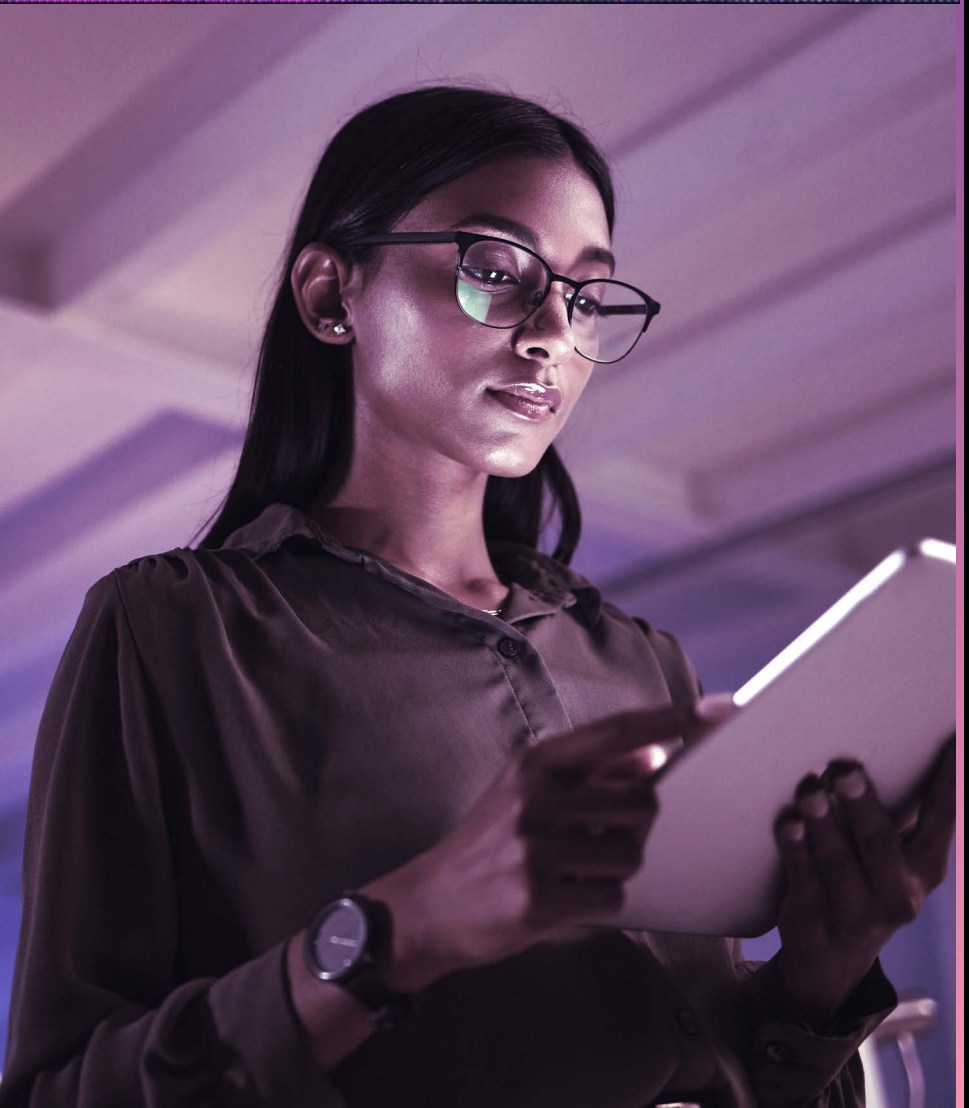


Commvault

eBOOK

Aller au-delà de la simple récupération post-attaque

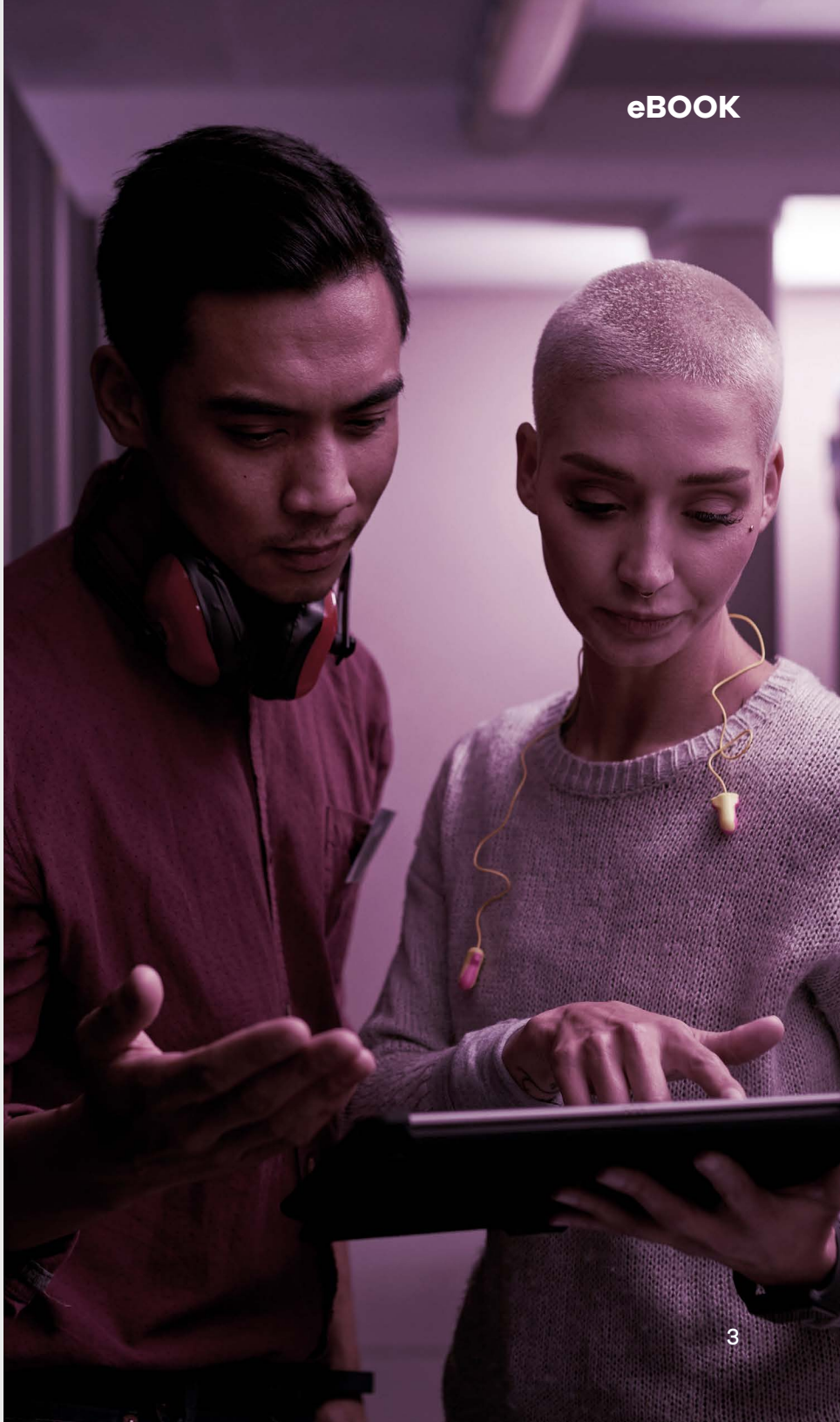
POURQUOI UNE STRATÉGIE DIFFÉRENTE EST NÉCESSAIRE LORSQUE L'ATTAQUE VOUS FRAPPE

CONTENTS

Vous avez installé des détecteurs de fumée dans votre maison, appris à vos enfants à composer le 18 et savez comment contacter la compagnie d'assurance qui détient votre police d'assurance habitation. Vous êtes prêt à faire face à un incendie.

