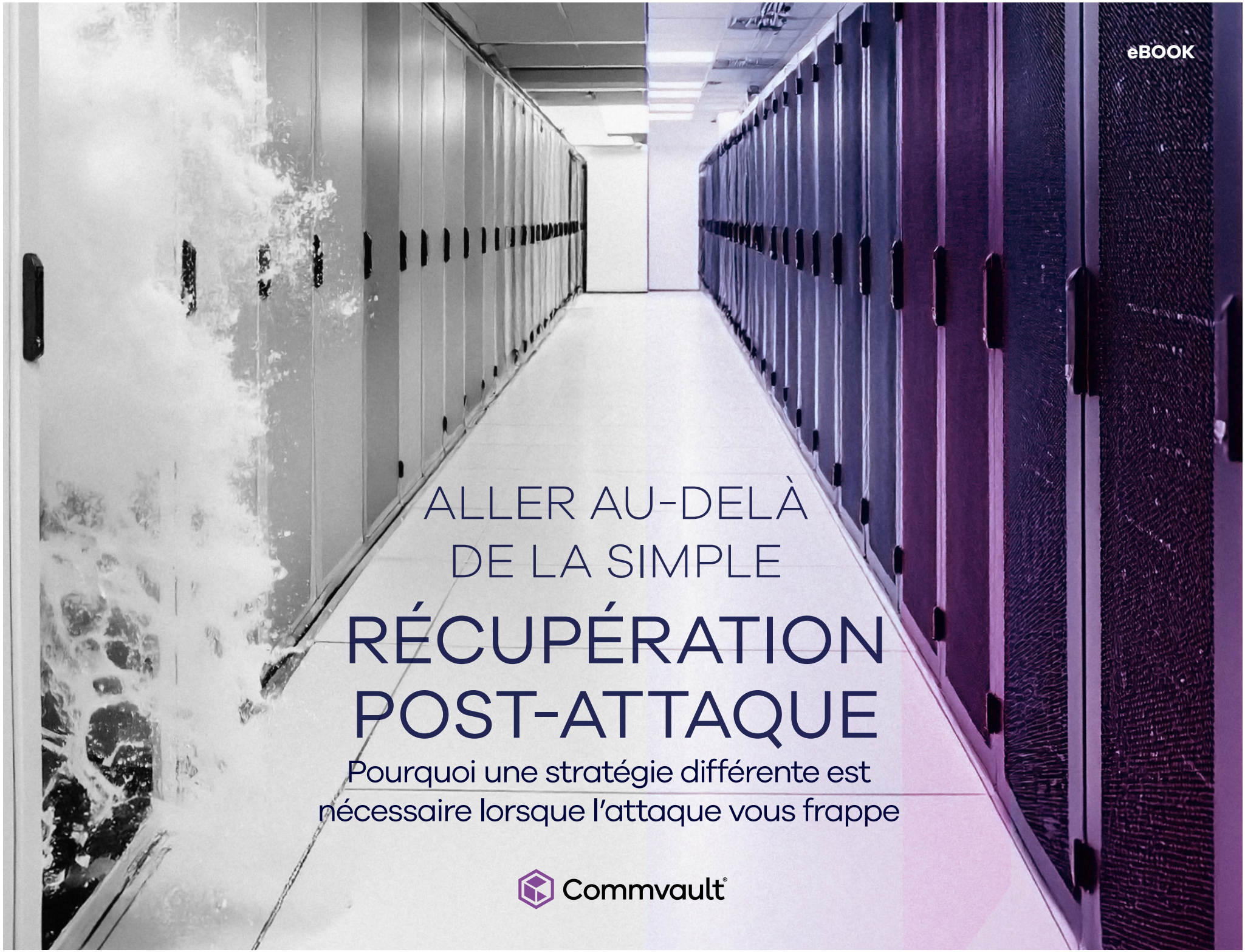
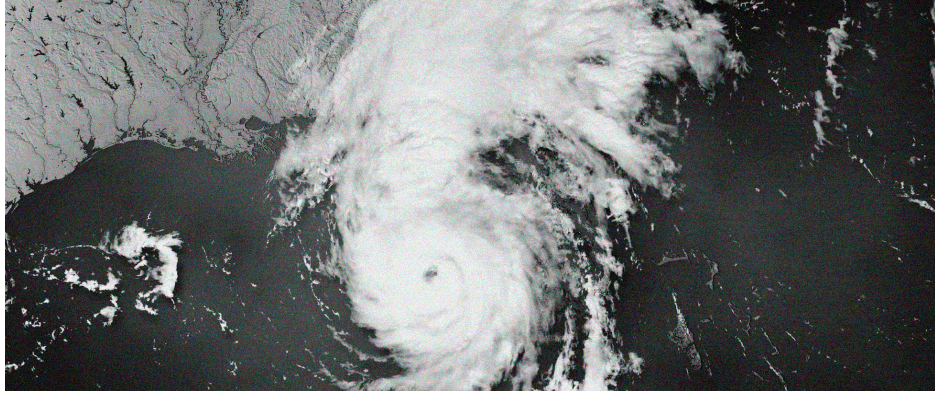


