CLOUDFLARE

SINTESI DEL PRODOTTO

Prevenzione della perdita dei dati (DLP)

Proteggi i dati sensibili e garantisci la conformità normativa su app Web, private, SaaS, cloud, intelligenza artificiale ed e-mail.

La prevenzione della perdita di dati (DLP) più integrata per l'era agentica

Con Cloudflare DLP, puoi rilevare e bloccare l'esfiltrazione di dati sensibili su tutta la rete e le applicazioni (SaaS, IA, cloud, private ed e-mail) senza interrompere o rallentare la produttività degli utenti.

Proteggi la tua proprietà intellettuale, il codice sorgente, le informazioni di identificazione personale (PII) dei clienti e altri dati per:

- **Applicare la conformità** utilizzando profili predefiniti per dati finanziari, cartelle cliniche e numeri di previdenza sociale.
- **Proteggere i dati aziendali** bloccando i caricamenti sensibili su siti di archiviazione cloud o di condivisione file non autorizzati.
- **Proteggere i prompt IA** scansionando e redigendo dati sensibili o codice sorgente negli input di strumenti come ChatGPT e GitHub.
- **Ottenere visibilità sullo spostamento dei dati** su tutta la forza lavoro ibrida.

Basata sul perimetro globale di Cloudflare, l'ispezione avviene a pochi millisecondi dall'utente, garantendo una protezione rapida ed economica su larga scala.

Fornitore di infrastruttura

Vulnerabilità SaaS identificate, come file di SharePoint sensibili ampiamente condivisi, per contribuire a mitigare la perdita di dati.

Leggi il case study

Banca digitale leader

Sicurezza consolidata in un'unica dashboard, garantendo la rigorosa conformità dei dati e la protezione dal ransomware per una piattaforma bancaria mobile-first.

Fornitore di telemedicina

Dati sensibili dei pazienti protetti(PHI/HIPAA) e accesso accelerato per una forza lavoro remota in rapida crescita tramite DLP e CASB.

Cloudflare fa la differenza

Sicurezza SaaS e IA semplificata

Gestisci l'utilizzo dell'intelligenza artificiale da parte dei dipendenti bloccando i contenuti sospetti e riduci i rischi di esfiltrazione identificando e correggendo i dati sensibili archiviati negli ambienti SaaS e cloud.

Gestione unificata delle politiche

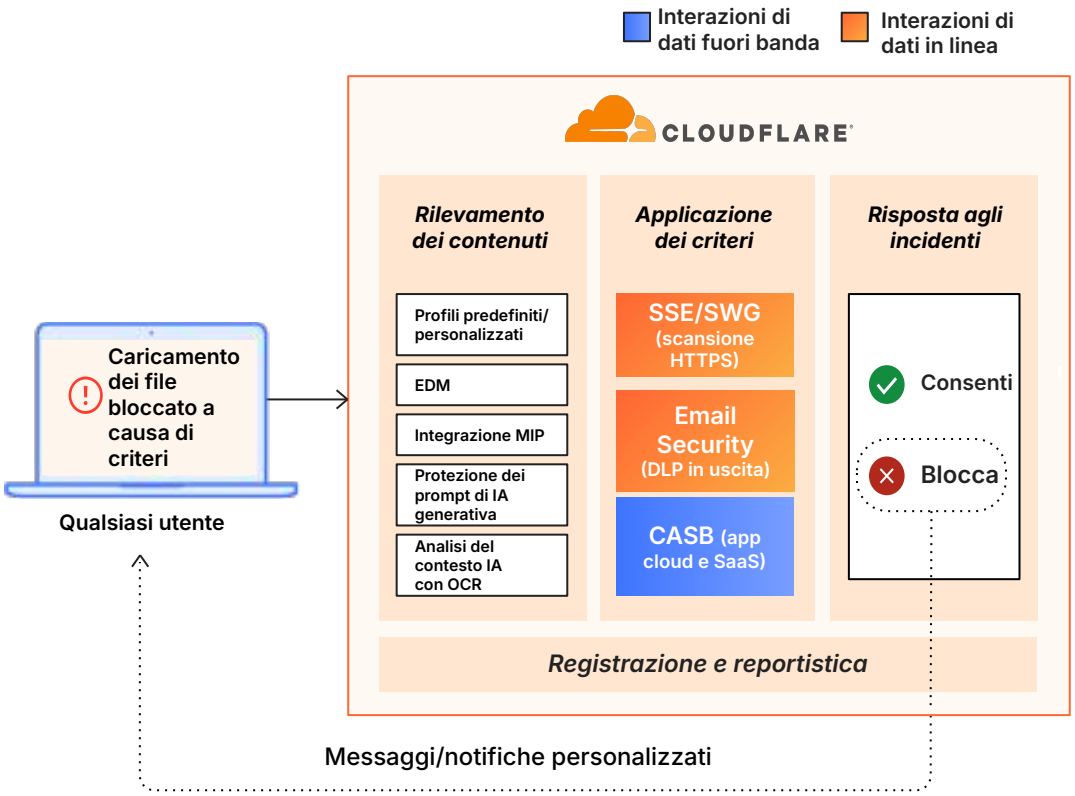
Configura i profili DLP, le voci dei rilevamenti e le etichette di riservatezza di Microsoft Purview per consolidare le protezioni su traffico in uscita, documenti, PDF e immagini.

