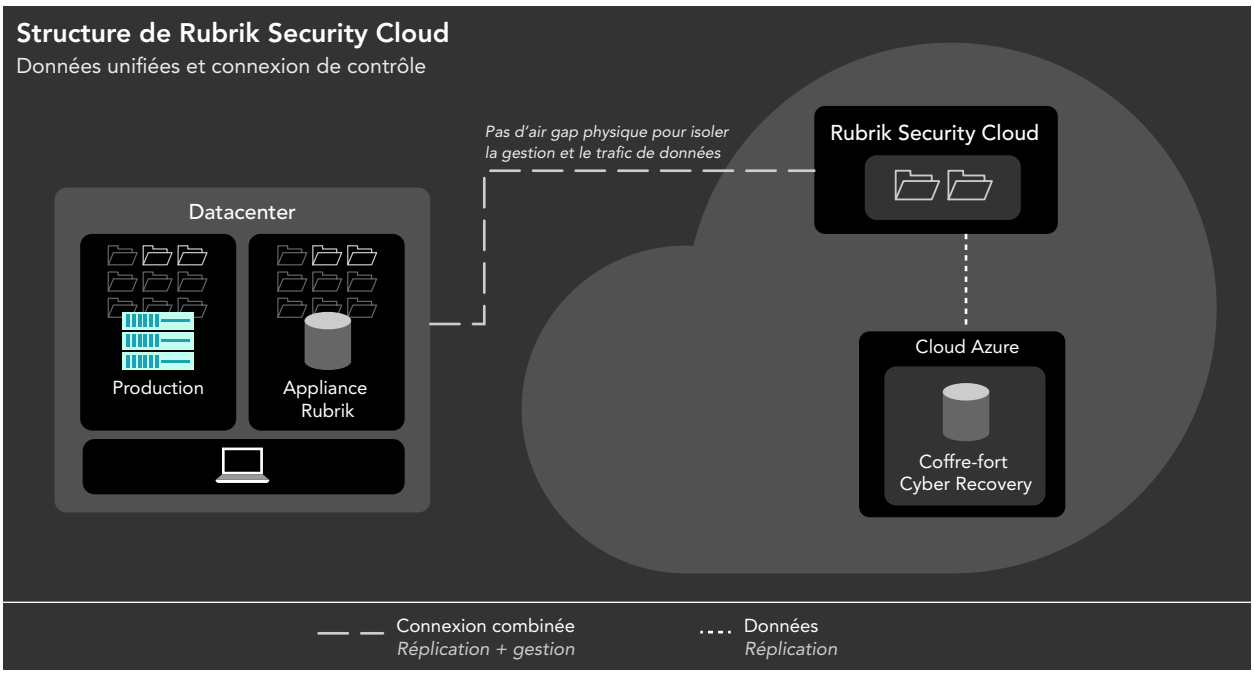

Figure 2 : Structure générale de Rubrik Security Cloud. Source : Principled Technologies.

Fonctions prises en charge

Coffre-fort de récupération

Les coffres-forts sont le stockage dédié qui héberge les copies chiffrées des sauvegardes effectuées par la solution dans votre environnement de production. Les coffres-forts ne font pas partie des solutions de sauvegarde de production. Ils servent, indépendamment, d'emplacement de sauvegarde isolé à partir duquel les clients peuvent restaurer les sauvegardes validées.

Dell propose plusieurs options de coffre-fort, y compris sur site, sur un site de colocation distant ou dans un Cloud public. Le coffre-fort sur site tire parti d'un PPDD opérationnel isolé physiquement (air gap), qui réside dans votre datacenter, potentiellement dans le même rack que votre solution de sauvegarde. Une solution à air gap est généralement physiquement isolée de l'environnement de production. Un coffre-fort colocalisé hors site nécessite des connexions réseau dédiées à un coffre-fort physique, comme pour une version sur site, mais le coffre-fort est séparé géographiquement dans un datacenter distant. Dell fournit également des coffres-forts dans le Cloud public, en partenariat avec les fournisseurs de services Cloud Amazon Web services (AWS), Microsoft Azure et Google Cloud. Les coffres-forts de Cloud public peuvent offrir une flexibilité de configuration pour répondre aux besoins des clients.[6, 7, 8]

Rubrik Cyber Recovery est un composant de Rubrik Security Cloud. Fourni via un modèle de logiciel as-a-service, le coffre-fort de récupération utilise le stockage sur Microsoft Azure uniquement. La plupart des documents accessibles au public que nous avons trouvés dans notre étude associent le coffre-fort Rubrik Cyber Recovery à Rubrik Cloud Vault, le niveau de sauvegarde, qui assure l'immuabilité.[9, 10] Ce coffre-fort ne nécessite aucun matériel supplémentaire et peut être utilisé par n'importe quelle version de la plateforme Rubrik Cloud Data Management (CDM) à partir de la version 6.02.

Immuabilité

L'immuabilité fait référence à la condition d'être immuable ou permanente. Les sauvegardes et copies de sauvegarde immuables permettent aux administrateurs d'établir une permanence pour des fichiers que ni les utilisateurs ni les systèmes ne peuvent modifier ou supprimer tant qu'un délai imparti n'est pas écoulé. Ensuite, les fichiers sont « transférés » : la solution les enlève automatiquement. Généralement, les solutions exécutent ce processus via des règles ou des définitions qui régissent la façon dont le système traite les fichiers.[11]

L'immuabilité de Dell PowerProtect Cyber Recovery repose sur des verrous de conservation, via la fonctionnalité Retention Lock, pour empêcher la suppression, la modification (sur une période donnée) ou l'expiration anticipée forcée des copies de sauvegarde. (Le PPDD est un système de fichiers à ajout uniquement, que l'organisation ait activé Retention Lock ou non.[12]) Les clients Dell gèrent les sauvegardes à l'aide de MTree PPDD, qui sont des partitions logiques définies par l'utilisateur avec des paramètres de rétention indépendants, qu'ils attribuent en tant que destinations d'application de sauvegarde.[13] Les clients peuvent choisir entre deux types de verrous de rétention : conservation et conformité. Les verrous de conformité sont les plus stricts et sécurisés des deux. Les clients activent les verrous de conservation par MTree, ce qui signifie que tous les fichiers d'une MTree donnée respectent la définition de verrouillage de conservation pour cette MTree et définissent la durée de conservation au niveau de chaque fichier. Une fois que les clients ont défini un verrou de rétention de conformité, aucun utilisateur ou système ne peut le supprimer. Un administrateur peut rétablir un verrou de conservation de gouvernance, l'option la moins stricte.[14]

L'immuabilité de la solution Rubrik repose également sur des verrous de rétention pour empêcher la suppression ou l'expiration anticipée forcée des copies de sauvegarde. À l'instar de PowerProtect Cyber Recovery, la solution Rubrik ajoute de nouvelles données au système de fichiers plutôt que d'écraser les données existantes. La solution imprime les données entrantes et les stocke avec les données. **La solution Rubrik n'active pas les verrous de rétention par défaut** et les clients doivent ouvrir un ticket auprès du support Rubrik ou activer une règle à deux personnes pour autoriser les verrous de rétention. (Avant Rubrik Cloud Data Management version 7.0.1, les clients devaient contacter le support Rubrik pour activer les verrous de rétention ; la documentation Rubrik n'indique pas clairement si les clients doivent toujours contacter le support pour que cela fonctionne ou non.) Une fois que les clients les ont activés, les verrous de rétention empêchent les utilisateurs ou les systèmes de supprimer des données en dehors des paramètres définis. Les verrous de conservation Rubrik nécessitent un serveur NTP (Network Time Protocol) externe pour la synchronisation de l'heure, ce qui pour les acteurs malveillants peut présenter une opportunité de manipuler la source NTP de référence et, par conséquent, de faire expirer prématurément les verrous de conservation.[15]

> *« La solution Rubrik n'active pas les verrous de rétention par défaut et les clients doivent ouvrir un ticket auprès du support Rubrik ou activer une règle à deux personnes pour autoriser les verrous de rétention. »*

Licences et abonnements

Dell PowerProtect Cyber Recovery est une solution sous licence. Lors de l'installation, Dell installe une licence d'évaluation de 90 jours par défaut. Au bout de 90 jours, les clients doivent acheter une nouvelle licence pour continuer à utiliser le produit. Dell propose des licences standard (permanentes) et des licences par abonnement.

