Enterprise Strategy Group

VALIDATION ÉCONOMIQUE

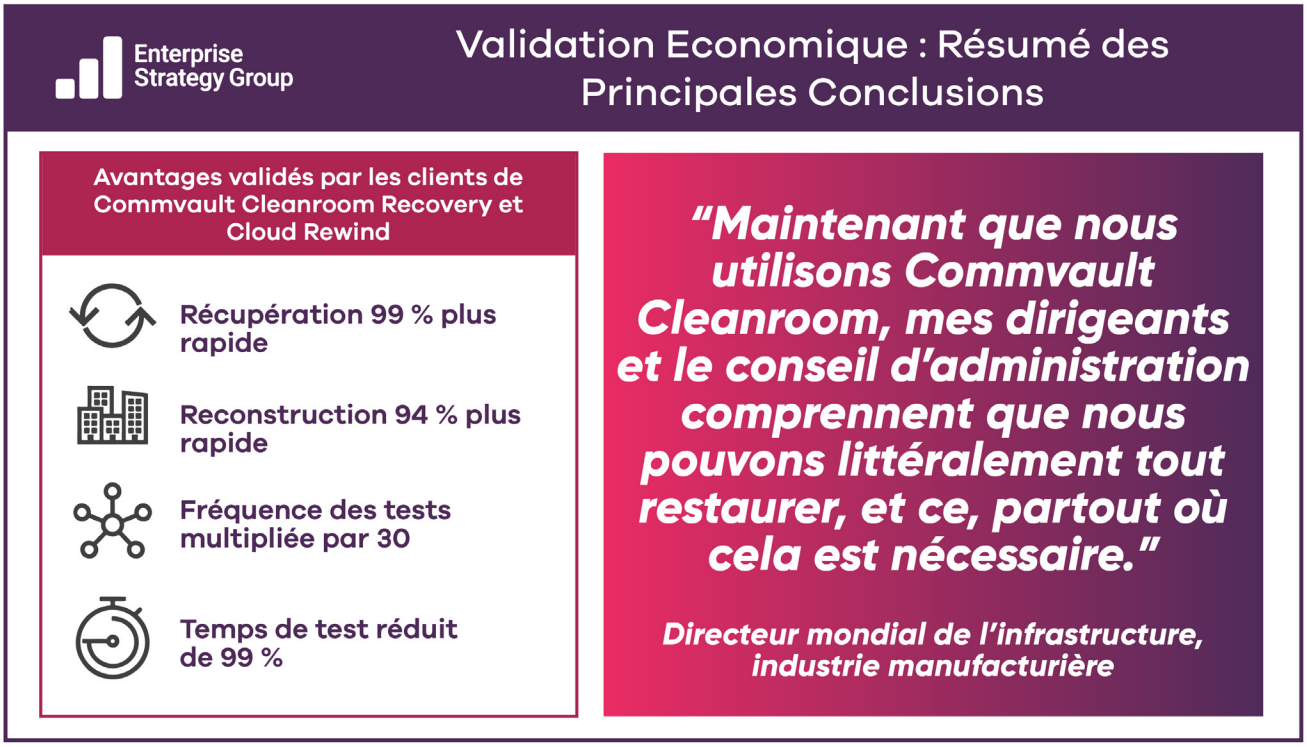
Validation économique : Analyse des avantages économiques de Commvault Cleanroom Recovery et Cloud Rewind

Modernisez votre plan de reprise après cyberattaque et accélérez la récupérabilité

Par Nathan McAfee, Analyste principal, Validation économique
Enterprise Strategy Group
June 2025

Commvault®

Table des matières



Introduction

Cette validation économique réalisée par Enterprise Strategy Group met l'accent sur les avantages quantitatifs et qualitatifs que les organisations peuvent attendre de l'adoption des technologies Commvault Cleanroom Recovery et Cloud Rewind.

Ces solutions, construites sur la plateforme Commvault Cloud, créent des options de récupérabilité qui surpassent la plupart des systèmes de résilience face aux cybermenaces. En complément de l'analyse présentée dans ce document, les avantages abordés peuvent également inclure ceux issus de la validation économique d'Enterprise Strategy Group consacrée à Commvault Cloud. Pour consulter cette étude, cliquez ici.

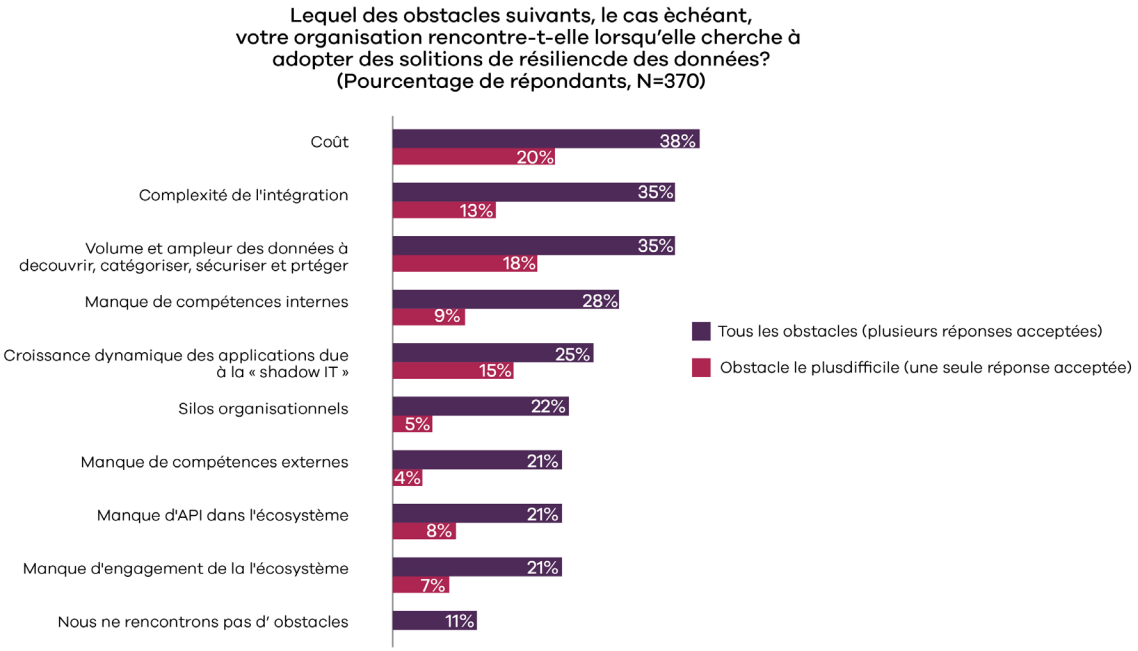
Les clients interrogés dans le cadre de cette analyse exercent dans divers secteurs à l'échelle mondiale, notamment l'énergie, la santé, la fabrication, l'éducation, la technologie, le conseil en informatique, les services financiers, le commerce de détail et l'administration publique. Leur chiffre d'affaires annuel varie de 2,4 milliards à 20,5 milliards de dollars. Bien que chacun des participants ait eu des cas d'usage uniques pour Commvault Cleanroom Recovery et Cloud Rewind, nous avons constaté que les avantages présentés dans notre modèle financier se reproduisent à l'échelle d'organisations de toutes tailles analysées.

