

DLP- en CASB-ondersteuning configureren voor generatieve AI en ChatGPT

Inhoud

[Inleiding](#)

[Overzicht](#)

Inleiding

Dit document beschrijft Cloud Access Security Broker (CASB) en Data Loss Prevention (DLP) ondersteuning voor Generative AI en ChatGPT.

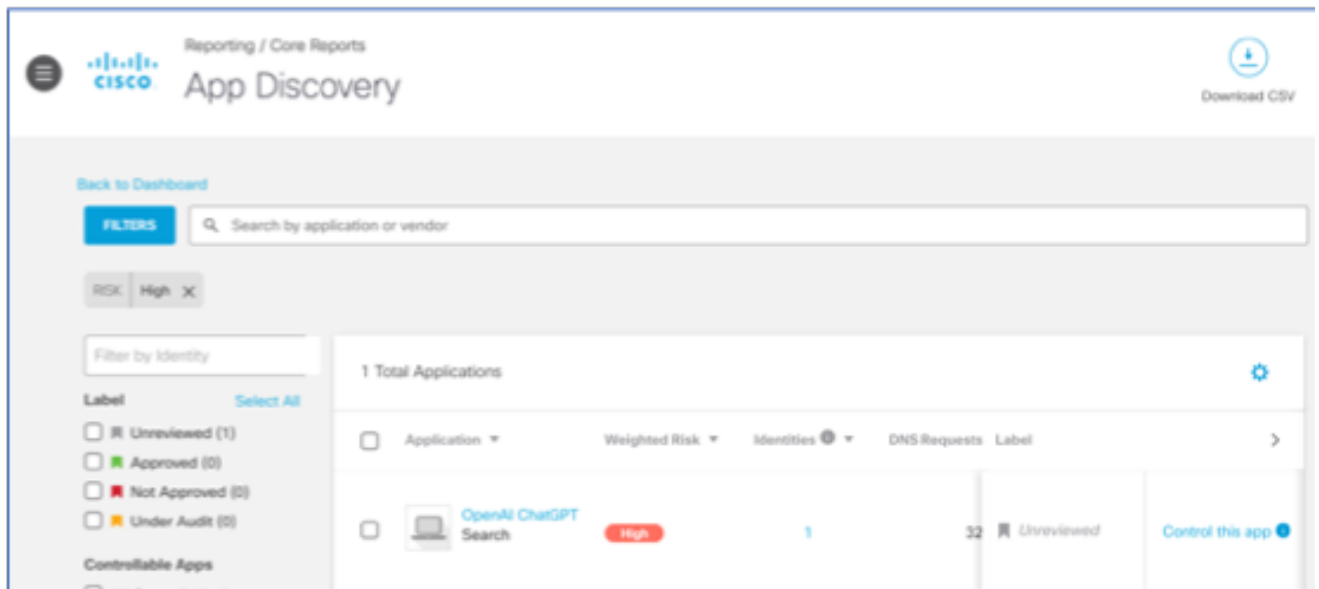
Overzicht

We hebben nieuwe Cloud Access Security Broker (CASB) en Data Loss Prevention (DLP) verbeteringen uitgebracht aan onze Umbrella productsuite, ontworpen om klanten te helpen het gebruik van ChatGPT binnen hun organisaties effectiever te beheren.

Deze verbeteringen stellen onze klanten in staat om ervoor te zorgen dat hun werknemers ChatGPT op een verantwoorde en veilige manier gebruiken en tegelijkertijd gevoelige informatie beschermen tegen potentiële risico's.

Hier zijn de belangrijkste kenmerken:

1. Het ontdekken van ChatGPT-gebruik in de organisatie:
Met behulp van het App Discovery-rapport (Rapporten -> Kernrapporten) kunnen klanten het gebruik van ChatGPT in hun hele organisatie identificeren en controleren.
Dit geeft hen waardevolle inzichten in hoe de medewerkers de tool gebruiken, waardoor ze het gebruik ervan kunnen optimaliseren en ervoor kunnen zorgen dat ze voldoen aan hun interne beleid.



