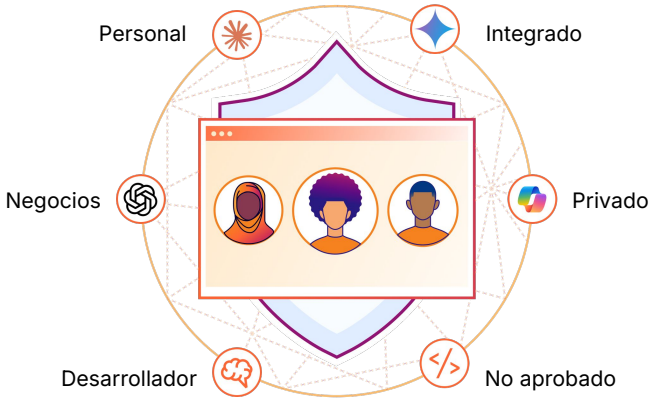
CLOUDFLARE

RESUMEN DE LA SOLUCIÓN

Uso seguro de la IA generativa y agéntica por parte de los usuarios

Capacita a tus equipos para utilizar cualquier herramienta de IA de forma segura con las protecciones implementadas por la plataforma SASE de Cloudflare.



Recuperar el control, aumentar la productividad

La adopción apresurada de la IA está generando un rastro de riesgos crecientes, como las filtraciones de datos, los incumplimientos normativos y una superficie de ataque en expansión. Bloquear la IA por completo solo sacrifica tu ventaja competitiva, y experimentar con soluciones puntuales solo añade complejidad.

Cloudflare protege el uso de la IA en tu organización al ampliar la visibilidad, mitigar los riesgos y proteger los datos de forma integral en todos los entornos de IA:

- **Identifica la Shadow AI** y gestiona las políticas para todas las herramientas de IA autorizadas y no autorizadas.
- **Refuerza la gobernanza de la IA** con controles de acceso basados en la identidad y la gestión de la postura.
- **Evita la pérdida de datos** mediante el bloqueo de información confidencial en los prompts del usuario, la implementación de protecciones temáticas y el escaneo de las configuraciones erróneas en las herramientas de IA.

Implementa mas servicios de Cloudflare para adoptar la IA de forma segura, independientemente de si tu estrategia de IA implica limitar el uso a aplicaciones específicas o experimentar con una gama más amplia de herramientas diversas.

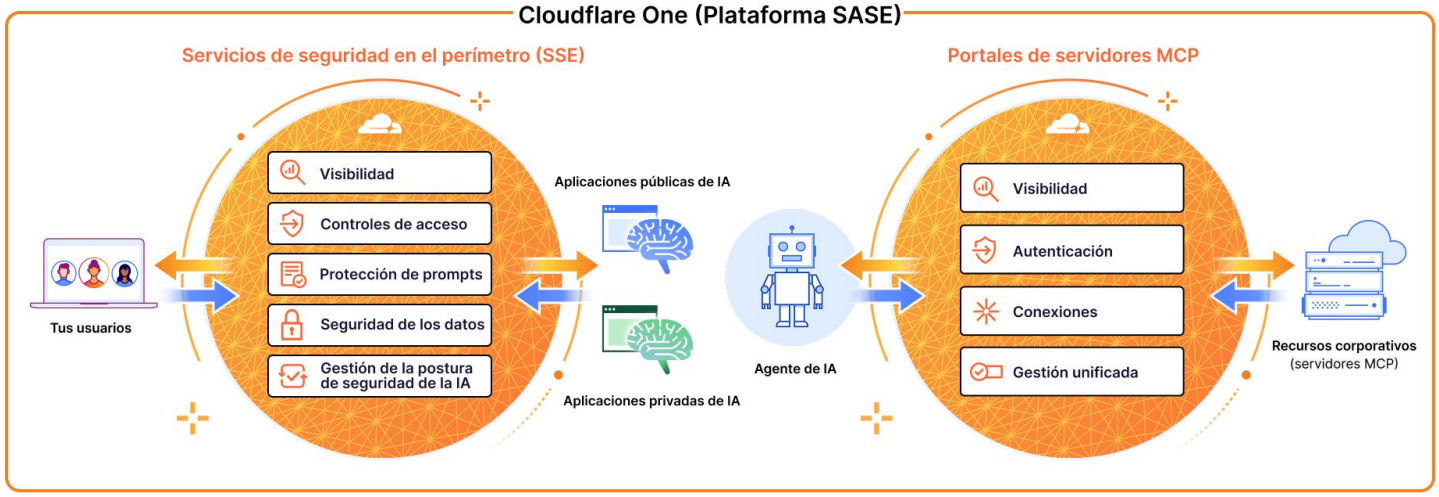
¿Por qué SASE para proteger el uso de la IA por parte de los usuarios?