Rubrik intègre Rubrik Cyber Recovery dans Rubrik Security Cloud (RSC). Pour utiliser Rubrik Cyber Recovery, les clients doivent disposer d'un abonnement à Rubrik Enterprise Edition. La durée d'abonnement est de trois ans.[16, 17] En cas de défaillance du RSC, les charges applicatives SAP HANA et Db2 nécessitent des outils tiers pour restaurer les données, ce qui peut entraîner des coûts d'abonnement supplémentaires.[18]

Accès à la gestion

La gestion du système Dell PowerProtect Cyber Recovery est locale, quelle que soit la topologie choisie par les clients pour le déploiement. Du fait que la solution initie la récupération depuis le coffre-fort, les administrateurs se connectent à l'interface de gestion depuis leur coffre-fort, quel que soit son emplacement. Les coffres-forts sur site offrent aux administrateurs un accès local, ne nécessitant pas d'accès Internet. En effet, les cyberattaques peuvent gravement entraver

la connexion à Internet, soit par déni de service, soit en raison d'une coupure de la connexion à Internet pour sécuriser les données, comme le recommande le NIST (National Institute of Standards and Technology). Les coffres colocalisés permettent d'avoir un accès physique à l'appareil depuis un site distant et utilisent des connexions en dehors du réseau public internet. Les coffres-forts basés sur le Cloud nécessiteraient un accès à Internet pour la récupération, ce qui pourrait retarder la récupération sur site jusqu'à ce que la cyberattaque prenne fin et que la connectivité réseau normale reprenne.

La gestion de Rubrik Cyber Recovery nécessite un accès à Rubrik Security Cloud, qui nécessite un accès à Internet. Comme nous l'avons noté, ce type de connectivité peut retarder la récupération sur site jusqu'à ce que la fonctionnalité réseau revienne à la normale après une cyberattaque.

Étant donné que les clients doivent avoir accès à RSC pour utiliser les fonctionnalités Rubrik Cyber Recovery, RSC devient un point de défaillance unique. Si ce service devenait inaccessible, cela pourrait entraver la récupération des données à partir du coffre-fort pour le client concerné. Rubrik peut récupérer 10 charges applicatives lors d'une interruption de service RSC, mais deux charges applicatives de base de données nécessitent des outils tiers et l'aide du support Rubrik pour les récupérer.[19, 20] En outre, les comptes d'administrateur compromis ou les acteurs malveillants ayant accès à la plateforme RSC auraient accès à l'ensemble du parc, plutôt qu'à un seul coffre-fort.

Plus d'aide avec Managed Detection and Response de Dell

Certaines organisations peuvent ne pas se sentir à l'aise à l'idée de faire cavalier seul en matière de cybersécurité. Dell propose à ces clients Managed Detection and Response (MDR), un service entièrement géré qui surveille et détecte les menaces et les risques, et travaille avec les clients pour atténuer ces risques. Selon Dell, le service offre les avantages suivants :[21]

- Support fiable, y compris des conseils d'experts pour le déploiement et la configuration des plateformes d'analytique de sécurité de détection et réponse étendues (XDR) prises en charge par Dell
- Réponse aux menaces et configuration de la sécurité, y compris jusqu'à 40 heures de configuration de la sécurité liée aux services incluses par trimestre
- Détection et investigation 24/7, comprenant une recherche proactive des menaces spécifique à l'environnement de chaque client afin de découvrir de nouvelles menaces ou des variantes de menaces connues qui échappent aux systèmes de sécurité
- Initiation aux réponses aux cyberincidents, y compris 40 heures d'assistance annuelle en cas d'incident à distance qui permet de lancer rapidement les activités d'enquête

Associée à APEX Cyber Recovery Services, MDR permet aux clients de choisir parmi de nombreuses options pour surveiller, détecter et limiter les menaces et les risques. La disponibilité d'options peut impliquer une couverture étendue ou une approche hybride adaptée aux besoins de votre organisation.

Pour plus d'informations sur MDR, rendez-vous sur **https://www.dell.com/en-us/dt/services/managed-services/managed-workplace-services/managed-detection-response.htm**.

Fluidité

Configuration

La configuration de Dell PowerProtect Cyber Recovery consiste à installer un logiciel sur un système Linux ou à créer une appliance VMware® vSphere® à partir d'un modèle Open Virtualization Format (OVF). L'installation du logiciel nécessite 14 étapes,[22] tandis que le déploiement de l'appliance vSphere alternative s'effectue en 8 étapes ne prenant que 5 minutes.[23] Après l'installation, les administrateurs peuvent accéder à la solution via des navigateurs Web à partir de l'environnement isolé.

Les clients doivent déployer séparément CyberSense, un moteur d'analytique de la sécurité intelligent entièrement automatisé et intégré.[24] Les instructions d'installation de CyberSense dans Dell PowerProtect Cyber Recovery ne sont pas disponibles publiquement.[25]

Dell propose plusieurs métriques que les utilisateurs peuvent ajuster, notamment l'objectif de détection de destruction (DDO), l'objectif d'évaluation de destruction (DAO), le point de Cyber Recovery (CRP), le temps de Cyber Recovery (CRT), l'intervalle de synchronisation Cyber Recovery et le nombre de copies de données Cyber Recovery. Dell recommande également de caractériser les données qui ont besoin d'une protection. Ces données peuvent être essentielles pour les missions, stratégiques pour l'entreprise, dépendantes des services d'infrastructure de base ou d'autres applications, ou générales, telles que les binaires d'applications, les images de démarrage et les catalogues de sauvegarde. La gamme d'options offre aux clients un contrôle total sur leur environnement de sauvegarde et la possibilité de personnaliser la classification de leurs données. Les Dell Consulting Services peuvent également fournir une assistance et des suggestions supplémentaires.[26]

La configuration Rubrik se compose également de plusieurs étapes. Avant de créer un cluster, les services de support Rubrik doivent installer et configurer Rubrik CDM. Puis, un administrateur télécharge et installe la version la plus récente ou souhaitée de CDM (15 étapes).[27] L'administrateur peut ensuite configurer un cluster Rubrik à l'aide de l'interface utilisateur ou de la CLI. Vous pouvez configurer le cluster à l'aide de l'interface utilisateur ou de la CLI, les deux approches comptent 24 étapes.[28, 29] L'administrateur peut ensuite enregistrer les clusters Rubrik à l'aide d'une méthode en ligne (12 étapes)[30] ou hors ligne (18 étapes).[31] L'administrateur active ensuite l'authentification multifacteur (MFA), qui nécessite 13 étapes.[32] Finalement, l'administrateur ajoute le compte initial (6 étapes) et tous les autres comptes.[33] La Figure 3 illustre le nombre maximal d'étapes possibles pour configurer chaque solution de cyber-récupération.

Les clients Rubrik ne peuvent pas régler d'autres métriques, ce qui pourrait réduire la flexibilité pour répondre à leurs besoins. Selon l'un des commentateurs : « l'essentiel de l'interface utilisateur est assez simple et facile, mais certaines parties manquent un peu de détails quant à l'utilisation de certaines options, ou l'option n'est pas disponible. Tout en facilitant l'expérience utilisateur, de nombreux réglages ne sont pas proposés et nécessitent l'ouverture d'un tunnel de support pour qu'une personne du support puisse apporter une modification à l'environnement du client. »[34]

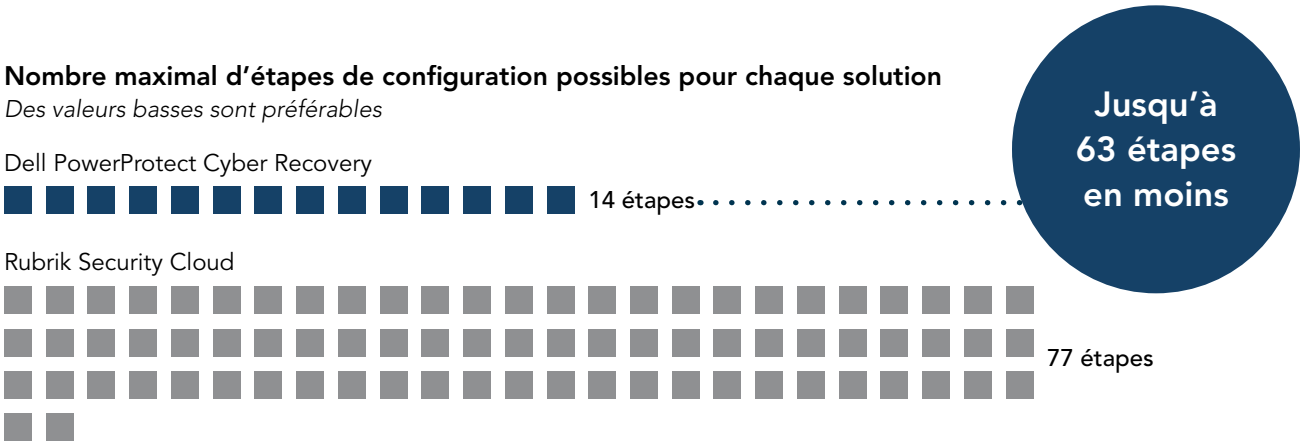

Figure 3 : Nombre maximal d'étapes possibles pour configurer Dell PowerProtect Cyber Recovery et Rubrik Security Cloud. Des valeurs basses sont préférables. Source : Principled Technologies.

