eBOOK

COMMENT LA VÉRITABLE CYBER RÉSILIENCE FAIT SES PREUVES SOUS PRESSION





LES CYBERATTAQUES SONT PLUS RAPIDES, PLUS INTELLIGENTES ET PLUS DIFFICILES À DÉTECTER. POUR ÊTRE PRÊT À Y FAIRE FACE, IL VOUS FAUT PLUS QU'UN SIMPLE PLAN: IL VOUS FAUT UNE VÉRITABLE CYBERRÉSILIENCE.

Commvault®

Contents

Préparation ou Véritable Cyberrésilience

Tous les fournisseurs revendiquent la résilience, et la plupart des organisations pensent être prêtes. Pourtant, lorsqu'une véritable cyberattaque survient, les failles des dispositifs de préparation commencent à apparaître.

De nombreuses stratégies de reprise ont été conçues pour faire face à des perturbations prévisibles, et non aux menaces intelligentes et adaptatives de l'IA de nouvelle génération. Les modèles d'IA avancés sont capables de cartographier de manière autonome l'ensemble de la surface d'attaque d'une entreprise en quelques heures, de découvrir des vulnérabilités passées inaperçues pendant des décennies et de permettre aux attaquants d'agir et de s'adapter plus rapidement que n'importe quel cycle de correctifs.

Aujourd'hui, les cyberattaques se propagent plus vite, restent dissimulées plus longtemps et ciblent de plus en plus les systèmes sur lesquels les organisations s'appuient pour restaurer leurs activités. Par conséquent, plusieurs défis deviennent de plus en plus difficiles à relever :

- **Les sauvegardes ne constituent plus une solution de repli garantie :** les attaquants ciblent de plus en plus les systèmes de sauvegarde afin de compromettre les capacités de restauration. Dans certains cas, les données de sauvegarde peuvent être chiffrées, supprimées ou compromises, rendant plus difficile l'identification d'un point de restauration fiable.
- **Les attaquants peuvent rester indétectés pendant longtemps :** les acteurs malveillants peuvent demeurer dans les environnements pendant de longues périodes, se déplacer latéralement et établir des mécanismes de persistance. Il devient alors difficile de déterminer quand l'attaque a commencé et quelles données peuvent être restaurées en toute sécurité.
- **La restauration peut réintroduire des risques :** sans validation appropriée, la restauration des systèmes peut réintroduire involontairement des logiciels malveillants ou des configurations compromises, prolongeant ainsi les conséquences de l'incident.

La préparation suppose que la restauration sera propre, rapide et fiable. Or, la réalité devient de plus en plus complexe. Avec l'IA de nouvelle génération qui accélère le rythme et l'ampleur des attaques, les organisations ont besoin d'une visibilité renforcée et d'une capacité de réponse plus rapide sur l'ensemble de leurs environnements.

92%

des responsables de la sécurité informatique déclarent que les cybermenaces alimentées par l'IA les obligent à renforcer significativement leurs dispositifs de défense. [1]

[1] The State of AI Cybersecurity 2026, Darktrace

La Cyberrésilience Pour Une Nouvelle Réalité

Les cyberattaques ne se contentent plus de perturber les systèmes : elles corrompent les données, compromettent les identités et érodent la confiance. Les attaquants progressent souvent discrètement au sein des environnements, établissant des mécanismes de persistance et se propageant d'un système à l'autre avant même d'être détectés. Lorsqu'un incident est enfin identifié, il est souvent difficile de déterminer quelles données sont restées intactes et lesquelles peuvent être restaurées en toute sécurité.

L'IA de nouvelle génération rend cette réalité encore plus pressante. Les mêmes capacités d'IA qui permettent aux défenseurs de renforcer leur posture de sécurité sont également utilisées pour concevoir et accélérer les attaques à chaque étape de leur cycle de vie, de la reconnaissance jusqu'à l'exploitation des vulnérabilités. À mesure que le délai entre la découverte d'une vulnérabilité et son exploitation continue de se réduire, les organisations doivent adopter des stratégies de cyberrésilience qui vont bien au-delà de la simple application de correctifs.

