COHESITY

LIVRE BLANC

Au-delà de la restauration : un guide destiné aux RSSI qui souhaitent utiliser les données de sauvegarde pour renforcer la cyber-résilience

TABLE DES MATIÈRES

Synthèse

Les cyberattaques étant de plus en plus nombreuses et leurs conséquences de plus en plus graves, les RSSI doivent cesser de se concentrer uniquement sur la prévention et adopter une approche plus large axée sur la cyber-résilience. Ils doivent pour cela s'assurer que leur entreprise est capable de résister aux attaques, c'est-à-dire d'y répondre rapidement, de restaurer ses systèmes de manière sécurisée et d'empêcher toute récidive.

Ce livre blanc remet en question les perceptions traditionnelles des systèmes de sauvegarde avancés en les considérant comme des composants essentiels d'une stratégie de gestion des risques liés à la cybersécurité. Il montre que des sauvegardes modernes et sécurisées peuvent être bien plus que de simples outils de restauration, et devenir des ressources précieuses pour rechercher les menaces, contrer rapidement les cybercriminels et répondre plus vite aux incidents. Elles peuvent notamment fournir la visibilité et le contrôle nécessaires pour maintenir l'intégrité opérationnelle lorsque les défenses de sécurité primaires sont contournées ou isolées. En exploitant la mine d'informations historiques contenues dans leurs systèmes de sauvegarde, les entreprises peuvent acquérir des connaissances plus approfondies sur les menaces potentielles, accélérer leur réponse aux incidents, restaurer plus rapidement et de manière sécurisée, et mettre en place une pratique de cybersécurité plus résiliente.

1. Recherche de menaces améliorée

La recherche de menaces est une pratique proactive de cybersécurité qui consiste à rechercher activement des preuves de menaces cachées sur le réseau d'une entreprise afin de neutraliser les cybercriminels le plus tôt possible dans la séquence d'attaque. Les méthodes traditionnelles de recherche de menaces s'appuient souvent sur des agents de terminaux et des journaux système.

Presque toutes les plateformes de ransomware à la demande (RaaS, Ransomware as a Service) intègrent désormais une technique de contournement courante : le BYOVD (Bring Your Own Vulnerable Device Driver). Dans cette approche, le cybercriminel déploie un pilote de périphérique signé qui existe sous le niveau du système d'exploitation pour empêcher la solution de sécurité des terminaux et la journalisation de détecter les attaques. C'est là que les données de sauvegarde deviennent une ressource inestimable pour la recherche de menaces.

Utiliser les données de sauvegarde pour rechercher des menaces présente plusieurs avantages clés, notamment :

- **Recherche de menaces passive** : les copies de sauvegarde étant isolées de l'environnement primaire, les cybercriminels (notamment les gangs de ransomware qui intègrent des techniques de contournement à leur plateforme RaaS pour échapper aux contrôles de sécurité courants tels que l'EDR et le XDR) ne peuvent pas les altérer ni les contourner. Cette isolation permet de rechercher les menaces de manière efficace et discrète.
- **Contexte historique** : les données de sauvegarde permettent aux analystes d'examiner l'état du système et les modifications apportées aux données au fil du temps, et ainsi d'identifier les schémas subtils d'activité malveillante qui se répètent sur le long terme.
- **Couverture complète** : les sauvegardes contiennent souvent des données provenant de l'ensemble de l'entreprise. Elles fournissent ainsi une vue d'ensemble qui peut révéler des liens entre des événements apparemment sans rapport.
- **Analyse hors ligne** : les chasseurs de menaces (threat hunters) peuvent éviter d'alerter les cybercriminels actifs et ainsi compromettre leurs efforts de détection en analysant les données de sauvegarde hors ligne.
- **Restauration des données supprimées ou altérées** : les sauvegardes peuvent permettre de détecter des attaques sophistiquées en retrouvant des preuves qui ont été supprimées ou modifiées sur les systèmes actifs.

2. Conformité réelle des données

Avec l'avènement de la sécurité assistée par l'intelligence artificielle (IA), les outils de gestion de la posture de sécurité des données (DSPM, data security posture management) se combinent aux systèmes de sauvegarde pour offrir une solution puissante et doublement efficace. Les outils de DSPM ne se contentent pas d'analyser les systèmes informatiques, les réseaux et les magasins de données pour rechercher des informations sensibles telles que des données médicales ou financières. Ils indiquent également où se trouvent ces données, qui y a accédé, et à quelle fréquence. Associés à des systèmes de sauvegarde avancés, ils permettent aux responsables de la conformité de réduire considérablement le risque d'exposition des données sensibles.

