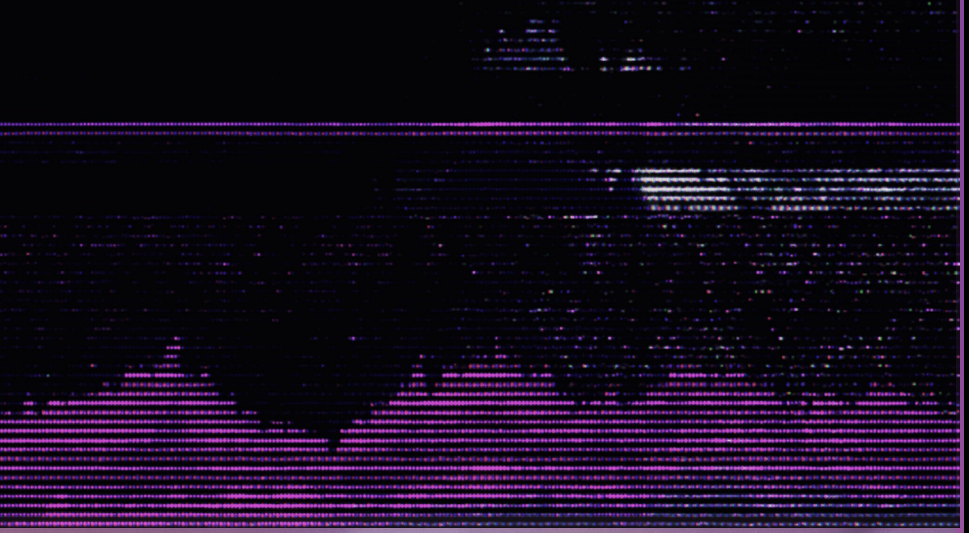




Commvault + Stordata

eBOOK

# Au-delà de la reprise après sinistre

POURQUOI VOUS AVEZ BESOIN D'UNE STRATÉGIE DIFFÉRENTE LORSQUE LES CYBERATTAQUES FRAPPENT

# SOMMAIRE


03 Reprise après sinistre

04 Reprise après cyberattaque

05 Portée de la conception prête pour la cyber-récupération

06 Les tests de reprise après sinistre ne suffisent pas

07 Les tests de reprise après cyberattaque sont critiques

09 Comment le cloud de Commvault aide




© 2024 Commvault

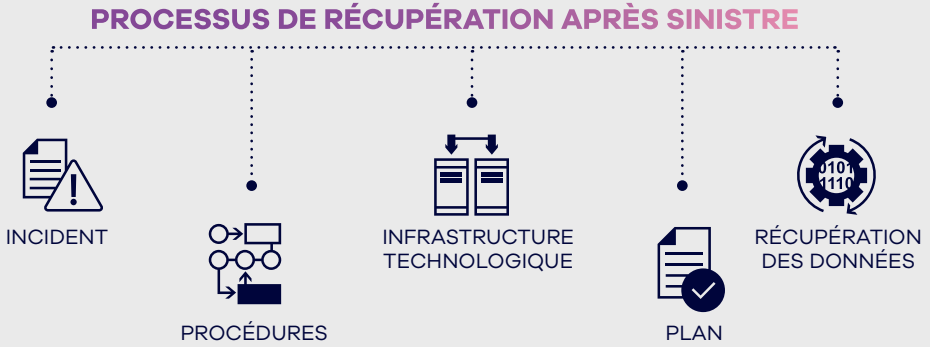





# RÉCUPÉRATION APRÈS SINISTRE

Vous avez besoin d'un plan de récupération après sinistre pour gérer des événements prévisibles comme les défaillances matérielles ou les catastrophes naturelles telles que les incendies et les inondations. En général, ces incidents ne sont pas intentionnels et ne visent pas activement vos données.

La récupération 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 vous remettre en ligne même si certaines données sont perdues. Ce processus vise à assurer la continuité des activités, à minimiser l'impact à long terme et à protéger les données critiques.





© 2024 Commvault

# RÉCUPÉRATION CYBER

En revanche, la récupération cyber traite des attaques malveillantes telles que les rançongiciels ou les violations de données, où les attaquants tentent activement de nuire à vos systèmes et de corrompre vos données. Cela pourrait concerner un sous-ensemble de données ou l'ensemble de l'infrastructure, y compris un site de basculement de reprise après sinistre.

Les cyberattaques impliquent souvent une investigation et une remédiation avant la récupération, ce qui peut prolonger le calendrier. Vous devez contenir l'attaque et vous assurer qu'il ne reste aucune faille. Chaque élément de votre environnement, du matériel aux données et aux sauvegardes, doit être examiné pour détecter une éventuelle infection avant la restauration, car les attaquants pourraient avoir caché des logiciels malveillants ou modifié des fichiers de sauvegarde. Vous devrez minimiser les dommages, prévenir la perte de données et maintenir la posture de sécurité.

