Les 4 meilleures façons de sécuriser vos données pour garantir une restauration propre et fiable

Les données sont exposées à de nombreuses menaces, qu'il s'agisse de cyberattaques, de pannes matérielles ou de catastrophes naturelles. Une stratégie de sauvegarde robuste et multicouche protège vos données, garantit la continuité de l'activité, réduit le risque de perte de données et renforce votre posture de sécurité globale.

Voici quatre mesures de posture de sécurité qui vous permettront de garantir que vos données sont toujours saines et récupérables.

1. Mettez en œuvre un contrôle d'accès et une authentification

- **Assurez-vous que seuls les utilisateurs autorisés peuvent accéder à vos données.** Il est essentiel d'ajouter une couche de sécurité supplémentaire pour se protéger contre les menaces internes et externes. Activer l'authentification multifacteur (MFA) partout est un moyen efficace de vous protéger contre ces menaces tout en conservant vos stratégies existantes de gestion des identités et des accès.
- **Limitez l'accès et les autorisations en fonction des rôles des utilisateurs.** Appliquez le contrôle d'accès basé sur les rôles (RBAC) pour fournir un accès et des autorisations limités et granulaires aux utilisateurs de votre environnement de sauvegarde en fonction de leur rôle spécifique. Cela permet de garantir que chaque personne dispose uniquement des privilèges d'accès minimaux nécessaires à l'exercice de ses responsabilités.

2. Privilégiez la protection et l'intégrité des données

- **Mettez en œuvre un coffre-fort de données immuable.** Utilisez Cohesity NetBackup Flex Appliance ou Cohesity FortKnox pour bénéficier d'un stockage sécurisé, inviolable et immuable en local ou dans le cloud, et ainsi protéger vos données contre toute altération.
- Mettez en œuvre une stratégie de sauvegarde 3-2-1 pour les charges de travail critiques. Conserver trois copies des données sur deux supports différents, avec au moins une copie stockée hors site sur un support immuable et ineffaçable, garantit la redondance des données et vous assure qu'elles sont toujours récupérables.
- Empêchez l'exfiltration des données grâce à un chiffrement robuste. Protégez vos données contre tout accès non autorisé pendant leur transmission et leur stockage. Utilisez un chiffrement robuste pour toutes vos données, qu'elles soient stockées en local ou dans le cloud, afin d'empêcher tout accès non autorisé et tout vol de données.

3. Tirez parti de la surveillance et de la détection de la sécurité

- Utilisez l'automatisation pour détecter intelligemment les menaces utilisateur. Notre moteur de risque adaptatif surveille en permanence le comportement des utilisateurs afin de détecter toute activité suspecte. Dès qu'elle détecte une anomalie ou

une action suspecte de la part d'un utilisateur, la plateforme déclenche automatiquement des mesures de sécurité (notamment l'authentification multifacteur) afin de verrouiller l'accès aux données de sauvegarde.

- Accélérez l'identification des menaces et votre réponse. Cohesity offre des capacités de recherche rapide des menaces. Celles-ci recherchent de manière proactive les indicateurs de compromission et répondent aux menaces. Nous proposons également une analyse complète du champ d'action des zones affectées dans l'ensemble de l'environnement. Celle-ci est jusqu'à 93 % plus rapide que l'analyse traditionnelle des logiciels malveillants.

4. Renforcez la configuration de votre système

- **Créez un digital jump bag.**™ Un digital jump bag est un référentiel protégé et fiable qui offre un accès rapide aux outils nécessaires à l'acquisition et à l'analyse à distance. Il contient les outils, les logiciels, les fichiers de configuration et la documentation nécessaires pour répondre à un incident dans un magasin sécurisé et immuable, hors de portée des cybercriminels.
- **Réduisez l'exposition du réseau**. Mettez en place des contrôles d'accès au réseau afin de restreindre l'accès réseau aux systèmes et données de sauvegarde et d'empêcher tout accès non autorisé. Segmentez facilement votre réseau et créez un environnement de salle blanche pour renforcer la sécurité et minimiser l'impact de toute violation potentielle.
- **Mettez en œuvre une restauration des données en salle blanche**. Créez un environnement séparé et sécurisé pour les opérations de recherche de preuves et de restauration afin de minimiser le risque de contamination.
- **Maintenez tous les systèmes et logiciels à jour**. Mettez régulièrement à jour vos logiciels et installez les correctifs de sécurité afin de bénéficier de nouvelles fonctionnalités et de mesures de sécurité améliorées.

Partagez ces lignes directrices avec votre équipe et encouragez-la à mettre en œuvre ces mesures essentielles pour protéger les données de votre entreprise et renforcer votre posture de sécurité.

Vous trouverez des blueprints et des bonnes pratiques pour concevoir un environnement de sauvegarde pour votre entreprise dans le document *Topologies modernes de sécurité et de gestion des données : un guide pour les responsables informatiques*.

COHESITY

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

9100085-001-FR 6-2025