Intégrer votre solution DSPM à un système de sauvegarde avancé présente plusieurs avantages :

- **Identification rapide des systèmes qui ne sont pas sauvegardés**. Les solutions DSPM détectent et classent automatiquement les ressources de données de divers environnements, notamment les données fantômes et les bases de données oubliées. Certaines de ces données sont probablement déjà couvertes par des stratégies de sauvegarde existantes. Cependant, il est également probable que d'importants volumes de données sensibles ne soient pas couverts. En les associant à des systèmes de sauvegarde avancés via l'intégration d'API, les équipes de sécurité peuvent facilement analyser les lacunes de la couverture de la sauvegarde, puis prendre les mesures nécessaires pour ajouter ces sources de données aux stratégies de sauvegarde de votre entreprise. À la clé : une sécurité plus résiliente et moins de risques.
- **Fréquence optimisée des sauvegardes et des rétentions en fonction de la criticité des données dans les magasins de données sauvegardés par Cohesity.**
- **Restauration prioritaire des données en fonction de leur criticité pour l'activité.**
- **Analyse « juste à temps » des preuves d'incident lié aux données, ce qui rationalise le processus de réponse aux incidents (et améliore donc les temps de réponse).** Les copies sauvegardées des données offrent un environnement riche pour l'activité de DSPM, lui permettant de mettre en lumière et de protéger des données auparavant « sombres ».
- **Meilleure conformité aux exigences réglementaires telles que le RGPD et la norme SEC 8-K, qui exigent d'informer rapidement les autorités réglementaires ou les personnes concernées.**

3. Réponse aux incidents et restauration complètes

Il est essentiel d'avoir une stratégie solide de réponse aux incidents et de restauration pour minimiser l'impact des incidents de sécurité sur l'entreprise. Voyons maintenant en détails comment utiliser les données de sauvegarde pour renforcer la réponse aux incidents et garantir une restauration sécurisée.

Détection des ransomwares, des attaques de type wiper et des menaces internes

Les schémas de données et les activités utilisateur inhabituels dans les opérations de sauvegarde et de restauration peuvent être les signes avant-coureurs d'une attaque potentielle. Ces anomalies peuvent déclencher des alertes qui accélèrent les efforts de tri et d'investigation, et ainsi permettre aux équipes de répondre plus rapidement.

Réponse aux ransomwares

Les personnes chargées de répondre aux incidents peuvent utiliser les données de sauvegarde immuables comme des ressources dotées d'une solide chaîne de contrôle. Cela leur permet de rechercher des preuves dans le système de fichiers, de découvrir les artefacts, et d'identifier les modifications malveillantes que des ransomwares et attaques de type wiper pourraient avoir apporté aux configurations et autres fichiers. En utilisant un système de sauvegarde avancé, il est possible d'effectuer cette analyse sur une série de snapshots conservés au fil du temps afin de mieux comprendre le déroulement de l'attaque.

Les intervenants peuvent également rechercher des IOC passivement dans des copies de sauvegarde stockées dans un environnement sécurisé et isolé sans que les cybercriminels susceptibles d'être encore actifs sur le réseau ne viennent les perturber ou ne soient alertés. Les données de sauvegarde peuvent également révéler que d'anciennes vulnérabilités ont été exploitées lors de l'attaque. Elles fournissent ainsi un contexte précieux pour réduire la surface d'attaque et éviter de nouvelles attaques. Aujourd'hui, la majorité des opérateurs de ransomware exploitent les vulnérabilités existantes pour s'introduire sur vos systèmes (les exploits étant ensuite intégrés aux plateformes RaaS en quelques jours). Si vous ne les corrigez pas avant de restaurer vos systèmes, vous risquez non seulement que le même cybercriminel lance de nouvelles attaques, mais également que des milliers d'autres affiliés utilisant la plateforme RaaS fassent de même.

Les sauvegardes immuables sont des copies de données qui ne peuvent être ni altérées, ni supprimées. Cette immuabilité garantit que les données de sauvegarde restent intactes et peuvent être récupérées même si les données primaires sont compromises par un ransomware.