Mais ne comptez pas sur ces mêmes mesures pour vous protéger contre le vol d'identité. Au contraire, pour faire face à cette menace, vous faites attention à la manière dont vous partagez vos données, vous gardez le numéro de téléphone de votre banque à portée de main et vous surveillez les mouvements sur votre compte bancaire. Parce qu'il s'agit d'un problème différent, qui nécessite une approche différente.

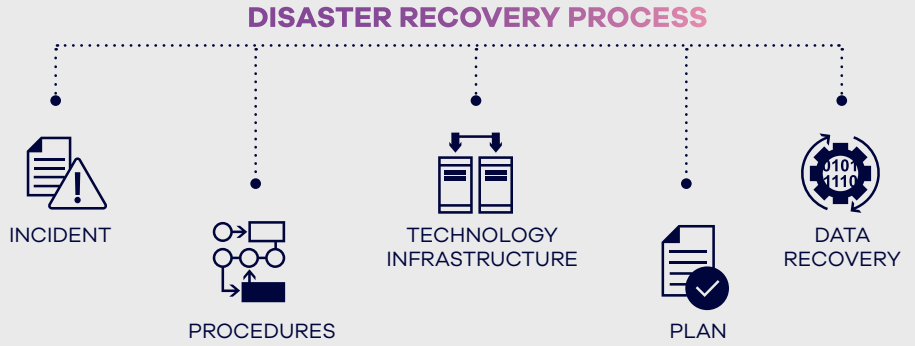
Il en va de même au sein d'un datacenter ou sur la question d'une sauvegarde de données. La reprise après sinistre et la reprise au moment d'une attaque ne sont pas la même chose. Il est essentiel de comprendre les différences et d'élaborer une stratégie préparation et de test complète afin que votre entreprise soit prête en cas de problème.



