

Protégez les données critiques avec une stratégie de sauvegarde 3-2-1

Les données sont au cœur de tous les aspects de votre activité, ce qui rend leur protection primordiale. Le risque d'exfiltration, de suppression ou de corruption de données peut provenir de différentes sources, notamment les ransomwares, les catastrophes naturelles et les erreurs humaines.

Dans tous les cas, les sauvegardes constituent la dernière ligne de défense, ce qui fait des données de sauvegarde une cible d'attaque standard. Il est impératif de déployer une stratégie solide de résilience des données et de l'entreprise autour de vos données de sauvegarde. La stratégie de sauvegarde 3-2-1 est une méthode éprouvée pour maintenir la résilience en cas d'incident sur les données.

Définition de la stratégie de sauvegarde 3-2-1

La stratégie de sauvegarde 3-2-1 offre une base solide qui équilibre diversité, redondance et stockage hors site, assurant ainsi la disponibilité et la résilience des données essentielles. Son nom fait référence au *quoi*, au *où* et au *comment* de votre approche de sauvegarde.

Quoi : trois copies

Conservez trois copies de vos données, à savoir vos données de production plus deux sauvegardes. Cette redondance garantit que même si une copie devient inaccessible ou corrompue, vous en avez toujours deux à votre disposition pour la restauration. Le maintien de trois copies réduit considérablement le risque de perte permanente de données.

Où : deux supports différents

Stockez les copies de données dans deux formats ou sur deux supports différents. La diversification offre une protection supplémentaire contre certains types de défaillances. Par exemple, le stockage d'une copie sur un disque dur externe physique et d'une autre dans le cloud protège contre les défaillances matérielles et les atteintes à la sécurité en ligne. Cette approche minimise les risques de perte simultanée de toutes les copies.

Comment : une copie immuable ou isolée physiquement

Veillez à ce qu'une copie de sauvegarde soit immuable et/ou isolée physiquement afin de garantir l'intégrité et la disponibilité des données critiques pour la cyber-résilience et la protection contre les ransomwares.

De nombreuses réglementations relatives à la conformité et à la conservation des données imposent de stocker les données dans un état inaltérable pendant une période spécifique. Les [sauvegardes immuables](#) garantissent l'authenticité et la fiabilité de la copie de sauvegarde, ce qui en fait une source fiable pour la récupération et les exigences de conformité.

La dernière recommandation est de conserver une copie des données hors site. Cela signifie qu'elle doit être géographiquement séparée de l'endroit où vous créez et conservez vos données primaires. Il s'agit d'une protection contre les dangers physiques tels que les ouragans, les incendies, les inondations et autres catastrophes susceptibles d'endommager physiquement votre site. Le fait de disposer d'une copie hors site vous permet de récupérer vos données et de poursuivre vos activités en cas de catastrophe ou de vol.

STRATÉGIE DE SAUVEGARDE 3-2-1



Principales raisons de mettre en œuvre une stratégie 3-2-1



CYBER-RÉSILIENCE

« Le ransomware est la seule forme de criminalité basée sur les crypto-monnaies en passe de croître en 2023 », selon la société d'analyse de la blockchain [Chainalysis](#). Dans son étude de mi-année, le cabinet a indiqué que les attaquants avaient extorqué 175,8 millions de dollars de plus qu'à la même date en 2022.

Si les cybercriminels s'emparent à la fois des données de production et des données de sauvegarde, ils peuvent paralyser votre organisation et la tenir en otage. Cela leur permet d'extorquer des paiements plus élevés ou de perturber votre activité de manière irrémédiable. Avec une stratégie de sauvegarde 3-2-1 en place, vous pouvez rapidement récupérer en restaurant à partir d'un environnement de récupération isolé situé hors site, disposant d'un chiffrement des données et existant sur un périphérique de stockage immuable et indélébile.



