CLOUDFLARE

RESUMEN DE PRODUCTO

Agente de seguridad de acceso a la nube

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

Seguridad SaaS diseñada para la era de la IA

Protege tus entornos SaaS, de IA y de la nube sin disminuir la productividad. Detecta al instante errores de configuración, Shadow IT y riesgos de datos en tu fuerza de trabajo híbrida con Cloudflare CASB.

- **Automatiza el cumplimiento normativo:** detecta y corrige al instante las brechas de seguridad, como el intercambio no autorizado de archivos o una autenticación multifactor débil, en Microsoft 365, Google Workspace y GitHub.
- **Detiene el uso de la Shadow AI y Shadow IT:** detecta aplicaciones no autorizadas y bloquea el acceso a sitios de almacenamiento en la nube o de intercambio de archivos no aprobados.
- **Utiliza la IA de forma segura:** obtén visibilidad sobre la adopción de herramientas de IA y aplica restricciones de inquilinos en plataformas como ChatGPT y Gemini para garantizar el acceso corporativo únicamente.
- **Gestiona el riesgo de terceros:** identifica y revoca las integraciones de terceros de riesgo que tienen acceso a tus datos corporativos.

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

EESTI RAUDTEE

Proveedor de infraestructura

Identificación de 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 de seguros

Adopción segura de la IA generativa mediante el bloqueo de las entradas de datos confidenciales a herramientas como ChatGPT sin afectar la productividad de los usuarios.

Leer el caso práctico

Proveedor de telemedicina

Datos confidenciales de los pacientes (PHI/HIPAA) protegidos y agilización del acceso para una fuerza de trabajo remota en rápido crecimiento mediante DLP y CASB.

Las ventajas con Cloudflare

Implementación instantánea y sin cliente

Conéctate a aplicaciones SaaS y de IA como Microsoft 365, GitHub, Slack y ChatGPT en minutos a través de la API. Analiza de inmediato los riesgos históricos, las configuraciones erróneas y la exposición de datos sin instalar clientes.

Gestión continua del estado de los datos en la nube y SaaS

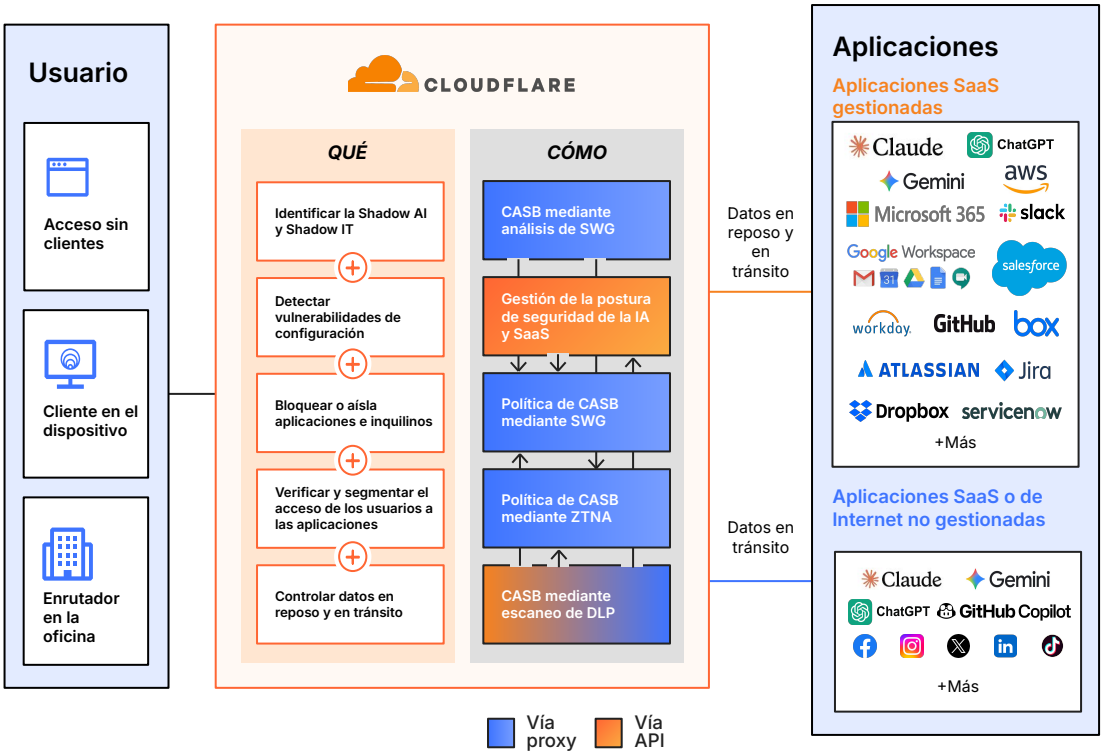
Identifica las desviaciones de seguridad y las configuraciones inseguras en tu SaaS y almacenamiento en la nube. Detecta y revierte errores de configuración críticos, como buckets públicos de S3 o permisos de proyectos abiertos, antes de que provoquen una fuga.

