

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

La IA ya ha llegado, y la seguridad tradicional se va quedando atrás



El 98 %

de las organizaciones usa aplicaciones no autorizadas, incluidos elementos de Shadow IA. Estos "puntos ciegos" suponen un riesgo de exposición de datos y de incumplimiento normativo.¹

50%

Tasa de éxito en los ataques de inyección de instrucciones, el principal riesgo de seguridad según OWASP para aplicaciones LLM.²



El 97 %

de las organizaciones que experimentan incidentes de seguridad relacionados con la IA carece de controles de acceso apropiados para la IA.³



El 93 %

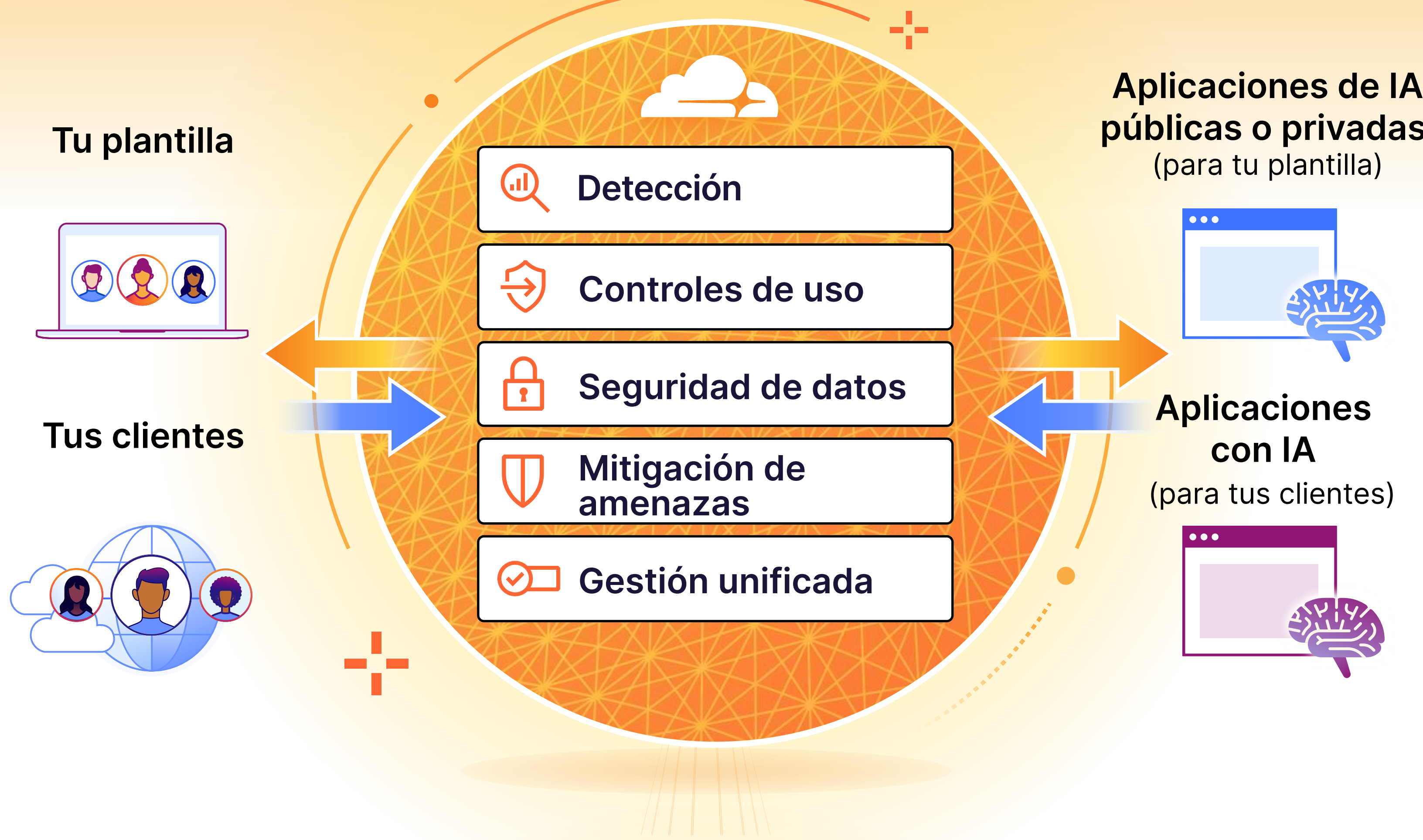
de los empleados admite incluir información en herramientas de IA sin autorización.⁴



