DLP y CASB integrados

Cloudflare One mejora la visibilidad de los datos y reduce el riesgo de exfiltración cuando los datos se mueven a través de todas las aplicaciones web, SaaS y autoalojadas/privadas.

Protege los datos en todas partes

Actualmente, aproximadamente el 81 % de las fugas están relacionadas con datos almacenados en entornos de nube.

Hoy en día, las organizaciones procesan más datos que nunca. Los clientes confían a las empresas su información personal. Para hacer su trabajo, actualmente los trabajadores del conocimiento necesitan utilizar y compartir datos en los entornos de nube y SaaS. El código es ahora la joya de la corona de una empresa, y su volumen crece rápidamente día a día. Básicamente, los datos confidenciales ahora están en todas partes.

Prevención de pérdida de datos (DLP) integrada + Agente de seguridad de acceso a la nube (CASB) multimodo

Las soluciones DLP y CASB de Cloudflare, integradas en una plataforma SSE modular, amplían fácilmente la visibilidad y unifican los controles de protección de datos en todo el entorno (aplicaciones, usuarios y dispositivos). La simplicidad y la flexibilidad de implementación que ofrece a los administradores garantizan que las políticas sean funcionales, y que por lo tanto realmente se utilicen.

75 % Reducción de los costes asociados al uso de varias soluciones específicas [1]

69 % Minimización del tiempo dedicado a tareas de poco valor (es decir, la instalación y la configuración de políticas de protección contra amenazas) [1]

20 % Disminución de la probabilidad de una fuga de datos y de los costes relacionados [2]

Adopta las aplicaciones SaaS y la nube de forma segura

Evita sanciones de conformidad

Mitiga los daños financieros y a la reputación causados por las infracciones de la conformidad de los datos gracias a una aplicación más ágil de las políticas para los datos regulados.

Simplifica la seguridad de SaaS

Ofrece a tu empresa la adopción segura y con confianza de las nuevas aplicaciones SaaS. Elimina los puntos ciegos con la detección y el control continuos de los riesgos de SaaS.

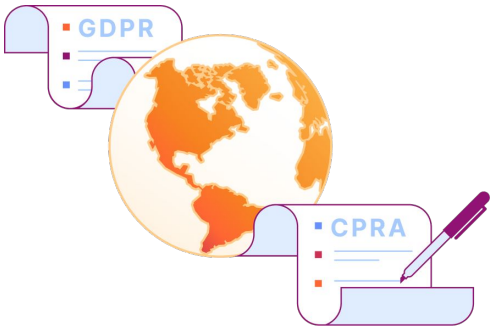
Escala a tu propio ritmo

Aumenta la seguridad de los datos sin interrumpir las operaciones diarias. La configuración es sencilla y la experiencia del usuario final es eficaz.

Principales casos de uso de DLP y CASB

Simplifica el cumplimiento de la normativa

Reduce el riesgo de infracciones de la conformidad causadas por la fuga de datos con una postura de seguridad Zero Trust integral. DLP identifica y aplica controles a las clases de datos regulados (información de identificación personal, información médica, información financiera). Además, mantén registros detallados de auditoría de datos mediante registros y análisis SIEM adicionales para facilitar las tareas de conformidad.

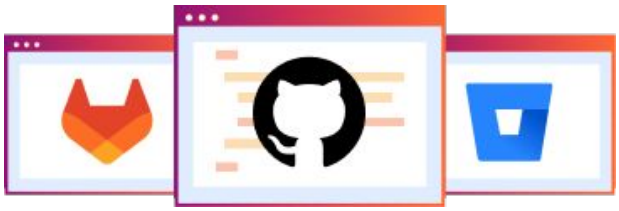


Aumenta la visibilidad de los datos y de los riesgos de errores de configuración

No puedes proteger lo que no conoces. Cloudflare CASB analiza las suites SaaS en busca de errores de configuración y de amenazas de los datos con la ayuda de medidas de detección DLP integradas para datos confidenciales. Consigue rápidamente visibilidad del uso de aplicaciones no autorizadas, como las herramientas emergentes de IA ChatGPT y Bard. A continuación, reduce los riesgos permitiendo, bloqueando, aislando o aplicando controles Zero Trust para acceder a ellas.