Atténuation des ransomwares

Les attaques par ransomware constituent une menace croissante pour les entreprises de toutes tailles. Lorsqu'une telle attaque se produit, posséder des sauvegardes sécurisées et fiables peut transformer un événement potentiellement catastrophique en une perturbation mineure. Bien que cela puisse sembler évident, il est important de revenir sur ce point tant le nombre d'entreprises qui ne profitent pas des mesures de sécurité de base est important. Ces mesures sont les suivantes :

- **Sauvegardes immuables et renforcement du système** : en combinant des snapshots de sauvegarde immuables avec des principes comme le WORM (Write Once, Read-Many) et le Zero Trust (notamment l'accès au moindre

privilège, l'authentification multifacteur, le chiffrement des données et la séparation des tâches), vous empêchez vos données de sauvegarde de devenir une cible.

- **Sauvegardes par air-gap** : les sauvegardes par air gap sont physiquement isolées du réseau, offrant ainsi une couche de sécurité supplémentaire. Ainsi, même en cas de violation du réseau, les sauvegardes sont protégées des attaques par ransomware.
- **Planification de sauvegarde régulières** : mettre en œuvre des plannings de sauvegarde réguliers permet de s'assurer que les données sont constamment mises à jour et protégées. Plus les sauvegardes sont fréquentes, moins l'entreprise perdra de données en cas d'attaque.
- **Cloner des systèmes** pour effectuer des tests de pénétration complets sans risque pour la production.
- **Exercices réalistes de bout en bout** : Ne vous contentez plus d'exercices théoriques, faites des simulations à grande échelle pour tester de bout en bout et améliorer en permanence les personnes, les processus et les technologies. Clonez vos systèmes de production et soumettez l'ensemble de l'équipe à des scénarios impliquant du chiffrement ou de la destruction pour être sûr de tester tous les aspects de la réponse et de la restauration. Ainsi, lorsque votre entreprise sera confrontée pour la première fois à une véritable cyberattaque destructrice, vos équipes sauront déjà comment réagir.

Tests et exercices

Il est essentiel de régulièrement faire des tests et des exercices pratiques pour s'assurer que le processus de sauvegarde et de restauration est efficace et que toutes les parties prenantes savent exactement quoi faire en cas d'incident.

- **Exercices de reprise après sinistre** : organiser régulièrement des exercices de reprise après sinistre permet de simuler des scénarios concrets pour que l'équipe puisse s'entraîner et affiner ses procédures de réponse. Ces exercices permettent d'identifier les faiblesses potentielles et les domaines à améliorer.
- **Tests automatisés** : les tests automatisés des données de sauvegarde permettent de vérifier l'intégrité et la capacité de récupération des sauvegardes sans intervention manuelle. Cette automatisation permet de s'assurer que les sauvegardes sont fiables et qu'elles peuvent être restaurées rapidement en cas de besoin.
- **Documentation et manuels** : conserver une documentation détaillée et des manuels de restauration permet de s'assurer que chacun connaît ses responsabilités et les étapes à suivre en cas d'incident. Il est recommandé de mettre régulièrement à jour ces manuels en fonction des résultats des tests et des exercices.

Surveillance rigoureuse et création de rapports détaillés

Pour que la réponse aux incidents et la restauration soient efficaces, il faut une surveillance rigoureuse et une création de rapports détaillés qui permettent de confirmer que les opérations de sauvegarde se déroulent sans heurt et que les éventuels problèmes sont rapidement résolus.

- **Surveillance en temps réel** : surveiller les processus de sauvegarde en temps réel permet de détecter et de résoudre immédiatement toute défaillance ou problème afin d'éviter une perte potentielle de données.
- **Alertes automatisées** : les alertes automatisées informent l'équipe informatique de toute irrégularité ou défaillance dans le processus de sauvegarde pour lui permettre d'intervenir et de corriger rapidement la situation.
- **Création de rapports complets** : des rapports détaillés sur l'état des sauvegardes, les taux de réussite et les temps de restauration permettent d'évaluer l'efficacité de la stratégie de sauvegarde et de mettre en évidence les points à améliorer. En mettant en œuvre ces stratégies de sauvegarde avancées, les RSSI peuvent s'assurer que leurs entreprises sont capables de répondre aux incidents et de restaurer rapidement et efficacement leurs activités. Cette approche complète permet non seulement de minimiser les temps d'arrêt et les pertes de données, mais aussi de renforcer la résilience globale de l'entreprise face aux menaces à venir.

4. Intégrité et conformité des données

Garantir l'intégrité et la conformité des données aux exigences réglementaires est une préoccupation essentielle pour les entreprises, en particulier dans le domaine de la cybersécurité. Les données de sauvegarde jouent un rôle déterminant à cet égard, car elles constituent une source d'information unique, fiable et vérifiable, qui peut être utilisée pour auditer, vérifier et restaurer l'intégrité des données. Voici comment les données de sauvegarde peuvent contribuer à améliorer l'intégrité et la conformité des données.