Protege el ciclo de vida de la IA con Cloudflare

en la IA generativa y agéntica

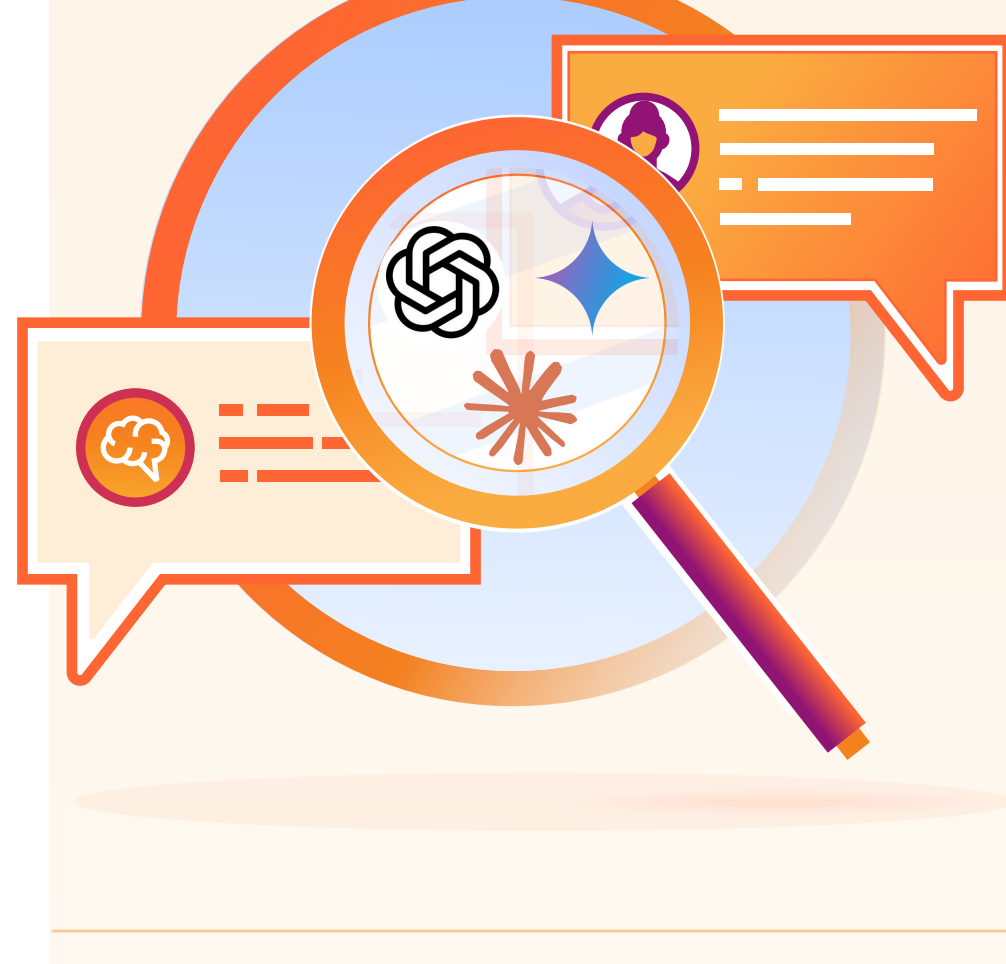
Seguridad humano-IA



Seguridad de la IA agéntica



La seguridad está integrada en el desarrollo de la IA en Cloudflare



Protege la utilización de la IA generativa por parte de los empleados

- Detecta elementos de Shadow AI
- Evalúa los riesgos de las aplicaciones de IA
- Gestiona la postura de las aplicaciones de IA
- Limita la entrada de datos confidenciales
- Aplica medidas de seguridad en las instrucciones y las respuestas

Protege las aplicaciones y las cargas de trabajo con IA

- Descubre los puntos finales de Shadow AI
- Protege los modelos de IA y los datos de entrenamiento contra el abuso
- Evita que la información de identificación personal quede expuesta en las instrucciones y las respuestas
- Aplica la moderación de contenido



Protege lo que desarrollas

- Crea servidores MCP con autenticación / autorización integrada
- Registra y restringe las solicitudes / respuestas de los modelos de IA, el uso de tokens y los costos
- Evita las interrupciones del servicio con modelos de recuperación y limitación de velocidad

La diferencia de Cloudflare

Protección integral del ciclo de vida de la IA

Una plataforma para garantizar la comunicación humano-IA, e IA-recursos, desde el desarrollo hasta la implementación.

Seguridad de IA, en línea y en tiempo real

Protege las instrucciones y las respuestas de la IA en tiempo real con controles que abarcan entornos de IA públicos y privados.

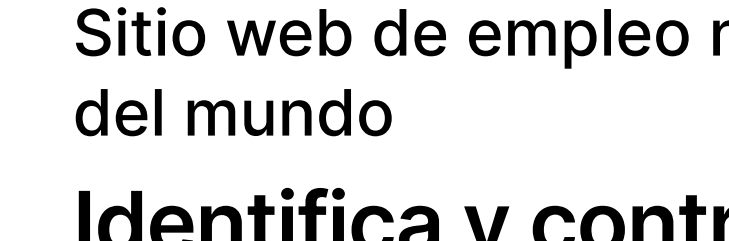
Arquitectura global de IA preparada para el futuro

Utiliza nuestra red global para lograr una aplicación coherente en el perímetro con la escala y el rendimiento que exige la IA.

Implementación independiente de los modelos

Los controles de seguridad funcionan para todos los modelos de IA de tu entorno, lo que proporciona un enfoque unificado para gestionar las implementaciones de IA.

Casos prácticos



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

mediante la prevención del envío de información confidencial por parte de los clientes a los puntos finales de IA generativa de acceso público



Empresa de tecnología financiera impulsada por IA

Reducción de los costes de inferencia en un 95 %

gracias a la adopción de Cloudflare para almacenar en caché y ejecutar las respuestas de los proveedores de modelos de IA

Cloudflare te ayuda a proteger la implementación de la IA

[Leer casos de uso](#)

1. Varonis, 2025 State of Data Security
2. Liu, S., Wang, Z., Chen, Y., Deng, G., Liu, Y., & 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