Commvault + Stordata







© 2024 Commvault

# PORTÉE DE LA CONCEPTION PRÊTE POUR LA CYBER-RÉCUPÉRATION

## SCÉNARIOS

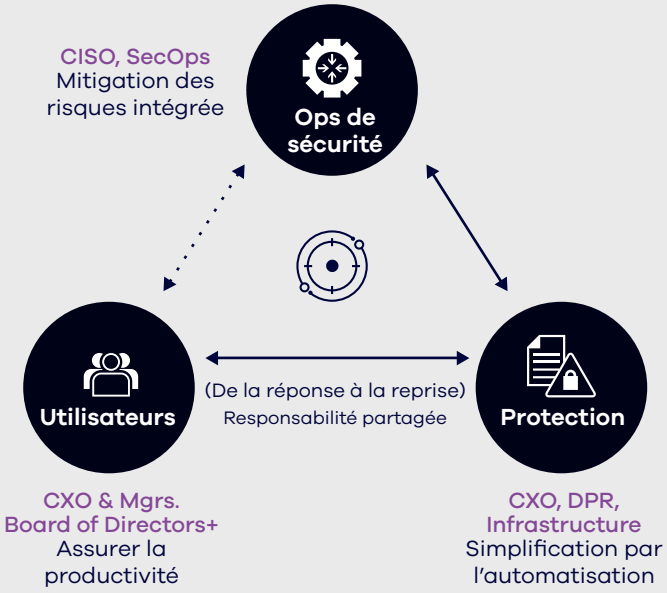
La cyber-récupération entraîne généralement un ensemble de besoins différents par rapport aux plans de reprise après sinistre / continuité d'activité.

| ÉLÉMENTS | REPRISE APRÈS SINISTRE CONTINUITÉ DES ACTIVITÉS | RÉCUPÉRATION CYBER |
|---|---|---|
| **ENGAGEMENT** | Perte totale des opérations sur site | Datos, redes, seguridad |
| **RECUPERACIÓN** | Basculer/restaurer le RTO, reconstruire | Restauración selectiva para reparación |
| **RESSOURCES** | Pile de disponibilité complète | Validation de la restauration, reconstruction reconstruction |
| **PLANIFICATION** | Persistente | Élastique |

Ces stratégies peuvent être combinées pour converger les ressources et les processus.

## ORGANISATION

La reprise après cyberattaque implique une collaboration avec une responsabilité partagée, à travers toute l'organisation (personnes, processus)




L'intégration et l'automatisation des notifications, des actions informées et des flux de travail fluides à travers les équipes peuvent accélérer les résultats.

## CAPACITÉS

Les exigences de récupération cybernétique dépendent des objectifs de l'organisation

- Sauvegardes de coffre-fort sécurisées, isolées et immuables
- Détection précoce des motifs suspects
- Analyse cybernétique et assainissement des données
- Validation automatique de la récupération
- Récupération rapide et planifiée

Commvault® + Stordata


© 2024 Commvault

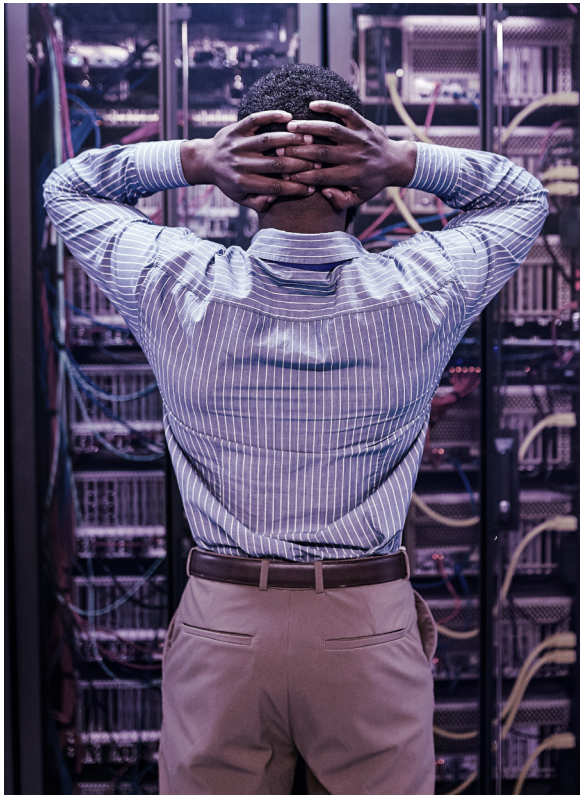
# LES TESTS DE REPRISE APRÈS SINISTRE NE SONT PAS SUFFISANTS

Les tests de reprise après sinistre sont importants, mais la reprise après cyberattaque est beaucoup plus complète. Bien que les deux visent à restaurer la fonctionnalité opérationnelle après des perturbations, des différences fondamentales nécessitent des réponses distinctes. Les plans traditionnels de reprise après sinistre peinent à aborder efficacement les menaces nuancées et les complexités que présentent les cyberattaques.

