CLOUDFLARE

SINTESI DELLA SOLUZIONE

Proteggi i tuoi dati sensibili

Migliore architettura di rete per una protezione dei dati più efficace, più produttiva e più agile.

Protezione unificata per i dati ovunque

La protezione dei dati non è un obbligo nuovo, ma il passaggio ad architetture cloud ibride, insieme alla rapida adozione dell'intelligenza artificiale, introduce nuove sfide:

- Il **93% dei dipendenti** ammette di inserire informazioni negli strumenti IA senza approvazione [1]
- Il **79% di tutti i Paesi** ha normative sulla privacy dei dati [2]

Cloudflare applica controlli coerenti lungo tutto il ciclo di vita dei tuoi dati:

- **Proteggi ovunque:** applica controlli coerenti su Web, SaaS, e-mail e traffico cloud.
- **Blocca l'esfiltrazione dell'IA:** analizza i prompt della GenAI per bloccare i dati sensibili e governare l'utilizzo dell'IA.
- **Gestisci i rischi dei dati:** scopri e gestisci lo shadow IT e la shadow AI ed esegui la scansione delle app SaaS/cloud con CASB.

"L'aumento di tutti questi strumenti di intelligenza artificiale non autorizzati ci fa riconsiderare il nostro approccio alla sicurezza. Stiamo esaminando SASE ora". - *Responsabile di Infosec,* ***AllSaints***

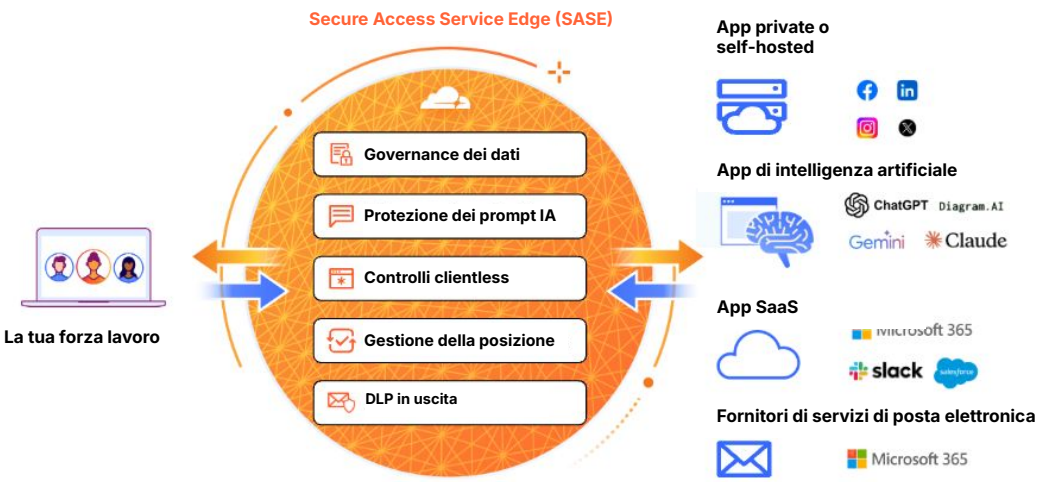
Perché scegliere SASE rispetto alla DLP aziendale?

La piattaforma Secure Access Service Edge (SASE) di Cloudflare è progettata per posizionarsi tra la tua forza lavoro e ogni applicazione e origine dati. Ciò rende SASE un punto di partenza ideale per molti che vogliono iniziare a proteggere i dati in modo sicuro.