Défis

La plupart des professionnels de l'informatique chevronnés connaissent des récits d'incidents de récupération au cours desquels les données n'ont pas pu être restaurées dans un état exploitable. Cela résulte généralement

d'une planification, d'outils, d'une mise en œuvre ou de tests inadéquats, ou encore d'un manque général d'expertise pour naviguer dans la complexité des environnements informatiques hybrides actuels.
Les recherches menées par **Enterprise Strategy Group** ont permis d'identifier les principaux obstacles auxquels les organisations sont confrontées en matière de résilience des données et ont mis en évidence les problèmes suivants (voir la figure 1).[1]

Figure 1. Obstacles à l'adoption de solutions de résilience des données



Source: Enterprise Strategy Group, désormais intégré à Omdia

Dans le cadre de notre analyse, nous avons interrogé des clients de **Commvault Cleanroom** et **Cloud Rewind** afin de comprendre certains des défis spécifiques auxquels ils étaient confrontés dans leurs précédentes méthodologies et solutions de résilience cyber. Ces défis se sont révélés constants dans la majorité des entretiens :

- **Capacité à restaurer complètement et de manière cohérente.** La possibilité de sauvegarder des données ne représente que la moitié du travail; la capacité à restaurer efficacement les données et l'infrastructure associée est ce qui minimise l'impact d'une perte et d'un événement de récupération. Les recherches d'Enterprise Strategy Group ont montré que seulement 11 % des répondants déclaraient que leur organisation était capable de restaurer l'intégralité de ses données de façon régulière.[2]

- **Récupérabilité de l'état de la plateforme.** De nombreuses organisations élaborent leurs plans de reprise autour de la possibilité de restaurer les données. Bien que cela soit important, ce n'est qu'une partie de la solution.

[1] Source: Enterprise Strategy Group Research Report, Achieving Cyber and Data Resilience: The Intersection of Data Security Posture Management With Data Protection and Governance, September 2024.

[2] Source: Enterprise Strategy Group Research Report, Cloud Data Protection Strategies at a Crossroads, August 2023.

Les organisations doivent également être capables de recréer rapidement l'écosystème complet, y compris les applications, les pilotes, les réseaux et les connexions, avant même que la restauration des données ne soit possible. En outre, lors de la recréation de l'infrastructure sous-jacente, les interdépendances exigent que les composants soient recréés dans un ordre précis et séquentiel.

- **Complexité et coût des tests de récupérabilité.** Les plans de reprise ne sont que rarement testés de manière complète avant qu'un véritable incident de récupération ne se produise. Les entretiens menés avec des clients ont révélé que peu d'entreprises réalisent des tests de récupérabilité complets ; beaucoup construisent leur stratégie autour de tests annuels qui ne couvrent qu'une petite partie de leurs systèmes critiques. Ces décisions découlent du coût et de la complexité qu'implique la réalisation de tests exhaustifs de récupération complète, laissant ainsi les organisations exposées à un niveau élevé de risque auto-infligé et à une vulnérabilité potentielle.

- **Incapacité à annuler les changements indésirables de récupération.** Revenir en arrière après une modification, ou même après un événement de récupération inefficace, est difficile, voire impossible, pour la plupart des organisations. Ces retours en arrière peuvent être extrêmement perturbateurs et entraînent trop souvent une perte de données ainsi qu'un temps d'arrêt non planifié.

- **Capacité à vérifier et à assainir les données avant la restauration.** Un problème majeur lors de la récupération après une attaque par ransomware consiste à pouvoir vérifier que les données sont saines avant leur restauration. Les environnements de test traditionnels rendent cette tâche complexe, incertaine et souvent impossible.

- **Récupérabilité dans des environnements isolés.** A De nombreuses organisations se trouvent limitées à une restauration dans le même environnement que celui où la sauvegarde a été effectuée, ou dans un autre environnement qui ne peut pas être certifié comme totalement exempt de toute infection potentielle. Lors d'un scénario de récupération cyber, cet environnement peut être endommagé ou indisponible. Dans une situation de récupération après une attaque par ransomware, les organisations doivent pouvoir restaurer leurs données dans un environnement isolé et à la demande, afin de garantir qu'elles sont propres et exemptes de réinfection. Bien que la plupart des organisations considèrent la reprise après sinistre (Disaster Recovery – DR) et la récupération cyber (Cyber Recovery – CR) comme un seul et même processus, elles échouent souvent lors d'un véritable incident cyber, ce qui peut entraîner des conséquences majeures sur la carrière des responsables lorsque le rançsomware frappe.

- **Plans dédiés à un paysage de menaces différent.** The La différence fondamentale entre la DR et la CR réside dans la reconnaissance de menaces distinctes. Les plans de DR traditionnels ne prennent pas toujours suffisamment en compte la complexité d'une cyberattaque, en particulier d'une attaque par rançongiciel. La CR nécessite donc des plans spécifiques, axés sur la récupération dans un environnement isolé et vérifiable comme propre.

- **Manque d'intégration entre les écosystèmes de résilience des données et de sécurité.** Enterprise Les entreprises que nous avons étudiées s'appuyaient

sur une collection d'outils, souvent plus de 15 solutions différentes pour la DR et la résilience cyber. Le manque d'API de qualité et d'interopérabilité conduit à la nécessité d'utiliser plusieurs outils et engendre un niveau élevé de dette technique.

- **L'auditabilité et la vérification des plans de récupération cyber.** Enterprise Strategy Group a constaté que l'auditabilité des tests et des plans de récupération constituait un défi pour les organisations que nous avons étudiées. Ces plans sont essentiels pour la haute direction, y compris les conseils d'administration ; ils sont exigés par certains organismes de conformité et de régulation, nécessaires pour conclure des affaires avec de nombreux clients, et même utiles pour réduire le coût des assurances cyber.

L'importance du retour à la viabilité minimale après une cyberattaque

L'impact d'une interruption d'activité peut être dévastateur, et la capacité de revenir rapidement à un état opérationnel viable après une attaque ou une panne est essentielle. La viabilité minimale correspond à la capacité de restaurer rapidement et proprement les capacités minimales (applications, actifs, processus, personnes) nécessaires au bon fonctionnement d'une organisation après une attaque. Il s'agit d'un élément clé de la continuité des activités. Une organisation doit avoir confiance en sa capacité à revenir rapidement à un état de viabilité minimale afin de minimiser les perturbations pour l'entreprise, tout en disposant d'un plan clair et bien défini pour assurer ultérieurement une récupération complète et une résilience renforcée.