La plataforma de perímetro de servicio de acceso seguro (SASE) de Cloudflare se ubica entre tu personal de trabajo y las herramientas de IA. Esto convierte a SASE en un punto de partida ideal para que muchos comiencen a utilizar la IA de forma segura.

Ya sea que los empleados estén chateando con ChatGPT o que los agentes de IA estén recopilando información de los recursos corporativos, la plataforma SASE de Cloudflare aplica controles de seguridad consistentes.

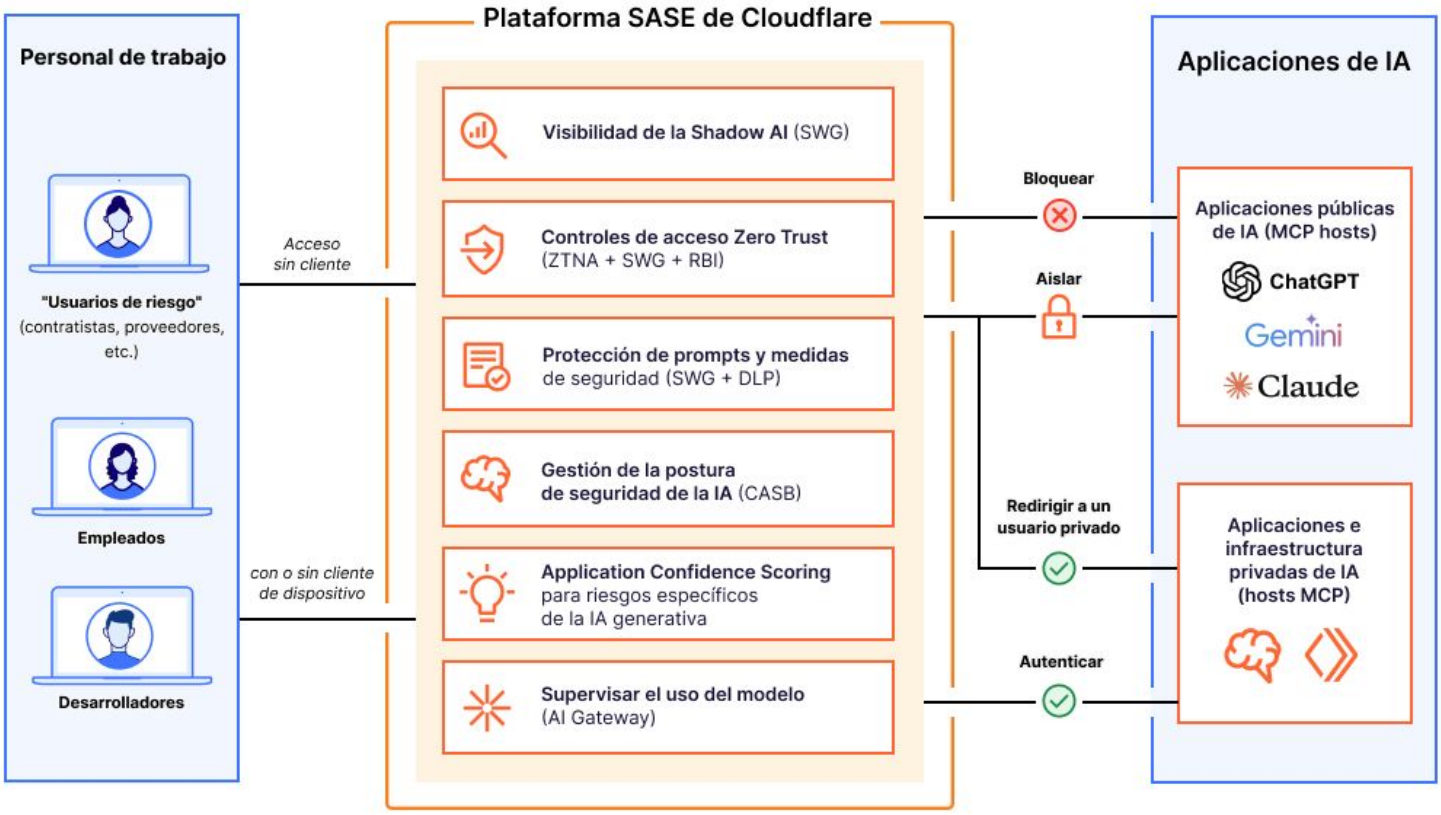
Comunicación segura de la IA generativa y agéntica