Protege la valiosa dirección IP y el código del desarrollador

CASB detecta y corrige los repositorios públicos mal configurados, como GitHub, que suponen un riesgo de fuga de código. Para el código fuente en tránsito, aplica controles DLP granulares para impedir que los usuarios realicen cargas o descargas en las aplicaciones o los dispositivos.



Primeros pasos con la protección de datos unificada

Sé más proactivo en tu protección de datos con un enfoque Zero Trust. Determina cómo los usuarios corporativos utilizan las aplicaciones SaaS, web y privadas e identifica de forma granular cuáles utilizan. A continuación, aplica controles de datos y políticas basadas en la identidad y los dispositivos para reducir tu superficie de ataque.

Consigue visibilidad del movimiento de los datos

- Detecta el uso compartido inapropiado de datos confidenciales en las aplicaciones SaaS
- Detecta las aplicaciones SaaS autorizadas y no autorizadas
- Integra los registros con proveedores SIEM para fines de auditoría*

Reduce el riesgo de exfiltración de datos

- Aplica controles de DLP sobre qué datos entran en cualquier aplicación y a dónde se mueven
- Aísla las amenazas de los datos que salen de las aplicaciones SaaS y las aplicaciones privadas*
- Protege el acceso a las aplicaciones SaaS, privadas/en la nube y autoalojadas

**utilizando las funcionalidades de ZTNA, SWG y/o el aislamiento remoto del navegador (RBI) en la plataforma SSE y SASE*

Cómo funciona DLP

Debido a la migración a la nube, el seguimiento y el control de la información confidencial es más difícil que nunca. Los empleados utilizan un número cada vez mayor de herramientas para manipular una enorme cantidad de datos. Al mismo tiempo, los gerentes de seguridad y de TI tienen dificultades para identificar quién debe acceder a los datos confidenciales, cómo se almacenan los datos y a dónde pueden dirigirse.

DLP te permite proteger tus datos según sus características, como por ejemplo palabras clave o patrones. Cuando hay tráfico de entrada y salida en la infraestructura corporativa, su inspección comprueba si contiene indicadores de datos confidenciales. Si se encuentran, el tráfico se permite o se bloquea según las reglas de los clientes.