eBOOK

ALLER AU-DELÀ DE LA SIMPLE RÉCUPÉRATION POST-ATTAQUE

Pourquoi une stratégie différente est nécessaire lorsque l'attaque vous frappe

Commvault®



VOTRE APPROCHE DE LA REPRISE COMMENCE ICI

Des événements météorologiques aux cyberattaques malveillantes, il n'y a pas de pénurie d'événements destructeurs menaçant vos opérations commerciales de nos jours. Nos flux d'actualités sont remplis de récits de dommages causés par les ouragans et le ransomware.

Dans le cadre de toute bonne pratique, vous avez besoin d'un plan pour que votre organisation puisse rapidement se remettre d'un incident. Vous voudrez vous concentrer sur la protection de vos employés, de vos clients et de toutes vos données, tout en atténuant les dommages à vos actifs, à vos finances et à votre réputation.

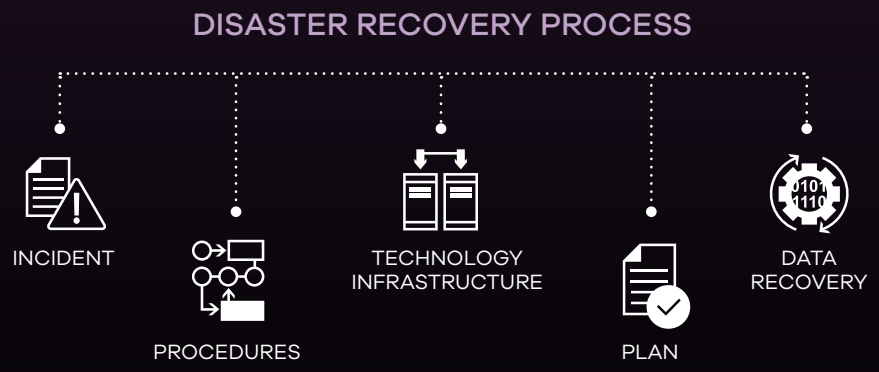
Mais rester résilient face à ces menaces nécessite une vigilance constante. La reprise après sinistre et la reprise après cyberattaque ne sont pas la même chose, il est donc crucial de comprendre les différences. Lisez la suite pour comprendre pourquoi vous devez avoir les deux types de plans de reprise dans votre arsenal–et apprenez comment définir la viabilité minimale dans votre organisation est une partie clé de la reprise après cyberattaque.

Avec une préparation approfondie, une stratégie de tests complète réalisée régulièrement, et des solutions pour une reprise et une reconstruction rapides de toutes vos applications et données – vous serez en mesure de surmonter les défis de la reprise.

POURQUOI VOUS AVEZ BESOIN D'UNE 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.



POURQUOI VOUS AVEZ BESOIN D'UNE REPRISE APRÈS CYBERATTAQUE

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.