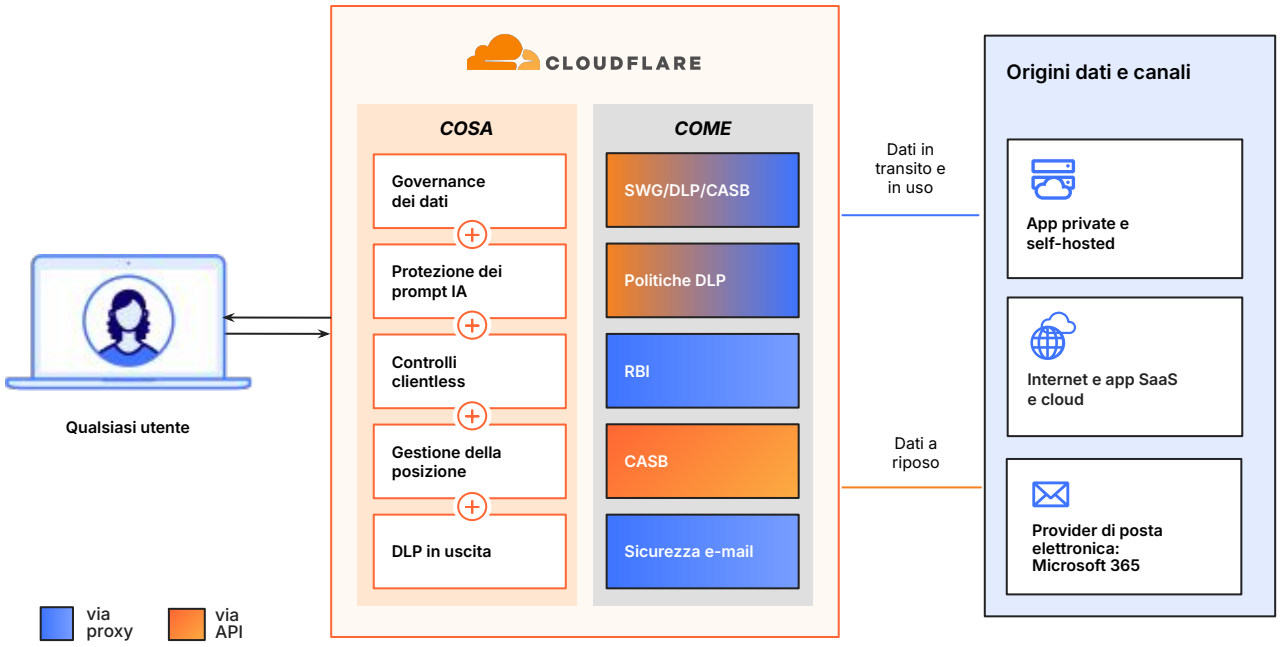
Che i dipendenti accedano ai dati nelle app SaaS, scarichino file sensibili o chattino con gli strumenti GenAI, la piattaforma SASE di Cloudflare applica controlli di sicurezza coerenti in tutte le interazioni con i dati.

Come funziona

La piattaforma SASE di Cloudflare si integra tra la tua forza lavoro e le tue risorse per unificare visibilità e controlli.



Protezione dei dati basata sull'intelligenza artificiale con la piattaforma SASE di Cloudflare
su traffico Web, SaaS, e-mail e cloud



Protezione dei dati in linea e in tempo reale

- **DLP granulare:** impedisci l'esposizione di dati sensibili con rilevamenti basati sul contesto per PII, codice sorgente, dati dei clienti e altro ancora.
- **DLP per le e-mail in uscita:** contrassegna automaticamente i dati sensibili nelle e-mail in uscita, prevenendo perdite di dati accidentali.
- **Protezione dei prompt:** rileva e blocca prompt IA e risposte rischiosi basati sull'intento (ad esempio, tentativi di jailbreak, abuso di codice, richieste di PII).

Accesso sicuro e controlli per i client

- **Accesso sicuro alle app:** applica regole ZTNA (Zero Trust Network Access), come la scansione DLP granulare per le connessioni di IA agentica, in tutte le applicazioni aziendali.
- **Controlli della posizione del dispositivo:** controlla l'accesso in base a controlli granulari della posizione, come la crittografia del disco e la DLP degli endpoint abilitati.
- **Controlli clientless:** applica controlli dei dati basati su browser per salvaguardare l'accesso di terze parti e le politiche BYOD dei dipendenti.

Shadow IT e rischi relativi alla posizione di sicurezza

- **Rilevamento dello shadow IT e della shadow AI:** rileva e gestisci lo shadow IT e la shadow AI nel tuo ambiente. Quantifica il rischio con i punteggi di affidabilità delle app e i parametri di trasferimento dei dati per mitigare rapidamente l'esposizione.
- **Gestione della posizione:** esegui la scansione delle app SaaS e degli ambienti cloud per identificare i rischi relativi alla posizione. Adotta misure prescrittive per rimediare ai risultati di sicurezza.
- **Controllo tenant:** blocca i tenant personali delle app SaaS per impedire l'esfiltrazione dei dati.

