DELL Technologies

Présentation de la solution

# Dell PowerProtect Cyber Recovery

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

## POURQUOI CHOISIR CYBER RECOVERY ?

Les cyberattaques ont pour objectif de compromettre vos données les plus précieuses, y compris vos sauvegardes. Il est donc impératif de protéger les données stratégiques et, en cas d'attaque, de les récupérer en assurant leur intégrité pour pouvoir relancer l'activité de l'entreprise.

*Voici les composants d'une solution cyberrésiliente :*

**Immuabilité des données**
Création de copies de données immuables pour préserver l'intégrité et la confidentialité des données avec des couches de sécurité et de contrôle.

**Isolement automatisé des données**
Isolation automatique des copies de données non modifiables de l'environnement de sauvegarde de production vers un coffre-fort numérique sécurisé avec un accès hautement restreint.

**Analytique intelligente**
Contrôles d'intégrité automatisés utilisant l'apprentissage automatique basé sur l'IA et l'indexation de l'ensemble du contenu avec des outils analytiques puissants dans un coffre-fort sécurisé pour déterminer si les données ont été affectées par un logiciel malveillant.

**Récupération et mesures correctives**
Workflows et outils permettant de procéder à une récupération après un incident via des processus de restauration dynamiques et vos procédures de reprise après sinistre existantes.

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

### Le défi : les cyberattaques sont l'ennemi numéro un des entreprises axées sur les données.

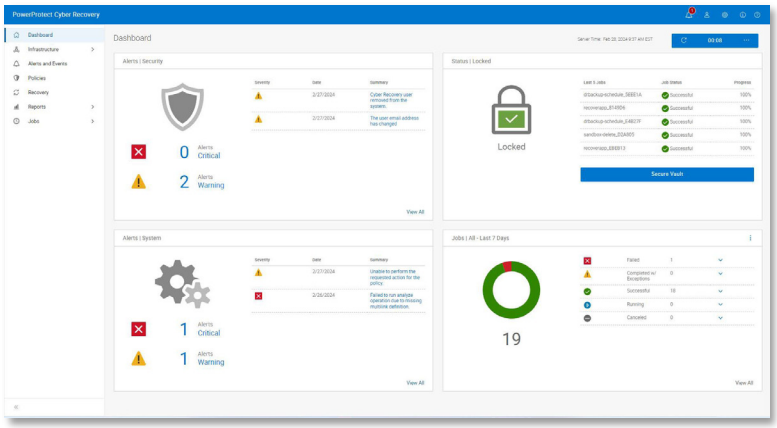
Les données représentent la devise de l'économie numérique. Cette ressource doit être protégée et facilement accessible, et sa confidentialité doit être préservée. Le marché mondial moderne repose sur le flux continu des données transitant dans des réseaux interconnectés. Les initiatives de transformation numérique et l'utilisation croissante de l'IA générative augmentent l'exposition des données sensibles.

Pour cette raison, les informations de votre organisation sont une proie désirable et très rentable pour les cybercriminels. Quel que soit leur secteur d'activité ou leur taille, les entreprises et administrations s'exposent à des risques de violation de données, de perte de chiffre d'affaires causée par les interruptions de service, d'atteinte à la réputation, ainsi qu'à des amendes élevées en cas de cyberattaque.

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

### La solution : Dell PowerProtect Cyber Recovery

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




PowerProtect Cyber Recovery offre une protection éprouvée, moderne, résiliente et intelligente visant à isoler les données stratégiques, à identifier les activités suspectes et à restaurer plus rapidement vos données pour faciliter une restauration intelligente de vos données critiques et rétablir au plus vite le fonctionnement normal des opérations métier. D'après une recherche Forrester Consulting, en cas de cyberattaque, PowerProtect Cyber Recovery contribue à réduire les interruptions de service de 75 % et à réduire de 80 % le nombre d'heures consacrées à la restauration.[2]

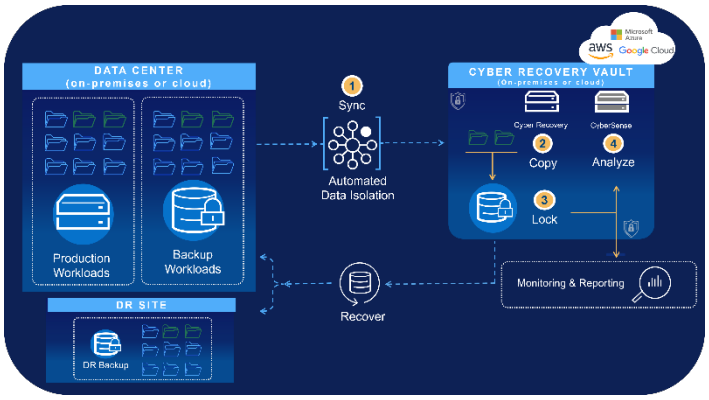
## PowerProtect Cyber Recovery : immuabilité, isolement et intelligence