Controles fáciles y rápidos de las clases de datos regulados

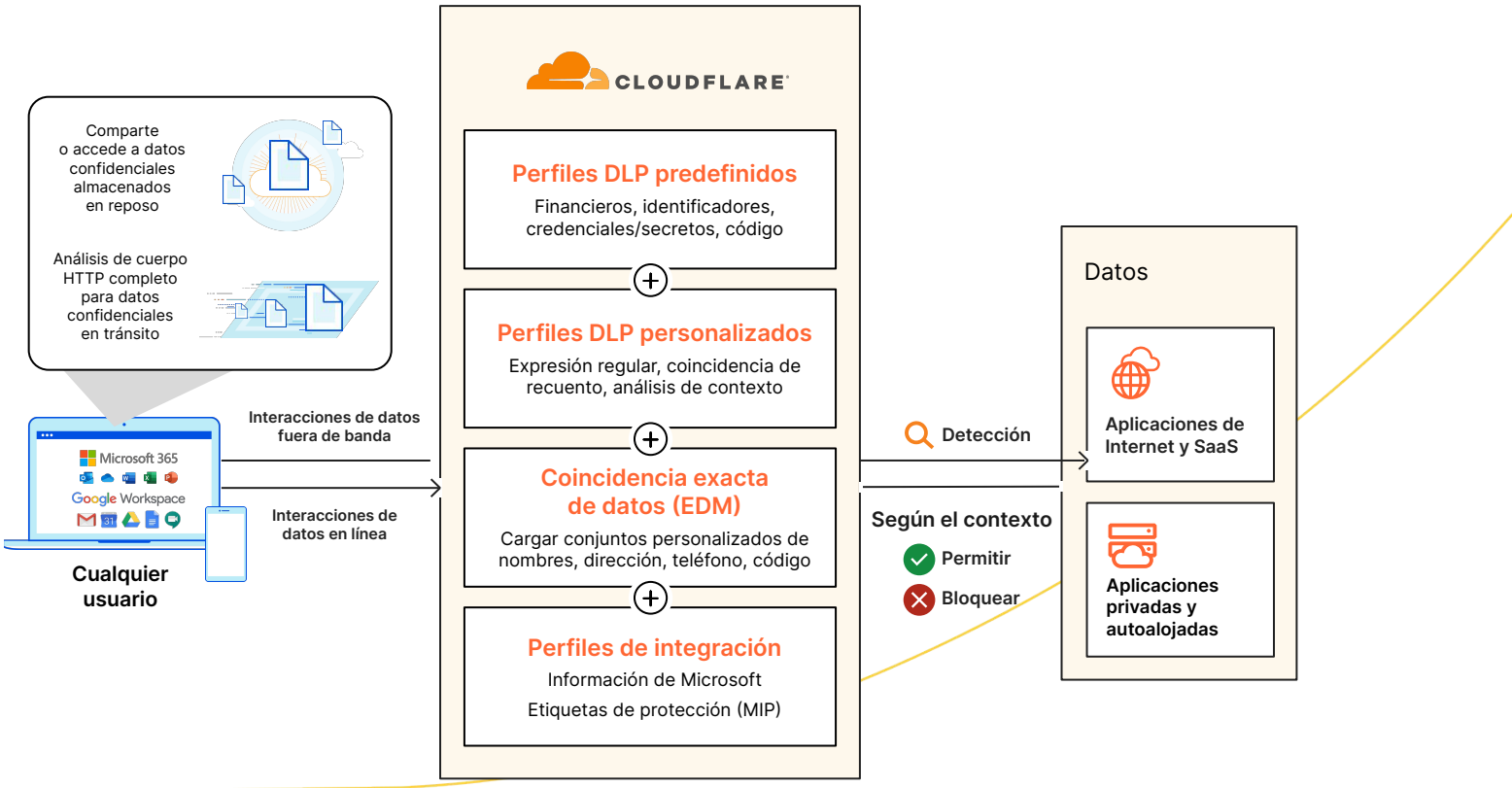
Los requisitos de conformidad son cada vez más estrictos y más amplios. Activa rápidamente perfiles DLP predefinidos para analizar el tráfico de red de los empleados y bloquear la compartición de datos regulados como información de identificación personal, información de salud protegida y otra información financiera (p. ej., números bancarios o de tarjetas de crédito).

Personalización avanzada para las necesidades de los datos en constante cambio

La definición de datos confidenciales puede variar drásticamente de una organización a otra, según el sector y las ubicaciones operativas. Aplica controles granulares a otros tipos de datos, como secretos, código, credenciales y direcciones IP, creando perfiles DLP personalizados con análisis de contexto y coincidencia exacta de datos.

Integración perfecta con las herramientas existentes de clasificación de datos

Mantener un inventario exhaustivo de los datos confidenciales supone una gran carga para los equipos de seguridad y, por lo tanto, requiere herramientas de clasificación de datos como MIP. Aumenta la agilidad, no la complejidad, con nuestras integraciones que recuperan automáticamente las etiquetas de confidencialidad y rellenan con ellas un perfil DLP.



Cómo funciona CASB

SSE desarrollado de forma nativa ofrece CASB en línea para un control de datos coherente en todas las aplicaciones y todos los dispositivos

Cada aplicación SaaS requiere diferentes consideraciones de seguridad, y opera fuera de las salvaguardas del perímetro tradicional. Conforme las organizaciones adoptan decenas de aplicaciones SaaS, resulta cada vez más difícil mantener la coherencia en términos de seguridad, visibilidad y rendimiento.

