

Protection et récupération des données multicloud

Lawrence Miller

- ✓ Défis de la gestion des données
- ✓ Cas d'utilisation en matière de protection et de récupération des données multicloud
- ✓ Exigences dans le cadre d'une solution de protection et de récupération des données multicloud

OBJECTIF DU DOCUMENT

Les données ont un rôle essentiel à jouer pour les entreprises d'aujourd'hui. C'est pourquoi leur perte (qu'elle soit causée par un ransomware, une panne matérielle ou tout autre incident) peut gravement perturber les opérations. Pour réduire ces risques, il est indispensable de mettre en place des mécanismes efficaces de sauvegarde et de récupération des données. Cette fiche technique met en lumière les solutions et les enjeux liés à la gestion des données, notamment au sein d'environnements multicloud.

Points clés :

- Bien que les architectures multicloud offrent de nombreux avantages, elles complexifient toutefois la gestion et la protection des données.
- Pour une protection avancée des données, voici quelques éléments essentiels : support cloud native, récupération immédiate, résilience face aux cybermenaces.

SOMMAIRE

- 2** Défis de la gestion des données
- 4** Cas d'utilisation en matière de protection et d'utilisation des données multicloud
- 5** Exigences dans le cadre d'une solution de protection et de récupération des données multicloud
- 6** Témoignage client

Les données constituent la clé de voûte de toute entreprise moderne, mais que se passe-t-il si vos données disparaissent ? Qu'il s'agisse d'un ransomware, d'une attaque par déni de service, d'un programme malveillant, d'un dysfonctionnement matériel ou d'une erreur humaine, lorsque vos données disparaissent, le bon fonctionnement de votre entreprise peut être mis en péril. Étant donné le caractère essentiel des données pour votre entreprise aujourd'hui, vous devez vous assurer d'avoir tous les outils nécessaires pour sauvegarder et récupérer vos données rapidement et efficacement.

Dans cette fiche technique, nous aborderons les défis induits par la gestion des données, plusieurs cas d'utilisation en matière de protection et de récupération des données multicloud, ainsi que les capacités et fonctionnalités dont vous avez besoin dans une solution moderne de protection et de récupération des données.

Défis de la gestion des données

Bien qu'elles aient conscience de l'importance de protéger leurs données, les entreprises rencontrent des difficultés à le faire en raison d'infrastructures informatiques complexes, du cloisonnement des données et de leur prolifération. Cela est notamment dû au fait que les entreprises développent toute une panoplie d'outils et de produits divers et variés visant à protéger leurs données pour répondre à différentes utilisations. De plus, les solutions traditionnelles sont coûteuses à entretenir et ne sont pas toujours

Bien qu'elles aient conscience de l'importance de protéger leurs données, les entreprises rencontrent des difficultés à le faire en raison d'infrastructures informatiques complexes, du cloisonnement des données et de leur prolifération.

interopérables avec les nouvelles technologies mises en place. Mais nombreuses sont les entreprises qui adoptent des stratégies axées sur le cloud avec des infrastructures multicloud.

Dans une architecture multicloud, une entreprise utilise deux ou plusieurs services de cloud computing provenant de différents fournisseurs de cloud afin d'améliorer ses capacités de reprise après sinistre, d'exploiter les meilleures technologies, d'optimiser les charges de travail des applications et de réduire les risques. Cette stratégie présente toutefois son lot de défis : [pour 87 % des entreprises ayant adopté une stratégie multicloud, la gestion du multicloud figure parmi leurs trois principaux défis en matière de cloud.](#)

Pourquoi ? Il arrive que les entreprises mettent en œuvre des architectures multicloud de manière involontaire en raison d'une gestion informatique décentralisée et d'une informatique parallèle (« *Shadow IT* ») généralisée. Ce n'est donc parfois pas une stratégie délibérée. Imaginez vos ressources humaines qui utilisent une application SaaS (« *Software-as-a-Service* ») pour la paie, tandis que vos équipes DevOps préfèrent créer des applications sur Amazon Web Services (AWS) et que votre service informatique gère votre infrastructure principale via Microsoft Azure. Mais il arrive également que ce soit le fruit d'une décision consciente mûrement réfléchie. Les stratégies multicloud génèrent par nature des données à différents emplacements. Que la démarche soit intentionnelle ou non, les données sont omniprésentes autour de nous, ce qui augmente la complexité de l'environnement informatique et pose un certain nombre de défis en matière de protection et de sécurisation des données.