SUR LA REPRISE APRÈS SINISTRE

Vous avez besoin d'un plan de reprise après sinistre pour faire face à des événements prévisibles tels que les pannes de matériel ou les catastrophes naturelles, comme les incendies et les inondations. En général, ces incidents ne sont pas intentionnels et ne visent pas activement vos données.

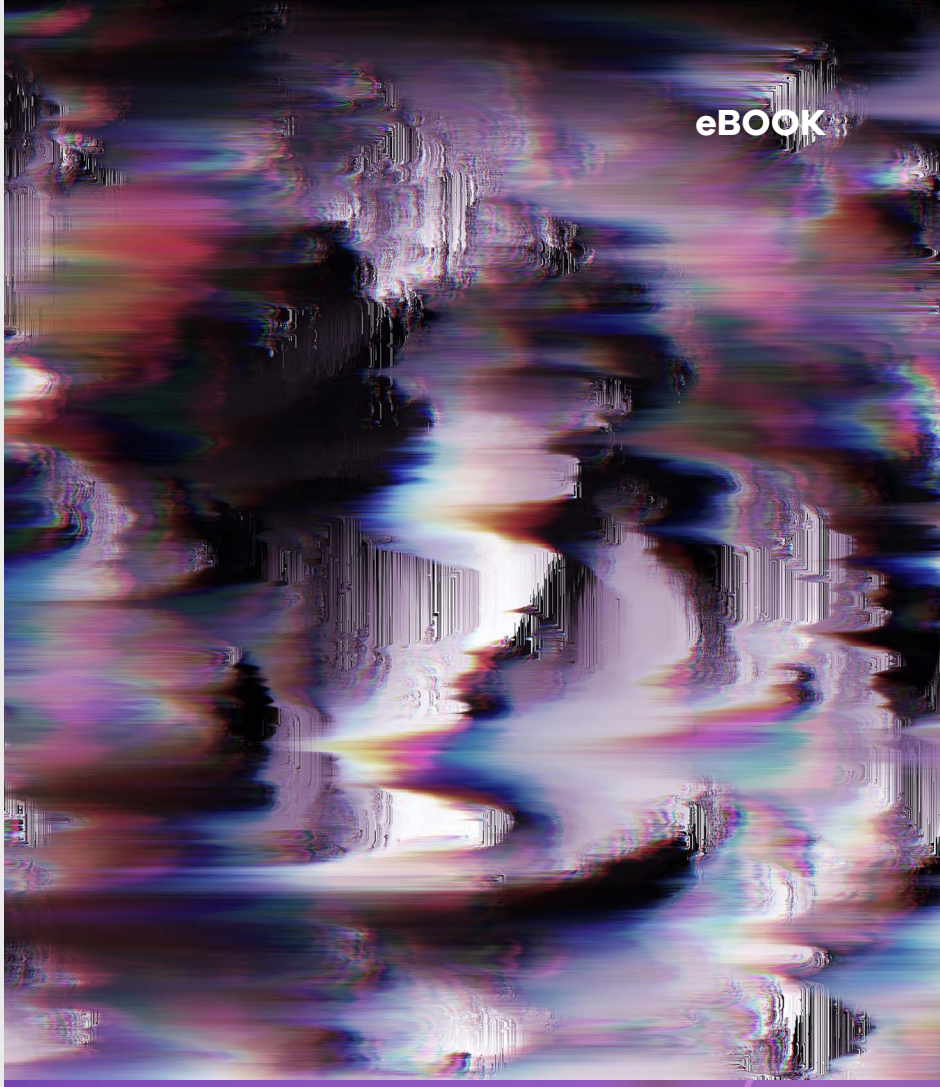
La reprise après sinistre suit généralement un plan prédéfini avec des étapes établies pour restaurer rapidement les systèmes. La restauration à partir de sauvegardes vous permet de reprendre vos activités, même dans le cas où certaines données auraient été perdues. Ce processus vise à assurer la continuité des activités, à minimiser l'impact à long terme et à protéger les données critiques.