La nouvelle réalité d'aujourd'hui :

- **L'IA accélère la vitesse et l'ampleur des attaques :** les techniques automatisées permettent aux attaquants d'agir plus rapidement et de s'adapter en temps réel. .
- **Les environnements hybrides et multicloud accroissent la complexité :** les données, les applications et les identités sont réparties entre plusieurs environnements, ce qui complique le maintien de la visibilité et du contrôle pendant les opérations de restauration.
- **La restauration doit s'effectuer sous une pression extrême :** les organisations doivent rétablir rapidement leurs activités, même lorsque l'étendue et les conséquences d'une attaque continuent d'évoluer.

La résilience n'est plus un objectif réservé aux organisations les plus matures : c'est désormais une capacité essentielle pour toutes les entreprises. Pour suivre le rythme de l'IA de nouvelle génération, les organisations ont besoin d'une résilience qui soit :

- **Continue :** toujours testée et opérationnelle
- **Validée :** fondée sur des données fiables et intègres
- **Unifiée :** couvrant les données, les identités et les charges de travail

Sans ces capacités, la restauration devient incertaine, ralentie par la complexité, les risques et le manque de confiance dans le résultat. La véritable cyberrésilience exige une approche plus rigoureuse et opérationnelle afin de garantir une restauration non seulement possible, mais aussi fiable.

Qu'est-Ce Que La Véritable Cyberrésilience ?

Si votre stratégie de restauration ne répond pas aux exigences d'aujourd'hui, ce n'est pas de la véritable cyber résilience.

L'IA exige une nouvelle approche, capable de surveiller en permanence l'état de vos données et de les restaurer instantanément. Commvault Cloud est la seule plateforme unifiée qui combine la protection des charges de travail cloud, sur site et SaaS avec la protection des identités, l'analyse des risques et la cyber restauration, contribuant ainsi à automatiser la cyber résilience et à en faire une capacité opérationnelle.

Commvault®

Voici à quoi ressemble la véritable cyberrésilience :

Une Restauration Saine

Des restaurations qui n'ont pas besoin d'être restaurées.

AVANT

Revenir à un état antérieur à l'attaque... et perdre tout ce qui a été créé ou modifié depuis.

MAINTENANT

Commvault Threat Scan peut aider à identifier les données compromises et à reconstruire une version saine de vos fichiers, réduisant ainsi le risque de réinfection.

Une Restauration Complète

Restaurez des données saines. Restaurez rapidement. Restaurez davantage.

AVANT

Vos données sont restaurées, mais vos applications, vos configurations et votre infrastructure cloud doivent encore être reconstruites de zéro. La restauration des données et la reprise d'activité sont deux choses bien distinctes.

MAINTENANT

Commvault can help recover your business across workloads, clouds and identities – from a single platform designed for the scale of today's attacks.

Une Restauration Rapide

Testez en continu. Restaurez en toute confiance.

AVANT

Tout le monde dispose d'un plan de restauration... que personne ne teste jamais. C'est un pari que vous faites au pire moment possible.

MAINTENANT

Avec Commvault, vous pouvez facilement déployer à la demande un Cleanroom isolé qui vous permet de valider en continu vos capacités de restauration.

Des Plans De Restauration Aux Opérations De Résilience

La restauration traditionnelle se concentre sur des événements isolés. La résilience moderne exige un cycle continu, à mesure que l'IA de nouvelle génération accélère le rythme des cybermenaces.

Les opérations de résilience (ResOps) comprennent :

01 **DÉCOUVRIR**
Comprendre vos données, vos systèmes et vos identités critiques.

02 **PROTÉGER**
Sécuriser et isoler les données grâce à des contrôles robustes.

03 **DÉTECTER**
Identifier les menaces, les anomalies et les ressources compromises.

04 **RESTAURER**
Restaurer des données saines et reconstruire les systèmes.

05 **VALIDER**
Tester en continu votre capacité de restauration.

06 **AMÉLIORER**
Renforcer les processus à partir des enseignements tirés des situations réelles.

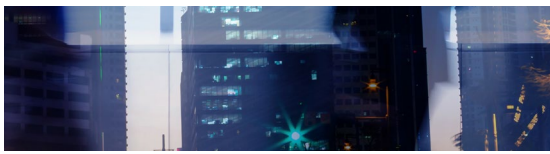
Ce cycle transforme la restauration, qui passe d'un processus réactif à une discipline opérationnelle proactive, conçue pour renforcer la résilience dans un environnement de menaces en constante évolution.