Maintenance

Nous avons observé qu'après la configuration, les interfaces utilisateur Dell et Rubrik pour l'exécution des opérations de maintenance quotidiennes sont similaires. Après la configuration, les clients peuvent configurer Dell PowerProtect Cyber Recovery pour effectuer les opérations suivantes :[35, 36]

- Générer automatiquement des rapports sur les tâches Cyber Recovery en fonction d'un planning et en réponse à une demande manuelle de l'utilisateur
    - Un utilisateur ou un planning crée des tâches lorsqu'il lance une règle, une opération de récupération, une sauvegarde du système ou une opération de nettoyage
- Surveiller automatiquement l'état du coffre-fort, la capacité de stockage, les opérations Cyber Recovery, les alertes en cas d'échec de la copie/synchronisation ou d'arrêt du coffre-fort Cyber Recovery, ainsi que les tâches Cyber Recovery
- Détecter automatiquement et en continu les attaques, puis une fois repérées afficher des alertes CyberSense par ordre de gravité, en indiquant le nombre de fichiers, d'hôtes et de politiques concernés, de menaces spécifiques détectées, le moment de l'attaque afin de déterminer quelle sauvegarde reste non contaminée et une liste des fichiers corrompus à utiliser dans l'analyse de l'attaque

De même, les clients peuvent configurer Rubrik pour effectuer les opérations suivantes :[37]

- Utilisez automatiquement Rubrik Security Cloud pour suivre, surveiller et afficher tous les événements de tous les clusters Rubrik connectés. Elle propose trois types d'événements :[38]
    - Critique : événements nécessitant une attention particulière, tels qu'un échec de sauvegarde, d'archivage ou de réplication
    - Avertissement : Une sauvegarde, un archivage ou une restauration a été effectuée
    - Information : information uniquement
- Analyser automatiquement et en continu les snapshots à la recherche d'indicateurs de compromission, nouveaux et existants, à l'aide de Threat Monitor, qui indique l'heure à laquelle la solution a pris un snapshot pour la dernière fois, la chronologie de l'événement, l'heure de détection, le nombre de fichiers modifiés, le nombre de fichiers suspects, le nom du cluster, ainsi que le type et le nom de l'objet

Prise en charge des charges applicatives anormales

Rubrik Security Cloud Threat Analytics et CyberSense analysent plusieurs types de charges applicatives, mais selon les sources que nous avons trouvées, CyberSense prend en charge deux fois plus de charges applicatives de détection des anomalies. Cela inclut l'analyse des types de charges applicatives suivants :

- Machines virtuelles
- Infrastructure principale
- Fichiers utilisateur susceptibles de contenir des documents, des contrats et des propriétés intellectuelles
- Bases de données
- Sauvegardes effectuées par d'autres clients

« En comptant le nombre de charges applicatives prises en charge que nous avons trouvé dans les données accessibles au public, nous constatons que CyberSense prend en charge 21 charges applicatives de détection des anomalies, tandis que Rubrik en prend en charge 7. »

En comptant le nombre de charges applicatives prises en charge que nous avons trouvé dans les données accessibles au public, nous constatons que CyberSense prend en charge 21 charges applicatives de détection des anomalies, tandis que Rubrik en prend en charge 7. Par conséquent, selon les données accessibles au public partagées par chacun d'eux, CyberSense prend en charge deux fois plus de charges applicatives que Rubrik Security Cloud Data Threat Analytics. Plus une solution de cyber-récupération peut analyser de données, plus elle a de chances de détecter des logiciels malveillants sournois ou d'autres corruptions.

Prise en charge des charges applicatives des machines virtuelles

Les charges applicatives de machine virtuelle font référence aux applications, services ou tâches que les machines virtuelles exécutent sur un serveur hôte physique ou un environnement de Cloud. Étant donné que ces charges applicatives peuvent varier dans leur fonctionnement et selon de nombreux autres facteurs susceptibles d'augmenter leur exposition aux logiciels malveillants, l'analyse des machines virtuelles est essentielle. Rubrik Security Cloud Data Threat Analytics, qui « comprend les services de détection des anomalies, de surveillance des menaces, de recherche des menaces et de récupération des données sur les ressources protégées »,[39] prend en charge l'analyse des charges applicatives de machines virtuelles suivantes :[40]

- VMware
- Nutanix® AHV
- Microsoft Hyper-V
- Microsoft Azure

CyberSense prend en charge l'analyse des charges applicatives de machines virtuelles suivantes :[41, 42, 43]

- VMware
- Amazon Web Services (AWS)
- Hyper-V, avec sauvegardes Dell Avamar ou Dell NetWorker

Selon VMware, « jusqu'à 80 % des charges applicatives virtualisées s'exécutent sur la technologie VMware ».[44] Au premier trimestre 2024, le fournisseur le plus populaire sur le marché des services d'infrastructure Cloud, Amazon Web services (AWS), contrôlait 31 % du marché. Microsoft Azure occupe la deuxième place avec 25 % de parts de marché.[45]

Infrastructure principale

L'infrastructure principale est constituée des composants et services fondamentaux qui permettent le fonctionnement d'un environnement technologique. Détecter les logiciels malveillants à ce niveau peut aider à réduire la gravité d'une attaque, car les fonctionnalités de l'infrastructure principale peuvent affecter de nombreux systèmes et utilisateurs. La documentation Rubrik Security Cloud ne mentionne pas la prise en charge de l'analyse de l'infrastructure principale.[46]

En revanche, CyberSense prend en charge l'analyse d'infrastructure principale suivante :[47]

- Active Directory
- DNS
- LDAP

Fichiers utilisateur susceptibles de contenir des documents, des contrats et des propriétés intellectuelles

Rubrik Security Cloud Threat Analytics prend en charge l'analyse des fichiers utilisateur suivants :[48]

- Jeux de fichiers et datasets NAS
- Groupes de volumes Windows
- Linux et Windows

CyberSense peut analyser les fichiers utilisateur Linux et Windows.[49]

Analyse des bases de données

CyberSense 7 versus
RSC Data Threat Analytics 0

Bases de données

Les applications peuvent utiliser différents types de bases de données pour de nombreuses raisons. Il est donc essentiel de pouvoir détecter la présence de logiciels malveillants dans différentes bases de données pour obtenir une réponse rapide. Rubrik Security Cloud Threat Analytics peut sauvegarder des bases de données, mais nous n'avons pas trouvé de documentation publique indiquant qu'il était possible d'analyser ces sauvegardes de base de données.

CyberSense prend en charge l'analyse des bases de données suivantes avec des analyses au niveau de la page :[50]

- SQL
- Oracle®
- SAP HANA
- Db2
- PostgreSQL
- Epic® Caché
- MariaDB/MySQL

Sauvegardes effectuées par d'autres clients

Certaines organisations peuvent disposer de sauvegardes de données provenant de plusieurs fournisseurs pour assurer la redondance, se conformer aux réglementations ou pour toute autre raison importante. La documentation Rubrik Security Cloud ne mentionne pas la prise en charge de l'analyse des sauvegardes effectuées par d'autres clients de sauvegarde.[51]

Avec un avantage évident dans cette catégorie, CyberSense prend en charge les sauvegardes d'analyse effectuées par les clients de sauvegarde suivants :[52, 53, 54]

- DNAS
- Échange
- SQL
- Avamar
- NetWorker
- CommVault
- Veritas NetBackup

Technologie d'analyse

Rubrik Security Cloud inclut de nombreux outils d'analyse et d'aide à l'analyse dans Data Threat Analytics :

- Rubrik Anomaly Detection affiche les fichiers suspects, les modifications de snapshots[55] et les détails des anomalies en tant qu'incidents d'anomalies que les clients peuvent étudier et utiliser dans le cadre d'une enquête sur les snapshots.[56] Le logiciel fournit également des options de récupération.[57]
- Rubrik VM Encryption Detection détecte les attaques sur les fichiers de disque virtuel VMware vSphere.[58]
- Rubrik Threat Monitoring affiche des informations sur les menaces et les correspondances détectées.[59]
- Rubrik Threat Hunt est une analyse initiée par l'utilisateur pour détecter les indicateurs de compromission.[60]
- Rubrik Quarantine isole les objets repérés lors d'une recherche de menaces.[61]

Rubrik RSC dispose également de Rubrik Backup Service Connectors pour chaque cluster Rubrik.

Les clients Rubrik doivent sélectionner l'outil adapté à leur tâche, peuvent devoir lancer des analyses manuellement ou utiliser plusieurs outils pour accomplir leur tâche. En revanche, Dell propose une option d'analyse CyberSense unique, que les clients peuvent trouver plus facile à gérer et à administrer.