**Voici pourquoi:**

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

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




© 2024 Commvault

# LES TESTS DE RÉCUPÉRATION APRÈS CYBERATTAQUE SONT CRUCIAUX



Les tests de récupération après cyberattaque consistent en une simulation pratique (ou un test opérationnel) de la restauration d'une application et de ses données à partir d'une sauvegarde. C'est ce type de processus de restauration qui se produira lors d'un incident cyber, et c'est le processus recommandé par le NIST. Les tests de reprise après sinistre et les tests de récupération après cyberattaque ont chacun leur place selon les scénarios applicables, mais la récupération après cyberattaque est beaucoup plus complète.

Les tests de récupération après cyberattaque renforcent la résilience de vos systèmes et de vos données, ainsi que la continuité des activités. La récupération des applications et des données critiques est chargée de complexités et de problèmes. Tester la récupération après cyberattaque permet de découvrir et de résoudre les erreurs lorsque les enjeux sont faibles.

Les tests donneront à vos équipes la pratique et la confiance nécessaires pour récupérer les applications et les données critiques lorsqu'un incident cyber se produit. En fait, le NIST recommande que "les sauvegardes des données soient effectuées, protégées, maintenues et testées" car "il vaut mieux identifier un problème inattendu lors des tests plutôt que lors d'un véritable événement cyber." Mais la réalité est que très peu d'organisations testent de manière complète, fréquente et réussie.



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



© 2024 Commvault



# 204 JOURS

Temps moyen pendant lequel un attaquant reste dans une entreprise[2]

# 92%

des entreprises qui paient la rançon ne récupèrent pas toutes leurs données[4]

Les attaquants commencent à se déplacer latéralement dans les

# 84 MINUTES

suivant une attaque[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


© 2024 Commvault



# COMMENT LE CLOUD DE COMMVAULT AIDE

Vous pouvez obtenir une résilience cyber proactive avec la récupération automatique **Commvault® Cloud Auto Recovery**, minimisant l'impact des menaces de données sur toutes les charges de travail et favorisant la continuité de votre activité. Auto Recovery offre une récupération cyber proactive automatisée grâce à une protection des données multicouche pour réduire le temps de récupération lors des cyberattaques et autres catastrophes. Avec un objectif de temps de récupération (RTO) potentiellement proche du temps réel et des objectifs de point de récupération (RPO) de moins d'une minute, Auto Recovery minimise l'impact des menaces de données de manière large à travers les environnements cloud, sur site et SaaS pour la continuité des activités.

**Commvault® Cloud Cleanroom™ Recovery** fournit un environnement de récupération isolé, sécurisé, propre et abordable à la demande pour tester les plans de récupération cyber, réaliser des analyses forensiques sécurisées et maintenir une continuité des activités ininterrompue.

Les menaces cyber constantes et les ransomware introduisent un risque existentiel et créent de la confusion et de l'anxiété organisationnelles. Cleanroom Recovery offre un banc d'essai unique pour valider l'efficacité des plans, technologies et processus de récupération cyber.



La récupération en salle blanche offre un environnement sécurisé où les données et les actifs critiques sont isolés et protégés contre les attaques. Les responsables de la sécurité et de l'informatique peuvent obtenir des informations précieuses sur des menaces inconnues, renforcer leurs stratégies et aider à garantir la continuité ininterrompue des activités.



© 2024 Commvault

# REPRISE APRÈS SINISTRE

**DÉFI**

Reprise après sinistre pour la continuité des activités et la récupération des sites en cas de catastrophes naturelles ou de pannes.

**SOLUTION**

**Commvault® Cloud Auto Recovery** est la plateforme de réplication de données la plus flexible et économique.

- Capacités RPO de moins d'une minute
- RTO proche de zéro possible pour une récupération instantanée des données
- Transformation des données lors de la réplication
- Orchestration en un clic de la production à la reprise après sinistre, et vice versa
- Exercices de simulation de reprise après sinistre pour la validation de la préparation à la récupération

# RÉCUPÉRATION CYBER

**DÉFI**

La récupération cyber pour restaurer les données et les applications affectées par des logiciels malveillants après un incident cyber.

**SOLUTION**

La récupération en salle blanche **Commvault® Cloud Cleanroom™** offre une restauration des applications simple, sécurisée et rapide.

- Établir et automatiser des salles blanches pour la récupération
- Regroupement logique de charges de travail hétérogènes
- Analyse sécurisée avec des outils intégrés et personnalisables
- Dépendance de la récupération et actions personnalisées
- Plan de contrôle Commvault accessible sur site sécurisé
- Surveillance, rapport et audit centrés sur la récupération

Bien qu'un plan de reprise après sinistre soit essentiel pour protéger l'infrastructure de votre entreprise, vous ne serez pas totalement protégé à moins que vous n'ayez également en place un plan de reprise après cyberattaque et une stratégie de test. Ceci est crucial pour assurer la sécurité de vos données et de votre réputation face à des attaques malveillantes.

Commvault® + Stordata


© 2024 Commvault

eBOOK

Découvrez comment Commvault peut aider à protéger votre organisation et parlez à votre partenaire pour planifier une démonstration pratique de la récupération Commvault® Cloud Cleanroom™.

commvault.com | 888.746.3849 | get-info@commvault.com

Commvault®

© 2024 Commvault. See here for information about our trademarks and patents. 08_24