La plataforma SASE de Cloudflare ofrece un panel de control y un plano de control unificados para gestionar las interacciones humano-IA y de IA-IA en toda su organización.



A diferencia de otros proveedores de SASE, Cloudflare también ayuda a conectar y proteger las aplicaciones y cargas de trabajo habilitadas para la IA de acceso público (como el bot de chat de IA de tu sitio web o los motores de recomendación).

Protección de la comunicación de los usuarios con aplicaciones de IA generativa mediante los controles de uso de IA en la plataforma SASE de Cloudflare



- **Visibilidad:** identifica y analiza el uso de la Shadow AI mediante la inspección del tráfico en línea. Evalúa los riesgos que plantean esas aplicaciones de IA con una puntuación transparente.
- **Controles de acceso:** bloquear, aislar, redirigir o permitir conexiones de usuario. Aplicar reglas de Zero Trust basadas en la identidad por aplicación.
- **Protección de prompts y medidas de seguridad:** detecta y bloquea los prompts de los usuarios según su intención (p. ej., intentos de jailbreak, abuso de código, solicitudes de información de identificación personal).
- **Seguridad de los datos:** evita la exposición de datos confidenciales con detecciones de prevención de pérdida de datos (DLP) impulsadas por IA para información de identificación personal, código fuente y más.
- **Gestión de la postura de seguridad de la IA:** integra con herramientas de IA generativa a través de la API (disponible ahora para ChatGPT, Claude, Google Gemini) para detectar errores de configuración mediante nuestro agente de seguridad de acceso a la nube (CASB).

Resultados para los clientes

indeed

Sitio web de empleo n.º 1 del mundo

Identificación y control de la Shadow AI

en paralelo con el proyecto de sustitución de la VPN.