L'analyse CyberSense va plus loin que l'analyse « uniquement en surface » de Rubrik RSC Data Threat Analytics. CyberSense effectue des analyses complètes du contenu des fichiers et des analyses au niveau des pages des bases de données, et peut détecter le chiffrement partiel des fichiers.[62] L'outil utilise une base de données d'apprentissage automatique (ML) formée par Index Engines sur des milliers de menaces de données et qui contient plus de 200 points d'analyse pour détecter la corruption des données.[63] À la différence de Rubrik Threat Monitoring et Threat Hunt, CyberSense ne s'appuie pas sur des agences externes de renseignements sur les menaces pour fournir des signatures de logiciels malveillants. Au lieu de cela, il découvre de nouvelles menaces.[64] **En outre, CyberSense ne repose pas sur des seuils arbitraires de modifications acceptables de fichiers ou de niveaux d'entropie entre les snapshots, susceptibles d'entraîner des faux négatifs**. Il n'effectue pas l'entraînement de son ML à partir d'une ligne de base fondée sur le comportement précédent du client.[65, 66, 67]

> *« CyberSense ne s'appuie pas non plus sur des seuils arbitraires de changements de fichiers ou de niveaux d'entropie acceptables entre les snapshots pouvant entraîner de faux négatifs…. »*

Le logiciel de détection des anomalies Rubrik s'appuie uniquement sur les métadonnées pour déterminer si un snapshot est corrompu avant d'effectuer une analyse de contenu. Par rapport au ML continu de CyberSense, le logiciel Rubrik détecte la corruption après avoir obtenu des signatures. Le système de détection des anomalies de Rubrik doit créer un modèle comportemental pour définir une référence normale pour un client. Cette opération peut nécessiter plusieurs sauvegardes. Le modèle

comportemental Rubrik nécessite au moins deux sauvegardes pour créer une référence des modifications typiques apportées à un système de fichiers en l'absence d'attaques. Toutefois, un seul ensemble de statistiques de changement peut ne pas suffire à établir ce qui est typique. Les événements métier peuvent déclencher plus ou moins d'activité ou des types d'activité plus suspects qui ne se sont pas produits entre le premier et le deuxième snapshot Rubrik. Plus la solution Rubrik analyse de sauvegardes, plus elle augmente la précision de l'entraînement de son modèle comportemental sur une référence.[68, 69]

CyberSense contient toutes ses analyses dans le coffre-fort. Dans le pipeline d'analyse du comportement du système de fichiers, Rubrik envoie à la plateforme Cloud Polaris des métadonnées sur les modifications apportées au système de fichiers du client, pour effectuer l'analyse du comportement, ce qui ouvre une surface d'attaque.[70]

Les clients peuvent utiliser Rubrik Threat Monitoring et Threat Hunt uniquement dans le cadre de l'édition Rubrik Enterprise.[71] Les clients doivent effectuer des analyses de recherche des menaces avec des privilèges RBAC (Role-based Access Control, ou Contrôle d'accès basé sur les rôles), et les utilisateurs doivent préciser les indicateurs de compromission spécifiques (IOC) qu'ils souhaitent rechercher.[72] Cela n'entre pas dans les pratiques d'excellence du secteur.[73] À l'instar de CyberSense, Threat Hunt prend en charge VMware, AHV, Hyper-V, les ensembles de fichiers NAS et les serveurs Linux et Windows.[74]

Les sections suivantes fournissent plus de détails sur la détection des menaces proposée par la solution Rubrik.

Métadonnées et statistiques du système de fichiers

Le modèle comportemental ML Rubrik Anomaly Detection consigne les modifications apportées au système de fichiers depuis le dernier snapshot (par exemple le nombre de fichiers ajoutés, supprimés ou déplacés) sous forme de métadonnées.[75] Ensuite, un modèle ML s'entraîne sur ces modifications pour créer une « référence » de modèle comportemental pour le système de fichiers. Rubrik signale un snapshot comme anormal s'il détecte trop de modifications. Lorsque l'analyse du comportement signale un snapshot, la solution lance une analyse du contenu des fichiers.[76] La surveillance des métadonnées peut ajouter une couche de sécurité, mais elle peut ne pas offrir la protection nécessaire pour prévenir ou réduire les interruptions de service liées à un événement.

> *« CyberSense n'a pas besoin d'une référence ; il surveille et analyse les modifications apportées au contenu des fichiers et des bases de données à partir des premières copies de sauvegarde. »*

À l'inverse, **CyberSense n'a pas besoin de référence. Il surveille et analyse les modifications apportées au contenu des fichiers et des bases de données à partir des premières copies de sauvegarde.** L'approche CyberSense offre plus de granularité, car le logiciel analyse même des parties d'un fichier ou des pages individuelles d'une base de données. À l'instar de la solution Rubrik, les analyses CyberSense incluent des propriétés de métadonnées et alimentent les résultats dans le moteur ML. Contrairement à la solution Rubrik, CyberSense ne se limite pas à l'analyse des métadonnées et les Index Engines ont entraîné leur moteur ML sur les attaques qu'ils ont préalablement documentées, et non sur les signatures ou le comportement antérieur des clients.[77, 78]

Seuils

Au cours de l'analyse du comportement, Rubrik ML détermine la probabilité qu'une anomalie se soit produite sur un système de fichiers. Si la solution Rubrik la trouve probable, elle effectue une analyse du contenu. Il peut s'agir d'un seuil déterminé par un modèle comportemental pour les « comportements anormaux ». Par exemple, la solution Rubrik peut signaler un comportement anormal lorsqu'elle détecte une recrudescence importante de fichiers nouveaux ou modifiés, ou une augmentation des indicateurs de caractère aléatoire ou de chiffrement.[79] Lors de l'analyse du contenu, Rubrik Anomaly Detection affiche les modifications apportées au contenu des fichiers et calcule la probabilité de chiffrement en calculant l'entropie du système de fichiers. L'entropie d'un système de fichiers permet de montrer la probabilité qu'une attaque par ransomware ait chiffré des fichiers. Si l'entropie dépasse un seuil d'anomalie, la solution alerte l'utilisateur.[80, 81] L'efficacité de la détection de la corruption des données dépend de la rigueur du seuil. Trop de tolérance peut entraîner des faux négatifs et, par conséquent, un faux sentiment de sécurité.[82] Les clients doivent définir des seuils de manière appropriée.

En revanche, CyberSense vérifie le chiffrement partiel d'un fichier en analysant le contenu du fichier pour fournir une confiance de 99,99 % (selon Dell et Index Engines) dans la détection de la corruption des données.[83]

Signatures et extensions de fichiers

Rubrik Threat Monitoring et Threat Hunts analysent les snapshots à la recherche d'IOC. Lorsque l'une des multiples sources de renseignements sur les menaces surveillées par Rubrik découvre un nouvel IOC, Threat Monitoring transmet le flux de menaces contenant des règles YARA (Yet Another Ridiculous Acronym, ou Encore un autre acronyme ridicule) pour l'identification du nouveau logiciel malveillant, également appelé signature du logiciel malveillant, à tous les clusters Rubrik. Les clusters commencent alors à analyser.[84] Une récente étude WatchGuard suggère que 57,8 % des logiciels malveillants évitent la détection des signatures. Des logiciel malveillants avancés, tel que BianLian, peut utiliser des méthodes pour contourner la reconnaissance des signatures, et les nouvelles variantes de logiciels malveillants peuvent avoir des signatures légèrement différentes de celles d'origine. En conséquence, l'actualisation de l'intelligence sur les menaces peut s'avérer plus difficile.[85]

En comparaison, CyberSense utilise plus de 200 analyses et fournit un modèle ML entraîné sur des milliers de variantes de rançongiciel. L'outil Index Engines a prouvé que la méthode CyberSense était capable de détecter des variantes sophistiquées inédites sans télécharger de signatures,[86] qui est un autre avantage permettant d'éviter d'avoir à utiliser Internet lors d'un événement.

Événements de chiffrement de masse

La solution Rubrik surveille les événements de chiffrement de masse en calculant l'entropie de l'ensemble du système de fichiers.[87] CyberSense est beaucoup plus granulaire. Elle ne se contente pas d'analyser le système de fichiers en général, ni même chaque fichier individuel, mais analyse des parties du contenu interne des fichiers. Selon les moteurs d'indexation, le calcul de l'entropie sur un fichier entier uniquement plutôt que sur des parties de celui-ci « ne détectera que le chiffrement extrême de l'ensemble du fichier » ou les événements de chiffrement de masse.[88]

Capacité de récupération

D'après les documents, nous considérons que la récupération avec Dell PowerProtect Cyber Recovery est un processus plus simple et plus fluide que celle avec Rubrik. Cette section du rapport, y compris ses sous-sections, met en contraste les fonctions de récupération des deux solutions et la manière dont les solutions mettent en œuvre ces fonctions.

