

FICHE SOLUTION

Proofpoint Data Security Posture Management pour Snowflake

Sécurisez votre environnement DPaaS (Data Platform-as-a-Service) en pleine expansion.

Principaux avantages

- Visibilité sur les données à grande échelle
- Application du principe du moindre privilège
- Réduction de la surface d'attaque
- Conformité continue

Snowflake a transformé la façon dont les entreprises gèrent les charges de travail de Big Data. Il les aide à collecter, stocker et analyser d'importants volumes de données de manière plus économique. Cependant, pour les équipes responsables de la sécurité et des données, Snowflake complique la gestion des mouvements et de la classification des données, ainsi que de l'accès à celles-ci. Ces défis augmentent les risques de compromissions et de problèmes de gouvernance.

Proofpoint Data Security Posture Management (DSPM) maximise la valeur de votre investissement Snowflake. Il simplifie la façon dont les équipes responsables de la sécurité et des données fournissent aux utilisateurs

les données dont ils ont besoin. Il résout des problèmes tels que la croissance rapide des données, la complexité de leur classification et les privilèges d'accès trop élevés. Il garantit également une conformité et une gouvernance continues, que les outils inadéquats de gestion des risques n'offrent pas.

En plus de ses fonctionnalités de base, Proofpoint DSPM s'intègre parfaitement à l'AI Data Cloud de Snowflake, vous permettant ainsi de tirer parti des fonctionnalités de sécurité et de conformité de Snowflake Horizon. Avec Proofpoint, vous bénéficiez d'un contrôle accru sur votre environnement Snowflake, avec pour résultat une accélération de l'adoption des technologies Snowflake et de fonctionnalités avancées telles que l'IA.

Cette suite de solutions fait partie de la plateforme Human-Centric Security intégrée de Proofpoint et vise à réduire les quatre catégories clés de risques liés aux utilisateurs.

Sécurité et gouvernance des données

Prise en charge de la gouvernance des accès

- Visibilité et contrôle

Fonctionnalités uniques

- Contexte des données
- Gouvernance de l'accès aux données
- Conformité des données

La nécessité d'une gouvernance continue des accès et d'une classification des données à grande échelle

Snowflake offre une flexibilité et une évolutivité exceptionnelles. Cependant, ces avantages se traduisent également par une multiplication des mouvements de données, des structures d'accès complexes et un partage excessif de données. Les équipes responsables de la sécurité et des données peuvent donc se retrouver face à certains défis :

Conflit entre l'octroi d'un accès et la prévention des risques – Si les équipes responsables des données ont pour mission d'octroyer aux utilisateurs un accès à d'importants ensembles de données, les équipes de sécurité doivent s'assurer que ces utilisateurs n'accèdent qu'aux données qu'ils sont autorisés à consulter et à utiliser.

Incapacité à classer les données – L'afflux rapide de données non structurées complique singulièrement la classification continue. Les équipes de sécurité peinent à appliquer des contrôles d'accès et à surveiller les utilisateurs qui pourraient essayer d'accéder à des données stratégiques ou sensibles.

Dissimulation des données stratégiques ou sensibles – Les données non structurées, telles que les blobs JSON et les résultats générés par l'IA, compliquent l'identification de l'emplacement des données stratégiques ou sensibles, ce qui rend l'accès aux données et leur contrôle plus difficiles.

Les fonctionnalités uniques de Proofpoint DSPM

Dans les environnements Snowflake, les difficultés associées à la gestion des mouvements et de la classification des données, ainsi que de l'accès à celles-ci augmentent le risque de compromissions de données et de problèmes de

gouvernance. Proofpoint DSPM résout ces défis grâce à des fonctionnalités uniques :

Identification continue et classification précise – Bénéficiez d'une visibilité totale sur les données critiques à tout moment. L'analyseur en un seul passage de Proofpoint DSPM permet une identification rapide et continue ainsi qu'une classification précise de vos données. Aucune configuration ni aucun ajustement manuel ne sont nécessaires.