La solution : Commvault Cleanroom Recovery et Cloud Rewind

Pour renforcer la résilience cyber et accélérer la reprise après sinistre (Disaster Recovery – DR) à la suite d'un incident de sécurité ou d'une attaque par ransomware Commvault propose Cleanroom Recovery. Cet environnement cloud automatisé, isolé et sécurisé permet aux organisations de valider leurs stratégies de récupération et d'enquêter sur les menaces à l'aide d'analyses forensiques. Il leur permet également de restaurer rapidement leurs environnements opérationnels, assurant ainsi la continuité des activités en cas d'interruption imprévue, de catastrophe, d'attaque par rançongiciel ou d'autres menaces.

Les capacités offertes par Commvault Cleanroom comprennent :

- **Élaborer un plan de récupération cyber efficace**

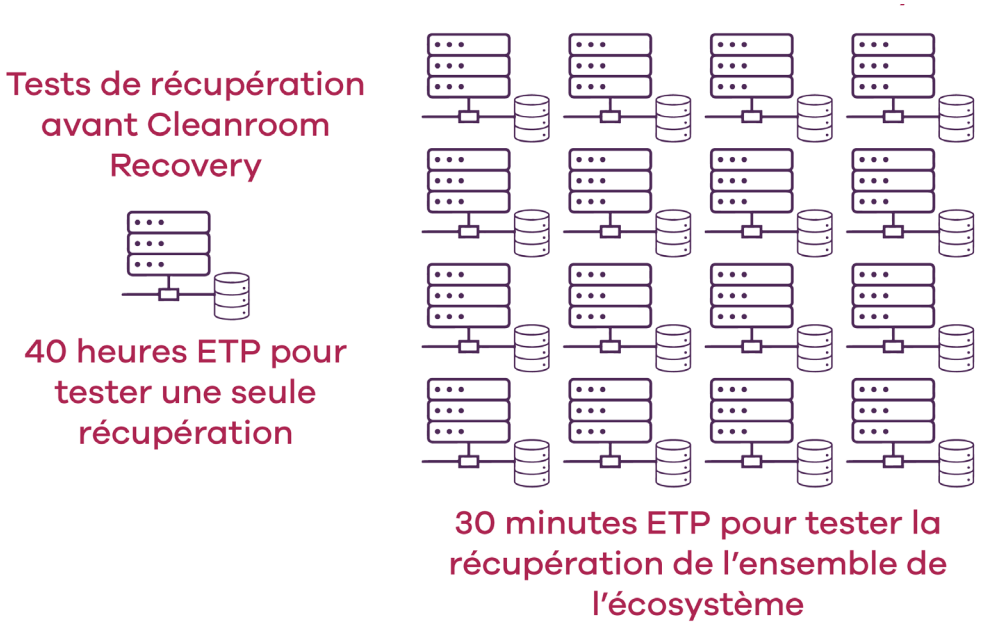
Trop souvent, les organisations réalisent leurs tests de récupérabilité à l'aide d'une simple liste de contrôle. Elles testent une partie du processus de récupération, puis la suivante, jusqu'à ce que toutes les cases soient cochées. Ce type de plan s'effondre rapidement dans le chaos d'un véritable événement de récupération, laissant l'organisation mal préparée à restaurer ses systèmes et à garantir la continuité de ses activités. De nombreux clients que nous avons interrogés ont accordé une grande importance à leur participation à la fois à l'événement immersif expérientiel de Commvault "Minutes-to-Meltdown", qui recrée le chaos d'une véritable cyberattaque, et aux programmes de certification en résilience cyber de Commvault, les considérant comme essentiels à la préparation de leurs équipes face aux cyberattaques et à leur niveau de récupérabilité.

- **Isolement basé sur le cloud.** A Cleanroom Recovery fonctionne dans des environnements cloud isolés tels qu'Azure et est conçu pour fonctionner conjointement avec Commvault Airgap Protect. Airgap Protect fournit des copies immuables et indélébiles des données protégées, tandis que Cleanroom Recovery offre un environnement totalement stérile et isolé, avec des contrôles d'accès à confiance zéro, un déploiement rapide et une mise à l'échelle illimitée selon les besoins.

  Airgap Protect aide les organisations à atténuer les risques liés aux rançongiciels, à maintenir la conformité des données et à soutenir la préparation à la récupération en cas d'incident cyber ou de perte de données.

- **Tests de récupérabilité.** Cleanroom Recovery facilite les tests de récupérabilité à l'échelle et à la fréquence les plus adaptées au modèle économique de l'entreprise. De plus, Commvault propose des formations à la récupérabilité qui reproduisent le chaos d'un véritable événement de récupération et développent les connaissances et l'expérience nécessaires à l'élaboration et à l'exécution d'un plan de récupération cyber (CR) efficace. Comme le montre la figure 2, les entreprises que nous avons analysées ont indiqué ne réaliser des tests de récupérabilité que sur un seul serveur ou une seule charge de travail par mois, chaque test nécessitant en moyenne 40 heures de travail en équivalent temps plein (ETP). Les tests effectués à l'aide de Commvault Cleanroom Recovery peuvent réduire considérablement le temps requis pour la réalisation de ces essais. Alors que la mise en place d'un environnement Cleanroom peut prendre aussi peu que 30 minutes, la durée totale d'un test de récupération dépend de la portée et de la complexité des systèmes et des données à restaurer. Cependant, cette solution offre la possibilité d'inclure des tests de récupérabilité pour l'ensemble de l'écosystème, dans un délai considérablement réduit par rapport aux méthodes traditionnelles, qui prennent souvent des jours ou des semaines et mobilisent un nombre important d'heures de travail en ETP. Dans le cadre de cette analyse, nous avons constaté que les tests de résilience réalisés avec Commvault Cleanroom Recovery peuvent réduire l'exposition au risque de 97 %, tout en améliorant significativement la capacité de récupération.

Figure 2. The Impact of Increasing Recovery Testing With Cleanroom Recovery



Source: Enterprise Strategy Group, désormais intégré à Omdia

- **Déploiement rapide.** Un environnement Cleanroom peut être créé et alimenté en quelques minutes. Cela réduit le temps nécessaire pour atteindre la viabilité minimale et permet aux entreprises de restaurer rapidement leurs activités principales lorsqu'une cyberattaque survient, assurant ainsi la continuité des opérations.

- **Analyse forensique.** Cleanroom Recovery fournit un environnement sécurisé et isolé pour l'analyse forensique des systèmes infectés, afin d'identifier la cause première d'une attaque. Cleanroom Recovery peut également isoler un environnement infecté afin d'explorer et de comprendre en toute sécurité l'étendue et le déroulement de l'infection, offrant ainsi des informations précieuses pour améliorer la prévention et la préparation face aux futures cyberattaques.