SUR LA RÉCUPERATION EN CAS D'ATTAQUE CYBER

En revanche, la reprise post-attaque elle adresse les conséquences des attaques malveillantes telles que les ransomwares ou les violations de données, où les attaquants tentent activement d'endommager vos systèmes et de corrompre vos données. Il peut s'agir d'un sous-ensemble de données ou de l'ensemble de l'infrastructure, y compris un site de sauvegarde dédié à la reprise après sinistre.

Les cyberattaques nécessitent souvent l'ouverture une enquête et des mesures correctives avant la reprise, ce qui peut allonger les délais de récupération. Pour éviter que l'impact de l'attaque n'augmente trop vite, il est impératif de contenir l'attaque et vous assurer qu'il n'y a pas d'autres actions malveillantes en cours. Chaque élément de votre environnement informatique, du matériel aux données et aux sauvegardes, doit être examiné à la recherche d'une infection avant la restauration, car les attaquants peuvent avoir caché des logiciels malveillants ou modifié des fichiers de sauvegarde. Vous devrez minimiser les dommages, prévenir les pertes de données et maintenir votre niveau de sécurité.



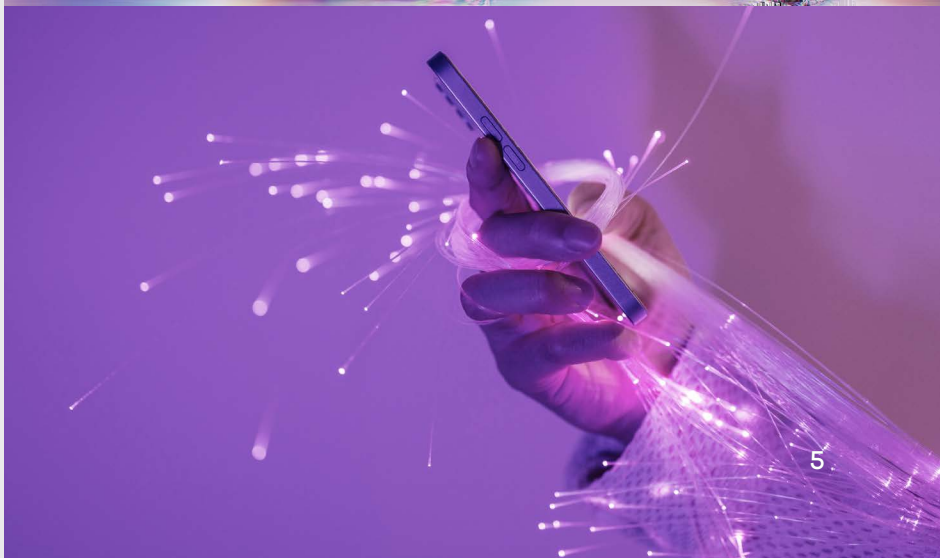


SCHÉMA DES PILIERS POUR GARANTIR LA CYBER-RÉCUPÉRATION

SCENARIOS

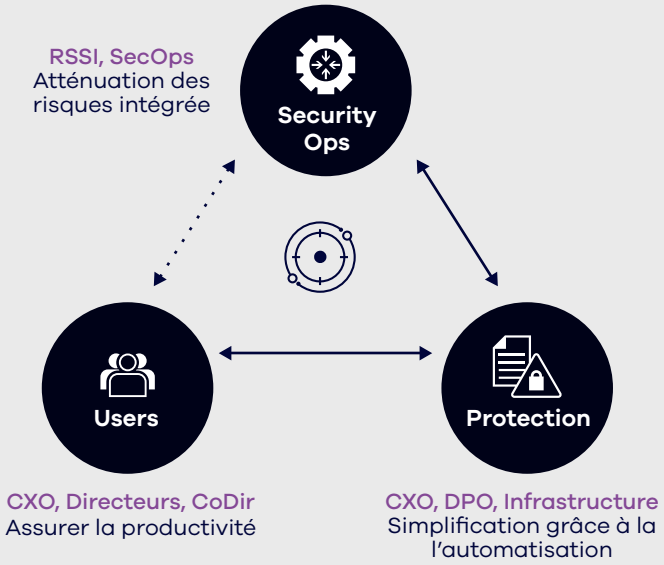
La capacité de cyber-récupération (CR) induit de nouveaux besoins par rapport plans de reprise d'activité ou de continuité de l'activité (PRA/CA)

ELEMENTS	PRA/CA	CR
COMPROMISSION	Perte complète des opérations sur site	Données, Réseau, Sécurité
RÉCUPÉRATION	Renversement/ retour RTO, reconstruction	Restauration sélective pour réparation
RESSOURCES	Disponibilité totale des piles logicielles	Validation, restauration, reconstruction
PROCESSUS	Persévérant	Elastique

Ces différentes stratégies peuvent être utilisées ensemble pour faire converger les ressources d'actifs et les processus métiers.

ORGANISATION

La capacité de cyber-récupération (CR) implique d'obtenir des résultats en matière de collaboration et de partage des responsabilités dans l'ensemble de l'organisation (personnel et processus)



Intégration et automatisation des notifications Des actions éclairées et des flux de travail continus au sein des équipes contribuent à améliorer les performances.

CAPACITES

Les pré-requis pour la cyber-récupération (CR) sont dépendants des objectifs propres à l'entreprise elle-même

- Sauvegardes sécurisées, isolées et immuables
- Détection avancée de mouvements et comportements suspects
- Analyse et assainissement des données fichiers
- Validation automatique des processus de récupération
- Récupération planifiée et accélérée

