Configuración del soporte de DLP y CASB para IA generativa y ChatGPT

Contenido

Introducción

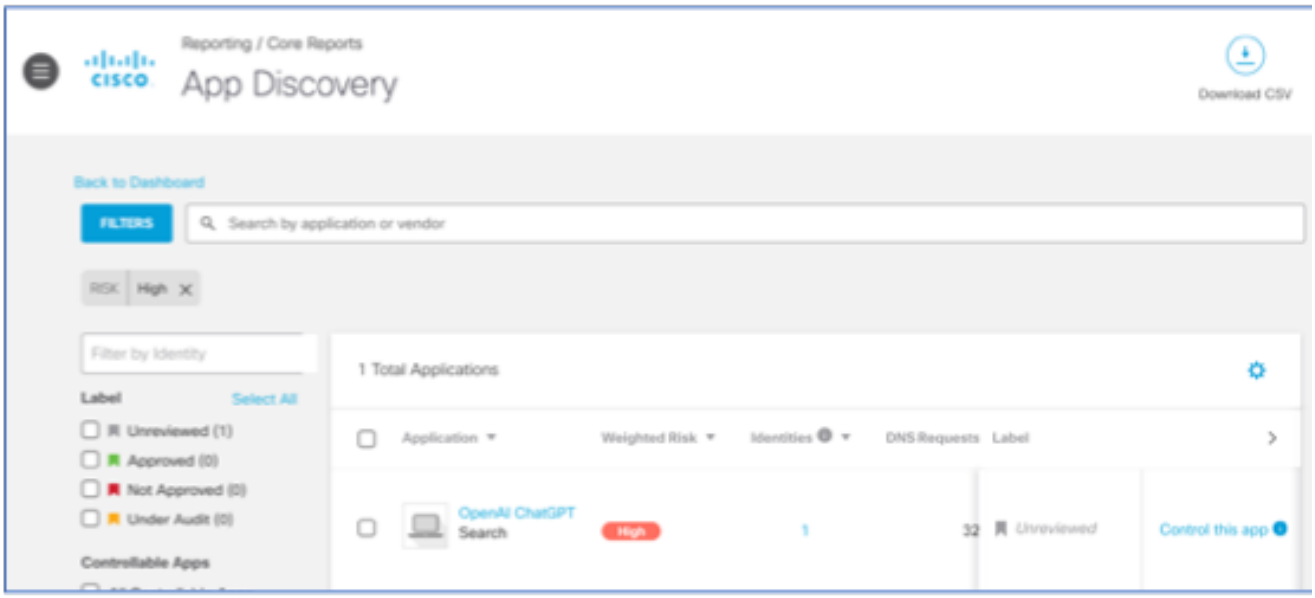
Este documento describe el soporte de Cloud Access Security Broker (CASB) y Data Loss Prevention (DLP) para Generative AI y ChatGPT.

Overview

Hemos lanzado nuevas mejoras en Cloud Access Security Broker (CASB) y Data Loss Prevention (DLP) a nuestro conjunto de productos Umbrella, diseñadas para ayudar a los clientes a gestionar el uso de ChatGPT en sus organizaciones de forma más eficaz.
Estas mejoras permiten a nuestros clientes garantizar que sus empleados utilizan ChatGPT de forma responsable y segura, al tiempo que protegen la información confidencial frente a posibles riesgos.

Estas son las características clave:

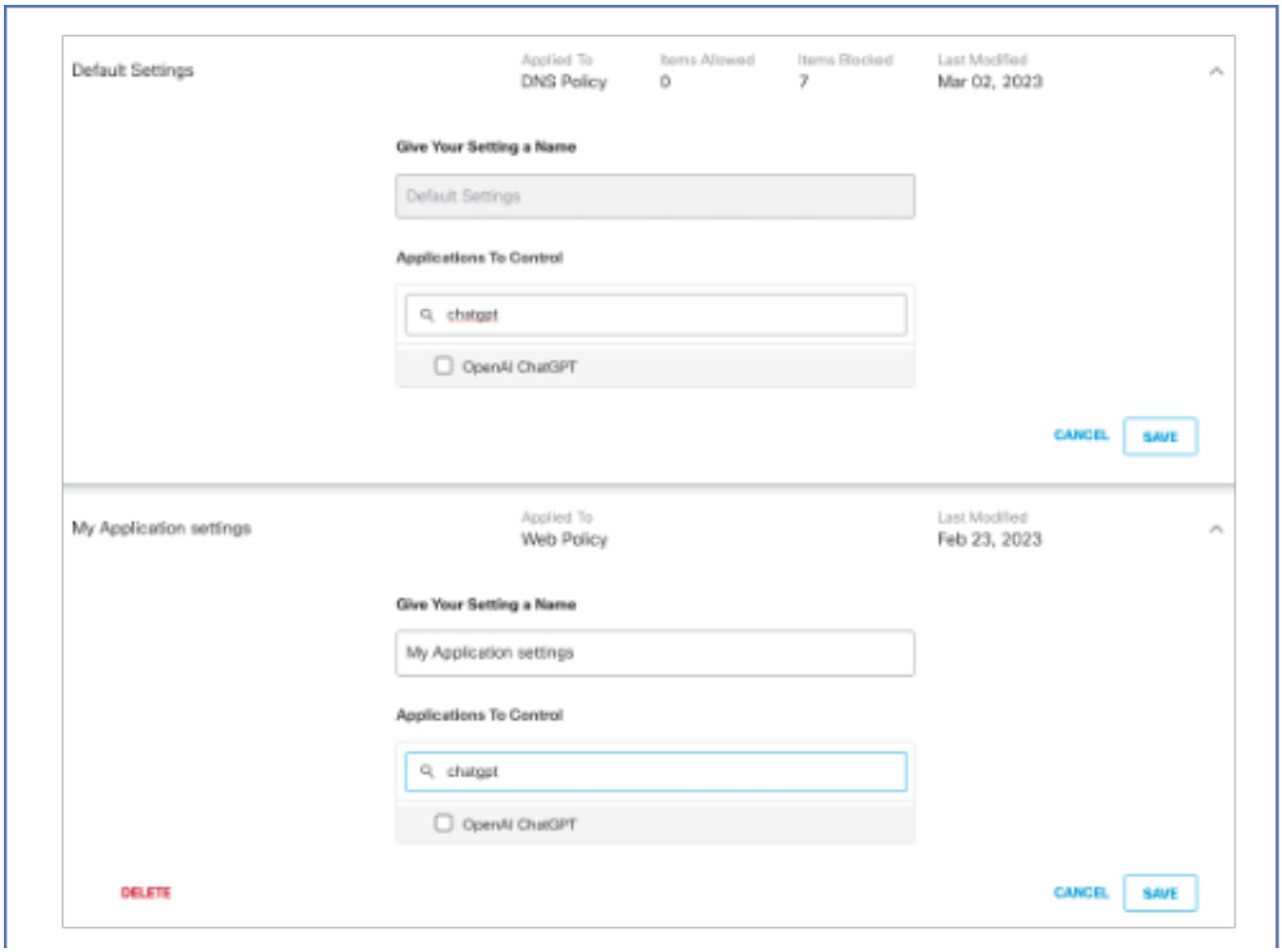
1. Descubrimiento del uso de ChatGPT en la organización:
   Mediante el informe de App Discovery (Informes -> Informes principales), los clientes pueden identificar y supervisar el uso de ChatGPT en su organización.
   Esto les proporciona información valiosa sobre el uso que hacen los empleados de la herramienta, lo que les permite optimizar su uso y garantizar el cumplimiento de sus políticas internas.