- **Récupération pilotée par l'IA.** Commvault utilise des rapports et une automatisation pilotés par l'intelligence artificielle tout au long du processus de récupération. Cela permet d'identifier le dernier point de récupération sain connu et de reconstruire l'ensemble de l'écosystème en ajoutant les dépendances dans l'ordre nécessaire.

- **Audit et rapports clairs et détaillés.** Commvault offre des capacités étendues de génération de rapports, utilisées pour des activités telles que les audits, les certifications d'assurance cyber et la réduction des primes d'assurance, ainsi que pour la conformité aux lois et réglementations locales et mondiales. Selon de nombreux clients interrogés, ces rapports détaillés répondent également aux exigences des conseils d'administration en matière de preuve de préparation aux cyberattaques.

Commvault Cloud Rewind offre des capacités de récupération et de reconstruction d'applications adaptées aux applications et infrastructures basées sur le cloud. Il est conçu pour aider les organisations à se remettre rapidement d'attaques cyber, de pannes ou de catastrophes, et leur permet de prioriser les éléments nécessaires pour maintenir la continuité des activités (c'est-à-dire la viabilité minimale).

Commvault Cloud Rewind offre les fonctionnalités suivantes

- **Récupération rapide des applications et des environnements cloud.** Cloud Rewind peut créer automatiquement une machine à remonter le temps pour les environnements applicatifs, permettant à une organisation de revenir en arrière dans le temps en restaurant les applications et l'infrastructure, ainsi que les éléments essentiels de l'environnement, jusqu'au point précédant une cyberattaque dommageable.

- **Découverte des configurations cloud.** Cloud Rewind détecte en continu les configurations des services cloud afin de cartographier les dépendances et de s'adapter à l'architecture et aux services cloud spécifiques d'une organisation.

- **Réduction du risque lié aux erreurs de configuration cloud.** L'automatisation et l'orchestration de Cloud Rewind réduisent le risque d'échec des applications grâce à des chemins et des processus de récupération prévisibles, tout en limitant le risque d'erreur humaine.

- **Résilience cyber continue.** Les clouds hyperscale nécessitent une résilience cloud hyperscale. Cloud Rewind prend en charge la récupération et la reconstruction instantanées à la fois dans la même zone et entre différentes zones, régions et comptes, offrant ainsi une flexibilité optimale pour une reprise rapide et des opérations commerciales ininterrompues.

- **Machine à remonter le temps cloud à double coffre brevetée.** Cloud Rewind utilise des coffres sécurisés et immuables pour la récupération instantanée des applications. Des coffres séparés sont utilisés pour la configuration cloud et pour les données applicatives, permettant ainsi des récupérations plus rapides et des opérations continues.

Validation économique par Enterprise Strategy Group

Enterprise Strategy Group a réalisé une analyse économique quantitative afin de comprendre comment Commvault Cleanroom Recovery et Cloud Rewind peuvent aider une organisation à atteindre ses objectifs informatiques et commerciaux. Notre processus de validation économique est une méthode éprouvée permettant de comprendre, de valider, de quantifier et de modéliser les propositions de valeur économiques d'un produit ou d'une solution. Ce processus s'appuie sur les compétences clés d'Enterprise Strategy Group en matière d'analyse de marché et de secteur, de recherche prospective et de validation technique et économique. Nous avons mené des entretiens approfondis avec des clients de Commvault afin de comprendre comment la transition vers Cleanroom Recovery et Cloud Rewind a affecté leurs organisations, en particulier leurs tests de récupération et leur capacité globale de restaurabilité en cas d'attaque cyber ou de rançongiciel, ainsi que face à d'autres menaces potentielles.

Les conclusions qualitatives et quantitatives ont servi de base à un modèle économique simple comparant les coûts et avantages attendus d'une amélioration de la récupérabilité grâce à Cleanroom et Cloud Rewind. Les organisations interrogées représentent un large éventail de secteurs à l'échelle mondiale, notamment l'énergie, la santé, la fabrication, les équipements industriels, le biomédical, l'éducation, la technologie, le conseil en informatique, les services financiers, le commerce de détail et le secteur public, avec des revenus annuels compris entre 2,4 et 20,5 milliards de dollars.

Analyse économique de Commvault Cleanroom et Cloud Rewind

L'analyse économique d'Enterprise Strategy Group a révélé que les organisations utilisant Commvault Cleanroom Recovery et Cloud Rewind comme base de leur stratégie de tests et de récupérabilité devraient bénéficier des avantages suivants :

- **Amélioration de la continuité des activités.** Une récupération rapide, propre et complète constitue la pierre angulaire d'une stratégie de continuité des activités efficace. Enterprise Strategy Group a constaté que les entreprises utilisant Commvault Cleanroom Recovery et Cloud Rewind ont une probabilité nettement plus élevée d'obtenir une récupérabilité complète.

- **Réduction des coûts de récupération et de test.** Nous avons constaté que le coût des tests de récupérabilité diminuait considérablement lors du passage à Cleanroom Recovery.

- **Réduction de la complexité et de la dette technique.** Cleanroom Recovery et Cloud Rewind font partie de Commvault Cloud, une plateforme complète de protection des données et de résilience cyber conçue pour les environnements hybrides modernes. Le passage à une solution simplifiée et hautement intégrée permet d'éliminer des décennies de dette technique et de réduire le nombre de collaborateurs, ainsi que le niveau de compétences requis, pour gérer et faire évoluer la solution Commvault.

Amélioration de la continuité des activités

La résilience des données constitue la priorité informatique numéro un pour plus d'un tiers (36 %) des organisations et figure parmi les cinq principales priorités pour 88 % d'entre elles. Les entretiens menés par Enterprise Strategy Group ont révélé que la plupart des organisations éprouvent des difficultés à élaborer, concevoir et tester des plans efficaces de résilience et de récupération cyber. Nous avons constaté que Commvault Cleanroom Recovery et Cloud Rewind constituent les éléments essentiels d'un plan de continuité des activités au niveau de l'entreprise, pour de nombreuses raisons, notamment :

« Avant d'adopter Commvault Cleanroom Recovery, nous effectuions des tests de récupérabilité une fois par an sur l'une de nos fermes de serveurs. Nous étions contraints de supposer que la récupération d'un serveur signifiait que nous pouvions tous les récupérer. Aujourd'hui, avec Cleanroom, nous réalisons des tests de récupérabilité mensuels sur l'ensemble de nos actifs critiques et nous savons que nous pouvons restaurer rapidement nos systèmes en cas de cyberattaque. »