Il est également important de noter que la démocratisation des données contribue à leur prolifération et à leur complexification. La démocratisation des données consiste à rendre l'ensemble des données et types de données facilement accessibles à tous les utilisateurs professionnels, plutôt que d'adopter le principe de sécurité du moindre privilège, ce qui pose davantage de défis en matière de gestion des données. À mesure que les entreprises lancent leurs propres solutions d'intelligence artificielle (IA), les volumes de données continueront d'augmenter de manière exponentielle et le déploiement de produits distincts et disparates dans des architectures multicloud et hybrides continuera d'être de plus en plus problématique.

Ce dont les entreprises ont besoin, c'est d'une solution moderne de protection et de récupération des données qui protège les systèmes et les charges de travail dans des environnements multicloud sur site et hybrides. Une solution entièrement intégrée, qui offre des capacités de sauvegarde granulaires et de récupération instantanée, renforce leur cyber-résilience, détecte les menaces et permet une reprise rapide après une cyberattaque. Une solution unifiée pour la gestion et la protection des données qui répond aux utilisations professionnelles d'aujourd'hui et de demain.

Ce dont les entreprises ont besoin, c'est d'une solution cloud native moderne pour la protection et la récupération de leurs données. Une solution entièrement intégrée, qui offre des capacités de sauvegarde granulaires et de récupération instantanée, renforce leur cyber-résilience, détecte les menaces et permet une reprise rapide après une cyberattaque.

Cas d'utilisation en matière de protection et de récupération des données multicloud

La protection et la récupération des données multicloud couvrent de nombreux cas d'utilisation. Voici certains des plus courants :

- **Sauvegarde et récupération** : Vous pouvez perdre des données de diverses manières, que l'intention soit malveillante ou non. C'est pourquoi il est essentiel de sauvegarder vos données si vous souhaitez pouvoir les récupérer. Pour ce faire, vous devez disposer d'un processus et d'un outil qui vous permettent de créer et de stocker des copies de données dans un emplacement sécurisé afin de les protéger contre toute perte ou tout dommage.
- **Sécurité et conformité des données** : Selon les secteurs, différentes règles peuvent s'appliquer concernant la manière de gérer vos données. Par exemple, le règlement général européen sur la protection des données (RGPD) s'applique à toute entreprise contrôlant ou traitant les informations personnelles identifiables (IPI) des résidents de l'Union européenne. Les entreprises qui ne garantissent pas une bonne gestion de leurs données conformément aux réglementations de leur secteur pourraient subir des répercussions juridiques, monétaires et financières.
- **Protection, détection et récupération des données contre les ransomwares** : La défense la plus efficace contre les ransomwares consiste à adopter une stratégie de sauvegarde immuable, ce qui vous permet de récupérer vos données rapidement et facilement, sans avoir à payer une quelconque rançon. Mais il est également important de mettre en place une stratégie de réponse efficace. Prenez un cadre de référence comme le NIST pour adopter les meilleures pratiques en matière de cybersécurité et développer de solides capacités de protection, de détection et de récupération de vos données.
- **Conservation à long terme et archivage** : Pour les entreprises qui génèrent régulièrement de nouvelles données, mais qui doivent conserver leurs données existantes, l'archivage des données est essentiel car cela leur permet de récupérer rapidement les deux types de données. Dans certains secteurs, la conservation des données pendant des périodes plus longues est nécessaire pour des raisons de conformité et de réglementation.
- **Reprise après sinistre et continuité des activités** : Dans un monde en constante évolution et « toujours connecté », un temps d'arrêt risque de nuire aussi bien à votre réputation qu'à vos résultats. Les entreprises doivent être capables de répondre à des exigences de plus en plus strictes en matière de durée maximale d'interruption admissible (DMIA), d'objectif de délai de récupération (ODR) et d'objectif de point de récupération (OPR) afin de garantir une reprise totale et rapide de leur activité après une panne ou tout autre événement majeur.

Exigences dans le cadre d'une solution de protection et de récupération des données multicloud

Les données étant de plus en plus critiques pour les entreprises, une solution de protection et de récupération des données de pointe pour le multicloud est essentielle. Vous trouverez les principales exigences ci-dessous :

