

DLP configureren om gevoelige gegevens te beschermen tegen gebruik door ChatGPT

Inhoud

[Inleiding](#)

[Overzicht](#)

Inleiding

In dit document wordt beschreven hoe u Data Loss Prevention (DLP) kunt gebruiken om gevoelige gegevens te beschermen tegen gebruik door ChatGPT.

Overzicht

De wereld van kunstmatige intelligentie bruist, met innovaties zoals het taalmodel van OpenAI, ChatGPT, die de leiding hebben. Deze AI-krachtpatser groeit razendsnel en transformeert tal van industrieën met zijn slimme, contextbewuste gesprekken. Maar met deze opwindende vooruitgang komen enkele potentiële uitdagingen - met name risico's op gegevensverlies.

Denk aan ChatGPT als een super-slimme gesprekspartner die tekst genereert op basis van wat u het voedt. Als er nu gevoelige informatie in de mix zit en deze niet goed wordt behandeld, bestaat het risico op datalekken. Dit benadrukt waarom het zo belangrijk is om een uitgebreid plan voor de preventie van gegevensverlies (DLP) te hebben.

Uw Umbrella DLP-oplossing is ontworpen om uw organisatie tegen deze risico's te beschermen. Hier zijn drie dringende use-cases die onze oplossing u kan helpen onmiddellijk aan te pakken en slechts ongeveer 5 minuten in beslag nemen om te implementeren.

A. Naleving van privacyregels zoals GDPR, HIPPA en PCI-DSS:

1. Ga naar **Beleid > Beheer > Beleid** ter voorkoming van gegevensverlies in uw overkoepelende dashboard.
2. Maak een nieuwe DLP-regel. Klik rechtsboven op **Regel toevoegen** en selecteer **Realtime regel**.
3. Geef uw regel een naam die gemakkelijk te herkennen is, zoals 'ChatGPT Protection', en kies het prioriteitsniveau (van laag tot kritisch) dat bij uw behoeften past.
4. Kies in het gedeelte **Classificaties** een of meer van de ingebouwde nalevingsclassificaties die relevant zijn voor uw organisatie. Dit kan bijvoorbeeld de 'Ingebouwde GDPR-classificatie' of 'Ingebouwde PCI-classificatie' zijn.
5. Selecteer in het gedeelte **Identiteiten** alle identiteiten die u wilt bewaken en beschermen. Indien mogelijk, raden we een brede selectie aan voor uitgebreide dekking.
6. Ga naar de sectie **Bestemmingen**, selecteer **Bestemmingslijsten** en toepassingen voor

opname en kies vervolgens OpenAI ChatGPT.

7. Nu is het tijd voor actie. In de sectie Actie kunt u kiezen voor Monitor of Blokkeren. Als u hier nieuw in bent, raden we u aan te beginnen met de actie 'Monitor'. Hierdoor kunt u gebruikspatronen observeren en een beter geïnformeerde beslissing nemen over de potentiële risico's en voordelen.
8. Als u de actie 'Monitor' hebt gekozen, moet u het DLP-rapport na een week of een maand bekijken. Dit laat u zien wie gevoelige informatie deelt met ChatGPT en wanneer, zodat u kunt beslissen of een 'Block'-actie vereist is.

Bescherming van persoonlijk identificeerbare informatie (PII): Om de PII in uw organisatie te beschermen tegen ChatGPT-risico's, gebruikt u gewoon dezelfde instructies als hierboven, maar in stap 4 selecteert u de 'Ingebouwde PII-classificatie' in plaats van de nalevingsclassificaties.

C. Bescherming van broncode en intellectuele eigendom: Als uw organisatie ChatGPT gebruikt voor activiteiten met broncode of ander intellectueel eigendom, gebruikt u deze stappen:

1. Maak eerst een nieuwe classificatie van broncodegegevens. Ga naar Beleid > Beheer > Beleidscomponenten > Gegevensclassificatie. Klik rechtsboven op de knop Toevoegen en geef uw gegevensclassificatie een herkenbare naam, zoals 'Broncode Classificatie'.
2. Kies Broncode uit de lijst met ingebouwde gegevensidentificatoren.
3. Klik op Save (Opslaan).
4. Na het opslaan, herzie de instructies voor 'Compliance with Data Privacy Regulations' hierboven, maar kies in stap 4 uw nieuw gemaakte broncode gegevensclassificatie in plaats van de ingebouwde.

Het proces is eenvoudig en kost slechts een paar minuten van uw tijd, maar de voordelen voor de beveiliging en naleving van uw organisatie zijn van onschatbare waarde. Wij raden u aan om deze stappen zo snel mogelijk te nemen om uw gegevensbescherming te versterken.

Wil je meer weten over Generatieve AI-risico's en hoe Umbrella je kan beschermen, bekijk dan het webinar [Bescherm je gevoelige gegevens tegen ChatGPT-gebruik](#).

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.