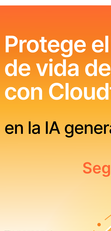
CLOUDFLARE

Acelera la adopción de la IA con el principio de la "seguridad por diseño"

La IA está aquí, y la seguridad tradicional se está quedando obsoleta

El 98 %
de las organizaciones utilizan aplicaciones no autorizadas, incluida la Shadow AI. Estos puntos ciegos corren el riesgo de exponer los datos y de infringir el cumplimiento normativo.[1]

50 %
es la tasa de éxito de los ataques de inyección de prompts, la el principal riesgo de seguridad según OWASP para las aplicaciones LLM.[2]



El 97%
de las organizaciones que experimentan incidentes de seguridad relacionados con la IA carecen de controles de acceso adecuados a la IA.[3]

El 93 %
de los empleados admite haber introducido información en herramientas de IA sin aprobación.[4]

Protege el ciclo de vida de la IA con Cloudflare

en la IA generativa y agéntica

Seguridad de la persona humana a la IA

Seguridad de la IA agéntica

Ampliación de la visibilidad
en todas las aplicaciones de IA, los puntos finales de API y conexiones de agentes de IA y servidores MCP.

Administración del riesgo
con medidas de seguridad, control de postura y mitigación de amenazas en tiempo real.

Protección de los datos
con protección de prompts y controles de acceso para empleados y agentes de IA.

La seguridad está integrada
al desarrollar la IA en Cloudflare

Uso seguro de la IA generativa por parte de los usuarios

- Detección de la Shadow AI
- Evaluar el riesgo de las aplicaciones de IA
- Gestionar el estado de las aplicaciones de IA
- Restringir las entradas de datos confidenciales
- Implementar medidas de seguridad en las solicitudes y las respuestas

Protección de las aplicaciones y cargas de trabajo con IA

- Identificar los puntos finales de la Shadow AI
- Proteger los modelos de IA y los datos de entrenamiento del abuso
- Evitar la exposición de la información de identificación personal en las solicitudes y respuestas
- Implementar la moderación de contenido

Protección para tus desarrollos

- Desarrollar servidores MCP con autenticación o autorización integrada
- Registrar y restringir las solicitudes y respuestas del modelo de IA, el uso de token y los costos
- Evitar las interrupciones del servicio con modelos alternativos y la limitación de velocidad

Las ventajas con Cloudflare

Protección integral del ciclo de vida de la IA
Una plataforma para proteger la comunicación entre el ser humano y la IA y entre la IA y los recursos desde el desarrollo hasta la implementación.

Seguridad de IA en línea y en tiempo real
Protección de las solicitudes y las respuestas de IA en tiempo real con controles que abarcan entornos de IA públicos y privados.

Arquitectura global de IA preparada para el futuro
Nuestra red global brinda la posibilidad de una aplicación perimetral consistente con la escala y el rendimiento que exige la IA.

Implementación independiente del modelo
Los controles de seguridad funcionan para todos los modelos de IA de tu entorno, lo que proporciona un enfoque unificado para controlar las implementaciones de IA.

Casos prácticos

indeed
Sitio web de empleo n.º 1 del mundo
Identifica y controla la Shadow AI
en paralelo con el proyecto de modernización del acceso remoto.

Empresa SaaS con IA
Protege la información de identificación personal
al evitar que los clientes envíen información confidencial a los puntos finales públicos de la IA generativa.

Cyndx
Empresa fintech impulsada por la IA
Logró una reducción de los costos de inferencia en un 95 %
mediante la adopción de Cloudflare para almacenar en caché y ejecutar las respuestas de los proveedores de modelos de IA.

Descubre cómo Cloudflare puede proteger tu adopción de IA

Lee casos de uso

1. Varonis, 2025 State of Data Security
2. Yi, J., Xie, Y., Zhu, B., Kiciman, E., Sun, G., Xie, X., & Liu, Y. (2024). Automatic and Universal Prompt Injection Attacks against Large Language Models.
3. IBM, 2025 Cost of a Data Breach
4. ManageEngine, The Shadow AI Surge in Enterprises

+55 (11) 3230 45231 | enterprise@cloudflare.com | www.cloudflare.com/es-LA

REV:BDES-4216.2025OCT17

CLOUDFLARE