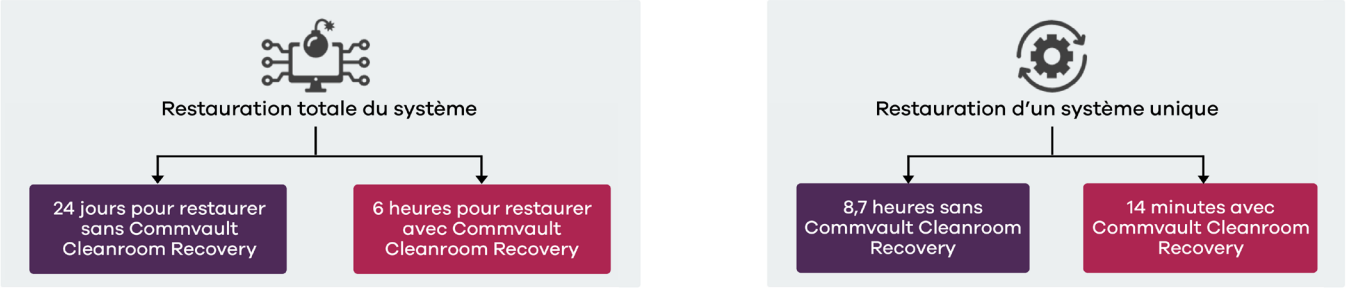
– Director, Global IT, Services and Solutions Provider

- **Activation des tests de récupérabilité.** Bien que la plupart des organisations aient indiqué que la résilience des données était une priorité absolue, seules quelques-unes de celles que nous avons interrogées pour cette analyse disposaient de plans de test antérieurs à Cleanroom Recovery qui soient complets, fréquents et fiables. Nous avons constaté que Cleanroom Recovery offre la flexibilité et la facilité d'utilisation nécessaires pour permettre tout niveau de test de récupérabilité adapté aux besoins d'une entreprise. Un environnement peut être déployé rapidement, et l'intelligence artificielle Metallic de Commvault automatise une grande partie des tests sans perturber les systèmes de production. Les utilisateurs peuvent adapter les séquences de récupération pour restaurer les données selon un ordre logique et prioritaire, et les réseaux, le stockage et les applications peuvent être restaurés afin de tester un scénario complet de récupération cyber à l'aide de Cloud Rewind.

- **Facilitation d'une récupération quasi instantanée.** Avec Cleanroom Recovery, un environnement de récupération peut être déployé en quelques minutes, accélérant ainsi l'ensemble du processus de restauration. Nous avons constaté que la récupération prenait en moyenne 8,7 heures avant Cleanroom Recovery,

certains exemples nécessitant plusieurs fois ce délai. Comme le montre la figure 3, le directeur informatique d'un système universitaire a déclaré : **« Il fallait auparavant 24 à 36 heures pour restaurer une seule instance de serveur et jusqu'à 24 jours pour se remettre d'un incident cyber. Nous pouvons désormais tout restaurer en moins d'une heure. »**

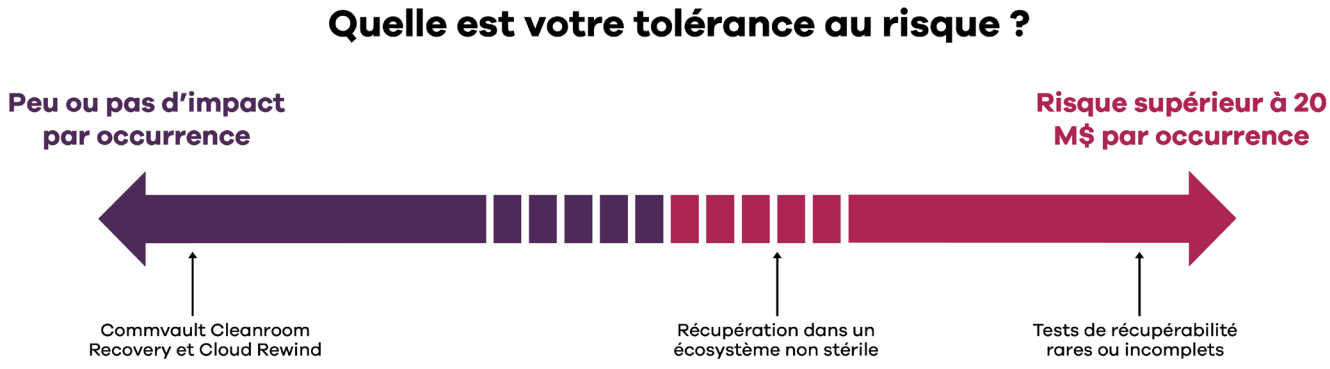
Figure 3. Avantages en matière de temps de récupérabilité



Source: Enterprise Strategy Group, désormais intégré à Omdia

Un autre exemple que nous avons étudié est celui d'une entreprise de fabrication d'équipements énergétiques qui effectue chaque soir des tests complets de récupération. Cela permet à cette organisation de disposer immédiatement d'un environnement prêt à être utilisé en cas de défaillance. Le directeur mondial de l'infrastructure de ce fabricant d'équipements énergétiques a expliqué : **« Chaque matin, je me réveille, je consulte mon rapport Cleanroom Recovery concernant la restauration effectuée la nuit précédente, et je sais que nous sommes protégés et capables de récupérer. Les interruptions d'activité sont coûteuses dans notre secteur, tant sur le plan financier qu'en matière de satisfaction client. Nous avons éliminé les temps d'arrêt en étant toujours capables de nous remettre des incidents cyber. »** Compte tenu du fait que les clients interrogés ont estimé le coût d'un incident cyber à 20 millions de dollars et que des exemples récents dans l'actualité dépassent les 100 millions de dollars, sans compter l'impact négatif incommensurable sur leur réputation, les entreprises doivent évaluer leur tolérance au risque et s'assurer que leur stratégie de résilience correspond à ce niveau de tolérance (voir figure 4).

Figure 4. Understanding the Correlation Between Resilience Strategy and Risk



Source: Enterprise Strategy Group, désormais intégré à Omdia

- **Amélioration de la récupérabilité.** Une vérité fondamentale en matière de résilience des données est que si les données et l'infrastructure critiques ne peuvent pas être restaurées, elles ne devraient jamais être sauvegardées. En étudiant la situation des participants à notre analyse avant l'adoption de Commvault Cleanroom Recovery, nous avons constaté un trop grand nombre d'exemples où il n'existait aucune certitude de récupérabilité. Le directeur de l'infrastructure informatique d'un conglomérat industriel mondial a bien résumé cette réalité : **« Avec Cleanroom, je peux garantir absolument que ma dernière sauvegarde est récupérable. Par le passé, ce n'était qu'une question d'espoir et de théorie. »**

- **Passage d'une expertise réactive à une approche proactive.** Les capacités d'intelligence artificielle de Cleanroom Recovery ont souvent été décrites comme une innovation déterminante pour trois raisons principales : la rapidité et la complétude de la récupération, la capacité à isoler et à identifier la cause des défaillances, et la manière dont le personnel informatique peut libérer du temps pour adopter une réflexion plus proactive en tirant parti des outils d'automatisation et d'orchestration Metallic AI de Commvault, qui représentent un complément significatif à leurs équipes informatiques. Le directeur de l'ingénierie des solutions informatiques d'un réseau hospitalier a déclaré : **« Depuis notre passage à Cleanroom Recovery et Cloud Rewind, j'ai pu réaffecter certains de mes meilleurs collaborateurs à des travaux tournés vers l'avenir, qui nous permettent de résoudre des problèmes ayant un impact sur nos médecins et nos patients. Grâce à cette évolution, notre personnel est plus heureux et collabore mieux, ce qui conduit à une amélioration des soins aux patients et à une satisfaction et une fidélisation accrues de nos clients. »**

