

Dépannage du blocage des données des formulaires DLP en temps réel pour toutes les destinations

Table des matières

[Introduction](#)

[Informations générales](#)

[Dépannage](#)

[Conclusion](#)

Introduction

Ce document décrit comment résoudre les problèmes liés à la configuration d'une règle DLP (Data Loss Protection) en temps réel pour bloquer toutes les données de formulaire.

Informations générales

Lors de la configuration d'une règle DLP en temps réel pour bloquer toutes les données de formulaire, il existe un risque que les vrais positifs et les faux positifs entraînent des conséquences imprévues pour les applications cloud. Ces conséquences peuvent avoir un impact sur le bon fonctionnement des applications cloud, notamment sur la possibilité que les utilisateurs ne puissent pas utiliser la page de connexion. Cet article vise à souligner ces risques et à fournir des étapes de dépannage pour résoudre les problèmes qui peuvent survenir.

Dépannage

En cas de problème lié au blocage de toutes les données de formulaire dans les règles DLP en temps réel, ces étapes peuvent aider à résoudre le problème :

1. Affiner les identificateurs de données : cette étape permet de trouver un équilibre entre le blocage efficace des données sensibles et la transmission sans interruption des données de formulaire légitimes.
 - Consultez les détails des événements DLP bloqués via le rapport Data Loss Prevention (Reporting > Additional Reports > Data Loss Prevention) pour identifier les identificateurs de données spécifiques déclenchant la règle DLP.
 - Envisagez d'affiner les identificateurs de données en ajustant les niveaux de tolérance ou en ajoutant des termes de proximité afin de réduire les faux positifs tout en conservant leur capacité à correspondre selon les besoins.

2. Exclure les URL bloquées : en excluant les URL, vous pouvez vous assurer que les pages de connexion et les autres composants essentiels de vos applications ne sont pas affectés par la règle DLP bloquante.
 - Analysez le journal d'activité via Activity Search (Reporting > Core Reports > Activity Search) et les détails de l'événement DLP pour identifier les URL qui sont bloquées.
 - Ajoutez ces URL à une liste de destinations configurée sous « Sélectionner les listes de destinations et les applications à exclure ».
3. Modifier le comportement de la règle DLP - Si les problèmes persistent et que les conséquences imprévues l'emportent sur les avantages du blocage de toutes les données de formulaire, vous devez modifier le comportement de la règle DLP pour arrêter l'analyse des données de formulaire. Il est possible de modifier le comportement en sélectionnant simplement « Téléchargements de fichiers et données de formulaire des applications contrôlées uniquement ».

Conclusion

Lors de la configuration d'une règle DLP en temps réel pour bloquer toutes les données de formulaire, il est essentiel de connaître les risques associés aux conséquences imprévues. Ces risques peuvent avoir un impact sur le bon fonctionnement des applications cloud, notamment sur la possibilité d'utiliser la page de connexion. Suivez les étapes de dépannage décrites dans ce guide pour limiter ces risques et assurer le bon fonctionnement de vos applications cloud tout en préservant la protection des données.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.