REPRENEZ VOS ACTIVITÉS AVEC UNE VIABILITÉ MINIMALE

Lorsqu'une cyberattaque met votre organisation hors ligne, la pression est forte pour restaurer les opérations le plus rapidement possible afin de minimiser les dommages financiers et réputationnels. Ainsi, un aspect important de la reprise après cyberattaque est de définir la viabilité minimale de votre entreprise – c'est-à-dire l'ensemble minimal de systèmes, de données et de processus que vous devez restaurer pour rester opérationnel après une perturbation.

01 Identifier les actifs critiques

Cela comprend systèmes (infrastructure, applications critiques, outils de communication) ; données (opérationnelles, de conformité, de sauvegarde) ; et processus (opérations commerciales, informatiques et de sécurité, engagement client).

02 Évaluer l'impact d'une panne

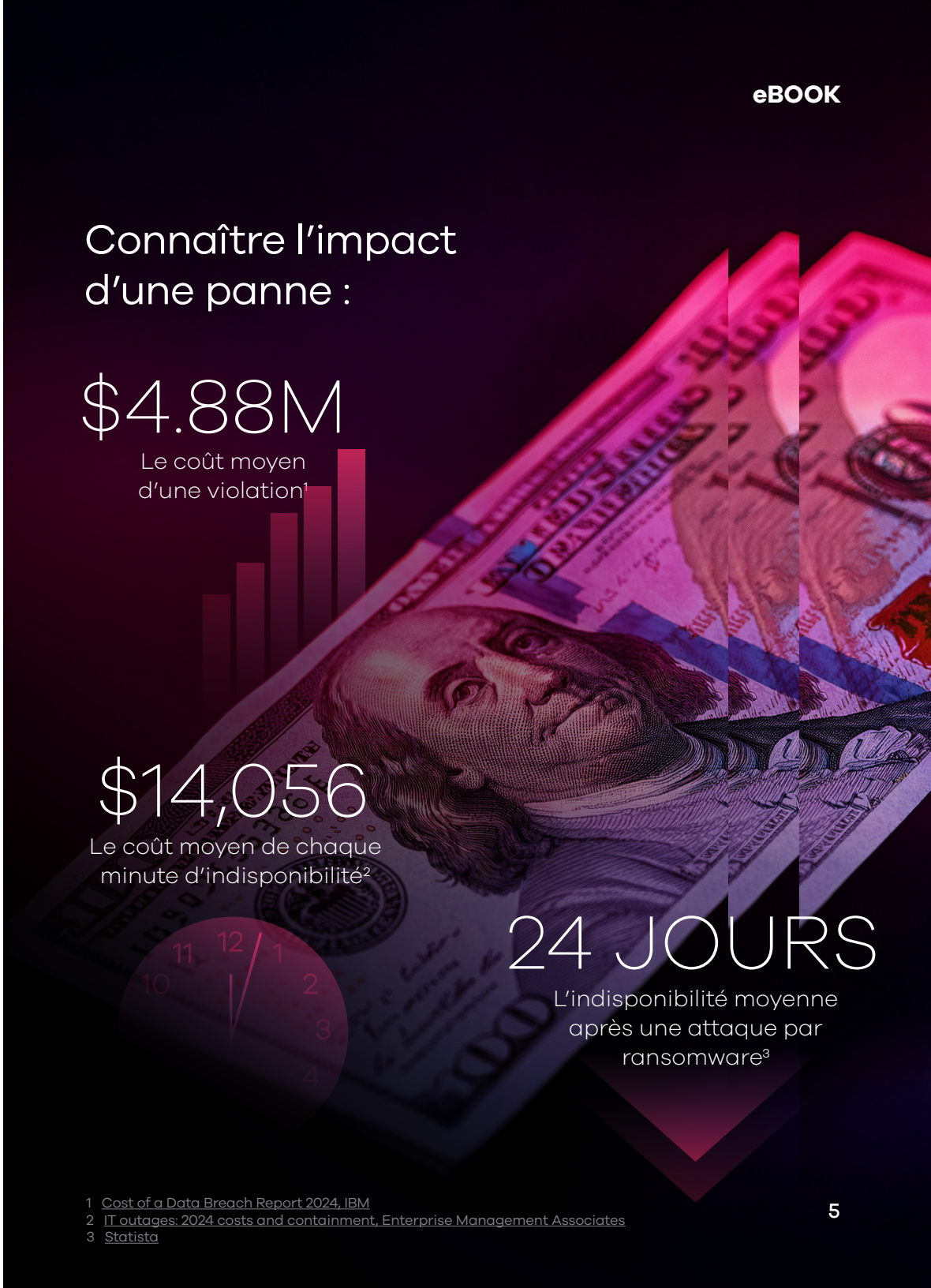
Combien coûte à votre organisation de ne pas être opérationnel ? Comprendre les effets de l'indisponibilité sur chacun de vos actifs critiques est essentiel pour la prise de décision et pour aider à prioriser leur reprise.

