CLOUDFLARE

RESUMEN DE PRODUCTO

Prevención de pérdida de datos

Protege los datos confidenciales y garantiza el cumplimiento normativo en aplicaciones web, privadas, SaaS, en la nube, de IA y de correo electrónico.

La solución de prevención de pérdida de datos (DLP) más integrada para la era agéntica

Con DLP de Cloudflare, puedes detectar y bloquear la exfiltración de datos confidenciales en toda tu red y aplicaciones (SaaS, en la nube, de IA y de correo electrónico) sin interrumpir ni disminuir la productividad del usuario.

Protege tu propiedad intelectual, código fuente, información de identificación personal del cliente (PII) y otros datos para:

- **Aplicar el cumplimiento normativo** con perfiles prediseñados para datos financieros, registros médicos y números de seguridad social.
- **Proteger los datos corporativos** mediante el bloqueo de las cargas confidenciales a sitios no autorizados de almacenamiento en la nube o de intercambio de archivos.
- **Proteger los prompts** mediante el escaneo y la reacción de datos confidenciales o código fuente en las entradas de herramientas como ChatGPT y GitHub.
- **Obtener visibilidad del movimiento de datos** en toda tu fuerza de trabajo híbrida.

Desarrollada en el perímetro global de Cloudflare, la inspección se produce a milisegundos del usuario, lo que garantiza una protección rápida y rentable a escala.

Proveedor de infraestructura

Identificación de vulnerabilidades de SaaS, como la distribución extensiva de archivos confidenciales de SharePoint, que favorece la mitigación de la pérdida de datos.

Leer el caso práctico

Banco digital líder

Consolidación de la seguridad en un único panel de control, lo que garantiza el cumplimiento normativo estricto de los datos y la protección contra ransomware para su plataforma de banca móvil.

Proveedor de telemedicina

Protección de datos confidenciales de los pacientes (PHI/HIPAA) y acceso ágil para una fuerza de trabajo remota en rápido crecimiento mediante DLP y CASB.

Ventajas de Cloudflare

Seguridad SaaS e IA simplificada

Controla el uso de la IA de los empleados mediante el bloqueo del contenido sospechoso, y reduce los riesgos de exfiltración mediante la identificación y corrección de los datos confidenciales almacenados en entornos SaaS y en la nube.

Gestión unificada de políticas

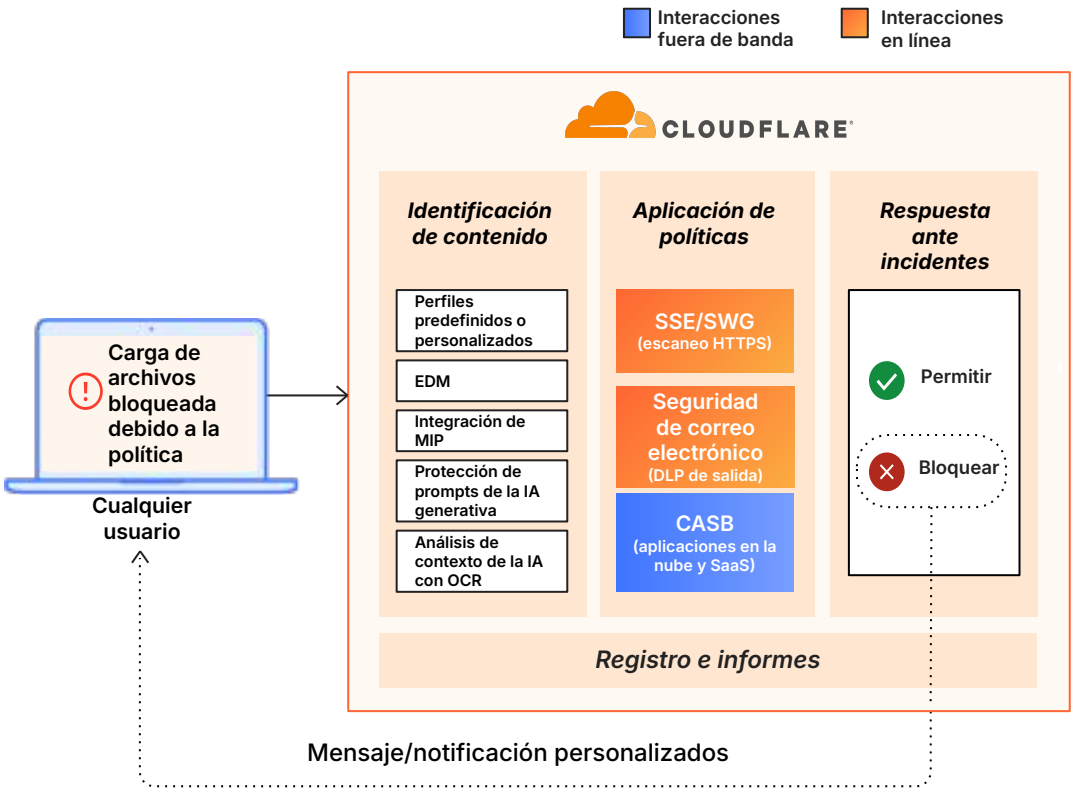
Configura perfiles de DLP, reglas de detección y etiquetas de confidencialidad de Microsoft Purview para consolidar las medidas de protección en el tráfico de salida, los documentos, los archivos PDF y las imágenes.