Controlli dei dati adattivi

Fornisci feedback per ciascun rilevamento per addestrare l'analisi del contesto IA e migliorare la precisione del rilevamento.
La funzionalità DLP si adatta ai modelli di dati e al traffico specifici dell'utente per ridurre i falsi positivi.

Vuoi approfondire questo prodotto? Consulta la nostra architettura di riferimento o parla con un esperto.

Protezione dei dati su tutti i canali dello spazio di lavoro



Come funziona

Cloudflare DLP offre un'ispezione automatizzata e sensibile al contesto su HTTPS e traffico e-mail.

Integrato in modo nativo nel framework Zero Trust di Cloudflare, elimina le lacune di sicurezza consolidando la protezione dei dati in un'unica piattaforma unificata, garantendo visibilità e controllo senza interruzioni su ogni canale.

Funzionalità DLP di esempio	
Profili DLP	Distribuisci profili predefiniti per informazioni di identificazione personale (PII), PHI, dati finanziari e credenziali, oppure crea profili personalizzati per proteggere risorse proprietarie come nomi di progetti interni o proprietà intellettuale non rilasciata.
Microsoft Information Protection (MIP)	Acquisisci etichette di sensibilità MIP per applicare automaticamente i criteri (ad esempio, Blocca "Riservato") senza taggare nuovamente i file.
Exact Data Match (EDM)	Carica set di dati con hash (ad esempio, un database specifico del cliente) per rilevare valori esatti anziché modelli generici. Blocca record specifici riducendo drasticamente i falsi positivi.
Impronta digitale dei documenti	Proteggi i documenti sensibili creando e archiviando "impronte digitali" (hash/pattern) univoche che vengono poi confrontate con il traffico di rete per identificare e bloccare documenti simili.
Protezione dei prompt di IA generativa	Impedisci che i dati sensibili (codice sorgente, informazioni di identificazione personale (PII) del cliente) vengano incollati negli LLM pubblici. Ispeziona le richieste HTTPS a strumenti come ChatGPT o Gemini per imporre un utilizzo sicuro dell'IA.
Analisi del contesto IA e punteggio di affidabilità	Utilizza il machine learning per analizzare il contesto e le parole chiave di prossimità. Imposta le soglie di sicurezza per bloccare automaticamente le corrispondenze ad alto rischio registrando gli eventi a bassa sicurezza per l'ottimizzazione.
Optical Character Recognition (OCR)	Scansiona ed estrai automaticamente il testo dai file di immagini (PNG, JPG/JPEG) per impedire agli utenti di aggirare la sicurezza eseguendo screenshot di documenti sensibili.
Formazione e affiancamento degli utenti	Visualizza notifiche personalizzabili, in tempo reale, che informano istantaneamente gli utenti sulle violazioni dei criteri di sicurezza.
Analisi forense e registrazione unificate	Combina la registrazione granulare degli eventi con l'ispezione sicura del payload. Analizza frammenti di dati specifici e il contesto dell'utente per convalidare istantaneamente gli incidenti e ottimizzare i criteri.