03 Créer un plan

Ensuite, vous devez créer votre plan pour restaurer vos actifs les plus critiques en cas de panne – et tester, tester, tester. Assurez-vous que vos employés sont formés à leur rôle dans la reprise.

04 Se concentrer sur une récupération propre et validée

Enfin, il est important de noter que vous devez valider que vous restaurez une copie propre de vos données ; disposer de copies isolées (air-gapped) vous aidera à accélérer la reprise de ces données. Et vous devriez effectuer une analyse forensique dans une salle de reprise isolée pour trouver la cause première et aider à prévenir les futures attaques.



Connaître l'impact d'une panne :

$4.88M

Le coût moyen d'une violation[1]

$14,056

Le coût moyen de chaque minute d'indisponibilité[2]

24 JOURS

L'indisponibilité moyenne après une attaque par ransomware[3]

1 Cost of a Data Breach Report 2024, IBM
2 IT outages: 2024 costs and containment, Enterprise Management Associates
3 Statista

SCHÉMA DES PILIERS POUR GARANTIR LA CYBER-RÉCUPÉRATION

SCENARIOS

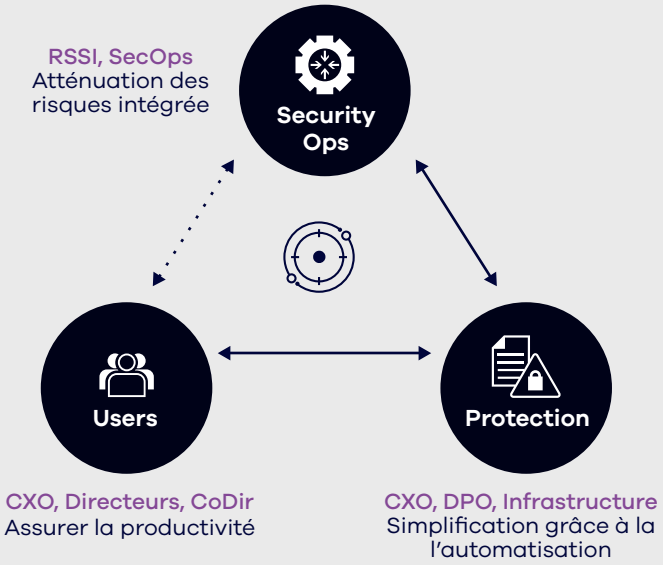
La capacité de cyber-récupération (CR) induit de nouveaux besoins par rapport plans de reprise d'activité ou de continuité de l'activité (PRA/CA)

