Configuración de DLP para proteger los datos confidenciales del uso de ChatGPT

Contenido

Introducción

En este documento se describe cómo utilizar la prevención de pérdida de datos (DLP) para evitar que ChatGPT utilice datos confidenciales.

Overview

El mundo de la inteligencia artificial está zumbando, con innovaciones como el modelo de lenguaje de OpenAI, ChatGPT, liderando la carga. Esta potencia de la IA ha crecido a un ritmo vertiginoso, transformando numerosos sectores con sus conversaciones inteligentes y contextuales. Pero con estos emocionantes avances surgen algunos retos potenciales, en concreto, los riesgos de pérdida de datos.

Piense en ChatGPT como un partner de conversación superinteligente que genera texto en función de lo que le proporcione. Ahora, si hay información confidencial en la mezcla y no se maneja correctamente, existe el riesgo de que se produzcan violaciones de datos. Esto pone de manifiesto la importancia de contar con un plan integral de prevención de la pérdida de datos (DLP).

La solución Umbrella DLP se ha diseñado para proteger a su organización frente a estos riesgos. A continuación se indican tres casos prácticos urgentes que nuestra solución puede ayudarle a abordar de inmediato y cuya implementación solo le llevará unos 5 minutos.

A. Cumplimiento de las regulaciones de privacidad de datos como GDPR, HIPPA y PCI-DSS:

1. Vaya a Políticas > Gestión > Política de prevención de pérdida de datos en el panel de Umbrella.
2. Comience a crear una nueva regla DLP. Solo tiene que hacer clic en Agregar regla en la parte superior derecha y seleccionar Regla en tiempo real.
3. Dé a su regla un nombre fácil de reconocer, como 'Protección ChatGPT', y elija el nivel de gravedad (desde Bajo a Crítico) que se adapte a sus necesidades.
4. En la sección Clasificaciones, seleccione una o varias de las clasificaciones de conformidad integradas relevantes para su organización. Esta podría ser la 'Clasificación de GDPR integrada' o la 'Clasificación de PCI integrada', por ejemplo.
5. En la sección Identidades, seleccione todas las identidades que desea supervisar y proteger. Si es factible, recomendamos una amplia selección para una cobertura

completa.

6. Pase a la sección Destinos, seleccione Listas de Destinos y Aplicaciones para Inclusión, y luego elija OpenAI ChatGPT.
7. Ha llegado el momento de actuar. En la sección Acción, puede elegir entre Supervisar o Bloquear. Si es nuevo en esto, le recomendamos que empiece con la acción "Supervisar". Esto le permite observar los patrones de uso y tomar una decisión más informada sobre los riesgos y beneficios potenciales.
8. Si ha seleccionado la acción "Supervisar", asegúrese de retirar el informe de DLP después de una semana o un mes. Muestra quién comparte información confidencial con ChatGPT y cuándo, lo que le ayuda a decidir si se requiere una acción de bloqueo.

B. Protección de la información de identificación personal (PII): Para proteger la PII de su organización frente a los riesgos de ChatGPT, siga las mismas instrucciones que las anteriores, pero en el paso 4, seleccione la "Clasificación de PII integrada" en lugar de las clasificaciones de conformidad.

Protección del Código Fuente y de la Propiedad Intelectual: Si su organización utiliza ChatGPT para actividades que implican código fuente u otra propiedad intelectual, siga estos pasos:

1. En primer lugar, cree una nueva clasificación de datos de código fuente. Vaya a Políticas > Gestión > Componentes de política > Clasificación de datos. Haga clic en el botón Add en la parte superior derecha y dé a su clasificación de datos un nombre reconocible, como "Clasificación de código fuente".
2. Elija Código fuente de la lista de Identificadores de datos integrados.
3. Click Save.
4. Después de guardar, vuelva a consultar las instrucciones de "Cumplimiento de la normativa de privacidad de datos" anteriores, pero en el paso 4, elija la recién creada clasificación de datos de código fuente en lugar de las incorporadas.

El proceso es sencillo y solo le llevará unos minutos, pero las ventajas para la seguridad y el cumplimiento de su organización son inestimables. Le instamos a que tome estas medidas lo antes posible para reforzar su protección de datos.

Si desea obtener más información sobre los riesgos de la IA generativa y cómo Umbrella puede protegerle, vea el seminario web Proteja sus datos confidenciales del uso de ChatGPT.

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).