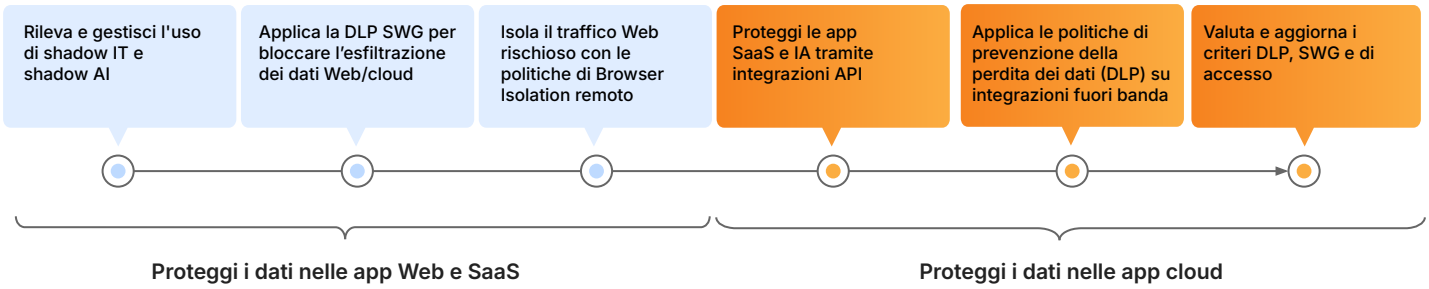
Integrazioni e reporting

- **Integrazioni CASB:** integra perfettamente con le principali piattaforme SaaS e AI (tra cui Microsoft 365, Google Workspace e ChatGPT) per scansioni CASB basate su API.
- **Integrazione Microsoft MIP:** sincronizza continuamente con Microsoft Information Protection (MIP) etichette per criteri DLP coerenti.
- **Osservabilità e analisi forense**: registra in modo sicuro i dati sul tuo SIEM preferito per l'audit oppure analizza i log all'istante tramite la dashboard o l'API.

Esempio di percorso di protezione dei dati

Inizia con l'individuazione dell'utilizzo di shadow IT e shadow AI per la visibilità della superficie di attacco. Configura i criteri DLP fondamentali su SWG per bloccare la perdita di dati ad alto rischio da app cloud non gestite e distribuisci RBI per il traffico web non approvato.

Quindi, distribuisci CASB per proteggere le app SaaS e IA autorizzate correggendo le configurazioni errate e applicando criteri di condivisione interna. Perfeziona e integra criteri granulari di DLP e accesso su SWG, e-mail e CASB per ottenere una prevenzione automatizzata e unificata su tutti i principali vettori di dati.



Casi d'uso di esempio per iniziare

- **Blocca l'esfiltrazione in tempo reale di PII/PHI** su tutti i canali di comunicazione e archiviazione non approvati.
- **Proteggi il codice sorgente e la proprietà intellettuale (IP)** dal furto interno e dalla distribuzione non autorizzata.
- **Applica politiche di protezione dei prompt** per le app GenAI per prevenire l'esposizione dei dati sensibili e la contaminazione dei modelli.
- **Previeni configurazioni errate** e applica controlli di accesso granulari su tutte le app SaaS e IA.

Risultati del cliente

EESTI RAUDTEE

Fornitore di infrastruttura
Leggi il case study

Mitiga la perdita di dati e le vulnerabilità SaaS

identificando fughe di dati e configurazioni errate.

APPLIED

Tecnologia assicurativa
Leggi il case study

Isola strumenti di IA generativa pubblici come ChatGPT

per impedire il copia-incolla di dati sensibili

Flo

App leader per la salute
Leggi il case study

Proteggi i dati dei pazienti

e ottieni la conformità con la sicurezza della posta elettronica e Zero Trust.

CREDIT SAISON INDIA

Prestatore NBFC
Leggi il case study

Proteggi le informazioni di identificazione personale (PII) e raggiungi la conformità

per evitare l'uscita indesiderata dei dati.

Sei pronto a parlarci delle tue esigenze di protezione dei dati?

Richiedi un workshop

1. Ricerca Manage Engine 2025: Fonte
2. 2025 United Nations Conference on Trade & Development: Fonte