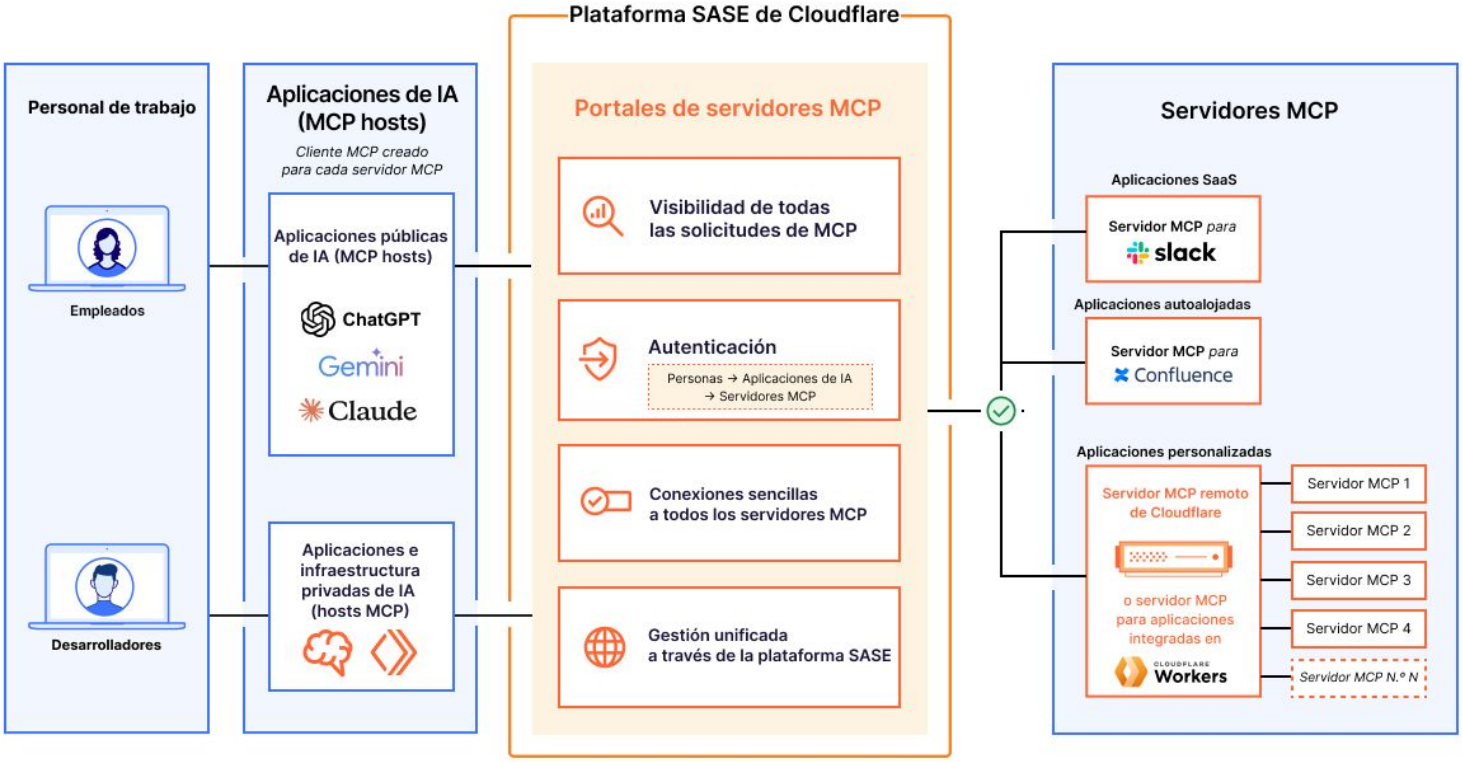
APPLIED

Tecnología de seguros

Aislamiento de las herramientas públicas de la IA generativa como ChatGPT

para bloquear la función de copiar y pegar datos confidenciales.

Protección de la comunicación de la IA agéntica (de la IA al recurso)
con los portales de servidores MCP en la plataforma SASE de Cloudflare



- **Visibilidad:** añade todos los registros de solicitud MCP para auditorías y análisis. Revisa y aprueba cada servidor MCP antes de añadirlo al portal.
- **Autenticación:** autentica el acceso del usuario al portal en función de su identidad. Limitar el acceso a los servidores MCP según el principio de mínimo privilegio.
- **Conexiones:** conecta todos los servidores MCP accesibles con una sola URL, en lugar de configurar individualmente cada servidor MCP.
- **Administración unificada:** aplica las mismas políticas de acceso específicos para las conexiones de IA que para los usuarios humanos.
- **Personalización de herramientas por portal:** selecciona las herramientas específicas y las plantillas de prompts disponibles para cada usuario.

Nota: los portales de servidores MCP de Cloudflare son compatibles con cualquier servidor MCP, incluidos (entre otros) cualquier servidor MCP remoto desarrollado o implementado en Cloudflare. Esta capacidad está disponible como un control de acceso a la red Zero Trust (ZTNA).

Más información acerca de nuestra visión en este blog.

¿Te interesa conocer cómo Cloudflare puede proteger tu uso de la IA?

Solicitar seminario