La documentation Rubrik indique quelles fonctionnalités de récupération fonctionnent pour quels types de machines virtuelles. Cela peut sembler offrir un niveau de granularité utile, mais les nombreuses stipulations et variations rendent la récupération complexe. Par exemple, lorsque les clients Rubrik ont besoin de restaurer des données, des fichiers et des systèmes, ils doivent sélectionner les objets snapshot qu'ils souhaitent inclure dans leur plan de récupération. Après avoir créé un ou plusieurs plans de récupération, Rubrik propose de nombreuses options de restauration, notamment les suivantes :[89, 90, , 91 92, 93]

- Récupérer les fichiers par téléchargement ou les écraser et les restaurer dans un dossier distinct, les exporter vers un hôte différent ou vers un service en cluster
- Récupérer des fichiers pour les machines virtuelles par téléchargement ou les écraser et les restaurer dans un dossier distinct ou les exporter vers une autre machine virtuelle
- Prendre un snapshot complet d'une machine virtuelle ou d'un disque par les moyens suivants :
    - Le montage direct, qui crée une nouvelle machine virtuelle à partir du snapshot
    - Le montage de disques virtuels, qui crée de nouveaux disques virtuels à partir du snapshot
    - La récupération instantanée, qui remplace la machine virtuelle actuelle par une nouvelle machine virtuelle créée par le snapshot
    - L'exportation, qui crée une nouvelle machine virtuelle à partir du snapshot dans un datastore sélectionné
    - La restauration par lots des machines virtuelles
- La restauration Cyber Recovery en bloc pour les plans de reprise après sinistre par montage direct et exportation
- Rubrik Security Cloud Orchestrated Application Recovery pour la reprise après sinistre destinée aux machines virtuelles vers un sandbox isolé, un site distant ou sur place

La récupération par lots de Rubrik démontre une fois de plus sa complexité. Le Tableau 1 présente les fonctionnalités de récupération par lots fournies par Rubrik en fonction de l'hyperviseur.[94]

Tableau 1 : Les fonctionnalités de récupération par lots fournies par Rubrik pour différents hyperviseurs. Source : Rubrik.

Options de création de machines virtuelles				
	Montage direct	**Montage direct avec migration facultative**	**Exporter**	**Restauration instantanée**
Machines virtuelles vSphere	Disponible, utilise le cluster Rubrik comme magasin de données	Non disponible	Disponible, utilise le magasin de données de l'hyperviseur restauré	Disponible, utilise le cluster Rubrik comme magasin de données
Machines virtuelles AHV	Disponible, utilise le cluster Rubrik comme magasin de données	Disponible, utilise le cluster Rubrik comme magasin de données et le conteneur Nutanix pour toutes les écritures ultérieures	Disponible, utilise le conteneur Nutanix comme magasin de données	Non disponible
Machines virtuelles Hyper-V	Disponible, utilise le cluster Rubrik comme magasin de données	Non disponible	Disponible, utilise le magasin de données de l'hyperviseur restauré	Disponible, remplace la machine virtuelle actuelle par une nouvelle à partir du snapshot. Utilise le cluster Rubrik comme magasin de données.

Pour la solution Rubrik, le magasin de données restauré se trouve généralement sur le cluster Rubrik et non dans l'environnement de production, ce qui peut créer des problèmes. Nous présentons ces problèmes dans la section suivante, "Rubrik limitations". En revanche, PowerProtect peut placer les données récupérées dans des environnements de récupération ou de production pour fournir une récupération plus rapide et plus fluide, qui pourrait limiter les interruptions de service.

Le Tableau 2 présente des informations supplémentaires de Rubrik sur la restauration des machines virtuelles vSphere.[95] Comme indiqué dans le tableau, la plupart des magasins de données de récupération vSphere se trouvent sur le cluster Rubrik.

Tableau 2 : Fonctionnalités de récupération fournies par Rubrik pour les machines virtuelles vSphere. Source : Rubrik.

Fonctionnalités de récupération fournies par Rubrik pour vSphere				
Action	**Datastore**	**État de l'alimentation**	**Réseau**	**Source VM**
Restauration de fichiers	Sans objet	Sans objet	Sans objet	Aucune incidence
Montage direct	Cluster Rubrik local	Activé ou désactivé	Déconnecté	Aucune incidence
Monter des disques virtuels	Cluster Rubrik local	Date	Déconnecté	Aucune incidence
Restauration instantanée	Cluster Rubrik local	Date	Connecté (en option)	Éteint et renommé
Exporter	Magasin de données de l'hyperviseur	Éteint	Déconnecté	Aucune incidence
Restauration sur place	Magasin de données de l'hyperviseur	Date	Identique à la machine virtuelle source	La récupération sans déplacement remplace les fichiers de disque virtuel de la machine virtuelle source par les données de disque virtuel du snapshot, sans modifier les propriétés de la machine virtuelle.

De manière générale, la solution Rubrik n'implémente pas la récupération en bloc et les options de récupération en bloc sont limitées et complexes. Comme le détaille la section "Dell PowerProtect Data Manager offers the equivalent of Rubrik "mass restore"" de ce rapport, Dell PowerProtect est plus rationalisé et facile à utiliser.

Démystifier la restauration de masse

La solution Rubrik fait la promotion de la récupération de masse, qui consiste à restaurer rapidement les opérations métier en récupérant des applications, des fichiers ou des utilisateurs à grande échelle.[96] Elle offre de nombreuses options de récupération de masse. Toutefois, la solution Rubrik stocke généralement les données récupérées sur le cluster Rubrik et non dans l'environnement de production.[97] Les charges applicatives dépendent de la disponibilité du système Rubrik jusqu'à ce que la solution termine sa migration. Le cluster Rubrik local est un stockage de niveau 3, de sorte que les clients doivent effectuer une migration supplémentaire vers leur environnement de production pour revenir aux niveaux de performances planifiés. Avec ce point de défaillance unique et des performances réduites au moment où le système termine la migration, nous ne pouvons pas considérer la récupération comme terminée tant que la solution Rubrik ne restaure pas les charges applicatives dans l'environnement de production.

Dell PowerProtect offre également une récupération de masse en permettant aux utilisateurs de sélectionner plusieurs machines virtuelles pour la récupération dans son interface utilisateur de récupération.

Dell PowerProtect Data Manager offre l'équivalent de la « restauration de masse » de Rubrik

Par rapport à la solution Rubrik, la solution Dell propose également plusieurs options de récupération équivalentes pour les machines virtuelles vSphere. Dell PowerProtect peut placer les données de machines virtuelles dans des environnements de récupération ou de production. La plupart des options Rubrik placent les données sur le cluster Rubrik uniquement. Le Tableau 3 présente les options de récupération Dell.[98, 99, 100, 101]

Tableau 3 : Options de récupération Dell. Source : Principled Technologies.

Options de récupération Dell	
Type	**À propos de la fonction**
Restauration au niveau fichier	Ne restaure que les fichiers infectés sur place ou par restauration
Machine virtuelle en direct	Restaure une machine virtuelle sur le cluster avec une migration ultérieure vers la production
Restaurer vers un nouvel emplacement	Restaure dans l'environnement d'origine ou un nouvel environnement (par exemple, une salle blanche ou une infrastructure de récupération). Les utilisateurs peuvent lors du processus sélectionner plusieurs machines virtuelles à la fois pour une restauration en bloc ou à grande échelle
Machine virtuelle d'accès/en direct	Crée une copie isolée des données de production
Orchestration de la récupération	Permet aux administrateurs de planifier la restauration ou de la rendre disponible à la demande ; hiérarchise la restauration automatique des machines virtuelles vers l'environnement de production ou de récupération

Limites de Rubrik

La solution Rubrik met en quarantaine les snapshots infectés par des logiciels malveillants pour analyse ultérieure. Toutefois, la solution Rubrik ne met pas en quarantaine les snapshots par défaut. Les clients peuvent ensuite télécharger les fichiers mis en quarantaine et effectuer eux-mêmes une analyse approfondie, manuellement ou à l'aide d'outils tiers, ce qui présente un risque d'exposition à des logiciels malveillants.[102, 103]

> *CyberSense effectue son analyse sans que l'utilisateur n'ait à effectuer ses propres analyses d'investigation, et le logiciel automatise la création de points de restauration.*

Par défaut, CyberSense analyse les fichiers et les bases de données. Les utilisateurs n'ont pas besoin de mettre les snapshots en quarantaine manuellement. **CyberSense effectue son analyse sans que l'utilisateur n'ait à effectuer ses propres investigations, et le logiciel automatise la création de points de restauration.**[104]

