CLOUDFLARE

RESUMEN DE PRODUCTO

Agente de seguridad de acceso a la nube

Visibilidad y control integrales de los entornos SaaS, de IA y de nube, que protegen los datos sin ralentizar la innovación.

Seguridad SaaS diseñada para la era de la IA

Protege tus entornos SaaS, de IA y de nube sin ralentizar la productividad. Detecta al instante los errores de configuración, el Shadow IT y los riesgos relacionados con los datos en todo tu equipo híbrido gracias a Cloudflare CASB.

- **Automatiza la conformidad:** detecta y soluciona al instante las vulnerabilidades de seguridad, como el uso compartido no autorizado de archivos o una autenticación multifactor débil, en Microsoft 365, Google Workspace y GitHub.
- **Bloquea la Shadow AI y el Shadow IT:** identifica las aplicaciones no autorizadas y bloquea el acceso a sitios no autorizados de almacenamiento en la nube o de intercambio de archivos.
- **Protege el uso de la IA:** benefíciate de visibilidad sobre la adopción de herramientas de IA y aplica restricciones de inquilinos en plataformas como ChatGPT y Gemini para garantizar el acceso solo corporativo.
- **Gestiona el riesgo de terceros:** identifica y revoca las integraciones de terceros peligrosas que tengan acceso a tus datos corporativos.

La protección en línea y basada en API de Cloudflare CASB, desarrollada en nuestra red global, garantiza una seguridad rápida y rentable a escala.

EESTI RAUDTEE

Proveedor de infraestructura

Identificación de las vulnerabilidades de SaaS, como el uso compartido masivo de archivos confidenciales de SharePoint, para ayudar a mitigar la pérdida de datos.

Leer el caso práctico

APPLIED

Proveedor de software para aseguradoras

Protección de la adopción de la IA generativa al bloquear la entrada de datos confidenciales en herramientas como ChatGPT, sin afectar a la productividad de los equipos.

Leer el caso práctico

Proveedor de telemedicina

Protección de los datos confidenciales de los pacientes (PHI/HIPAA) y acceso más rápido para los equipos de trabajo remotos y en rápido crecimiento gracias a DLP y CASB.

La diferencia de Cloudflare

Implementación instantánea sin cliente

Conéctate a aplicaciones SaaS y de IA como Microsoft 365, GitHub, Slack y ChatGPT en unos minutos a través de la API. Analiza al instante los riesgos históricos, los errores de configuración y la exposición de datos sin necesidad de instalar ningún cliente.

Gestión continua de la postura de datos en la nube y en SaaS

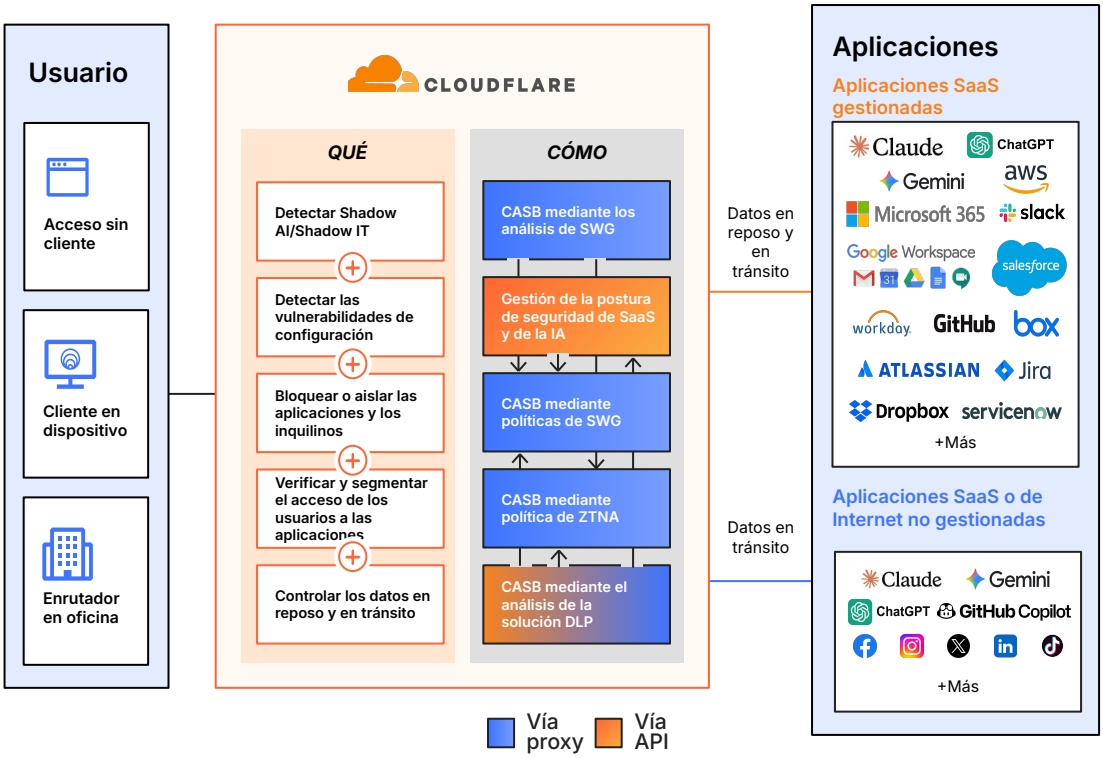
Identifica las desviaciones de seguridad y las configuraciones poco seguras en tu almacenamiento en SaaS y en la nube. Detecta y revierte los errores de configuración críticos, como los buckets públicos de S3 o los permisos de proyectos abiertos, antes de que ocasionen una fuga de datos.