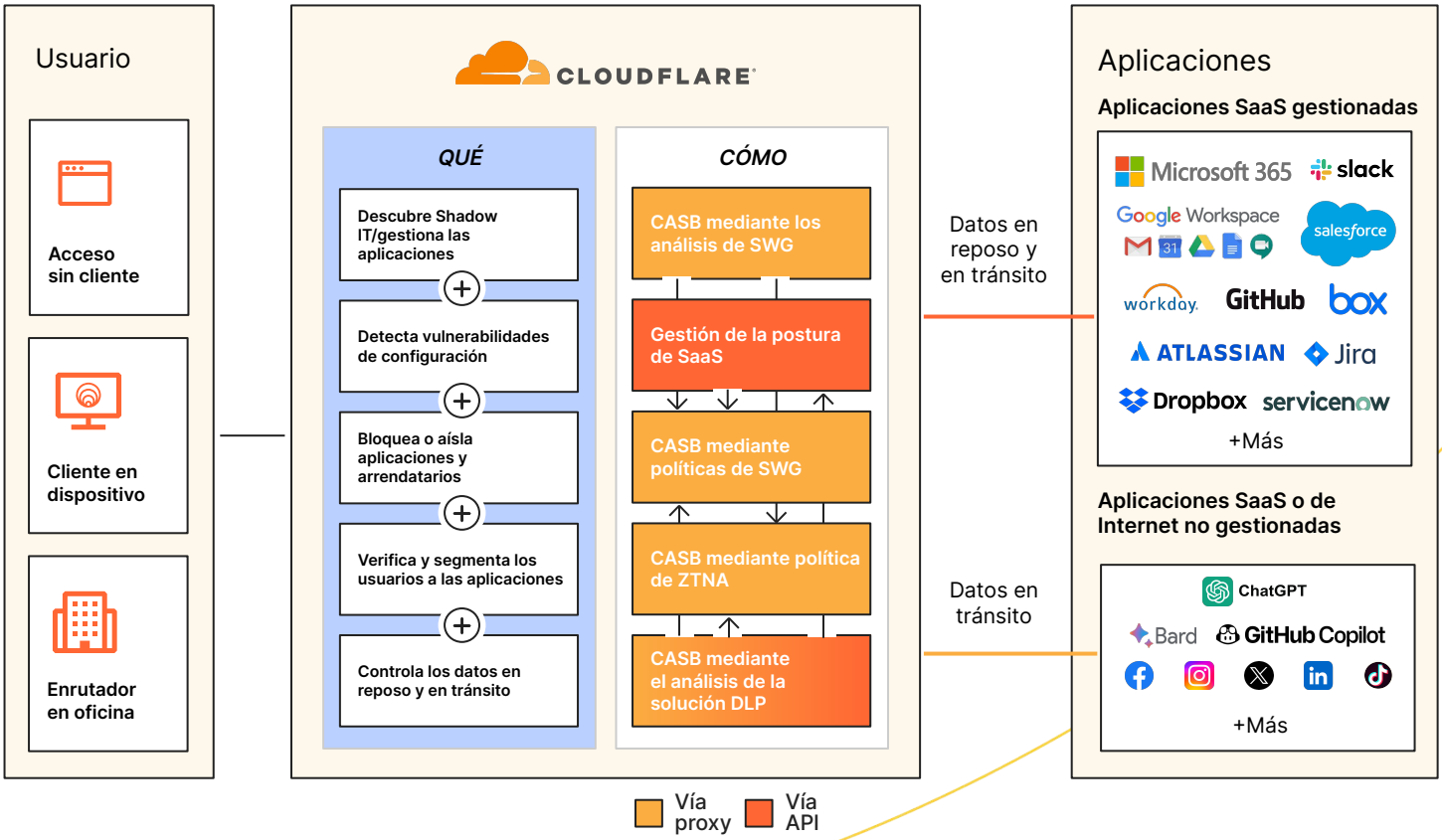
Para proteger los datos en tránsito, nuestro CASB en línea aplica controles de ZTNA, SWG y de aislamiento remoto del navegador (RBI) delante de tus aplicaciones.

- Registra cada solicitud HTTP para identificar la Shadow IT.
- Bloquea/aísla las amenazas y el intercambio de datos de riesgo.
- Accede de forma segura a cualquier aplicación SaaS.