16221272854164



16221291406100

2. Granulaire controle over ChatGPT-toegang:

Klanten kunnen nu de toegang tot ChatGPT voor iedereen blokkeren of alleen toegang verlenen aan specifieke gebruikers of groepen gebruikers.

Deze gedetailleerde controle helpt om het gebruik van ChatGPT te beheren in overeenstemming met de beveiligings- en nalegingsvereisten. Blokkering is mogelijk via zowel DNS- als webbeleid door openAI ChatGPT binnen toepassingsinstellingen te selecteren.

Default Settings

Applied To
DNS Policy

Items Allowed
0

Items Blocked
7

Last Modified
Mar 02, 2023

Give Your Setting a Name

Default Settings

Applications To Control

chatgpt

☐ OpenAI ChatGPT

CANCEL

SAVE

My Application settings

Applied To
Web Policy

Last Modified
Feb 23, 2023

Give Your Setting a Name

My Application settings

Applications To Control

chatgpt

☐ OpenAI ChatGPT

DELETE

CANCEL

SAVE

16221268217748

3. Beoordeling van het gebruiksrisico van ChatGPT met DLP:

Real Time DLP stelt klanten nu in staat om het type gevoelige informatie te controleren dat wordt verzonden en gedeeld met ChatGPT. Dit helpt bij het beoordelen van het risico dat gepaard gaat met het gebruik van ChatGPT en het nemen van passende maatregelen om potentiële datalekken of -inbreuken te beperken.

Om DLP-monitoring voor ChatGPT mogelijk te maken, kunnen klanten realtime-regels gebruiken met de bestemming ingesteld op Alle bestemmingen of openAI ChatGPT kiezen specifiek uit de lijst met beschikbare toepassingen.

Advanced Search

Identity

Search Identities

File Owner

Search File Owners

Destination URL

Search Destination URLs

Application

Search Applications

APPLICATION OpenAI ChatGPT X

Tenant

Search Tenants

Rule

ChatGPT

RULES

ChatGPT

2023 at 10:14 AM

Name	Destination	Rule	Action
Form	OpenAI ChatGPT	ChatGPT	Blocked
Form	OpenAI ChatGPT	ChatGPT	Blocked
Form	OpenAI ChatGPT	ChatGPT	Blocked
Form	OpenAI ChatGPT	ChatGPT	Blocked
Form	OpenAI ChatGPT	ChatGPT	Monitored
Form	OpenAI ChatGPT	ChatGPT	Monitored
Form	OpenAI ChatGPT	ChatGPT	Monitored
Form	OpenAI ChatGPT	ChatGPT	Monitored
Form	OpenAI ChatGPT	ChatGPT	Monitored
Form	OpenAI ChatGPT	ChatGPT specific	Blocked
Form	OpenAI ChatGPT	ChatGPT	Monitored

Results

16221283948052

4. Veilig gebruik van ChatGPT met DLP:
- Door onze DLP-oplossing te gebruiken, kunnen klanten nu vragen naar ChatGPT blokkeren die gevoelige informatie bevatten. Dit zorgt ervoor dat medewerkers veilig en beveiligd ChatGPT kunnen blijven gebruiken, zonder de organisatie bloot te stellen aan potentiële risico's.
- Om DLP-blokkering voor ChatGPT in te schakelen, kunnen klanten realtime-regels gebruiken met de bestemming ingesteld op Alle bestemmingen of openAI ChatGPT kiezen specifiek uit de lijst met beschikbare toepassingen.



16221311959572

5. Lekken van broncode naar ChatGPT voorkomen met DLP:

Met een nieuwe broncode data identifier kunnen klanten DLP gebruiken om het delen van broncode met ChatGPT in de gaten te houden en te stoppen, waardoor hun waardevolle intellectuele eigendom (IP) wordt beschermd.

6. NIEUWE categorie Generatieve AI-toepassingen:

Een nieuwe Generative AI-applicatiecategorie werd geïntroduceerd om gebruiksdetectie en -preventie voor een breder scala aan tools aan te pakken.

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.