Conformité réglementaire

Les entreprises sont soumises à de nombreux cadres réglementaires qui imposent des exigences strictes en matière de protection et d'intégrité des données. Les données de sauvegarde permettent de se conformer à ces réglementations et d'apporter la preuve de cette conformité en fournissant une piste d'audit et en encourageant la rétention des données.

- **Pistes d'audit :** les solutions de sauvegarde peuvent conserver des journaux complets de toutes les activités de sauvegarde et de restauration. Ces journaux sont très utiles en cas d'audit de conformité, car ils permettent de savoir en détails qui a accédé aux données, à quel moment, et quelles actions ont été menées.
- **Stratégies de rétention des données :** il est souvent nécessaire d'adhérer à des stratégies de rétention des données strictes pour pouvoir respecter des réglementations telles que le RGPD, l'HIPAA et la loi SOX. Les solutions de sauvegarde automatisées permettent de faire appliquer ces stratégies en veillant à ce que les données soient conservées pendant la durée requise et supprimées de manière sécurisée lorsqu'elles ne sont plus nécessaires.

Stockage de données sécurisé et contrôle d'accès

Il est fondamental de protéger les données de sauvegarde contre tout accès non autorisé et de les stocker de manière sécurisée pour garantir l'intégrité et la conformité des données.

- **Chiffrement** : chiffrer les données de sauvegarde au repos et en transit les sécurise contre tout accès non autorisé. Les informations sensibles sont protégées par des protocoles de chiffrement puissants afin que personne ne puisse les lire sans les clés de déchiffrement appropriées.
- **Contrôles d'accès basé sur les rôles (RBAC)** : mettre en œuvre le RBAC permet de garantir que seules les personnes autorisées peuvent accéder aux données de sauvegarde. Ce contrôle limite l'exposition et réduit le risque de violation ou d'utilisation abusive des données.
- **Authentification multifacteur (MFA)** : mettre en œuvre la MFA pour accéder aux systèmes de sauvegarde ajoute une couche de sécurité supplémentaire. Ainsi, même si les identifiants sont compromis, il est impossible d'accéder aux données sans autorisation.

Reprise après sinistre et plan de continuité de l’activité

Une stratégie de conformité complète repose sur une reprise après sinistre et un plan de continuité de l'activité efficaces. Grâce aux données de sauvegarde, les entreprises peuvent rapidement restaurer leur activité en cas de perturbation et poursuivre leurs opérations sans que cela ait trop d'impact.

- **Bilan d’impact sur l’activité (BIA)** : un bilan d'impact sur l'activité permet aux entreprises de comprendre l'impact potentiel d'une perte ou d'une corruption de données sur leurs opérations. Les données de sauvegarde jouent un rôle crucial dans ce bilan, car elles fournissent un moyen fiable de restaurer les systèmes et les données critiques.
- **Objectif de délai de restauration (RTO) et objectif de point de restauration (RPO)** : les entreprises qui ont des objectifs de RTO et de RPO clairs peuvent restaurer leurs données dans des délais acceptables et avec un minimum de pertes de données. Les solutions de sauvegarde doivent être conçues pour répondre à ces objectifs.
- **Plan de continuité** : les données de sauvegarde sont indispensables à tout plan de continuité, car elles permettent aux entreprises de poursuivre leurs activités pendant et après un sinistre. Tester régulièrement les plans de reprise après sinistre en utilisant les données de sauvegarde permet d'améliorer l'efficacité et la fiabilité des processus de restauration.

Dans l'environnement réglementaire complexe d'aujourd'hui, il est essentiel de garantir l'intégrité et la conformité des données pour maintenir la confiance et la fiabilité des opérations. En exploitant efficacement leurs données de sauvegarde, les entreprises peuvent répondre aux exigences réglementaires, protéger l'intégrité de leurs données et maintenir des mesures de sécurité solides. Pour atteindre ces objectifs, les entreprises peuvent mettre en œuvre des solutions de sauvegarde avancées qui fournissent des pistes d'audit complètes, appliquent des stratégies de rétention des données, et proposent un stockage sécurisé et des contrôles d'accès. Elles peuvent ainsi sereinement s'appuyer sur des bases solides pour poursuivre leur croissance et développer leur résilience.