RSC Rubrik en mode de gestion RSC uniquement est un point de défaillance unique pour de nombreuses fonctionnalités. Plus inquiétant, une attaque pourrait provoquer une interruption du service RSC qui affecte la connectivité Internet de l'utilisateur ou la connectivité entre le site de l'utilisateur et le RSC. Suite à de telles attaques, la solution fournit un ensemble limité de fonctionnalités aux utilisateurs, disponibles via l'interface utilisateur Rubrik CDM ou une automatisation basée sur API, mais uniquement si les utilisateurs ont créé un compte de service RSC avant l'attaque.[105, 106]

Une organisation peut restaurer les charges applicatives et les données suivantes sans le service RSC : MongoDB, Microsoft Exchange, fichiers, snapshots Hyper-V, Live Mount from Managed volumes, fichiers hôtes NAS, Oracle, SQL Server, VCD, et VMware.[107] La récupération SAP HANA sans le RSC nécessite des outils tiers, tels que Studio et Cockpit Cross, et le support de Rubrik via le tunnel de support. La récupération d'IBM Db2 sans le service RSC nécessite des outils IBM tiers et la prise en charge de Rubrik via le tunnel de support.[108]

Air gap/isolation

La NIST définit un air gap comme « une interface entre deux systèmes à laquelle (a) ils ne sont pas connectés physiquement et (b) avec laquelle il n'a pas de connexion logique automatisée (c'est-à-dire que les données sont transférées à travers l'interface uniquement manuellement, sous contrôle humain) ».[109]

Les air gaps peuvent aider à contrôler le flux de données d'une source à une cible, constituant un composant important de toute stratégie de cyber-récupération et de protection contre les rançongiciels. Si une attaque ou un événement compromet vos systèmes de sauvegarde de production, la capacité à empêcher le trafic depuis vos systèmes de production vers les sauvegardes protégées dans vos coffres-forts de cyber-récupération peut offrir une sécurité intégrée.

Isolement physique

Dans le film Mission impossible, vous avez peut-être vu un exemple de solution physiquement isolée, où le personnage principal devait contourner toutes les autres fonctions de sécurité des locaux pour accéder à des données sensibles sur un système informatique qui n'était connecté à aucun réseau externe. L'isolation physique peut également utiliser des segments normalement déconnectés de la gestion de réseau physique dédiée pour transporter les copies de sauvegarde de vos systèmes de production vers le coffre-fort. Déconnectés, ces air gaps opérationnels créent une barrière physique que les données ne peuvent pas franchir automatiquement, ce qui en complique l'accès pour les acteurs malveillants.

Les organisations peuvent isoler physiquement Dell PowerProtect Cyber Recovery pour aider à mettre en place une stratégie d'air gap opérationnelle. La solution utilise une connexion physique dédiée et effectue la réplication des données sous la forme d'une opération d'extraction à partir du coffre-fort plutôt que d'une opération d'envoi à partir de la solution de sauvegarde. Lors de la copie/réplication, la solution active la connexion, chiffre les données et les migre sur la ligne dédiée.[110] À la fin de la réplication, la solution désactive à nouveau la connexion du côté du coffre-fort. Cette solution, en appliquant des politiques de rétention verrouillées, rend les copies dans le coffre-fort immuables de sorte que même si un utilisateur ou un système obtenait un accès, il ne pourrait ni les modifier ni les supprimer. Aucun trafic de gestion ne traverse le chemin de réplication. Ainsi, **même si des acteurs malveillants prennent le contrôle de votre solution de sauvegarde sur site,**

le coffre-fort lance et déconnecte le chemin de réplication et utilise des extractions de données unidirectionnelles à partir de la source de données, ce qui limite l'accès direct au coffre-fort.[111]

Isolement logique

L'isolement logique, en revanche, utilise des systèmes pouvant résider sur le même réseau physique, mais crée une séparation et un contrôle logiques du réseau pour s'assurer que les systèmes ne puissent pas s'envoyer de données entre eux. La solution utilise des implémentations de sécurité supplémentaires, telles que le chiffrement et le hachage, ainsi que RBAC et l'authentification multifacteur, pour s'assurer qu'un système ou un utilisateur non autorisé ne peut pas lire les données résidant dans un autre système.

Rubrik décrit sa fonctionnalité de cyber-récupération comme utilisant une stratégie d'air gap logique.[112] [113] De nombreuses déclarations publiques de Rubrik remettent en question la nécessité de l'air gaps. Dans une présentation Rubrik intitulée « Rubrik Security – Air Gap and immuability », il est affirmé que leur solution native est « air gapped », car il n'y a aucun moyen d'accéder aux sauvegardes ni de les modifier une fois que la solution les prend, même si l'appliance Rubrik reste sur le réseau physique.[114] Toutefois, un acteur incorrect authentifié peut toujours accéder à l'interface graphique de l'appliance, ce qui peut avoir des conséquences pour la récupération. Pour atténuer ce problème, Rubrik dispose de verrous de rétention qui empêchent l'expiration des sauvegardes, ce qui les rend immuables. Une fois activés, ces verrous de rétention empêchent également la réinitialisation et l'effacement des paramètres d'usine d'un cluster Rubrik. Selon le Rubrik CDM Security Guide, la solution désactive globalement les verrous de rétention sur le cluster par défaut et oblige les clients à contacter le support Rubrik pour les activer.[115] Les sources accessibles au public ne précisent pas si le support Rubrik peut également désactiver les verrous de rétention, ce qui laisse planer le spectre d'un acteur malveillant autorisé toujours en mesure de contourner les couches de sécurité.

« Aucun trafic de gestion ne traverse le chemin de réplication. Ainsi, même si des acteurs malveillants prennent le contrôle de votre solution de sauvegarde sur site, le coffre-fort lance et déconnecte le chemin de réplication et utilise des extractions de données unidirectionnelles à partir de la source de données, ce qui limite l'accès direct au coffre-fort. »

Conclusion

Les organisations doivent prendre activement en compte de nombreux vecteurs d'attaque sur leurs datacenters. Un bon plan de protection des données vise à protéger toutes les données, en particulier les données stratégiques essentielles aux opérations. Nous avons examiné les informations accessibles au public sur Dell PowerProtect Cyber Recovery et Rubrik Secure Cloud pour voir comment les deux solutions abordent la gestion, la protection et la récupération des données.

PowerProtect Cyber Recovery isole physiquement les copies de sauvegarde des données stratégiques dans un coffre-fort et garantit leur capacité de restauration en cas de cyberattaque. La solution utilise une stratégie d'air gap opérationnelle avec isolation physique, ce que Rubrik Secure Cloud ne peut pas revendiquer : la solution repose sur l'isolation logique.

Dans CyberSense, CyberRecovery utilise l'analytique basée sur le ML pour évaluer l'intégrité des données dans le coffre-fort et identifier les données de sauvegarde propres à restaurer. Rubrik Secure Cloud, en revanche, propose un outil d'analytique entraîné par ML qui recherche les anomalies au lieu d'effectuer des analyses approfondies sur les fichiers.

En outre, la solution Cyber Recovery offre plusieurs options de récupération, en tirant parti des données non compromises du coffre-fort pour faciliter un retour efficace et fluide aux opérations. Dans de nombreux cas, PowerProtect Cyber Recovery peut offrir des fonctionnalités et des avantages qui manquent à Rubrik Secure Cloud, offrant ainsi une solution potentiellement plus sécurisée, capable d'effectuer une analyse plus approfondie afin de minimiser les interruptions de service et d'accélérer la récupération.

---

1. Anastasia Dergacheva et Jesse R. Taylor, « Study Finds Average Cost of Data Breaches Continued to RISE in 2023 », consulté le 25 juillet 2024, https://www.morganlewis.com/blogs/sourcingatmorganlewis/2024/03/study-finds-average-cost-of-data-breaches-continued-to-rise-in-2023.
2. Dell, « Guide de solutions Dell PowerProtect Cyber Recovery », consulté le 18 avril 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf.
3. Dell, « Guide de solutions Dell PowerProtect Cyber Recovery ».
4. Rubrik, « Rubrik Security Cloud Architecture and Security Implementation », consulté le 18 avril 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/wp-rubrik-security-cloud-architecture-and-security-implementation.pdf.
5. Rubrik, « Rubrik Security Cloud Architecture and Security Implementation », consulté le 18 avril 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/wp-rubrik-security-cloud-architecture-and-security-implementation.pdf.
6. Rob Emsley, « Public Cloud Vault to Secure, Isolate and Recover Data », consulté le 20 mars 2024, https://www.dell.com/en-us/blog/public-cloud-vault-to-secure-isolate-and-recover-data/.

