Configurer DLP pour empêcher l'utilisation de données sensibles par ChatGPT

Table des matières

Introduction

Ce document décrit comment utiliser Data Loss Prevention (DLP) pour protéger les données sensibles contre l'utilisation de ChatGPT.

Aperçu

Le monde de l'intelligence artificielle bourdonne, avec des innovations comme le modèle de langage d'OpenAI, ChatGPT, qui mène la charge. Cette puissance de l'IA se développe à un rythme effréné, transformant de nombreux secteurs grâce à ses conversations intelligentes et contextuelles. Mais ces avancées prometteuses s'accompagnent de défis potentiels, en particulier les risques de perte de données.

Considérez ChatGPT comme un partenaire de conversation super intelligent qui génère du texte en fonction de ce que vous lui fournissez. Désormais, s'il y a des informations sensibles dans la combinaison et qu'elles ne sont pas traitées correctement, il y a un risque de violation des données. Cela souligne pourquoi il est si important de disposer d'un plan complet de prévention des pertes de données (DLP).

Votre solution Umbrella DLP a été conçue pour protéger votre entreprise contre ces risques. Voici trois cas d'utilisation urgents que notre solution peut vous aider à résoudre immédiatement et dont la mise en oeuvre ne prend qu'environ 5 minutes.

A. Conformité aux réglementations sur la confidentialité des données telles que le RGPD, la HIPPA et la norme PCI-DSS :

1. Accédez à Politiques > Gestion > Politique de prévention de la perte de données dans votre tableau de bord Umbrella.
2. Commencez à créer une nouvelle règle DLP. Cliquez simplement sur Add Rule en haut à droite et sélectionnez Real Time Rule.
3. Donnez à votre règle un nom facile à reconnaître, comme « ChatGPT Protection », et choisissez le niveau de gravité (de Faible à Critique) qui correspond à vos besoins.
4. Dans la section Classifications, sélectionnez une ou plusieurs des classifications de conformité intégrées pertinentes pour votre organisation. Il peut s'agir par exemple de la « classification GDPR intégrée » ou de la « classification PCI intégrée ».
5. Dans la section Identités, sélectionnez toutes les identités que vous souhaitez

surveiller et protéger. Si possible, nous recommandons un large choix pour une couverture complète.
6. Passez à la section Destinations, sélectionnez Listes de destinations et applications à inclure, puis choisissez OpenAI ChatGPT.
7. Il est maintenant temps d'agir. Dans la section Action, vous pouvez choisir de Surveiller ou de Bloquer. Si vous n'êtes pas familiarisé avec cette fonctionnalité, nous vous recommandons de commencer par l'action « Surveiller ». Cela vous permet d'observer les modèles d'utilisation et de prendre une décision plus éclairée sur les risques et les avantages potentiels.
8. Si vous avez choisi l'action « Surveiller », assurez-vous de récupérer le rapport DLP après une semaine ou un mois. Vous voyez qui partage des informations sensibles avec ChatGPT et quand, et vous aide à décider si une action 'Bloquer' est nécessaire.

B. Protection des informations d'identification personnelle (PII) : Pour protéger les informations d'identification personnelle de votre organisation contre les risques de ChatGPT, suivez les mêmes instructions que ci-dessus, mais à l'étape 4, sélectionnez la « Classification intégrée des informations d'identification personnelle » au lieu des classifications de conformité.

C. Protection du code source et de la propriété intellectuelle : Si votre organisation utilise ChatGPT pour des activités impliquant du code source ou d'autres éléments de propriété intellectuelle, procédez comme suit :

1. Commencez par créer une nouvelle classification des données de code source. Accédez à Politiques > Gestion > Composants de la politique > Classification des données. Cliquez sur le bouton Add en haut à droite et donnez à votre classification de données un nom reconnaissable, comme « Source Code Classification ».
2. Sélectionnez Code source dans la liste des identificateurs de données intégrés.
3. Cliquez sur Save.
4. Après l'enregistrement, consultez à nouveau les instructions relatives à la « Conformité aux réglementations sur la confidentialité des données » ci-dessus, mais à l'étape 4, choisissez votre classification des données de code source nouvellement créée au lieu des classifications intégrées.

Le processus est simple et ne prend que quelques minutes de votre temps, mais les avantages pour la sécurité et la conformité de votre entreprise sont inestimables. Nous vous invitons à prendre ces mesures dès que possible pour renforcer votre protection des données.

Vous voulez en savoir plus sur les risques d'IA générative et comment Umbrella peut vous protéger, regardez le webinaire Protégez vos données sensibles de l'utilisation de ChatGPT.

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.