5 bonnes pratiques pour trouver et sécuriser les données sensibles

Pour gérer davantage de données à plusieurs endroits, il est essentiel de savoir où elles se trouvent (et de les protéger correctement) pour optimiser votre posture en matière de risques liés aux données. Suivez ces 5 bonnes pratiques pour trouver et sécuriser vos données sensibles.

1. Découvrez toutes vos données, y compris vos données secondaires

Utilisez la classification basée sur l'IA pour détecter toutes les données de votre parc informatique, notamment les fichiers, les sauvegardes, les archives et les environnements cloud. Cette visibilité proactive vous permettra d'éviter les surprises en mettant en évidence les copies cachées et les référentiels inconnus.

Pourquoi c'est important :

Les zones d'ombre dans les sauvegardes, les archives ou les snapshots peuvent dissimuler des données sensibles et aggraver les dommages en cas de violation.

Avantage pour vous :

Avoir une visibilité totale vous permet de réduire l'exposition des données et d'éviter les failles de conformité avant qu'une attaque ne se produise.

2. Autorisez une classification automatisée et très précise

Utilisez la correspondance de modèles basée sur l'IA pour réduire les faux positifs (lorsque des données non sensibles sont classées à tort comme sensibles) et identifier plus précisément les données sensibles contextuelles dans les DCP, les PHI, les PCI, la propriété intellectuelle et d'autres catégories critiques.

Pourquoi c'est important :

La classification automatisée garantit l'évolutivité et la cohérence des jeux de données en constante expansion.

Avantage pour vous :

Vous gagnerez du temps, améliorerez la précision et ferez évoluer la protection des données sans ajouter de tâches manuelles.

3. Marquez les données avec des métadonnées contextuelles

Enrichissez vos données sensibles avec des métadonnées (notamment des étiquettes de classification, des balises de localisation et des informations sur la propriété) afin de les trier plus rapidement et de répondre plus efficacement en cas de violation potentielle.

Pourquoi c'est important :

Marquer automatiquement les données existantes et nouvelles avec des métadonnées permet d'évaluer les risques plus rapidement et plus précisément.

Avantage pour vous :

Vous pouvez agir rapidement et en toute confiance lorsque des incidents surviennent, car vous avez des informations plus claires sur les risques encourus.

4. Classez les données à risque élevé par degré d'exposition et de sensibilité

Signalez les éléments sensibles qui sont particulièrement exposés (par exemple, les dossiers partagés, les compartiments de stockage d'objets, les copies de sauvegarde non sécurisées) ou essentiels à la conformité. Concentrez vos efforts de protection sur les zones les plus à risque.

Pourquoi c'est important :

Toutes les données ne présentent pas le même niveau de risque, donc vous ne devez pas toutes les protéger de la même manière. Comparez vos données à une devise. Certaines données correspondent à une pièce d'un euro, d'autres à un billet de 100 euros.

Avantage pour vous :

Une fois que vous aurez ciblé vos efforts de protection, vous réduirez le temps passé à répondre aux incidents.

5. Intégrez la classification à la réponse aux incidents

En cas d'incident ou de violation, utilisez immédiatement les informations de classification pour identifier quelles données sensibles ont été affectées et respecter les obligations réglementaires.

Pourquoi c'est important :

Savoir quelles données sensibles ont été touchées permet d'accélérer la recherche de preuves, d'évaluer les risques avec plus de précision et d'améliorer la création de rapports de conformité.

Avantage pour vous :

Vous pouvez évaluer les dommages potentiels pendant une cyberattaque et rationaliser la création de rapports réglementaires en toute confiance.

Suivez ces 5 bonnes pratiques pour identifier et classer les données sensibles, et vous serez sur la bonne voie pour optimiser votre posture de risque lié aux données.

Prêt à approfondir la classification de vos données grâce à des intégrations alimentées par un API ? Lisez le blog intitulé La nouvelle intégration de la DSPM avec Cyera montre la puissance des API ouvertes.

COHESITY

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

9100086-001-FR 6-2025