

# Dell PowerProtect Cyber Recovery pour Microsoft Azure

Coffre-fort de Cloud public sécurisé pour protéger les données stratégiques contre les rançongiciels et les cyberattaques destructrices

## Pourquoi choisir Dell PowerProtect Cyber Recovery pour Azure ?

Les cyberattaques ont pour objectif de détruire, voler ou compromettre vos données les plus précieuses, d'une manière ou d'une autre, 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. *Dans le cas contraire, votre entreprise peut-elle survivre ?*

**Isolement et gouvernance des données**  
Un environnement de coffre-fort de données isolé utilisant Azure et déconnecté des réseaux internes ou de sauvegarde avec accès restreint

**Copie et air gap automatisés** Copies des données protégées vers un coffre-fort numérique sécurisé protégé par un air gap opérationnel entre les environnements de production et celui du coffre-fort

**Récupération et mesures correctives** Utilisez des workflows et des outils pour gérer la récupération après des incidents via des processus de restauration dynamiques

**Planification et conception de la solution**  
Conseils d'experts de Dell Technologies pour sélectionner les données stratégiques, les applications et les autres ressources reposant sur une solution mature et fiable

**Déploiement simplifié**  
Accès rapide à un coffre-fort de Cloud public avec un achat et un déploiement simplifiés via Azure Marketplace

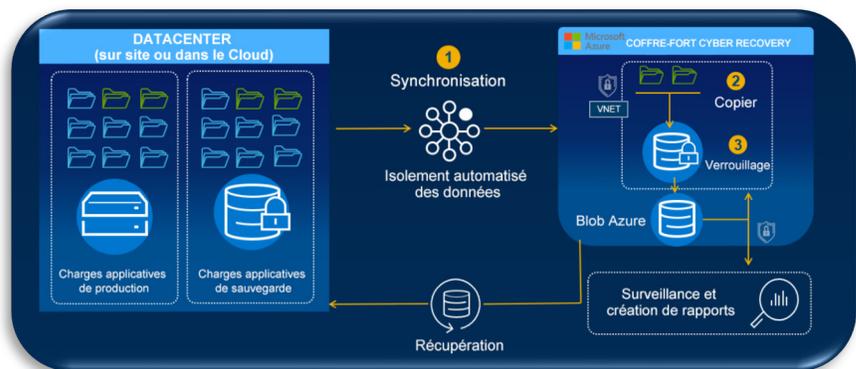
## Les cyberattaques menacent toutes les entreprises axées sur les données

La protection de votre organisation commence par la protection de vos données. Le paysage des cybermenaces est en constante évolution et continue de se développer parallèlement à l'amélioration des technologies. S'éloignant des logiciels malveillants et rançongiciels, les nouvelles stratégies d'attaque impliquent maintenant l'extorsion numérique, et ces attaques continuent d'exposer les données internes sensibles des organisations. Avec la menace moderne des cyberattaques, et l'importance de maintenir la confidentialité, la disponibilité et l'intégrité des données, en particulier pour les entreprises, les écoles et les organisations axées sur les données d'aujourd'hui, ces dernières ont besoin de solutions et stratégies modernes pour protéger leurs données et systèmes essentiels.

Les attaques sont incessantes, et leur coût continue d'augmenter. L'idée reçue selon laquelle seuls des entreprises ou des secteurs d'activité spécifiques sont ciblés est fautive : en réalité, les entreprises de toute taille et de tout secteur sont des cibles potentielles.

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

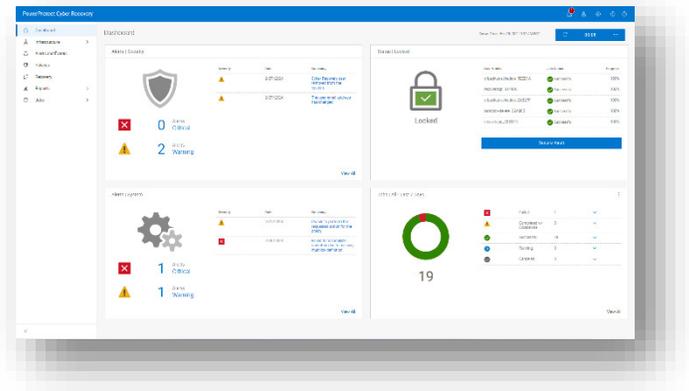
## La solution : PowerProtect Cyber Recovery pour Azure



Dell PowerProtect Cyber Recovery pour Azure offre une protection éprouvée, moderne et intelligente visant à isoler les données stratégiques et à rétablir rapidement le fonctionnement normal des opérations métier.