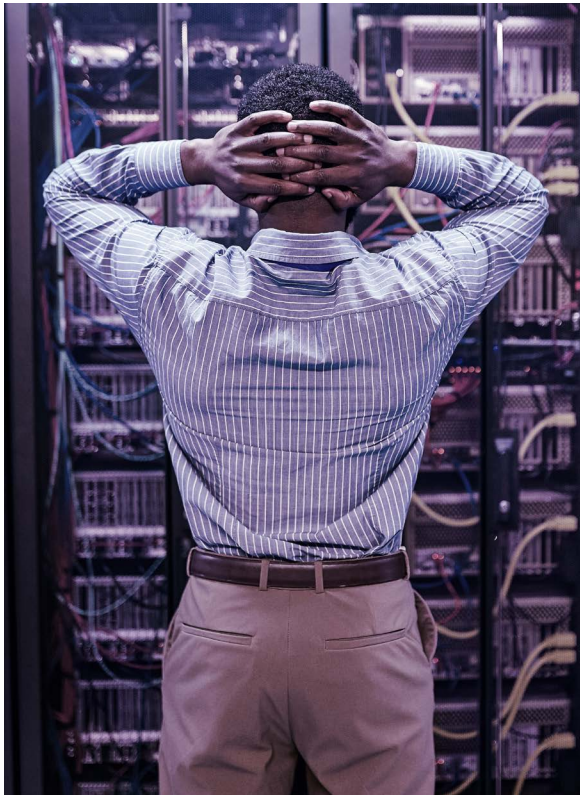
PARCE QUE LES SEULS TESTS DE REPRISE APRÈS SINISTRE NE SUFFISENT PAS

Les tests de reprise après sinistre sont importants, mais la reprise cybernétique est beaucoup plus complète. Bien que les deux visent à rétablir la fonctionnalité opérationnelle après des perturbations, les différences fondamentales nécessitent des réponses distinctes. Les plans traditionnels de reprise après sinistre peinent à répondre efficacement aux menaces nuancées et à la complexité des cyberattaques.

Voici pourquoi:

- Nature de la menace
- Portée et objectif
- Méthodes et outils
- Intégrité et vulnérabilité des données

Par conséquent, si les plans de reprise après sinistre constituent une base précieuse pour la réponse aux incidents, il peut s'avérer périlleux de s'y fier face à une cyberattaque. Un plan de reprise après sinistre dédié, soutenu par des outils spécialisés, du personnel et des tests fréquents, est essentiel pour atténuer les risques spécifiques et les complexités de ces attaques malveillantes.



LA REPRISE POST-ATTAQUE CYBER DOIT ABSOLUMENT ÊTRE ÉPROUVÉE PAR DES TESTS

Le test de reprise post-attaque est un exercice réel (ou test opérationnel) de restauration d'une application et de ses données à partir d'une sauvegarde. C'est le type de processus de récupération qui se produira en cas d'incident cyber, lequel est recommandé par le NIST. Les tests de reprise après sinistre et les tests de reprise post-attaque ont chacun leur place dans les scénarios applicables, mais la reprise après attaque cyber est beaucoup plus complète.

Ces tests permettent d'ailleurs d'assurer la résilience de vos systèmes et de vos données, ainsi que la continuité de vos activités dans leur ensemble. La récupération d'applications et de données critiques est une opération complexe qui pose de nombreux problèmes. Les tests de cyber-reprise permettent de détecter les erreurs et de les résoudre lorsque les enjeux sont faibles.

Les tests permettront à vos équipes de s'entraîner et de s'assurer qu'elles peuvent récupérer les applications et les données critiques en cas d'incident cyber. En fait, le NIST recommande que «les sauvegardes de données soient réalisées, protégées, maintenues et testées», car «il est préférable d'identifier un problème inattendu pendant les tests que lors d'une réelle cyber-attaque»[1]. Toutefois, il est intéressant de constater qu'en réalité, très peu d'entreprises procèdent à des tests complets, fréquents et réussis.

[1] https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-84.pdf

204 JOURS

Temps moyen de présence d'un attaquant dans le réseau de l'entreprise[2]

92%

des entreprises payant la rançon ne récupèrent pas l'ensemble de leurs données[4]

Les attaquants débutent leurs mouvements latéraux dans les

84 MINUTES

suivant l'intrusion[3]

[2] https://www.ibm.com/reports/data-breach
[3] https://www.crowdstrike.com/resources/reports/threat-hunting-report/
[4] https://www.sophos.com/en-us/content/state-of-ransomware

COMMENT COMMVAULT CLOUD Y RÉPOND?