- **Enquête en environnement isolé.** When Lorsqu'une intrusion ou une infection se produit, le processus d'enquête peut durer des mois, voire plus longtemps, afin de comprendre comment le problème est entré dans l'écosystème informatique et comment il s'est propagé. De plus, plus d'un tiers des organisations victimes d'une attaque par rançongiciel réussie ont subi une nouvelle attaque dans les douze mois suivants. Lorsque nous avons demandé aux personnes interrogées pourquoi elles pensaient que ces réattaques se produisaient, elles ont mentionné la complexité liée à l'identification et à la correction de tous les aspects d'une violation ou d'une infection avant la restauration. Un expert en sécurité et en récupération d'une entreprise spécialisée dans la résilience cyber a résumé la situation ainsi : **« Si nous ne pouvons pas faire confiance à l'intégrité des données lors d'un événement de récupération, nous ne pouvons pas les restaurer dans notre environnement de production. Avec Cleanroom Recovery, nous pouvons isoler l'environnement restauré et faire fonctionner notre entreprise minimale viable à partir de celui-ci. Cela nous permet de poursuivre nos activités dans un environnement protégé et isolé. »** D'autres personnes interrogées ont évoqué la nécessité de conserver la disponibilité d'un environnement infecté à des fins d'assurance. Un vice- président de l'infrastructure d'une société de services mondiale a expliqué : **« Cleanroom nous permet de laisser notre environnement infecté dans une instance véritablement protégée, où nous pouvons l'examiner et comprendre comment il s'est propagé. Cela nous permet également de répondre aux exigences d'assurance et de conformité tout en restaurant la viabilité minimale ailleurs, ramenant ainsi l'entreprise à un fonctionnement normal (ou à la viabilité minimale) sans interruption. »**

« Nous rencontrons Commvault chaque trimestre pour examiner nos plans de récupérabilité et partager les meilleures pratiques. Aucun de nos autres fournisseurs informatiques ne fait cela. Nous travaillons avec plus de 100 fournisseurs ; Commvault est incontestablement au premier rang en ce qui concerne la façon dont ils nous traitent comme de véritables partenaires. »

– Directeur informatique, système universitaire

- **Assistance à la préparation fournie par Commvault.** La qualité des programmes de formation et d'apprentissage proposés par Commvault à ses clients s'est distinguée lorsque nous avons examiné la combinaison de technologie et d'expertise qu'offre l'entreprise. Nous avons entendu : **« Là où Commvault excelle vraiment, c'est en nous aidant à tester la récupérabilité dans un état de chaos. Nous avions l'habitude de suivre une liste de contrôle et de dire que tout allait bien. Cependant, lors d'un véritable incident cyber, les choses ne se déroulent pas de manière ordonnée. Commvault nous aide à reproduire efficacement ce chaos et à planifier l'imprévisible. »** Cela est rendu possible grâce à des initiatives telles que Minutes-to-Meltdown de Commvault, une session approfondie dirigée par des experts de Commvault visant à aider les participants à comprendre les attaques par rançongiciel modernes. Cet événement hautement immersif implique la participation active des participants dans les rôles de RSSI, DSI et autres, afin d'élaborer un plan pour améliorer la préparation cyber. Commvault Recovery Range est un laboratoire pratique simulant de véritables cyberattaques, axé sur la réussite des récupérations. Les participants se livrent une course contre la montre pour sauver une grande entreprise en situation d'attaque. Des programmes complets de certification en résilience cyber sont également proposés par Commvault à ses clients.

- **Élimination de la complexité lors d'un événement de récupération.** La récupération va bien au-delà de la simple restauration de données. Plusieurs systèmes doivent être remis en service dans un ordre précis afin de respecter les dépendances. Un responsable informatique d'une entreprise mondiale de solutions de sauvegarde a expliqué : **« Notre matrice de récupération comporte plus de vingt niveaux distincts de remise en service des services dans le bon ordre. Avec Cleanroom Recovery, nous automatisons ce processus exactement dans le bon ordre pour garantir le succès. »**

- **Flexibilité des options de récupération.** La récupération après une véritable cyberattaque peut nécessiter la réparation ou la reconstruction de l'infrastructure sous-jacente, voire des sites physiques. Commvault Cleanroom Recovery et Cloud Rewind peuvent créer un environnement de récupération en quelques minutes, totalement indépendant du matériel ou de l'emplacement.

- **Amélioration de la satisfaction client et accélération de la croissance de l'entreprise.** Lorsque nous avons interrogé les participants sur l'impact commercial des tests de récupérabilité, ils ont partagé de nombreux témoignages sur la façon dont leurs clients percevaient leurs capacités améliorées. Un vice-président des services cloud a expliqué : **« Lorsque je dis à mes clients que nous pouvons tester la restaurabilité chaque mois au lieu d'une fois par an, ils nous accordent un niveau de confiance plus élevé pour faire affaire avec nous. Ce faisant, nous offrons un niveau de service que nos concurrents ne peuvent pas ou ne veulent pas égaler. »** Ils ont également

expliqué qu'ils avaient pu vendre davantage de services cloud précisément grâce à leur adoption de Cleanroom Recovery : **« Nous fidélisons mieux nos clients et en gagnons de nouveaux, car nous pouvons démontrer notre engagement en faveur de la préparation à la récupération cyber. Nos revenus ont augmenté de 3,5 % directement grâce à cette adoption de Commvault Cleanroom Recovery. »**