7. Brian White, « Dell's PowerProtect Cyber Recovery Expands to Microsoft Azure », consulté le 20 mars 2024, https://www.dell.com/en-us/blog/dells-powerprotect-cyber-recovery-expands-to-microsoft-azure/.
8. Dell, « Cyber Recovery on Google Cloud Platform », consulté le 20 mars 2024, https://infohub.delltechnologies.com/en-US/l/dell-powerprotect-cyber-recovery-reference-architecture/cyber-recovery-on-google-cloud-platform/.
9. Chris Mellor, « Up to $5m compensation if Rubrik Cloud Vault recovery busted », consulté le 20 mars 2024, https://blocksandfiles.com/2022/02/24/up-to-5m-compensation-if-rubrik-cloud-vault-recovery-busted/.
10. Kristina Avrionova, « Frequently Asked Questions about Rubrik Cloud Vault », consulté le 20 mars 2024, https://www.rubrik.com/blog/company/22/3/faq-about-rubrik-cloud-vault.
11. Chris Wahl, « Recover Fast from Ransomware Attacks: The Magic of an immutable Backup architecture », consulté le 22 mars 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/rwp-recovering-fast-from-ransomware-attacks.pdf.
12. Dell, « Data Domain Invulnerability Architecture: Enhancing Data Integrity and Recoverability », consulté le 7 juin 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/h7219-data-domain-data-invul-arch-wp.pdf.
13. Dell, « Consolidate Governance and Compliance Archive Data », consulté le 4 avril 2024, https://infohub.delltechnologies.com/en-US/l/dell-powerprotect-data-domain-retention-lock/consolidate-governance-and-compliance-archive-data/.
14. Dell, « Guide de solutions Dell PowerProtect Cyber Recovery », consulté le 24 mars 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf.
15. Rubrik, « Retention-locked SLA Domain attributes », consulté le 2 avril 2024, https://docs.rubrik.com/en-us/8.0/ug/cdm/attributes_of_retention_locked_sla_domains.html.
16. Rubrik, « Rubrik Cyber Recovery », consulté le 20 mars 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/solutions-brief/brf-rubrik-cyber-recovery.pdf.
17. Rubrik, « Rubrik Licensing: Subscribe to Simplicity », consulté le 20 mars 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/data-sheet/rubrik-licensing-data-sheet.pdf.
18. Rubrik, « Workloads require third-party tools for recovery », consulté le 6 mai 2024, https://docs.rubrik.com/en-us/saas/saas/workloads_require_third_party_tools_for_recovery.html.
19. Rubrik, « Recoverable workloads during RSC service disruption », consulté le 6 mai 2024, https://docs.rubrik.com/en-us/saas/saas/recoverable_workloads_during_rsc_service_disruption.html.
20. Rubrik, « Workloads require third-party tools for recovery ».
21. Dell, « Renforcement de votre posture de sécurité avec Managed Detection and Response », consulté le 2 avril 2024, https://www.delltechnologies.com/asset/pl-pl/services/managed-services/technical-support/managed-detection-and-response-datasheet.pdf.
22. Dell, « Dell PowerProtect Cyber Recovery 19.13 Installation Guide », consulté le 20 mars 2024, https://www.dell.com/support/manuals/en-us/cyber-recovery/irs_p_19.13_installation/installing-the-cyber-recovery-software?guid=guid-8718978d-ddd0-4dc0-bca7-fb04a2f3d1fb&lang=en-us.
23. Dell, « Guide d'installation de Dell PowerProtect Cyber Recovery 19.13 ».
24. Dell, « Guide d'installation de Dell PowerProtect Cyber Recovery 19.13 ».
25. Dell, « Installing CyberSense in Dell PowerProtect Cyber Recovery », consulté le 20 mars 2024, https://infohub.delltechnologies.com/en-US/l/ransomware-protection-secure-your-data-on-dell-powerflex-with-powerprotect-cyber-recovery-1/installing-cybersense-in-dell-powerprotect-cyber-recovery-1/.
26. Dell, « Guide de solutions Dell PowerProtect Cyber Recovery ».
27. Rubrik, « Downloading and installing Rubrik CDM », consulté le 20 mars 2024, https://docs.rubrik.com/en-us/saas/install/download_install_cdm_on_appliance_nodes.html.
28. Rubrik, « Setting up a Rubrik cluster using the UI », consulté le 20 mars 2024, https://docs.rubrik.com/en-us/saas/install/setting_up_ui.html.
29. Rubrik, « Setting up a Rubrik cluster using the CLI », consulté le 20 mars 2024, https://docs.rubrik.com/en-us/saas/install/setting_up_cli.html.
30. Rubrik, « Registering Rubrik clusters using the online method », consulté le 20 mars 2024, https://docs.rubrik.com/en-us/saas/install/registering_clusters_online.html.
31. Rubrik, « Registering Rubrik clusters using the offline method », consulté le 2 avril 2024, https://docs.rubrik.com/en-us/saas/install/registering_clusters_offline.html.
32. Rubrik, « Enabling MFA », consulté le 21 mars 2024, https://docs.rubrik.com/en-us/saas/install/rsc_enabling_mfa.html.
33. Rubrik, « Adding the initial account », consulté le 21 mars 2024, https://docs.rubrik.com/en-us/saas/saas/adding_the_initial_account.html.
34. TrustRadius, « Learning Rubrik by putting the pieces together Brik by Brik », consulté le 21 mars 2024, https://www.trustradius.com/reviews/rubrik-2023-09-20-21-03-04.
35. Dell, « Guide de solutions Dell PowerProtect Cyber Recovery ».

36. Index Engines, « CyberSense®: How it Works », consulté le 21 mars 2024, https://www.indexengines.com/how-it-works.
37. Rubrik, « Anomaly event details », consulté le 21 mars 2024, https://docs.rubrik.com/en-us/saas/saas/anomaly_event_details.html.
38. Rubrik, « Events page », consulté le 21 mars 2024, https://docs.rubrik.com/en-us/saas/saas/common/events_page.html.
39. Rubrik, « RSC Data Threat Analytics », consulté le 21 mars 2024, https://docs.rubrik.com/en-us/saas/saas/ri_ransomware_monitoring.html.
40. Rubrik, « RSC Data Threat Analytics ».
41. Dell Technologies, « Dell PowerProtect Cyber Recovery: Reference Architecture », consulté le 06 mai 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/h18661-dell-powerprotect-cyber-recovery-reference-architecture-wp.pdf.
42. Dell Technologies, « Dell EMC Avamar for Hyper-V », consulté le 16 mai 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/docu89876.pdf.
43. Dell Technologies, « Dell EMC NetWorker Module for Microsoft for Hyper-V », consulté le 16 mai 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/docu92011.pdf.
44. VMware, « Accelerate IT. Innovate with your Cloud »,9 mai 2024, https://www.vmware.com/files/pdf/VMware-Corporate-Brochure-BR-EN.pdf.
45. Statista, « Cloud infrastructure services vendor market share worldwide from fourth quarter 2017 to first quarter 2024 », 17 juillet 2024, https://www.statista.com/statistics/967365/worldwide-cloud-infrastructure-services-market-share-vendor/.
46. Rubrik, « RSC Data Threat Analytics ».
47. Dell Technologies, « CyberSense® for PowerProtect Cyber Recovery », consulté le 27 juin 2024, https://www.delltechnologies.com/asset/en-gb/products/data-protection/briefs-summaries/h18214-cybersense-for-dellemc-powerprotect-cyber-recovery-solution-brief.pdf.
48. Rubrik, « RSC Data Threat Analytics ».
49. Index Engines, « CyberSense® Support Matrix »,consulté le 21 mars 2024, https://www.indexengines.com/csmatrix.
50. Dell Technologies, « CyberSense® for PowerProtect Cyber Recovery ».
51. Rubrik, « Keep Your Databases Running in the Face of Any Threat ».
52. Index Engines, « CyberSense® Support Matrix ».
53. Dell Technologies, « Dell EMC Avamar for Hyper-V ».
54. Dell Technologies, « Dell EMC NetWorker Module for Microsoft for Hyper-V ».
55. Rubrik, « Anomaly incidents », consulté le 2 avril 2024, https://docs.rubrik.com/en-us/saas/saas/anomaly_incident.html.
56. Rubrik, « Data Threat Analytics events », consulté le 2 avril 2024, https://docs.rubrik.com/en-us/saas/saas/ri_events.html.
57. Rubrik, « Viewing Anomaly Detection », consulté le 2 avril 2024, https://docs.rubrik.com/en-us/saas/saas/viewing_ri_investigations.html.
58. Rubrik, « VM Encryption Detection », consulté le 2 avril 2024, https://docs.rubrik.com/en-us/saas/saas/vm_encryption_detection.html.
59. Rubrik, « Viewing the Threat Monitoring page », 2 avril 2024, https://docs.rubrik.com/en-us/saas/saas/viewing_the_threat_monitoring_page.html.
60. Rubrik, « Initiating a threat hunt »,consulté le 2 avril 2024, https://docs.rubrik.com/en-us/saas/saas/initiating_a_threat_hunt.html.
61. Rubrik, « Quarantining matched files or objects », consulté le 2 avril 2024, https://docs.rubrik.com/en-us/saas/saas/quarantining_matched_objects_or_files.html.
62. Dell, « CyberSense® for PowerProtect Cyber Recovery ».
63. Dell, « CyberSense® for PowerProtect Cyber Recovery ».
64. Index Engines, « The Power of CyberSense's Machine Learning », consulté le 2 avril 2024, https://go.indexengines.com/csmachinelearning.
65. Index Engines, « The Power of CyberSense's Machine Learning ».
66. Index Engines, « The Power of CyberSense's Machine Learning ».
67. Dell, « CyberSense® for PowerProtect Cyber Recovery ».
68. Rubrik, « Anomaly Detection behavioral model », consulté le 20 mai 2024, https://docs.rubrik.com/en-us/saas/saas/anomaly_detection_behavioral_model.html.
69. Amazon, « Training ML Models », consulté le 2 avril 2024, https://docs.aws.amazon.com/machine-learning/latest/dg/training-ml-models.html.
70. Rubrik, « Defense in Depth with Polaris Radar »,consulté le 21 mars 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/Defense-In-Depth-Polaris-Radar-Technical-White-Paper.pdf.
71. Rubrik, « Data Threat Analytics dashboard », consulté le 21 mars 2024, https://docs.rubrik.com/en-us/saas/saas/ri_dashboard.html.
72. Rubrik, « Initiating a threat hunt »,consulté le 21 mars 2024, https://docs.rubrik.com/en-us/saas/saas/initiating_a_threat_hunt.html.
73. SentinelOne, « What Is A Malware File Signature (And How Does It Work)? », consulté le 4 avril 2024, https://www.sentinelone.com/blog/what-is-a-malware-file-signature-and-how-does-it-work/.