Las sencillas integraciones API de CASB proporcionan rápidamente visibilidad de los riesgos en todas tus aplicaciones SaaS gestionadas

Conéctate a las aplicaciones SaaS más populares (Google Workspace, Microsoft 365, etc.) en solo unos minutos con rápidas integraciones API de solo lectura.

Garantiza la eficacia de tu postura de seguridad SaaS y ofrece a tus equipos informáticos y de seguridad visibilidad de los permisos, los errores de configuración, el acceso inadecuado y los problemas de control que podrían poner en riesgo tus datos y a tus usuarios. A continuación, soluciona rápidamente las amenazas que haya identificado CASB aplicando políticas SWG con un solo clic y el análisis DLP integrado.



Qué dicen nuestros clientes

"Actualmente, Cloudflare One ayuda a evitar que nuestros usuarios compartan datos y códigos confidenciales con herramientas como ChatGPT y Bard, lo que nos permite aprovechar la IA de forma segura...

De cara al futuro, estamos entusiasmados con las continuas innovaciones de Cloudflare para proteger los datos y, en particular, con su visión y hoja de ruta para servicios como DLP y CASB".

— **Applied Systems**, Tanner Randolph, director de seguridad de la información

APPLIED

Cloudflare sustituyó las soluciones específicas Zscaler ZIA y Cisco AnyConnect VPN.

En términos más generales, ha ayudado a Applied Systems a consolidar la seguridad para todos sus usuarios, aplicaciones y redes.

Leer caso práctico

Qué dicen los analistas

FORRESTER

Cloudflare ha sido reconocido como "competidor sólido" en el informe "The Forrester Wave™: Zero Trust Platforms", 3.er trimestre de 2023

Los sitios web de Cloudflare continúan su impulso disruptivo en el mercado de SSE, como avalan los reconocimientos de los analistas, y han recibido las puntuaciones más altas posibles, 5,0/5,0, en los criterios de innovación, plan de desarrollo, flexibilidad y transparencia de precios, y su capacidad para habilitar y proteger a los usuarios híbridos.

Según el informe, *"las distintas políticas de red, DLP y control de acceso de Cloudflare se gestionan desde una única consola, lo que permite a los clientes una implementación y una protección rápidas contra las amenazas transmitidas por Internet".*

Leer informe completo

Gartner®

Cloudflare es el único nuevo proveedor reconocido en el informe 2023 Gartner® Magic Quadrant™ for SSE

Cloudflare ha sido reconocido en el informe 2023 Gartner® Magic Quadrant™ for Security Service Edge (SSE). Creemos que nuestro reconocimiento valida nuestro compromiso para continuar avanzando en nuestra plataforma Zero Trust para ayudar a proteger el trabajo híbrido.

Leer informe completo

Funcionalidades integradas de DLP

Perfiles DLP	Define los patrones de datos que deseas detectar. • **Perfiles DLP predefinidos:** información financiera (p. ej., números de tarjetas de crédito), identificadores nacionales (información de identificación personal), información sanitaria (información médica protegida), credenciales y secretos (p. ej., claves de GCP/AWS) y código fuente. • **Perfiles personalizados**: crea detecciones personalizadas para identificar tipos únicos de datos confidenciales (p. ej., nombres de proyectos internos, nombres de productos no publicados).
Clasificación de datos	Integra DLP con proveedores de clasificación de datos de terceros, como las etiquetas de confidencialidad de Microsoft Information Protection (MIP). Recupera la información de clasificación del proveedor, rellena el perfil DLP de Cloudflare y activa la política para permitir o bloquear los datos coincidentes.
Recuento de coincidencias	Establece recuentos de coincidencias personalizados para el número de veces que se puede detectar cualquier entrada habilitada en el perfil antes de que se active una acción, como el bloqueo o el registro.
Análisis de contexto	Análisis de contexto para restringir las detecciones de DLP en función de palabras clave de proximidad (a una distancia de unos 1000 bytes).
Conjuntos de datos personalizados	Analiza el tráfico web y las aplicaciones SaaS en busca de datos específicos definidos en un conjunto de datos personalizado. Para mayor confidencialidad, puedes excluir/encriptar con hash los datos en los registros. • **Coincidencia exacta de datos:** especifica los conjuntos más importantes de información de identificación personal, como nombres de clientes, direcciones, números de teléfono y números de tarjetas de crédito. Todos los datos encriptados antes de llegar a Cloudflare. • **Listas de palabras personalizadas:** protege los datos no confidenciales, como las direcciones IP y los números SKU.