### Immuabilité : PowerProtect Data Domain

PowerProtect Data Domain constitue la base de Dell PowerProtect Cyber Recovery. Dotée de plusieurs couches de sécurité Zero-Trust, cette solution fournit des copies de sauvegarde immuables pour garantir l'intégrité et la confidentialité des données. Les fonctionnalités telles que la chaîne de confiance matérielle, Secure Boot, le chiffrement, Retention Lock, l'accès basé sur les rôles et l'authentification multifacteur garantissent la capacité de restauration de vos données.

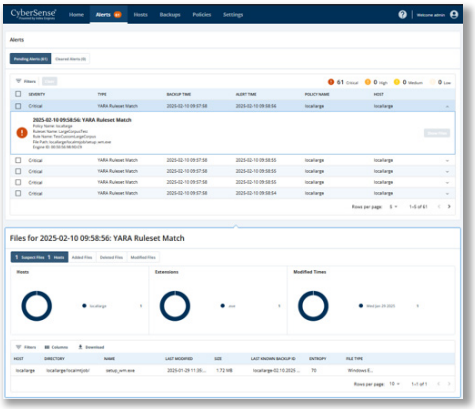
### Isolement : coffre-fort Cyber Recovery

Le coffre-fort PowerProtect Cyber Recovery constitue un environnement isolé doté de plusieurs couches de protection qui assurent une résilience contre les cyberattaques, même internes. L'isolation automatisée des données permet de copier en toute sécurité (Sync) les données de sauvegarde essentielles (y compris celles des systèmes ouverts et de l'ordinateur central) dans un coffre-fort physiquement isolé, à l'écart de la surface d'attaque de la production, sans jamais exposer le chemin de gestion aux menaces. Ensuite, une copie immuable est automatiquement créée pour empêcher la modification des données. Grâce à une gestion, à un réseau et à des services dédiés indépendants de l'environnement de production, des informations d'identification de sécurité distinctes et une authentification multifacteur sont requises pour accéder aux données à des fins de restauration et de test.




### Intelligence : CyberSense®

PowerProtect Cyber Recovery est la première solution à intégrer entièrement CyberSense® pour des restaurations plus intelligentes en cas de cybermenaces, le tout au sein du coffre-fort sécurisé Cyber Recovery. CyberSense n'est pas une simple solution de métadonnées : grâce à une analyse complète du contenu, elle détecte la corruption des données après une attaque avec une précision de 99,99 %[3] et facilite une restauration intelligente et rapide. CyberSense examine les sauvegardes de données immuables pour en observer l'évolution au fil du temps et utilise l'apprentissage automatique basé sur l'IA pour détecter les signes de corruption indiquant une attaque par rançongiciel. CyberSense détecte les suppressions massives, le chiffrement intégral et partiel, et d'autres modifications suspectes résultant d'attaques sophistiquées dans l'infrastructure principale (y compris Active Directory, DNS, etc.), les fichiers utilisateur et les bases de données. Des alertes de seuil personnalisées peuvent être créées et, si des signes de corruption sont détectés, le tableau de bord des alertes et les rapports d'investigation post-attaque facilitent le diagnostic rapide de l'ampleur et de l'impact de l'attaque, y compris l'identification d'une copie propre des données pour restaurer vos systèmes stratégiques. Les règles YARA personnalisées et la recherche de signatures de logiciels malveillants permettent de personnaliser et d'habiliter les organisations à se défendre de manière proactive contre les cybermenaces.




## PowerProtect Cyber Recovery : options de déploiement

### Cyber Recovery dans les environnements hybrides et multicloud

Les données stratégiques peuvent se trouver dans de nombreux emplacements différents au sein d'une entreprise, qu'elles soient sur site, colocalisées dans différents datacenters ou dans plusieurs Clouds et régions du monde entier. Quel que soit l'emplacement, les données doivent être sécurisées et non compromises lorsqu'une récupération est nécessaire après une cyberattaque.