Gouvernance des accès – Appuyez-vous sur des graphiques dynamiques détaillés pour voir comment vos collaborateurs et vos ressources accèdent aux données. Identifiez qui a accès à des banques de données spécifiques et déterminez si ces personnes disposent des autorisations appropriées. Identifiez les utilisateurs inactifs, mal configurés ou surprovisionnés. Assurez-vous que les utilisateurs ne peuvent accéder qu'aux données nécessaires.

Gestion des identifiants de connexion – Identifiez les utilisateurs qui ont accès à des données stratégiques et sensibles, mais qui ne sont pas soumis à certaines mesures de sécurité indispensables (comme l'authentification multifactor). Appliquez des règles d'authentification plus strictes à ces utilisateurs.

Gestion des risques – Identifiez les voies d'attaque susceptibles d'entraîner des compromissions ou des fuites de données. Examinez des graphiques en temps réel qui hiérarchisent vos risques en fonction de la valeur des données et de la probabilité de succès des attaques. Attribuez une valeur monétaire à vos données, avec des classements conçus pour aider les équipes responsables de la sécurité et des données à évaluer les conséquences de fuites de données potentielles. Réduisez votre surface d'attaque et réduisez vos coûts de stockage en identifiant les données abandonnées. Surveillez en permanence les activités anormales, comme les pics inattendus de téléchargements de données ou les accès à partir d'emplacements inhabituels. Utilisez ces informations pour résoudre les problèmes à haut risque plus rapidement.

Conformité des données – Anticipez les défis liés aux réglementations et réduisez les risques grâce à des outils avancés conçus pour prendre en charge des protocoles de conformité rigoureux tels que les normes ISO 27001, SOC 2 et PCI DSS, le CSF 2.0 du NIST et le CIS Benchmark de Snowflake.

Architecture d'analyse sur site – Ayez une confiance totale dans la sécurité de vos données. Proofpoint DSPM s'exécute sous la forme d'une application native à Snowflake et déploie des analyseurs au sein de votre environnement. Vous avez ainsi l'assurance que vos données ne quittent jamais votre périmètre sécurisé.

Maximisez la valeur de votre investissement Snowflake

En optimisant les workflows de vos équipes responsables des données et de la sécurité, Proofpoint DSPM vous aide à maximiser la valeur de votre investissement Snowflake.

Optimisation de l'utilisation des technologies Snowflake – Grâce à Proofpoint DSPM, l'utilisation des données est plus sécurisée pour un large éventail d'utilisateurs au sein de votre entreprise. Les clients de Snowflake peuvent ainsi tirer davantage parti de la pile technologique Snowflake, y compris de ses fonctionnalités d'IA.

Réduction du nombre d'inconnues – Proofpoint DSPM supprime les points de friction entre les équipes responsables des données et de la sécurité en rationalisant le processus d'octroi de niveaux d'accès appropriés aux utilisateurs. Vous avez ainsi l'assurance que vos données sont à la fois accessibles et protégées.

Contextualisation des exigences en matière de Zero Trust et de conformité – Proofpoint DSPM prend en charge la mise en œuvre d'un modèle Zero Trust et d'autres cadres de sécurité en classant avec précision les données stratégiques et sensibles et en gérant efficacement l'accès des utilisateurs.



Proofpoint, Inc. est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risque des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris 85 % des entreprises du classement Fortune 100, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via la messagerie, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur www.proofpoint.com/fr.

Suivez-nous : [LinkedIn](#)

Proofpoint est une marque commerciale de Proofpoint, Inc. aux États-Unis et dans d'autres pays. Toutes les autres marques citées dans ce document sont la propriété de leurs détenteurs respectifs. ©Proofpoint, Inc. 2025

DÉCOUVRIR LA PLATE-FORME PROOFPOINT →