Commencez La Restauration Avec La Viabilité Minimale

Dans un modèle de véritable cyberrésilience, la restauration ne commence pas par tout restaurer : elle commence par restaurer ce qui compte le plus. La viabilité minimale est un concept fondamental de la cyberrésilience qui consiste à donner la priorité à la restauration des systèmes, des données et des processus les plus critiques afin de maintenir les activités essentielles de votre entreprise.

Lorsqu'une attaque survient, la viabilité minimale vous permet de :

- **Donner la priorité aux opérations critiques :** identifiez les systèmes et les données indispensables à la continuité de vos activités afin de concentrer les efforts de restauration là où ils auront le plus d'impact.
- **Restaurer des données fiables et intègres :** concentrez-vous sur la restauration de données validées afin de contribuer à réduire le risque de réinfection et d'éviter de restaurer des systèmes compromis.
- **Reprendre les opérations sous pression :** remettez rapidement en service les fonctions essentielles pendant que les autres opérations de restauration se poursuivent en parallèle.



- **Réduire la complexité pendant la restauration :** limitez le périmètre de la phase initiale de restauration afin d'aider vos équipes à prendre des décisions plus rapides et plus éclairées.

La viabilité minimale n'est pas l'objectif final de la restauration : c'est son point de départ. Elle fournit une approche maîtrisée et pragmatique pour remettre les activités en service tout en préservant la confiance dans vos données.

Pour en savoir plus sur les étapes permettant de restaurer vos activités et découvrir nos bonnes pratiques, consultez **Le Guide Ultime De La Viabilité Minimale**.

Comment Commvault Concrétise La Véritable Cyberrésilience

Commvault vous aide à atteindre une véritable cyber résilience en unifiant la protection, la restauration et la validation à l'échelle de votre environnement.

Commvault® Cloud

Commvault Cloud réunit les données, les applications et les infrastructures réparties entre les environnements cloud, SaaS, hybrides et sur site au sein d'une plateforme unique. Cette approche unifiée contribue à réduire la fragmentation et permet d'assurer une protection et une restauration cohérentes sur l'ensemble de votre patrimoine de données.

Commvault Cloud Threat Scan

La détection des menaces basée sur l'IA permet d'identifier les anomalies et de signaler les données potentiellement compromises dans les environnements de sauvegarde, contribuant ainsi à réduire le risque de réinfection lors de la restauration. En améliorant la visibilité sur les menaces, les équipes peuvent prendre des décisions plus éclairées quant aux données pouvant être restaurées en toute sécurité. Les workflows automatisés coordonnent les actions de réponse et de restauration entre les différents systèmes et applications, réduisant les interventions manuelles et aidant les équipes à restaurer leurs environnements plus efficacement.

Commvault Cleanroom™

Cleanroom fournit un environnement sécurisé et isolé permettant de tester des scénarios de restauration, de valider l'intégrité des données et de réaliser des analyses forensiques. Les organisations peuvent ainsi tester en continu leurs plans de restauration et renforcer leur confiance dans les résultats obtenus en conditions réelles. Cette solution peut également leur permettre **d'augmenter la fréquence des tests de restauration jusqu'à 30 fois**.

Commvault Cloud Rewind™

Cloud Rewind aide les organisations à restaurer des données fiables et intègres, puis à reconstruire rapidement leurs applications après un incident. En orchestrant les processus de restauration, il contribue à réduire les temps d'arrêt et favorise un rétablissement plus rapide des services critiques. Des organisations ont ainsi restauré plus de **800 ressources cloud et plus de 200 To de données en moins de 10 heures**, avec un temps moyen de restauration de quelques minutes par objet.

eBOOK

Testez Votre Résilience Avant Qu'une Attaque Ne Le Fasse

À mesure que les cybermenaces évoluent, la restauration ne consiste plus seulement à remettre les systèmes en service. Il s'agit désormais de restaurer rapidement et en toute confiance des données fiables, même lorsque les sauvegardes et les environnements ont pu être compromis.

La question n'est plus de savoir si vous pouvez restaurer vos systèmes. Elle est de savoir si vous pouvez les restaurer avec des données fiables, rapidement et en toute confiance.

PASSEZ L'ÉVALUATION:

www.commvault.com/cyber-resilience

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

Commvault®