PowerProtect Cyber Recovery est disponible et accessible via les sites de vente de Cloud public pour *AWS, Microsoft Azure* et *Google Cloud* afin de fournir un accès rapide et protéger les données dans un coffre-fort Cyber Recovery dans le Cloud. PowerProtect Cyber Recovery automatise la synchronisation des données stratégiques entre les systèmes de production et le coffre-fort Cyber Recovery dans le Cloud public. Contrairement aux solutions standard de sauvegarde dans le Cloud, l'accès aux interfaces de gestion est verrouillé par les contrôles réseau et impose l'utilisation d'autres informations d'identification de sécurité et d'une authentification multifacteur. La dispersion et la duplication des données sur plusieurs Clouds peuvent engendrer des risques en matière de sécurité et de conformité, des problèmes de synchronisation potentiels et des coûts de ressources accrus. Cette approche peut également réduire la visibilité sur vos différents environnements, et mener à une protection insuffisante contre les cybermenaces en évolution constante.

### Ready Node All-Flash de Dell avec PowerProtect Data Domain

Alors que les données stratégiques continuent de croître, la capacité à récupérer rapidement et efficacement après un cyberincident est primordiale pour garantir la continuité de l'activité et la cyberrésilience. Les organisations qui étendent la gestion des données stratégiques doivent exceller dans la récupération de leurs données à partir d'environnements de récupération isolés, tels que le coffre-fort Cyber Recovery. Ready Node All-Flash de Dell avec PowerProtect Data Domain offre une solution de cyberrestauration rationalisée, économe en énergie et rentable, dotée des outils analytiques CyberSense améliorés et de fonctionnalités de restauration rapide pour respecter les contrats de niveau de service de l'organisation. En utilisant moins de matériel, d'espace et d'énergie, les organisations peuvent améliorer la rapidité d'accès aux données, optimiser l'efficacité opérationnelle et garantir l'intégrité des données, ce qui se traduit par une réduction des interruptions de service et des coûts de maintenance globaux.

## PowerProtect Cyber Recovery : reprise de l'activité

### Récupération et mesures correctives

PowerProtect Cyber Recovery comprend des procédures de récupération et de restauration automatisées. Cela permet de remettre rapidement en ligne les systèmes stratégiques pour l'entreprise, en toute confiance. La récupération est intégrée à votre processus de réponse aux incidents. À l'issue d'un événement, l'équipe chargée de répondre aux incidents analyse l'environnement de production pour déterminer la cause première de l'événement. CyberSense fournit des rapports d'investigation après une cyberattaque pour comprendre la profondeur et l'étendue de l'attaque, ainsi qu'une liste des derniers jeux de sauvegardes fiables avant corruption. Ensuite, lorsque l'équipe de production est prête pour la récupération, Cyber Recovery fournit les outils de gestion et la technologie qui permet de récupérer les données.

### Planification et conception de la solution

Les services Dell Professional Services for Cyber Recovery vous aident à identifier les systèmes stratégiques pour l'entreprise à protéger et peuvent élaborer des cartes des dépendances pour les applications et services associés, ainsi que l'infrastructure requise pour les restaurer. Ces services génèrent également des exigences en matière de récupération, ainsi que d'autres options de conception possibles. Ils identifient les technologies adaptées pour analyser, héberger et protéger vos données, ainsi qu'un dossier commercial et une chronologie pour l'implémentation.

### Conclusion

Les initiatives industrielles telles que Sheltered Harbor utilisent PowerProtect Cyber Recovery pour protéger les clients, les institutions financières, mais aussi préserver la confiance du public vis-à-vis du système financier américain en cas d'attaque cybernétique causant une panne des systèmes critiques, y compris les sauvegardes. Avec des milliers de clients, Cyber Recovery avec CyberSense rassure les dirigeants d'entreprise et a prouvé qu'elle accélérait la récupération des données en cas de cybermenace.

Avec PowerProtect Cyber Recovery, vous savez que vous pouvez rapidement identifier et restaurer les données reconnues comme intègres, puis rétablir le fonctionnement normal des opérations métier après une cyberattaque.

***Il est temps de reprendre votre activité.***



[1] D'après l'étude « Global Data Protection Index 2024 Snapshot », réalisée par Vanson Bourne à la demande de Dell Technologies. Octobre 2023.
[2] Étude réalisée par Forrester Consulting à la demande de Dell Technologies, « The Total Economic Impact of Dell PowerProtect Cyber Recovery », août 2023
[3] D'après le rapport ESG « Index Engines' CyberSense Validated 99.99% Effective in Detecting Ransomware Corruption » réalisé à la demande d'Index Engines. Juin 2024