Funcionalidades de CASB multimodo

Visibilidad del riesgo y conformidad	
Análisis basado en API	Integra una aplicación SaaS de terceros para analizar los datos en reposo en busca de riesgos de seguridad, como errores de configuración, actividad no autorizada de los usuarios, Shadow IT y problemas de seguridad de los datos que se puedan producir después de que un usuario haya iniciado sesión correctamente. Más de 18 integraciones disponibles (p. ej., Microsoft 365, Google Workspace).
Detección de Shadow IT	Visibilidad de la Shadow IT en las aplicaciones SaaS y los orígenes de red privados que visitan tus usuarios finales. Revisa las aplicaciones detectadas y ajusta el estado de aprobación: Aprobado, No aprobado, En revisión y No revisado. Establece políticas granulares basadas en la identidad y los dispositivos* según corresponda.
Registro de auditoría	Registro completo* de todas las solicitudes, todos los usuarios y todos los dispositivos. Utiliza logpush* o API para la integración con herramientas existentes de almacenamiento o SIEM de terceros para la auditoría de conformidad.
Seguridad de los datos y prevención de amenazas	
Acceso Zero Trust*	Establece políticas de privilegio mínimo para cada aplicación a través de ZTNA a fin de limitar el acceso de los usuarios a los datos.
Controles del uso compartido de archivos*	Permite o bloquea la carga/descarga de archivos en función del tipo MIME mediante las políticas SWG HTTP.
Controles de las aplicaciones*	Permite o bloquea el tráfico a aplicaciones específicas o a tipos de aplicación determinados mediante las políticas SWG HTTP.
Controles de inquilinos*	Controla el tráfico de los inquilinos de las aplicaciones SaaS a través de SWG para evitar la pérdida de datos.
Controles del navegador*	Protege los datos en uso en un navegador restringiendo las acciones de descarga, carga, copiar/pegar, entrada de teclado e impresión en aplicaciones y páginas web aisladas gracias al aislamiento remoto del navegador (RBI). Evita la fuga de datos en dispositivos locales y controla la entrada de los usuarios en sitios web sospechosos.
Análisis DLP*	Analiza el tráfico HTTP a través de SWG en busca de datos confidenciales mediante cadenas que coincidan con las palabras clave o expresiones regulares especificadas en la configuración del perfil DLP. Activa los perfiles DLP en una integración CASB y descubre si los archivos almacenados en tus aplicaciones SaaS contienen datos confidenciales. Amplía DLP a las aplicaciones privadas mediante el aislamiento remoto del navegador (RBI) sin cliente, que hereda todas las políticas HTTP.

**utilizando las funcionalidades de ZTNA, SWG y/o el aislamiento remoto del navegador (RBI) en la plataforma SSE y SASE*

¿Por qué Cloudflare?

Una plataforma unificada

Acceso seguro mediante la verificación y segmentación de cualquier usuario a cualquier recurso

Protección contra amenazas que abarca todos los canales con información sobre amenazas y aprendizaje automático e IA basada en la red

Protección de datos con mayor visibilidad y control de los datos en tránsito, en reposo y en uso

Una red programable

Mayor eficacia al simplificar la conectividad y la gestión de políticas

Mayor productividad al garantizar una experiencia de usuario rápida, fiable y coherente en todas partes

Mayor agilidad, gracias a su capacidad para innovar rápidamente y satisfacer tus nuevos requisitos de seguridad.

¿Te interesa hablar de tus necesidades de protección de datos?

Solicitar seminario

¿Necesitas más tiempo?

Más información sobre [la plataforma SSE y SASE de Cloudflare]

1. Estudio 2023: techvalidate.com/product-research/cloudflare/charts
2. Informe de IBM "Cost of Breach": https://www.ibm.com/reports/data-breach