Réduction des coûts de récupération et de tess

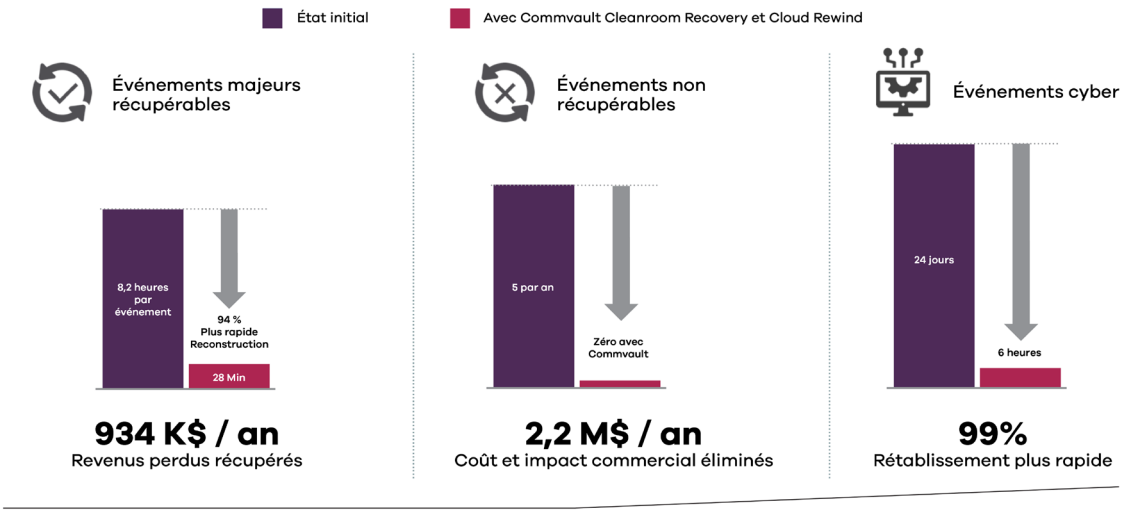
« Passer à Commvault Cleanroom Recovery ne représente pas seulement une économie de coûts. Le niveau d'expertise nécessaire pour réellement créer un environnement de récupération propre dépasse nos compétences. » Switching to Commvault Cleanroom Recovery is not just a cost savings. The level of expertise it would take to truly create a clean recovery environment is beyond our skillset. »

– Director of IT Solutions Engineering, Global Cloud Services

Comparer les coûts avant et après la migration vers Commvault Cloud pour les tests de récupération s'avère complexe en raison des différences considérables dans la manière dont les organisations effectuent leurs tests après l'adoption de Commvault. Les entreprises que nous avons étudiées sont passées de tests effectués chaque année sur une petite partie de leur écosystème à des tests mensuels couvrant l'ensemble de leurs plateformes de données, de stockage et d'applications, y compris une organisation qui réalise des tests complets de récupérabilité chaque nuit afin de réduire l'impact potentiel des interruptions d'activité. Bien qu'il existe des variations entre ces exemples, nous avons constaté que les avantages suivants étaient constants parmi toutes les organisations que nous avons étudiées :

- **Réduction de l'impact des interruptions d'activité.** En examinant les avantages d'une amélioration des capacités de récupération, la première mesure que la plupart des organisations ont mentionnée est la variation du temps d'arrêt en fonction de l'accélération du processus de restauration. Nous avons constaté que Commvault Cloud Rewind peut réduire le nombre d'incidents de récupération mineurs par an et diminuer l'impact de chaque événement. Pour les incidents majeurs, aucun des interlocuteurs n'a déclaré que leur situation précédente pouvait être comparée à l'état complet de récupération que fournit Commvault Cleanroom Recovery. Nous avons supposé que les états restaurés étaient équivalents dans nos mesures portant sur l'impact de différents scénarios de récupération pour notre entreprise modèle (voir figure 5).

Figure 5. Avant et après Commvault Cleanroom Recovery et Cloud Rewind



De plus, l'impact commercial d'un événement cyber peut se chiffrer en millions.

Source: Enterprise Strategy Group, désormais intégré à Omdia

« Nous bénéficions de réductions sur notre assurance cyber grâce aux améliorations qu'apporte Cleanroom Recovery. Commvault rend la documentation détaillée de notre plan extrêmement simple. Cela nous permet d'économiser plus de 100 000 dollars par an. »

– Global Infrastructure Director, Industrial Manufacturing

- **Suppression des obstacles financiers aux tests.** Les organisations que nous avons interrogées ont donné de nombreuses raisons expliquant pourquoi leurs plans de tests de récupérabilité ne correspondaient pas à leurs objectifs de résilience cyber. La première raison était le coût en temps des employés à temps plein (ETP) pour effectuer les tests, et la seconde, le coût et la complexité liés à la création et à la maintenance d'un environnement de test. Nous avons étudié des exemples fournis par des clients qui avaient dépensé jusqu'à 20 millions de dollars pour tenter de créer un environnement similaire à Cleanroom Recovery, avec des résultats moins efficaces que ceux que Cleanroom Recovery a démontré être capable d'apporter. D'autres ont tenté de créer des environnements de récupération basés sur le cloud, mais ont constaté que leur vitesse était insuffisante et que les résultats étaient inférieurs aux attentes. Le directeur informatique d'un système universitaire a déclaré : **« Cleanroom est 60 % moins cher que l'utilisation d'environnements de récupération basés sur des machines virtuelles, et nous pouvons atteindre la viabilité minimale directement à partir d'un Cleanroom. Il n'y a aucun moyen que nous puissions facilement faire fonctionner notre entreprise minimale viable à partir d'une récupération sur machine virtuelle. »**

- **Réduction des coûts en ETP pour la planification et les tests de récupération.** Le coût moyen des tests pour les entreprises que nous avons étudiées comprenait des tests mensuels mobilisant cinq employés à temps plein pendant un total de 40 heures, soit une dépense annuelle de 141 864 dollars. En

passant à Cleanroom, ces coûts sont tombés à moins de 11 000 dollars par an. Cependant, nos recherches ont montré que le nombre de tests est passé de 12 par an à 365 par an, avec une seule personne consacrant une demi- heure à chaque test.

- **Impact des conseils et des bonnes pratiques fournis par l'IA.** Comme l'a expliqué le directeur informatique d'une société de services cloud : **« Tout ce que je peux automatiser dans mon processus de test et de récupération me fait gagner du temps et de l'argent et augmente les chances de réussite lorsqu'une cyberattaque se produit et qu'une récupération propre est nécessaire. L'IA de Commvault identifie en permanence des améliorations et des bonnes pratiques pour perfectionner nos plans de récupération cyber et réduire nos coûts. »**

- **Diminution des coûts d'assurance cyber et d'assurance commerciale.** Les personnes interrogées ont indiqué que l'assurance cyber et l'assurance commerciale étaient plus faciles à obtenir et à moindre coût, précisément grâce à leur investissement dans Commvault et à leur capacité à présenter des plans détaillés de tests et de récupération, ainsi que les rapports détaillés requis pour les audits de conformité et de réglementation.

« Nous faisons confiance à Commvault et à Microsoft et apprécions leur partenariat. Nous savons que notre solution Commvault Cloud est complète et sécurisée, et la flexibilité offerte par son intégration à Azure nous permet de nous concentrer sur notre activité. »

– Director of IT, University System

- **Réduction de la dette technique.** En examinant la situation des clients avant l'adoption de Cleanroom Recovery, nous avons constaté une opposition totale entre leurs besoins en matière de résilience cyber et leurs capacités réelles. Nous avons observé des plans fragmentés, incomplets, non testés et dont les coûts ne correspondaient pas aux bénéfices. Nous avons également vu des décisions prises sous contrainte ou imposées par des choix passés. Avec Cleanroom Recovery et Cloud Rewind, ces mêmes clients peuvent désormais aligner la fréquence et la complétude de leurs tests sur leurs objectifs de résilience cyber et planifier la récupération dans l'environnement le plus adapté à la situation rencontrée. Cela permet à ces clients de retrouver rapidement un état de viabilité minimale, garantissant la poursuite des opérations sans risque de perte d'activité ni atteinte à leur réputation et à la valeur de leur marque.