16221272854164

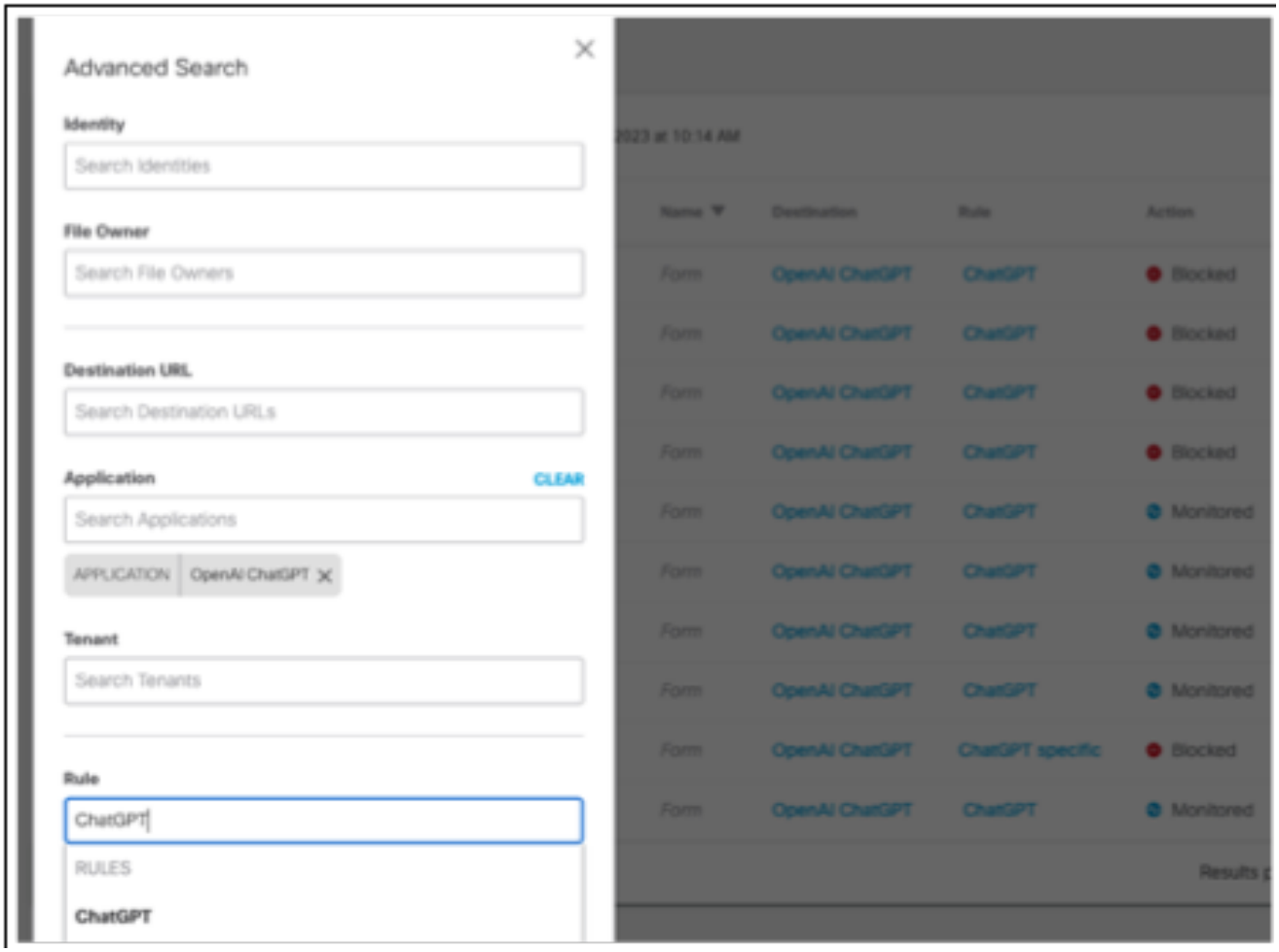
16221291406100

2. Control granular del acceso a ChatGPT:
   Los clientes ahora pueden bloquear el acceso a ChatGPT para todos o permitir el acceso solo a usuarios específicos o grupos de usuarios.
   Este control granular ayuda a administrar el uso de ChatGPT en línea con los requisitos de seguridad y cumplimiento. El bloqueo es posible a través de las políticas de DNS y Web seleccionando openAI ChatGPT en Configuración de la aplicación.



16221268217748

3. Evaluación del riesgo de uso de ChatGPT con DLP:
   Real Time DLP ahora permite a los clientes supervisar el tipo de información confidencial que se envía y comparte con ChatGPT. Esto ayuda a evaluar el riesgo asociado con el uso de ChatGPT y a tomar las medidas adecuadas para mitigar las filtraciones o brechas de datos potenciales.
   Para habilitar la supervisión de DLP para ChatGPT, los clientes pueden utilizar reglas en tiempo real con el destino establecido en Todos los destinos o elegir openAI ChatGPT específicamente de la lista de aplicaciones disponibles.



16221283948052

4. Permitir el uso seguro de ChatGPT con DLP:
   Gracias a nuestra solución de DLP, los clientes pueden bloquear ahora las solicitudes a ChatGPT que contengan información confidencial. Esto garantiza que los empleados puedan seguir utilizando ChatGPT de forma segura, sin exponer a la organización a riesgos potenciales.
   Para habilitar el bloqueo de DLP para ChatGPT, los clientes pueden utilizar reglas en tiempo real con el destino establecido en Todos los destinos o elegir openAI ChatGPT específicamente de la lista de aplicaciones disponibles.

16221311959572

5. Prevención de la fuga de código fuente a ChatGPT con DLP:
   Con un nuevo identificador de datos de código fuente, los clientes pueden utilizar DLP para vigilar y detener el uso compartido de código fuente con ChatGPT, protegiendo su valiosa propiedad intelectual (IP).

6. NUEVA categoría de aplicación de IA generativa:
   Se introdujo una nueva categoría de aplicaciones de IA generativa para abordar el descubrimiento y la prevención del uso de una gama más amplia de herramientas.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).