RÉSILIENCE AUX INCIDENTS

Dans notre [rapport de 2022](#), 27 % des personnes interrogées ont déclaré qu'une catastrophe naturelle avait entraîné une interruption des activités de leur entreprise au cours des deux années précédentes. La mise en œuvre d'une stratégie 3-2-1 permet d'atténuer les risques d'interruption des activités et de perte grave de données. La création d'un site de stockage de données hors site dans une zone à faible risque de catastrophe naturelle peut vous aider à récupérer rapidement si vous perdez des données de production à la suite d'un incident sur votre site principal. Quoi qu'il arrive, les données restent en sécurité et peuvent être restaurées.



CONTINUITÉ DES AFFAIRES

« Temps d'arrêt » est un gros mot. Les risques qui pèsent sur les communications, les opérations et la chaîne d'approvisionnement augmentent d'année en année, alors que les clients attendent des services et une exécution plus rapides. Il est essentiel de disposer d'une solide stratégie de résilience pour les entreprises. Une stratégie de sauvegarde 3-2-1 offre un moyen clair et rapide de restaurer les opérations de manière transparente et de maintenir la productivité.



RÉPUTATION PROFESSIONNELLE

La perte ou l'exfiltration de données à la suite d'une attaque peut faire plus que perturber la continuité des affaires. Elles peuvent avoir un effet dévastateur sur votre réputation et entamer définitivement la confiance de vos clients. Selon le rapport [2022 Thales Consumer Digital Trust Index](#), 82 % des victimes d'une violation de données ont constaté un impact négatif sur leur vie. Pour protéger la confiance des clients, il est essentiel de rétablir rapidement l'expérience client après une interruption. Cela s'ajoute aux plans d'atténuation et de remédiation. La récupération rapide des données des clients n'est qu'une partie de la démonstration d'un engagement en faveur de la sécurité et de la fiabilité des données, et peut renforcer votre position sur le marché.

Solutions clés en main 3-2-1

Veritas propose des options de sauvegarde complètes et clés en main, notamment les [appliances alimentées par NetBackup™](#) et [Veritas Alta™ Recovery Vault](#). Celles-ci vous aident à protéger, détecter et récupérer rapidement en cas d'incident, qu'il s'agisse d'une cyberattaque, d'une catastrophe naturelle ou d'une erreur humaine.

Les offres Veritas basées sur le cloud garantissent la redondance des données, l'évolutivité et l'accessibilité à distance. Elles fournissent une protection et une flexibilité supplémentaires pour les données critiques. Nous simplifions la mise en œuvre de la meilleure approche pour votre sauvegarde 3-2-1, afin que vous puissiez vous concentrer sur l'augmentation de la productivité, la réduction de vos coûts opérationnels et la fourniture d'une excellente expérience client.

En savoir plus sur les [solutions de reprise après incident de Veritas](#). >

À propos de Veritas

Veritas Technologies est un leader dans la gestion des données multi-cloud. Plus de 80 000 entreprises, dont 95 % des entreprises faisant partie du classement Fortune 100, font confiance à Veritas pour les aider à assurer la protection, la restauration et la conformité de leurs données. Veritas est réputée pour sa fiabilité à grande échelle, qui offre la résilience dont les clients ont besoin contre les interruptions qui pourraient survenir en cas de cyberattaque, par exemple de ransomware. Aucun autre fournisseur n'est en mesure d'égalier la capacité d'exécution de Veritas, avec la prise en charge de plus de 800 sources de données, de plus de 100 systèmes d'exploitation, de plus de 1 400 cibles de stockage et de plus de 60 plates-formes cloud, via une seule approche unifiée. Avec la technologie Cloud Scale, Veritas propose aujourd'hui sa stratégie de gestion autonome des données, qui réduit les coûts opérationnels tout en offrant une plus grande valeur ajoutée. En savoir plus sur www.veritas.com/fr/fr/. Suivez-nous sur Twitter : [@veritastechllc](https://twitter.com/veritastechllc).

VERITAS™

veritas.com/fr/fr

Pour obtenir les coordonnées pour le monde entier, consultez la page :

veritas.com/fr/fr/company/contact