Vous pouvez bénéficier d'une stratégie de cyber-résilience proactive avec **Commvault® Cloud : Auto Recovery**, en réduisant l'impact des menaces sur les données sur l'ensemble des flux de travail, favorisant ainsi la continuité de l'activité. **Auto Recovery** offre une cyber-rétablissement proactif et automatisé grâce à une protection multicouche des données, réduisant ainsi le temps de récupération lors de cyber-attaques et autres incidents. Avec des objectifs de temps de réponses cibles actualisés en temps quasi réel et des capacités de reprise inférieures à une minute, Auto Recovery minimise l'impact des menaces au sens large. Que cela porte sur les grands ensembles de données, sur les charges de travail disponibles dans le cloud, sur site ou encore en mode SaaS, pour continuer à assurer la continuité de l'activité.

Commvault® Cloud Cleanroom™ Recovery de son côté offre une solution complète de récupération simple, sécurisée et économique « as-a-service » pour permettre aux entreprises de tester leurs plans de reprise post-attaque, effectuer des analyses « forensic » sécurisées et assurer une continuité d'activité ininterrompue.

Les cybermenaces, sans cesse présentes et en constante multiplication, à l'instar des ransomwares créent un risque existentiel et peuvent être sources de confusion et d'anxiété au sein des entreprises. Cleanroom Recovery offre une salle blanche virtuelle unique pour valider l'efficacité des plans de reprise, des technologies employées et des processus posés pour la cyber-reprise.

Cleanroom Recovery offre un environnement sécurisé où les données et les actifs critiques sont isolés et protégés des attaques. Les responsables de la sécurité et de l'informatique peuvent ainsi y obtenir des informations précieuses sur des acteurs inconnus, renforcer leurs stratégies et contribuer à assurer la continuité des activités.

RÉCUPÉRATION POST-SINISTRE

LE DÉFI:

Assurer la reprise après sinistre pour la continuité des activités et la reprise du site en cas de catastrophe naturelle ou de panne.

LA SOLUTION

Commvault® Cloud Auto Recovery Commvault Cloud Auto Recovery est la plateforme de réplication de données la plus flexible et économique du marché grâce à:

- Reprise en moins d'une minute
- Possibilité d'un temps de récupération cible quasi nul garantissant la récupération instantanée des données
- Transformation des données pendant la réplication
- Orchestration en un clic des flux de production vers la reprise d'activité, et vice versa
- Exercices d'évacuation des données pour la validation de l'état de préparation à la reprise

REPRISE POST-ATTAQUE

LE DÉFI:

Assurer la reprise post-attaque cyber pour récupérer l'ensemble des données et applications infectées pendant l'incident.

LA SOLUTION

Commvault® Cloud Cleanroom™ Recovery offre un ensemble d'applications simple à utiliser pour une reprise rapide et sécurisée.

- Créer et automatiser la gestion des salles blanches pour faciliter les phases de récupération
- Regroupement logique des flux de travail hétérogènes pour faciliter la catégorisation
- Analyse sécurisée et scanner de l'infrastructure avec des outils de série et entièrement personnalisables
- Règles de recuperation et personnalisation des actions
- Plan de contrôle Commvault accessible sur site
- Surveillance, rapports de bilans et audits centrés sur les capacités de récupération pour plus de conformité réglementaire

Si un plan de reprise après sinistre est essentiel pour protéger l'infrastructure de votre entreprise, vous ne serez pas totalement protégé si vous ne disposez pas également d'un plan de reprise cybernétique et d'une stratégie de test. Il s'agit là d'un élément essentiel pour protéger vos données et votre réputation contre les attaques malveillantes.

Rendez-vous ici pour en savoir plus sur comment Commvault peut vous aider à protéger votre entreprise et réserver une démonstration de Commvault® Cloud Cleanroom™ Recovery.

commvault.com | 01 73 13 00 23 | talktous@commvault.com

Commvault®