74. Rubrik, « Threat hunts », consulté le 21 mars 2024, https://docs.rubrik.com/en-us/saas/saas/ri_threat_hunts.html.
75. Rubrik, « Anomaly Detection features », consulté le 22 mars 2024, https://docs.rubrik.com/en-us/saas/saas/ri_features.html.
76. Rubrik, « Behavioral model ».
77. Index Engines, « The Power of CyberSense's Machine Learning ».
78. Dell, « CyberSense® for PowerProtect Cyber Recovery ».
79. Rubrik, « Behavioral model ».
80. Rubrik, « Anomaly Detection features ».
81. Rubrik, « Behavioral model ».
82. Dell, « CyberSense® for PowerProtect Cyber Recovery ».
83. Morningstar, « Index Engines' CyberSense Announces 99.99% SLA in Detecting Ransomware Corruption, Empowering Smarter Recovery », consulté le 17 juillet 2024, https://www.morningstar.com/news/pr-newswire/20240618ny41171/index-engines-cybersense-announces-9999-sla-in-detecting-ransomware-corruption-empowering-smarter-recovery.
84. Rubrik, « Threat Monitoring »,consulté le 22 mars 2024, https://docs.rubrik.com/en-us/saas/saas/threat_monitoring.html.
85. Index Engines, « The Power of CyberSense's Machine Learning ».
86. Index Engines, « The Power of CyberSense's Machine Learning ».
87. Rubrik, « Anomaly Detection features », consulté le 22 mars 2024, https://docs.rubrik.com/en-us/saas/saas/ri_features.html.
88. Index Engines, « The Power of CyberSense's Machine Learning ».
89. Rubrik, « Investigating and recovering anomalous files for filesets », consulté le 22 mars 2024, https://docs.rubrik.com/en-us/saas/saas/investigating_and_recovering_anomalous_files.html.
90. Rubrik, « Investigating and recovering anomalous files for virtual machines », consulté le 22 mars 2024, https://docs.rubrik.com/en-us/saas/saas/investigating_and_recovering_anomalous_files_for_virtual_machines.html.
91. Rubrik, « Full snapshot recovery of a virtual machine », consulté le 22 mars 2024, https://docs.rubrik.com/en-us/saas/saas/full_snapshot_recovery_of_a_virtual_machine.html.
92. Rubrik, « Recovery of a batch of Virtual machines », consulté le 22 mars 2024, https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html.
93. Rubrik, « Performing bulk recovery for Recovery plans », consulté le 22 mars 2024, https://docs.rubrik.com/en-us/saas/saas/performing_bulk_recovery_for_recoveryplans.html.
94. Rubrik, « Recovery of a batch of Virtual machines », consulté le 4 avril 2024, https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html.
95. Rubrik, « Recovery of virtual machines », consulté le 16 avril 2024, https://docs.rubrik.com/en-us/saas/saas/vs_recovery_vm.html.
96. Le magasin de données restauré se trouve généralement sur le cluster Rubrik et non dans l'environnement de production.
97. Rubrik, « Recovery of a batch of Virtual machines », consulté le 16 avril 2024, https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html.
98. Dell, « Restore plan », consulté le 16 avril 2024, https://infohub.delltechnologies.com/en-US/l/powerprotect-data-manager-protection-for-vmware-cloud-foundation-on-dell-emc-vxrail-1/restore-plan/.
99. Dell, « PowerProtect Data Manager overview », consulté le 16 avril 2024, https://infohub.delltechnologies.com/en-US/l/dell-powerprotect-data-manager-deployment-best-practices-1/powerprotect-data-manager-overview-4/.
100. Dell, « PowerProtect Data Manager 19.9 Administration and User Guide », consulté le 16 avril 2024, https://www.dell.com/support/manuals/en-us/enterprise-copy-data-management/pp-dm_19.9_ag/file-level-restore-of-a-powerprotect-backup-in-the-vsphere-client.
101. Dell, « Recovery Orchestration with PowerProtect Data Manager Overview », consulté le 16 avril 2024, https://www.youtube.com/watch?v=po2oMnAg_x4.
102. Rubrik, « Quarantine files or objects », 24 mars 2024, https://docs.rubrik.com/en-us/saas/saas/quarantine.html.
103. Rubrik, « Downloading quarantined files for forensic analysis », 24 mars 2024, https://docs.rubrik.com/en-us/saas/saas/downloading_quarantined_files_for_forensic_analysis.html.
104. Forrester, « The Total Economic Impact™ Of Dell PowerProtect Cyber Recovery », consulté le 16 avril 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/the-total-economic-impact-dell-powerprotect-cyber-recovery.pdf.
105. Rubrik, « Workload recovery during an RSC service disruption », consulté le 16 avril 2024, https://docs.rubrik.com/en-us/saas/saas/workload_recovery_during_rsc_outage.html.
106. Rubrik, « Rubrik CDM APIs and service account workflows », consulté le 16 avril 2024, https://docs.rubrik.com/en-us/saas/saas/rubrik_apis_sa_workflows.html.
107. Rubrik, « Recoverable workloads during RSC service disruption », consulté le 16 avril 2024, https://docs.rubrik.com/en-us/saas/saas/recoverable_workloads_during_rsc_service_disruption.html.

108. Rubrik, « Workloads require third-party tools for recovery », consulté le 16 avril 2024, https://docs.rubrik.com/en-us/saas/saas/workloads_require_third_party_tools_for_recovery.html.

109. NIST, « Computer Security Resource Center Glossary: air gap », consulté le 29 juillet 2024, https://csrc.nist.gov/glossary/term/air_gap.

110. Dell, « Guide de solutions Dell PowerProtect Cyber Recovery ».

111. Dell, « Dell PowerProtect Cyber Recovery: Reference Architecture ».

112. Adam Eckerle, « Debunking the Myths about Air Gaps », consulté le 14 mars 2024, https://www.rubrik.com/blog/technology/2021/11/debunking-the-myths-about-air-gaps.

113. Rubrik, « Air-Gap, Isolated Recovery, and Ransomware - Cost vs. Value », consulté le 14 mars 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/solutions-brief/Air-Gap-Isolated-Recovery-and-Ransomware-Cost-vs.-Value.pdf.

114. Brian Williams, « Rubrik Air Gap and Immutability », consulté le 14 mars 2024, https://vimeo com/561870246.

115. Rubrik, « Retention locks in the Rubrik cluster », consulté le 18 mars 2024, https://docs.rubrik.com/en-us/9.0/sg/security_guide/retention_locks_in_the_rubrik_cluster.html.

▶ Consultez la version originale en anglais de ce rapport

Ce projet a été réalisé à la demande de Dell Technologies.

Principled Technologies®

Facts matter.®