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

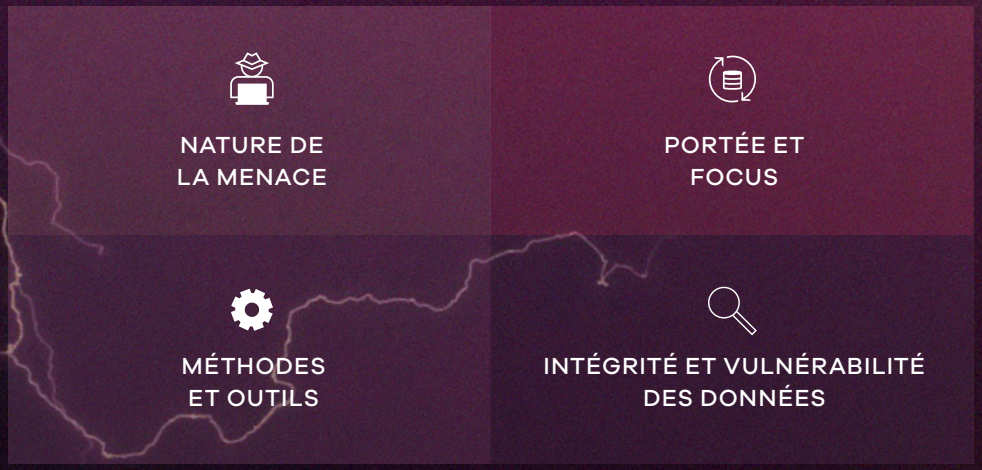
Les pré-requis pour la cyber-récupération (CR) sont dépendants des objectifs propres à l'entreprise elle-même

- 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

LA REPRISE APRÈS SINISTRE N'EST PAS SUFFISANTE

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 subtiles et les complexités que posent les cyberattaques.

Voici pourquoi :



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 APRÈS CYBERATTAQUE EST CRITIQUE

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.[1] 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». Toutefois, il est intéressant de constater qu'en réalité, très peu d'entreprises procèdent à des tests complets, fréquents et réussis.

CHIFFRES CRITIQUES :

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

Les attaquants débutent leurs mouvements latéraux dans les

48 MINUTES
suivant l'intrusion[3]

82% DES ENTREPRISES
qui des entreprises payant la rançon ne récupèrent pas l'ensemble de leurs données[4]

1 https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-84.pdf
2 https://www.ibm.com/reports/data-breach
3 https://go.crowdstrike.com/2025-global-threat-report.html
4 https://www.hiscoxgroup.com/news/blog/hiscox-cyber-readiness-report-2024

COMMENT COMMVAULT PEUT VOUS AIDER

AVEC COMMVAULT, VOUS POUVEZ :

- Sécuriser vos données critiques avec des copies isolées (air-gapped)
- Tester fréquemment pour confirmer que votre plan fonctionne et que vos employés savent quoi faire
- Valider que vous restaurez une copie propre de vos données
- Effectuer des analyses forensiques dans un environnement de reprise isolé et propre.

COMMVAULT SOLUTIONS :