- **Gestion unifiée** : Une solution unique et unifiée permet de gérer globalement des environnements multicloud, hybrides et sur site à grande échelle. En tant qu'assistant global intelligent, elle doit être en mesure de détecter les attaques potentielles de ransomwares, d'identifier les anomalies et de recommander les mesures correctives nécessaires, par exemple dans le cas de capacités supplémentaires envisagées.
- **Protection des données sur site, dans le cloud et SaaS** : Les données sont omniprésentes autour de nous. Une bonne stratégie de protection et de récupération des données doit protéger vos données où qu'elles soient : sur site, dans des environnements multicloud et hybrides, ou bien dans des applications SaaS. Optez pour des options de déploiement flexibles sur site et dans le cloud qui peuvent être autogérées ou gérées « en tant que service ».
- **Restauration massive instantanée des données** : Alors que les acteurs malveillants cherchent à exfiltrer ou détruire autant de données que possible, vous avez donc besoin d'une solution qui vous permet de les récupérer rapidement. Adoptez une solution qui maintient les snapshots entièrement hydratés pour améliorer les délais de récupération et restaurer instantanément des centaines de machines virtuelles (MV), de grandes bases de données et d'importants volumes de données non structurées, à grande échelle, à tout moment et en tout lieu.
- **Cyber-récupération** : Vérifiez l'intégrité de vos sauvegardes pour identifier un point de récupération « propre », par exemple, en cas d'attaque par ransomware qui ciblerait vos sauvegardes. Orientez-vous vers une solution qui vous permet de restaurer vos données en toute confiance à un niveau granulaire.
- **Évolutivité illimitée** : Évitez les mises à niveau complexes, risquées et coûteuses sur site, et déployez facilement votre solution sans perturbation. Optez pour une architecture évolutive et hyperscale ainsi qu'un système de fichiers distribué qui vous offre des capacités de recherche globale et vous aide à réduire votre empreinte en matière de données et de stockage grâce à une déduplication et une compression à longueur variable globales.

Les données étant de plus en plus critiques pour les entreprises, une solution de protection et de récupération des données de pointe pour le multicloud est essentielle.

Témoignage client

Ausenco renforce son niveau de sécurité et réduit son temps de gestion grâce à Cohesity DataProtect fourni en tant que service

Ausenco, fournisseur multinational de services d'ingénierie et de conseil, sauvegarde 100 To de données Microsoft 365 (M365) critiques pour ses plus de 3 000 collaborateurs. L'ancienne solution de sauvegarde de l'entreprise - le logiciel Veeam basé sur une infrastructure cloud autogérée - ne répondait plus aux besoins d'Ausenco en matière de sécurité et représentait 20 heures de gestion par semaine. Cohesity DataProtect fourni en tant que service a permis à Ausenco de gagner du temps en récupérant ces 20 heures par semaine (auparavant consacrées à la gestion de l'infrastructure de sauvegarde), de mettre en place des contrats de niveau de service (SLA) de 4 heures pour la récupération de fichiers, et d'obtenir des sauvegardes immuables, nécessaires à la cyber-assurance, pour davantage de tranquillité d'esprit. Le tout sans frais supplémentaires.

DÉFI

L'activité de services d'ingénierie et de conseil d'Ausenco est en plein essor, en particulier dans le secteur minier qui connaît une demande croissante en métaux pour batteries. L'entreprise sauvegarde 100 To de données M365 critiques pour ses plus de 3 000 collaborateurs. « Microsoft garantit une protection des données intégrée, mais ne suffit malheureusement pas dans le cadre de notre activité », explique Kalpesh Bhathella, directeur des services opérationnels d'Ausenco. « Nous avons besoin de conserver certains fichiers SharePoint et OneDrive indéfiniment et ne pouvons pas nous permettre de les perdre à cause de cyberattaques. »

Jusqu'en 2022, l'équipe informatique d'Ausenco a sauvegardé ses données M365 avec le logiciel Veeam, en utilisant l'infrastructure en tant que service (IaaS) d'AWS. Mais la gestion de l'infrastructure et des logiciels était complexe, monopolisant 50 % du temps d'un administrateur informatique. Autre inconvénient : les copies

de sauvegardes immuables, indispensables à la reprise après sinistre, nécessitent davantage d'infrastructures et de temps de gestion. « La sécurité est notre priorité absolue », déclare Kalpesh Bhathella. « Nos prospects nous posent toujours des questions à ce sujet et nous ont d'ailleurs demandé dernièrement si nous avions une cyber-assurance. Nous avons besoin de copies immuables, mais sans charge de gestion en plus. »

SOLUTION

Après avoir comparé Cohesity et Rubrik, Ausenco a porté son dévolu sur Cohesity DataProtect, une solution fournie en tant que service, qui offre des capacités de sauvegarde et de récupération pour les logiciels en tant que service (SaaS) comme M365 ainsi que d'autres données cloud ou sur site qu'Ausenco pourrait ajouter ultérieurement. « Nous avons aimé l'idée d'un service cloud entièrement géré, car une infrastructure autogérée n'a aucun sens à l'heure actuelle si l'informatique n'est pas votre cœur de métier », explique Kalpesh Bhathella. « Et seul Cohesity propose de créer des sauvegardes immuables par défaut. »

