CLOUDFLARE

DESCRIPCIÓN GENERAL
DE LA SOLUCIÓN

Descubre el uso que hacen los usuarios de la Shadow AI y la informática

Amplía la visibilidad de las herramientas de IA y SaaS no autorizadas con la inspección de tráfico de Cloudflare



Descubre lo invisible

La Shadow IT no es un problema nuevo, pero la rápida adopción de herramientas de IA no autorizadas está provocando una nueva crisis:

- El **20 %** de las organizaciones sufrió una fuga de datos debido a incidentes de seguridad con Shadow AI en 2025[1]
- El **85 %** de los responsables informáticos afirma que los empleados están adoptando herramientas de IA antes de que el equipo informático pueda evaluarlas[2]

Cloudflare restaura la visibilidad para que las organizaciones gestionen esta superficie de ataque en expansión:

- **Revisa el estado de las aplicaciones:** clasifica las aplicaciones de IA y SaaS como autorizadas, no autorizadas o en revisión
- **Aplica políticas basadas en el estado de las aplicaciones:** permite, bloquea, aísla, aplica detecciones de DLP a las interacciones, restringe la carga de archivos y mucho más
- **Analiza el uso de las aplicaciones:** supervisa las tendencias agregadas y realiza investigaciones granulares
- **Evalúa el riesgo de las aplicaciones:** evalúa la fiabilidad mediante puntuaciones de confianza de las aplicaciones

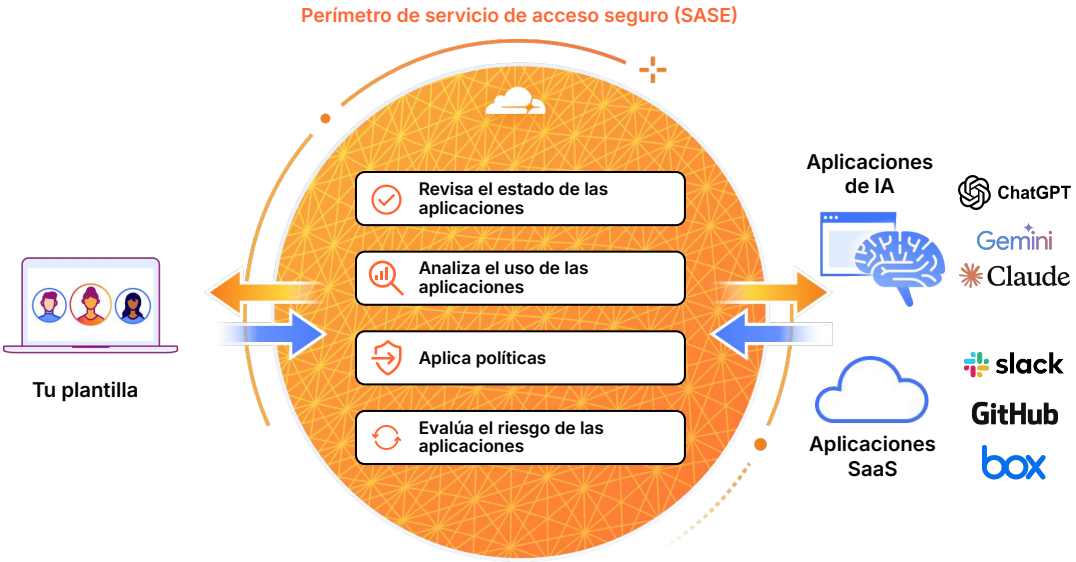
Riesgos únicos de la Shadow AI

La Shadow AI es diferente de la Shadow IT tradicional. Mientras que las aplicaciones SaaS almacenan o comparten principalmente archivos, las herramientas de IA transforman y aprenden de las aportaciones de los usuarios.

Esto significa que la propiedad intelectual, los datos de los clientes o el código fuente, todo ello información confidencial, pueden ser absorbidos de forma irreversible para el entrenamiento de modelos, sin posibilidad de eliminación.

Cómo funciona

La plataforma SASE de Cloudflare se sitúa entre tus usuarios y tus recursos para unificar la visibilidad y los controles.



Además, integra el CASB de Cloudflare a través de la API para buscar errores de configuración, actividad de los usuarios y datos confidenciales. Gestiona la postura de seguridad en las aplicaciones de IA (ChatGPT, Claude, Google Gemini) y otras aplicaciones SaaS. Utiliza CASB con tu proveedor de identidad para ver cuándo los usuarios se autentican en aplicaciones de terceros no autorizadas.