Commvault® Cloud Rewind™

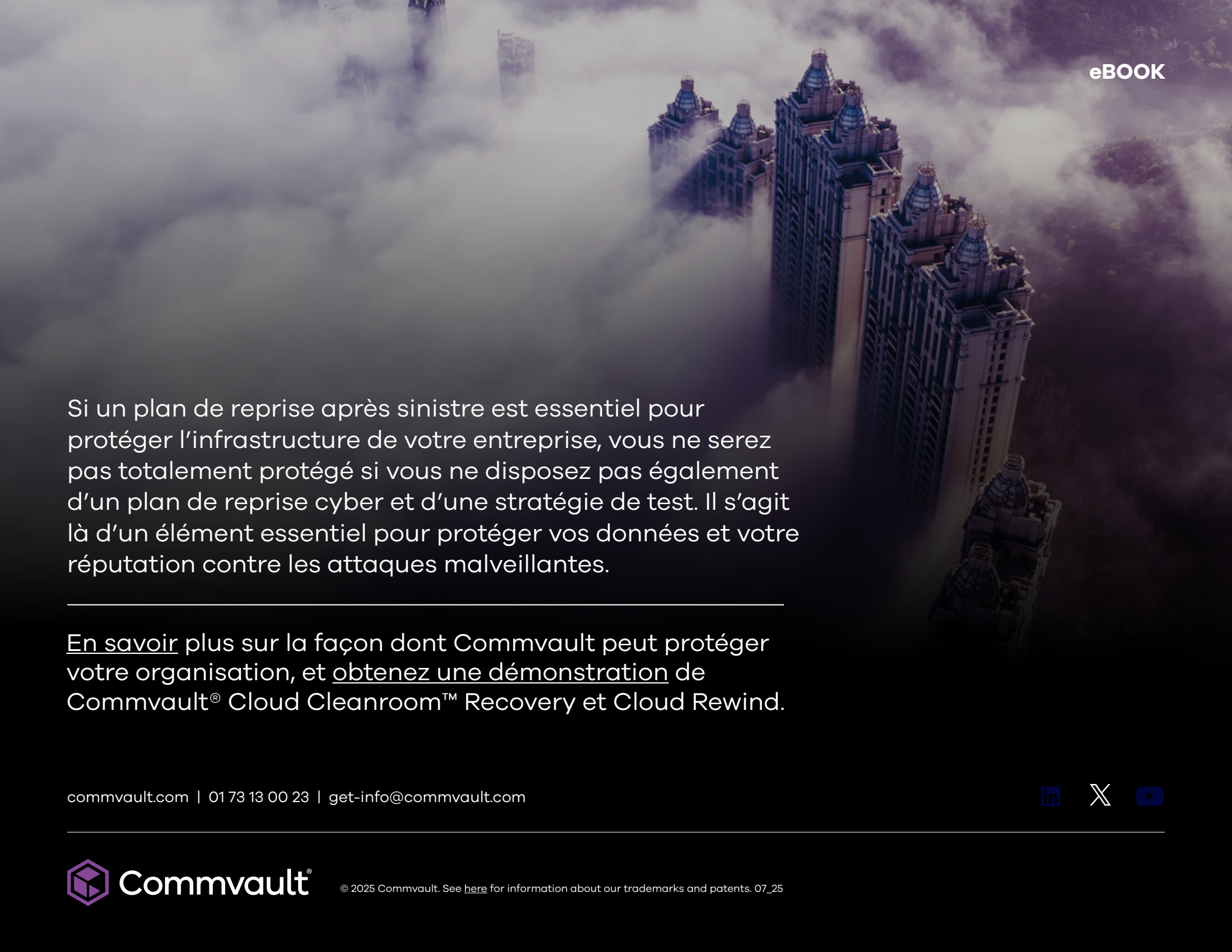
Cette solution va au-delà des sauvegardes traditionnelles et de la reprise après sinistre – en vous permettant de découvrir, protéger, restaurer et reconstruire continuellement pour établir une résilience cybernétique et maintenir des opérations commerciales continues. Vous pouvez revenir à un point spécifique dans le temps et reconstruire rapidement des applications cloud dynamiques et distribuées en cas de pannes et d'attaques de ransomware. Avec une machine temporelle cloud à double coffre brevetée, vous pouvez rapidement restaurer vos données, applications et configurations.

Commvault® Cloud Cleanroom™ Recovery

Cette solution fournit un environnement de reprise sécurisé et isolé à la demande. Cette solution est plus qu'un espace sécurisé. Elle permet aux organisations de tester l'efficacité de leurs plans de reprise après cyberattaque, de restaurer rapidement et proprement vos applications et données, et d'effectuer une analyse forensique sécurisée. Avec un stockage immuable isolé, une automatisation intégrée et une mise à l'échelle de la reprise renforcée par l'IA, Cleanroom Recovery vous aide à maintenir des opérations commerciales continues, même face à des menaces cybernétiques sophistiquées.

Commvault® Cloud for AD: Enterprise Edition

La gestion des identités et des accès est essentielle pour restaurer vos opérations après une attaque. Cette solution vous permet de protéger et d'accélérer la récupération des données AD en cas de corruption, de suppression accidentelle et d'attaques de ransomware grâce à la récupération forest-level automatisée.



eBOOK

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 cyber 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.

En savoir plus sur la façon dont Commvault peut protéger votre organisation, et obtenez une démonstration de Commvault® Cloud Cleanroom™ Recovery et Cloud Rewind.

commvault.com | 01 73 13 00 23 | get-info@commvault.com

Commvault®