Le service cloud de Cohesity a été rapidement opérationnel. Environ deux semaines ont suffi. L'équipe informatique n'a plus vraiment besoin d'y penser. « Après la configuration initiale, Cohesity a tout simplement fonctionné », ajoute Kalpesh Bhathella. « Dans les rares cas où nous avons sollicité de l'aide, Cohesity a tout de suite trouvé la solution. Nous n'avons jamais eu besoin d'intervenir. »

RÉSULTATS

Pour Ausenco, le principal avantage de la solution Cohesity résidait dans sa posture de sécurité renforcée. « Nous mettons tout en œuvre pour prévenir les cyberattaques, mais avoir la possibilité de restaurer des données M365 propres à partir des copies de sauvegarde immuables de Cohesity nous garantit une solution de repli sérieuse. Le stockage de sauvegardes immuables hors site nous a également permis de bénéficier d'une cyber-assurance et ainsi de répondre aux besoins de nos prospects. »

Grâce à un niveau de sécurité renforcé, Ausenco a pu réaliser des économies de coûts. « Les économies réalisées grâce à la suppression des frais mensuels d'une infrastructure cloud ont permis de financer entièrement Cohesity DataProtect », déclare Kalpesh Bhathella. « De plus, les 20 heures par semaine que nous consacrons auparavant à la mise au point et à la gestion de notre logiciel de sauvegarde et de notre infrastructure cloud, nous les avons gagnées. » Le poste qui dédiait auparavant 50 % de son temps à la gestion des sauvegardes peut désormais se concentrer sur des tâches à plus forte valeur ajoutée pour soutenir la transformation numérique de l'entreprise. Combinées à d'autres mesures prises en matière de cybersécurité, les sauvegardes immuables ont permis à Ausenco de bénéficier de tarifs avantageux sur sa police d'assurance cybernétique.

Pour la première fois, Ausenco propose des SLA de 4 heures dédiés à la récupération des e-mails ou des fichiers M365. Cette nouveauté a rencontré un franc succès auprès des équipes opérationnelles, d'ingénierie et de conseil de l'entreprise, particulièrement occupées. « Avec notre ancienne solution de sauvegarde, la restauration d'un fichier Exchange, SharePoint ou OneDrive perdu pouvait prendre des semaines, car notre administrateur informatique devait parcourir des centaines de sauvegardes pour le retrouver », explique Kalpesh Bhathella. « Le moteur de recherche de Cohesity est une sorte de Google des sauvegardes. Il suffit de saisir un nom de fichier ou une phrase et une liste de résultats apparaît. Le fichier que nous recherchons se trouve souvent en haut de cette liste. »

Ausenco compte désormais utiliser Cohesity DataProtect fourni en tant que service pour protéger d'autres charges de travail, en plus de M365, notamment les MV sur site et AWS. Afin que Ausenco gagne toujours plus en résilience, Kalpesh Bhathella prévoit de sauvegarder certaines charges de travail sur Microsoft Azure, une configuration de cloud hybride. L'équipe informatique pourra visualiser et gérer les sauvegardes et restaurations dans n'importe quel cloud à partir de la même interface Cohesity, bénéficiant ainsi d'une expérience de gestion unifiée.

Comme le résume Kalpesh Bhathella : « Avec Cohesity DataProtect fourni en tant que service, nous avons tout ce dont nous avons besoin pour protéger tout type de données dans le cadre du développement de notre entreprise : des sauvegardes immuables, des restaurations rapides et un excellent support, le tout sans avoir à nous soucier de la gestion de l'infrastructure. »

Les solutions Cohesity vous garantissent les bénéfices suivants :

- **des sauvegardes immuables (une condition essentielle pour gagner en résilience face aux cybermenaces) ;**
- **une restauration des e-mails et des fichiers M365 jusqu'à 99 % plus rapide (4 heures au lieu de deux semaines) ;**
- **un gain de temps de 20 h/semaine en termes de gestion ;**
- **aucun coût supplémentaire.**

EN SAVOIR PLUS

Découvrez des solutions avancées de protection et de récupération des données sur <https://www.cohesity.com/solutions/backup-and-recovery> et téléchargez notre guide « [Protéger, restaurer et exploiter au mieux vos données](#) » [pour sélectionner une plateforme de sécurisation et de gestion des données basée sur l'intelligence artificielle](#)

PROTECTION ET RÉCUPÉRATION DES DONNÉES MULTICLOUD

COHESITY