Controles de datos adaptativos

Brinda comentarios por cada detección para optimizar el análisis de contexto impulsado por IA y afinar la exactitud de las detecciones. DLP se adapta a tus patrones de datos y tráfico específicos para reducir los falsos positivos.

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

Protección de los datos en todos los canales



Cómo funciona

Cloudflare DLP ofrece una inspección automatizada y contextual del tráfico HTTPS y del correo electrónico.

Integrado de forma nativa en el marco Zero Trust de Cloudflare, elimina las brechas de seguridad al consolidar la protección de datos en una única plataforma unificada, lo que garantiza una visibilidad y un control eficientes en todos los canales.

Ejemplos de las capacidades de DLP	
Perfiles DLP	Implementa perfiles predefinidos para información de identificación personal, PHI, datos financieros y credenciales, o crea perfiles personalizados para proteger activos de propiedad exclusiva, como nombres de proyectos internos o propiedad intelectual no publicada.
Protección de Información de Microsoft (MIP)	Incorpora etiquetas de confidencialidad de MIP para aplicar políticas de forma automática (p. ej., bloquear "Confidencial") sin volver a etiquetar los archivos.
Coincidencia exacta de datos (EDM)	Carga conjuntos de datos con algoritmo Hash (p. ej., una base de datos de clientes específica) para detectar valores exactos en lugar de patrones genéricos. Bloquea registros específicos y reduce significativamente los falsos positivos.
Huella digital de documentos	Protege los documentos confidenciales creando y almacenando "huellas digitales" únicas (hashes/patrones) que luego se comparan con el tráfico de la red para identificar y bloquear documentos similares.
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.
Análisis de contexto de IA y puntuación de confianza	Utiliza el aprendizaje automático para analizar el contexto y las palabras clave de proximidad. Establece límites de confianza para bloquear automáticamente las coincidencias de alto riesgo y registrar los eventos de menor confianza para su optimización.
Reconocimiento óptico de caracteres (OCR)	Escanea y extrae automáticamente el texto de los archivos de imagen (PNG, JPG/JPEG) para evitar que los usuarios evadan la seguridad al hacer capturas de pantalla de documentos confidenciales.
Capacitación y educación de los usuarios	Muestra notificaciones personalizables en tiempo real que informan al instante a los usuarios sobre las infracciones de las políticas de seguridad.
Análisis forense y registro unificados	Combina el registro de eventos detallado con la inspección de la carga útil segura. Analiza fragmentos de datos específicos y el contexto del usuario para validar al instante los incidentes y ajustar las políticas.