Ejemplos de paneles de control

Filtra esta vista general de alto nivel del uso de las aplicaciones en función de:

- Aplicación y tipo de aplicación
- Estado de aprobación
- Protección ZTNA
- Número de usuarios

Si quieres obtener más información, haz clic en el nombre de cualquier aplicación de IA para ver los usuarios o grupos específicos que acceden a ella, su frecuencia de uso, ubicación y la cantidad de datos transferidos.

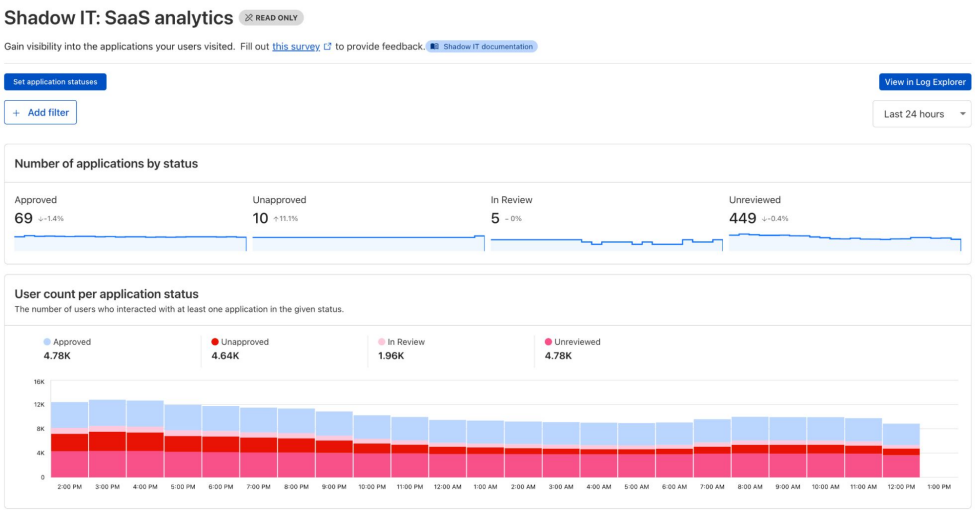


Figura 1: Panel de control de análisis de Shadow IT

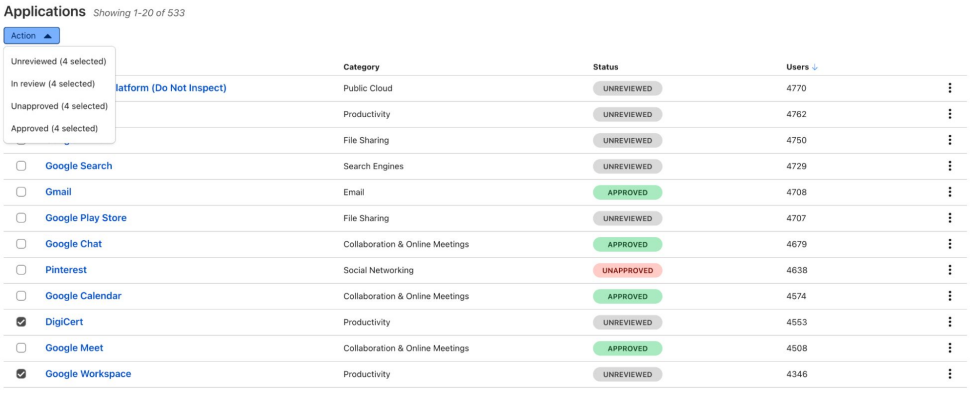


Figura 2: Identificación del estado de las aplicaciones

Organiza las aplicaciones y establece políticas de acceso en función del estado de aprobación:

- Aprobada (autorizada)
- No aprobada (no autorizada)
- En revisión
- Sin revisar

¿Necesitas más ayuda técnica?
Aprende a crear políticas con esta ruta de aprendizaje.

¿Quieres saber más sobre cómo proteger la adopción de la IA en tu organización?

Más casos de uso | Solicitar seminario

1. Informe "Cost of a Data Breach" de IBM, 2025: Fuente
2. Estudio de Manage Engine de 2025: Fuente

© 2025 Cloudflare, Inc. Todos los derechos reservados. | +34 518 880 290 | enterprise@cloudflare.com | cloudflare.com/es-es/