5. Visibilité et contrôle améliorés

Pour un responsable de la sécurité des systèmes d'information (RSSI), il est essentiel d'améliorer la visibilité et le contrôle des données et des processus de sauvegarde d'une entreprise afin de maintenir une sécurité robuste et une gestion des données efficace. En utilisant des solutions de sauvegarde avancées, les RSSI peuvent obtenir des informations complètes sur leur environnement de données, rationaliser les processus de gestion et mieux protéger les informations critiques. Découvrez comment améliorer la visibilité et le contrôle en utilisant efficacement les données de sauvegarde.

Gestion centralisée

Une approche de gestion centralisée consolide les opérations de sauvegarde. Elle permet ainsi de superviser à partir d'un seul endroit toutes les activités de sauvegarde dans l'ensemble de l'entreprise. Cette centralisation simplifie le processus de gestion et garantit la cohérence des pratiques en matière de protection des données.

- **Tableau de bord unifié** : un tableau de bord unifié offre une vue globale de l'ensemble de l'environnement de sauvegarde, notamment l'état des tâches de sauvegarde, l'utilisation du stockage et les problèmes potentiels. Cette visibilité en temps réel permet aux RSSI de surveiller efficacement l'état et les performances des sauvegardes.
- **Administration simplifiée** : les outils de gestion centralisée permettent de gérer plus facilement plusieurs systèmes et sites de sauvegarde. Simplifier l'administration rend les opérations plus efficaces et réduit le risque de mauvaises configurations ou d'erreurs.
- **Application de la stratégie** : un contrôle centralisé permet d'appliquer les stratégies de protection des données de manière cohérente dans toute l'entreprise. il est possible d'appliquer uniformément les stratégies de rétention des données, de chiffrement et de contrôle d'accès pour améliorer la conformité et la sécurité.

Rapports détaillés et analyses complètes

Créer des rapports détaillés et faire des analyses complètes permet d'obtenir des informations précieuses sur les opérations de sauvegarde dont les RSSI peuvent se servir pour prendre des décisions éclairées et optimiser leurs stratégies de protection des données.

- **Journaux d'audit** : des journaux d'audit détaillés permettent de suivre l'ensemble des accès et des activités liés aux données de sauvegarde. Ces journaux permettent de savoir qui a accédé aux données, quelles actions ont été effectuées, et à quel moment. Ils facilitent ainsi la surveillance de la sécurité et les audits de conformité.
- **Rapports personnalisables** : les outils de création de rapports personnalisables permettent aux RSSI de générer des rapports adaptés à des besoins spécifiques, notamment les exigences de conformité, les performances opérationnelles ou les audits de sécurité. Ces rapports offrent une vision claire et complète des activités de sauvegarde.
- **Analyse des tendances** : analyser les tendances des données de sauvegarde, notamment les schémas de croissance des données, l'utilisation du stockage et les temps de restauration, permet d'identifier les tendances à long terme et les domaines potentiellement préoccupants. Cette analyse facilite la planification stratégique et l'affectation des ressources.
- **Connaissances des données** : les outils d'analyse avancés peuvent fournir des connaissances plus approfondies sur les données de sauvegarde, notamment identifier les systèmes ou les départements qui génèrent le plus de données, les données les plus critiques et les vulnérabilités potentielles. Ces informations permettent de prendre des mesures de protection des données plus ciblées et plus efficaces.

Les RSSI peuvent s'assurer que les données de leur entreprise sont protégées, conformes et facilement disponibles en cas de restauration en adoptant des solutions de sauvegarde avancées qui offrent une gestion centralisée, un contrôle d'accès amélioré, une surveillance en temps réel, la création de rapports complets et l'automatisation. Ces capacités renforcent non seulement la posture de sécurité globale, mais fournissent également les informations et le contrôle nécessaires pour optimiser les stratégies de protection des données et soutenir la réussite à long terme de l'entreprise.

6. Informations stratégiques et prises de décision

Dans le domaine de la cybersécurité, il est essentiel de pouvoir prendre des décisions stratégiques pour gérer efficacement les ressources, anticiper les défis à venir et maintenir une posture de sécurité robuste. Les données de sauvegarde sont souvent sous-utilisées. Elles peuvent pourtant fournir des informations précieuses qui permettent de prendre des décisions éclairées et de renforcer la stratégie de sécurité globale d'une entreprise. Dans les sections précédentes, nous avons vu dans quels domaines le contexte historique permettait d'analyser les tendances pour détecter les menaces ou mieux comprendre le comportement de base en matière d'utilisation des données. Cette section explique comment les données de sauvegarde peuvent nous permettre d'obtenir des informations stratégiques sur la santé de l'entreprise.