Réduction de la complexité et de la dette technique

Commvault Cleanroom et Cloud Rewind reposent sur la plateforme de données Commvault Cloud Data Platform. Enterprise Strategy Group a mené ici une analyse économique complète sur les avantages de Commvault Cloud et a constaté que ces avantages étaient également réalisés par les autres clients interrogés dans le cadre de cette étude :

- **Efficacité des coûts.** Commvault Cloud peut réduire les coûts et offrir une structure de coûts beaucoup plus prévisible par rapport à d'autres environnements. Commvault constitue une pierre angulaire sur laquelle les entreprises peuvent s'appuyer pour optimiser leurs environnements cloud et réduire leurs dépenses globales tout en améliorant leur résilience et leur sécurité face aux cybermenaces.

- **Agilité accrue.** L'agilité, tant dans la manière dont les employés peuvent travailler que dans la capacité d'une organisation à protéger ses données en période de changements rapides, permet aux entreprises de se concentrer sur leur cœur d'activité plutôt que de se préoccuper de la sécurité et de la récupération des données après l'impact d'une cyberattaque ou d'autres menaces numériques. Un avantage majeur de l'approche de Commvault réside dans la profondeur et l'étendue inégalées de sa couverture des charges de travail au sein du secteur. Plusieurs clients interrogés ont décrit cela comme l'assurance apportée par Commvault qu' **"aucune charge de travail ne sera laissée pour compte"** dans la transition accélérée vers le cloud, visant à renforcer la résilience des données et la résilience cyber, tout en optimisant leur transformation avec pour objectifs sous- jacents la réduction des coûts et l'augmentation de l'agilité.

- **Réduction du risque.** Commvault, qui fournit des services de protection des données depuis plus de 27 ans, est intégré à la solution cloud de Microsoft depuis la création d'Azure en 2010, pour une approche holistique et native du cloud. En 2019, Commvault a étendu sa plateforme pour inclure une offre SaaS fondée sur la même technologie que le logiciel Commvault principal, permettant ainsi de sécuriser et de protéger les données, quel que soit leur emplacement ou la méthode de déploiement choisie pour la protection et la résilience des données (sur site, cloud public ou SaaS). Cette approche intégrée a permis aux clients communs de Microsoft et Commvault de remplacer, en moyenne, quinze solutions existantes de protection des données en migrant vers Commvault Cloud sur Azure, réduisant ainsi de manière significative le niveau de risque au sein de leur patrimoine de données.

Commvault Cloud combine la solution SaaS de Commvault et sa solution logicielle, offrant un plan de contrôle unifié qui fournit des fonctionnalités renforcées et une facilité d'utilisation à grande échelle. Cela permet aux organisations de bénéficier des capacités de sécurité des données et de récupération cyber attendues de Commvault, sans la complexité généralement associée à la protection de niveau entreprise, tout en offrant une feuille de route pour une transition fluide vers la protection des données en mode SaaS. Commvault Cloud renforce également de manière significative la posture de résilience cyber et de sécurité des données d'une organisation.

Conclusion

La plupart des organisations présentent un écart considérable entre leurs besoins en matière de résilience cyber et leur capacité réelle à restaurer rapidement leurs systèmes lorsqu'une cyberattaque survient. Le coût et la complexité des tests dépassent souvent leur budget et leurs compétences, et le véritable chaos qui accompagne un incident majeur de récupération est difficile à reproduire lors des tests. Bien que les recherches d'Enterprise Strategy Group

confirment que la résilience cyber figure parmi les cinq principales priorités pour 88 % des organisations, nos entretiens avec des clients de niveau entreprise ont révélé que la majorité d'entre eux ne réalisaient que des tests partiels et peu fréquents, se limitant à une simple liste de vérifications plutôt qu'à un plan éprouvé permettant une restauration complète. Nos entretiens avec les clients ont mis en évidence des coûts d'interruption d'activité allant de 10 000 dollars de l'heure à des exemples où les pertes atteignaient plusieurs millions de dollars par minute. Nous avons constaté que trop d'organisations investissent dans la résilience cyber comme si le risque concernait quelqu'un d'autre, et que le niveau de risque accepté par beaucoup devrait être considéré comme inacceptable.

Nous avons analysé l'impact que Commvault Cleanroom Recovery et Commvault Cloud Rewind peuvent avoir sur l'amélioration des tests de récupération, ainsi que sur la résilience et la récupération cyber dans leur ensemble. Nous avons constaté que Cleanroom Recovery ne fournit pas seulement un environnement de récupération bien supérieur à ce que la plupart des organisations peuvent créer, mais qu'il offre également des environnements stériles, alimentés par l'intelligence artificielle, qui peuvent réellement être utilisés pour restaurer la viabilité minimale, souvent en quelques minutes plutôt qu'en heures, jours, semaines ou mois, réduisant ainsi le temps d'arrêt à presque zéro. Nous avons également constaté que Cloud Rewind peut restaurer rapidement les applications et l'infrastructure associée dans le cloud en revenant à un point antérieur dans le temps, avant l'impact d'une cyberattaque. Nous pensons également que le partenariat entre Commvault et Microsoft dans la préparation et la récupération face aux cyberattaques offre un avantage supplémentaire en fournissant aux organisations une base solide pour faire face à l'ensemble des perturbations potentielles, tout en planifiant un retour rapide à la viabilité minimale.

De plus, nous pensons que Commvault a « trouvé la clé » de la récupérabilité, avec des exemples rapportés par des clients indiquant une reconstruction 94 % plus rapide (Cloud Rewind) et une récupération 99 % plus rapide (Cleanroom Recovery), permettant aux organisations de restaurer rapidement leurs systèmes et données critiques en cas de perturbation cyber. Nous avons constaté que les avantages d'un plan de préparation à la résilience cyber incluant Commvault Cleanroom Recovery et Commvault Cloud Rewind peuvent faire la différence entre une perte d'activité importante et un dommage durable à la marque, par rapport à des événements cyber résolus avec peu ou pas d'interruption des activités lorsqu'un plan de récupération intègre Commvault Cloud associé à Microsoft Azure.

Commvault Cleanroom Recovery et Cloud Rewind sont les pierres angulaires d'un plan de résilience cyber efficace et moderne. Enterprise Strategy Group recommande vivement à toute organisation présentant un décalage entre ses capacités de résilience et sa capacité à exécuter un plan de résilience cyber éprouvé d'explorer ce que Commvault et son long partenariat avec Microsoft peuvent faire pour aider à faciliter et à accélérer les étapes essentielles vers une véritable certitude et une récupération cyber complètes.