Control unificado de Shadow IT

Sin necesidad de utilizar varios paneles de control. Utiliza la información de CASB para detectar aplicaciones no aprobadas y luego activa al instante políticas Zero Trust para bloquear o aislar ese tráfico a través de Cloudflare Gateway, gestionando todo desde un único panel de control.

¿Quieres conocer 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 multimodal favorece una seguridad unificada en la nube para aplicaciones SaaS. Para proteger los datos en reposo, las integraciones de API sencillas analizan continuamente tus aplicaciones en busca de vulnerabilidades y riesgos potenciales.

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

Protección de datos fuera de banda y postura de seguridad SaaS (basada en API)	
Gestión del estado de seguridad de SaaS (SSPM)	Analiza las aplicaciones SaaS y el almacenamiento en la nube a través de la API para detectar configuraciones erróneas e integraciones de terceros riesgosas (p. ej., buckets públicos de S3, aplicaciones OAuth no autorizadas o infracciones de MFA).
Protección de datos SaaS (DLP)	Detecta archivos confidenciales (PCI, PII, secretos) mediante el análisis de datos en reposo, y corrige automáticamente las infracciones (por ejemplo, elimina archivos de acceso público) para garantizar el cumplimiento normativo.
Protección de datos en línea (basada en proxy)	
Detección de Shadow AI y Shadow IT	Visibilidad instantánea del uso no autorizado de las aplicaciones. Clasifica, bloquea y aísla automáticamente las aplicaciones de riesgo (p. ej., conversores de PDF no aprobados o herramientas de IA) en función de las puntuaciones de confianza de la aplicación.
DLP y OCR en línea	Detecta datos confidenciales en el tráfico con Coincidencia exacta de datos (EDM) y clasificadores avanzados. Utiliza el reconocimiento óptico de caracteres (OCR) para extender estas protecciones a las imágenes, bloqueando la fuga de datos.
Protección de prompts de la IA generativa	Evita que los datos confidenciales (código fuente, información de identificación personal del cliente) se peguen en los LLM públicos. Inspecciona las solicitudes HTTPS a herramientas como ChatGPT o Gemini para aplicar un uso seguro de la IA.
Control de usuarios	Aplica solo el acceso únicamente corporativo para aplicaciones como Microsoft 365, Google Workspace y Slack para evitar los inicios de sesión de cuentas personales en 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 riesgos del usuario	Detecta a los usuarios en riesgo correlacionando los hallazgos de CASB con las anomalías de comportamiento para asignar puntuaciones de riesgo dinámicas.
Logpush	El registro completo captura todas las solicitudes, usuarios y dispositivos. Exporta al instante registros CASB a Splunk, Datadog o S3 para el análisis SIEM.

 +55 (11) 3230 4523 | enterprise@cloudflare.com | www.cloudflare.com/es-LA

REV:BDES-8793.2026JAN15