## Cyber Recovery Vault dans Azure

PowerProtect Cyber Recovery pour Azure offre plusieurs couches de protection pour assurer la résilience contre les cyberattaques et les menaces qui viennent de l'intérieur. Il éloigne les données stratégiques de la surface d'attaque en les isolant physiquement et logiquement au sein d'Azure grâce à un air gap opérationnel sécurisé et automatisé. Contrairement aux solutions standard de sauvegarde dans le Cloud, l'accès aux interfaces de gestion est verrouillé par les contrôles réseau et peut imposer l'utilisation d'autres informations d'identification de sécurité et d'une authentification multifacteur. PowerProtect Cyber Recovery automatise la synchronisation des données entre les systèmes de production et le coffre-fort Cyber Recovery dans Azure, créant des copies immuables associées à des politiques de conservation verrouillées. En cas de cyberattaque, vous pouvez rapidement identifier une copie adéquate des données, récupérer les systèmes stratégiques et rétablir leur bon fonctionnement.



### Réduction des risques métier liés aux cybermenaces

Les workflows automatisés déplacent en toute sécurité les données stratégiques de l'entreprise vers un environnement isolé au sein d'Azure. Créez facilement des politiques de protection et surveillez les menaces potentielles en temps réel à l'aide d'un tableau de bord utilisateur intuitif. Le coffre-fort est maintenu en isolation logique par un air gap opérationnel. Ses composants ne sont jamais accessibles depuis l'environnement de production et lorsque l'air gap est déverrouillé, l'accès au stockage du coffre-fort reste extrêmement limité et protégé dans un réseau virtuel Azure sécurisé.

PowerProtect Cyber Recovery gère la synchronisation des données entre les systèmes de production et le coffre-fort sécurisé, ce qui crée des copies supplémentaires protégées. En cas de cyberattaque, les utilisateurs autorisés peuvent accéder rapidement aux données pour restaurer les systèmes stratégiques et remettre votre organisation sur les rails.

### Récupération et mesures correctives

PowerProtect Cyber Recovery pour Azure offre des options de restauration et de récupération flexibles qui permettent de remettre les données stratégiques en ligne rapidement. De plus, il est pris en charge par des programmes de restauration testés et documentés. Cyber Recovery pour Azure permet la récupération des données stratégiques à partir du coffre-fort après une cyberattaque et pour tester les procédures de récupération. Cela vous permet de restaurer vos données vers le datacenter de l'entreprise, un autre datacenter, un nouveau réseau virtuel ou un environnement propre au sein d'Azure.

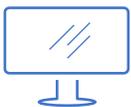
### Planification et conception des solutions

Faites confiance aux services Dell Technologies pour élaborer des stratégies, mettre en œuvre, adapter et faire évoluer un programme de récupération informatique afin de répondre aux besoins de votre organisation. Les services d'experts peuvent inclure l'alignement de la protection et de la restauration, le déploiement de technologies de cyber-récupération, la réponse à un cyberincident ou la formation des équipes sur les dernières compétences. En collaboration avec vos équipes, nos experts du secteur vous aident à déterminer les systèmes et données stratégiques à protéger et l'infrastructure nécessaire à la récupération.

### Déploiement simplifié

PowerProtect Cyber Recovery pour Azure est disponible en tant qu'offre commercialisable sur Azure Marketplace, ce qui vous permet de tirer parti de votre abonnement Azure existant. Dell Technologies s'engage à vous fournir un accès rapide à la gamme Dell d'offres de protection des données pour Azure en un simple achat. De plus, Dell Technologies vous offre la possibilité d'acheter Cyber Recovery pour Azure comme vous le souhaitez, sur Azure Marketplace ou directement auprès de Dell.

PowerProtect Cyber Recovery vous donne la confiance nécessaire pour protéger, identifier et restaurer les données fiables connues, et maintenir des opérations et une conformité normales après une cyberattaque.



En savoir plus sur Dell  
PowerProtect Cyber  
Recovery



Contactez un expert Dell  
Technologies



Afficher l'offre Azure  
Marketplace



Prenez part à la  
conversation avec  
#PowerProtect