Control unificado de Shadow IT

Deja de alternar entre distintas consolas. Utiliza la información de CASB para detectar las aplicaciones no aprobadas, y luego activa al instante políticas Zero Trust para bloquear o aislar ese tráfico a través de Cloudflare Gateway, con una gestión unificada desde un solo panel de control.

¿Quieres saber más sobre este producto? Consulta nuestra arquitectura de referencia o habla con un experto.

Seguridad integral para SaaS, IA y Shadow IT



Cómo funciona

Nuestra solución CASB multimodo ayuda a ofrecer una seguridad unificada en la nube para las aplicaciones SaaS. Para proteger los datos en reposo, sencillas integraciones API analizan continuamente tus aplicaciones en busca de vulnerabilidades y de riesgos potenciales.

Nuestros controles del acceso Zero Trust (ZTNA), de la puerta de enlace (SWG) y de aislamiento del navegador (RBI) se implementan eficazmente como un CASB en línea, combinando una configuración sencilla con una seguridad sólida.

Protección de datos fuera de banda y postura de seguridad de SaaS (basada en API)	
Gestión de la postura de seguridad de SaaS (SSPM)	Analiza el almacenamiento en la nube y en las aplicaciones SaaS a través de la API para detectar los errores de configuración y las integraciones de terceros peligrosas (por ejemplo, los buckets públicos de S3, las aplicaciones OAuth no autorizadas o las infracciones de MFA).
Protección de datos de SaaS (DLP)	Detecta los archivos confidenciales (como información de PCI, información de identificación personal, secretos) mediante el análisis de datos en reposo, y corrige las infracciones automáticamente (p. ej., elimina los archivos de acceso público) a fin de garantizar el cumplimiento.
Protección de datos en línea (basada en proxy)	
Detección de Shadow AI y Shadow IT	Visibilidad instantánea del uso de aplicaciones no autorizadas. Clasifica y bloquea/aísla automáticamente las aplicaciones de riesgo (p. ej., herramientas de IA o conversores de PDF no aprobados) en función de las puntuaciones de confianza de las aplicaciones.
DLP y OCR en línea	Detecta los datos confidenciales en el tráfico con Exact Data Match (EDM) y clasificadores avanzados. Utiliza el reconocimiento óptico de caracteres (OCR) para ampliar estas protecciones a las imágenes, bloqueando la fuga de datos.
Protección de las instrucciones de la IA generativa	Evita que los datos confidenciales (código fuente, información de identificación personal del cliente) se puedan pegar en los LLM públicos. Inspecciona las solicitudes HTTPS enviadas a herramientas como ChatGPT o Gemini para aplicar un uso seguro de la IA.
Control de inquilinos	Aplica el acceso solo corporativo a aplicaciones como Microsoft 365, Google Workspace y Slack para evitar los inicios de sesión de cuentas personales en los dispositivos corporativos.
Gestión unificada	
Cliente único	No se requiere un cliente CASB independiente. El cliente unificado gestiona ZTNA, SWG y CASB con inspección de paso único.
Puntuación de riesgo del usuario	Detecta los usuarios en riesgo correlacionando los hallazgos de CASB con anomalías de comportamiento para asignar puntuaciones dinámicas de riesgo.
Logpush	El registro integral captura todas las solicitudes, todos los usuarios y todos los dispositivos. Exporta al instante los registros CASB a Splunk, Datadog o S3 para el análisis SIEM.

 | +34 518 880 290 | enterprise@cloudflare.com |
www.cloudflare.com/es-es/

REV:BDES-8793.15ENE2026