Allocation des ressources optimisée

Il est essentiel d'allouer efficacement les ressources pour optimiser les investissements dans la sécurité. Les données de sauvegarde fournissent des informations détaillées sur les systèmes et les données les plus critiques. Les entreprises peuvent ainsi hiérarchiser leurs efforts de sécurité et allouer les ressources là où elles sont le plus nécessaires.

- **Identification des données critiques** : les données de sauvegarde permettent d'identifier les données et les systèmes essentiels au fonctionnement de l'entreprise. Comprendre la criticité des différents jeux de données permet aux entreprises de hiérarchiser leurs efforts de protection et de restauration.
- **Gestion des coûts** : analyser les schémas de stockage et d'utilisation des données de sauvegarde peut permettre d'identifier des pistes de réduction des coûts. Les entreprises peuvent optimiser leurs solutions de stockage, éliminer les données redondantes et réduire les coûts globaux de stockage tout en continuant à protéger leurs données.
- **Hiérarchisation des ressources** : les informations sur les données de sauvegarde permettent aux entreprises de concentrer leurs ressources sur les domaines les plus vulnérables ou à plus forte valeur ajoutée. Cette approche ciblée signifie que les ressources les plus critiques bénéficient du niveau de protection le plus élevé.

Informations stratégiques sur les entreprises

Au-delà de la sécurité et de la conformité, les données de sauvegarde peuvent également fournir des informations stratégiques qui soutiennent les objectifs plus larges de l'entreprise.

- **Efficacité opérationnelle** : analyser les données de sauvegarde peut révéler des inefficacités dans la gestion des données et les processus opérationnels. Les entreprises peuvent utiliser ces informations pour rationaliser les opérations, réduire les redondances et améliorer l'efficacité globale.
- **Utilisation des données** : comprendre comment les données sont utilisées dans l'entreprise permet de trouver des façons de mieux les utiliser et les gérer. Les informations tirées des données de sauvegarde peuvent éclairer les décisions relatives à l'archivage des données, à la gestion du cycle de vie et aux stratégies d'accès.
- **Innovation et croissance** : les données de sauvegarde peuvent révéler des tendances et des schémas qui favorisent l'innovation et la croissance de l'entreprise. En analysant l'évolution des données au fil du temps, les entreprises peuvent identifier de nouvelles opportunités, optimiser les processus et piloter des initiatives stratégiques.

En exploitant les données de sauvegarde pour obtenir des informations stratégiques et prendre des décisions, l'entreprise est plus à même de gérer efficacement ses ressources, d'anticiper les menaces, d'y répondre, et de rester en conformité avec les réglementations en vigueur. Les RSSI peuvent favoriser l'amélioration continue, optimiser l'allocation des ressources et soutenir la réussite à long terme de l'entreprise en intégrant les données de sauvegarde dans les stratégies opérationnelles plus larges. Les solutions de sauvegarde avancées qui proposent de solides capacités d'analyse, de création de rapports et d'automatisation permettent aux entreprises de libérer tout le potentiel de leurs données, et de les transformer en une ressource précieuse pour la planification stratégique et la prise de décision.

Conclusion

Les RSSI du monde entier sont confrontés à un défi de taille : protéger les données de leurs entreprises des menaces sophistiquées tout en se conformant à des réglementations strictes. Les meilleures solutions de sauvegarde ne se contentent pas d'assurer la reprise après sinistre, elles réduisent également les risques liés à la conformité et à la sécurité. Elles sont désormais indispensables pour bénéficier d'une cyberassurance de qualité.

Les systèmes de sauvegarde avancés sont un élément essentiel de la « défense en profondeur » et, en effet, la dernière ligne de défense d'une entreprise en cas de cyberincident. Déplacer efficacement et de manière sécurisée de gros volumes de données sensibles vers un stockage rentable, que ce soit dans le cloud ou en local, et définir un objectif de délai de restauration (RTO) réduit le risque de perte de données, de temps d'arrêt opérationnel et d'atteinte à la réputation de l'entreprise. Optimiser et exploiter cette technologie permet aux RSSI de renforcer la résilience, l'agilité et la valeur commerciale à long terme de leur entreprise dans un monde numérique de plus en plus complexe.

En savoir plus sur Cohesity.com/fr/

COHESITY

cohesity.com/fr
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

2000053-002-FR 4-2025