safetica

Protección de IA

Proteja los datos confidenciales mientras permite un uso productivo de la IA

La IA generativa está transformando la forma en que trabajan los empleados, al tiempo que crea nuevas vías de riesgo para la exposición de datos confidenciales. A medida que aumenta el uso de herramientas de IA, tanto aprobadas como no autorizadas, los equipos de seguridad necesitan una visibilidad que vaya más allá de saber qué herramientas se utilizan. Deben comprender quién utiliza la IA, qué datos confidenciales se comparten y dónde se necesita protección adicional, sin limitar los beneficios de productividad que ofrece la IA.

Obtenga el control sin bloquear el acceso a herramientas de IA

Safetica AI Protection proporciona visibilidad sobre la actividad de IA y el intercambio de datos confidenciales, junto con controles granulares que protegen los datos y permiten a los empleados utilizar la IA de forma productiva.

Con Safetica, los equipos de seguridad pueden:

Detectar el uso de herramientas de IA

aprobadas y no autorizadas en toda la organización para comprender qué aplicaciones utilizan los empleados.

Ver los datos confidenciales en su contexto

incluido quién los comparte, adónde se envían y cómo se utilizan.

Proteger los datos antes de que lleguen a la IA

mediante políticas DLP, controlando archivos confidenciales, contenido pegado, prompts y acciones de usuario de riesgo.

Aplicar controles granulares

en función de la aplicación de IA, la sensibilidad de los datos, el empleado, el departamento y la actividad.

Investigar los riesgos relacionados con la IA con mayor contexto

y determinar la respuesta adecuada en lugar de bloquear por completo el acceso a la IA.

safetica

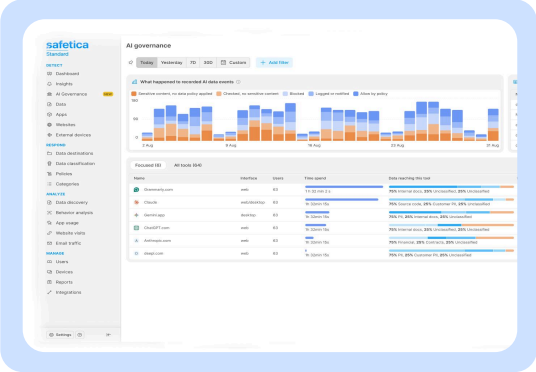
Gobierne el uso de la IA. Proteja los datos confidenciales.

Safetica ofrece una protección de IA por capas que combina la visibilidad sobre el uso de la IA en toda la organización con los controles que los equipos de seguridad necesitan para proteger los datos confidenciales frente a posibles exposiciones y gestionar los riesgos sin afectar a la adopción productiva de la IA.

Gobernanza de IA

Obtenga visibilidad y control a medida que aumenta el uso de la IA por parte de los empleados

Safetica AI Governance ayuda a los equipos de seguridad a comprender y gobernar el uso de herramientas de IA, tanto aprobadas como no autorizadas, proporcionando visibilidad sobre las aplicaciones que utilizan los empleados, los datos que comparten y dónde deben aplicarse controles. Puede:

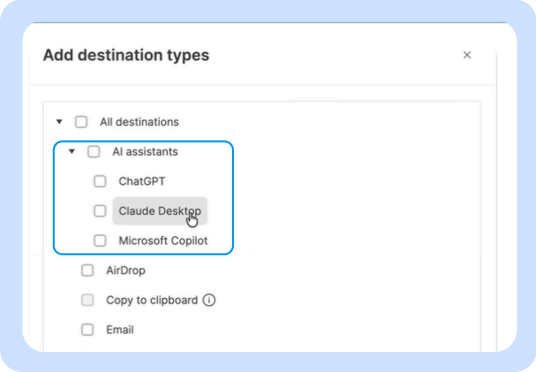


- **Descubrir su entorno de IA.** Mantenga una visión centralizada de las aplicaciones de IA aprobadas y no autorizadas en toda la organización.
- **Comprender la actividad de IA.** Vea quién utiliza la IA, con qué frecuencia se accede a las aplicaciones, qué datos y archivos se comparten y qué medidas de protección existen actualmente.
- **Convertir la visibilidad en control.** Supervise la actividad, restrinja el intercambio de datos confidenciales, limite el acceso de usuarios o grupos específicos o bloquee por completo las herramientas de riesgo.
- **Investigar con contexto.** Utilice prompts integrados y guiados por IA para explorar el uso y los riesgos, resumir los hallazgos e identificar acciones que puedan reforzar la protección.

Políticas de datos para asistentes de IA

Proteja los datos confidenciales antes de que lleguen a la IA

Safetica amplía la protección DLP a los asistentes de IA de uso habitual, ayudando a los equipos de seguridad a controlar la información confidencial compartida mediante archivos adjuntos, contenido copiado y pegado y prompts, al tiempo que permite un uso adecuado de la IA.
Los equipos de seguridad pueden:



- **Proteger los datos confidenciales antes de que lleguen a las herramientas de IA.** Aplique políticas DLP para supervisar y controlar archivos adjuntos confidenciales, texto pegado, prompts y otros datos compartidos con ChatGPT, Claude y Microsoft Copilot.
- **Aplicar controles en función del contexto.** Defina políticas según la sensibilidad de los datos, la herramienta de IA, el empleado, el departamento y la acción específica del usuario, en lugar de bloquear por completo el acceso a la IA.
- **Proteger los datos tanto en aplicaciones como en navegadores.** Mantenga la protección en las aplicaciones de escritorio compatibles y en navegadores basados en Chromium en macOS y Windows.
- **Permitir que continúe el uso productivo de la IA.** Restrinja las acciones de intercambio de datos que supongan un riesgo sin bloquear innecesariamente el acceso productivo a herramientas de IA aprobadas.

Con Safetica, obtiene la visibilidad necesaria para comprender el uso de la IA, el contexto para identificar riesgos reales y el control para proteger los datos confidenciales.

SAFETICA INC
99 S ALMADEN BOULEVARD #600
SAN JOSE, CA 95113

+1 (408) 668 1241
INFO@SAFETICA.COM
SAFETICA.COM