Cloudflare One for Data Protection

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

Protezione unificata per i dati ovunque

I moderni rischi legati ai dati richiedono una sicurezza moderna

Oggi i dati stanno esplodendo in volume, varietà e velocità e le organizzazioni si trovano ad affrontare rischi crescenti posti da:

Ambienti cloud e SaaS in espansione
↳ compresi strumenti di intelligenza artificiale emergenti opachi come ChatGPT
↳ portando all'esposizione del prezioso codice sorgente

La **suite di protezione dei dati di Cloudflare One** è progettata per rimanere in prima linea contro questi rischi decisamente moderni.

Unificando soluzioni mirate su un'unica piattaforma e rete, Cloudflare offre una protezione dei dati che è:

- **Più efficace**, grazie alla semplificazione della gestione di policy e connettività
- **Più produttiva**, garantendo esperienze utente rapide, affidabili e coerenti in qualsiasi posto
- **Più agile**, grazie all'innovazione rapida per rispondere ai requisiti di sicurezza in continua evoluzione

Un solo Security Services Edge (SSE) per proteggere i dati su app Web, SaaS e private

Adotta progressivamente Cloudflare nel tuo percorso verso SSE per:

1. Proteggere l'accesso ai dati con Zero Trust
2. Bloccare minacce come phishing e ransomware
3. Rilevare e bloccare le tue informazioni più sensibili

Naviga nei crescenti rischi legati ai dati...

Impronta SaaS tentacolare

L'82%

delle violazioni ha interessato i dati archiviati in ambienti cloud.[1]

E, naturalmente, i costi della violazione dei dati continuano ad aumentare, con un aumento del 15% negli ultimi 3 anni. [1]

Norme nuove e diversificate

Il 71%

di tutti i paesi ha una legislazione per proteggere i dati e la privacy.[2]

Negli Stati Uniti, **11 Stati** ora dispongono di leggi esaustive sulla protezione dei dati, rispetto alle 3 presenti nel 2021.[3]

Trasformazione digitale

L'89%

dei CISO afferma che procedere rapidamente con le iniziative di trasformazione digitale introduce rischi imprevisti nella protezione dei dati aziendali[4]

Caso d'uso 1: Protezione del codice degli sviluppatori

Problema

Il codice può essere esposto o oggetto di furto in molti strumenti di sviluppo, anche in luoghi ben visibili come archivi pubblici.

Soluzione

Esegui la scansione e risolvi i repository pubblici configurati in modo errato come GitHub che rischiano perdite di codice.Rileva il codice sorgente negli upload/download e applica i controlli.

→ GitHub

→ GitLab

→ Bitbucket

Caso d'uso 2: Visibilità dell'esposizione dei dati e gestione del rischio

→ OpenAI

→ Bard

→ GitHub Copilot

Problema

I dati abbracciano diversi ambienti SaaS e cloud, shadow IT non autorizzato e strumenti di intelligenza artificiale emergenti come ChatGPT, creando maggiori rischi di fuga di dati.

Soluzione

Esegui la scansione delle suite SaaS per configurazioni errate con rilevamenti DLP integrati per dati sensibili. Ottieni visibilità sull'utilizzo non autorizzato delle app, quindi consenti, blocca, isola o applica controlli Zero Trust per accedervi.

Caso d'uso 3: Rispetto delle normative

Problema

Requisiti legali più severi e più estesi per le aziende per mantenere i dati sicuri e privati, con sanzioni crescenti in caso di non conformità.

Soluzione

Identifica e applica controlli alle classi di dati regolamentati (informazioni di identificazione personali, sanitarie, finanziarie).Mantieni audit trail dettagliati tramite log e ulteriori analisi SIEM.Riduci la superficie di attacco con un approccio di sicurezza Zero Trust completo.

- ✓ GDPR
- ✓ DPDP
- ✓ CCPA
- ✓ CPRA
- ✓ GLBA
- ✓ PCI DSS
- ✓ HIPAA
- ✓ ISO
- ✓ Molti altri!

Come funziona

Una piattaforma unificata

Cloudflare riunisce visibilità e controlli di DLP, CASB, ZTNA, SWG, RBI e servizi di sicurezza e-mail in un'unica piattaforma per una gestione più semplice.

Una rete programmabile

Un piano di controllo con servizi basati sulla nostra piattaforma di sviluppo per applicare controlli sui dati in transito, in uso e inattivi in tutti i punti di applicazione: ambienti di app Web, SaaS o private.

Controlli di esempio con servizi componibili

Applica DLP per i dati in transito e proteggi l'accesso

- Esegui la scansione dei dati sensibili nel traffico e nei file e configura le policy di blocco con DLP.
- Scopri e gestisci lo shadow IT con CASB.
- Proteggi l'accesso ai dati nelle app con ZTNA.
- Blocca i tenant personali delle app SaaS per impedire l'esfiltrazione dei dati.

Isola le app per proteggere i dati in uso

- Blocca copia/incolla, upload/download, stampa, input da tastiera: il tutto senza un client del dispositivo.
- La distribuzione clientless è perfetta per dispositivi non gestiti, utenti di terze parti e strumenti di intelligenza artificiale come ChatGPT.
- Applica politiche DLP all'interno di app isolate.

Proteggi i dati a riposo nelle app SaaS

- Scansiona le app SaaS per individuare attività sospette, configurazioni errate e dati sensibili.
- Adotta misure prescrittive per rimediare ai rischi tramite le politiche SWG.

Integrazione per semplificare conformità e controlli

- Logpush al tuo SIEM preferito per la correlazione e il controllo.
- Integrazione con 18 delle suite SaaS più popolari per scansioni CASB basate su API.
- Sincronizza continuamente con le etichette Microsoft Information Protection (MIP) per i tuoi criteri DLP.

Migliore protezione dei dati con Cloudflare

Più efficace *grazie alla riduzione della complessità*

Semplifica la connettività con molte opzioni flessibili per inviare il traffico a Cloudflare per l'applicazione.

Utilizza scansioni basate su API per suite SaaS o modalità clientless per ZTNA e RBI per proteggere l'accesso alle app.Per inoltrare il traffico proxy, utilizza un client del dispositivo o le rampe di rete WAN tra i servizi di sicurezza.

Più produttivo grazie al miglioramento delle esperienze utente

La nostra rete è ovunque, garantendo che i controlli vengano applicati con un'ispezione a passaggio singolo vicino agli utenti finali e ai dati ovunque si trovino.

Affidabili e non intrusive, le esperienze degli utenti finali significano che l'applicazione dei controlli sui dati non interrompe mai il lavoro. Dimostrato più veloce dell'SSE dei concorrenti.

Più agile *grazie all'innovazione con velocità*

La nostra architettura di rete programmabile ci consente di sviluppare rapidamente funzionalità, così puoi adattarti ai nuovi rischi con agilità.

Adottiamo rapidamente nuovi standard e protocolli di sicurezza (come le connessioni solo IPv6 o la crittografia HTTP/3) in modo che la protezione dei dati rimanga aggiornata.

Cosa dicono i clienti

"Oggi, Cloudflare One aiuta a impedire ai nostri utenti di condividere dati e codici sensibili con strumenti come ChatGPT e Bard, permettendoci di sfruttare l'intelligenza artificiale in modo sicuro... Guardando al futuro, siamo entusiasti delle continue innovazioni di Cloudflare per proteggere i dati e, in particolare, i loro dati. visione e roadmap per servizi come DLP e CASB".

Tanner Randolph
Chief Information Security Officer (CISO)

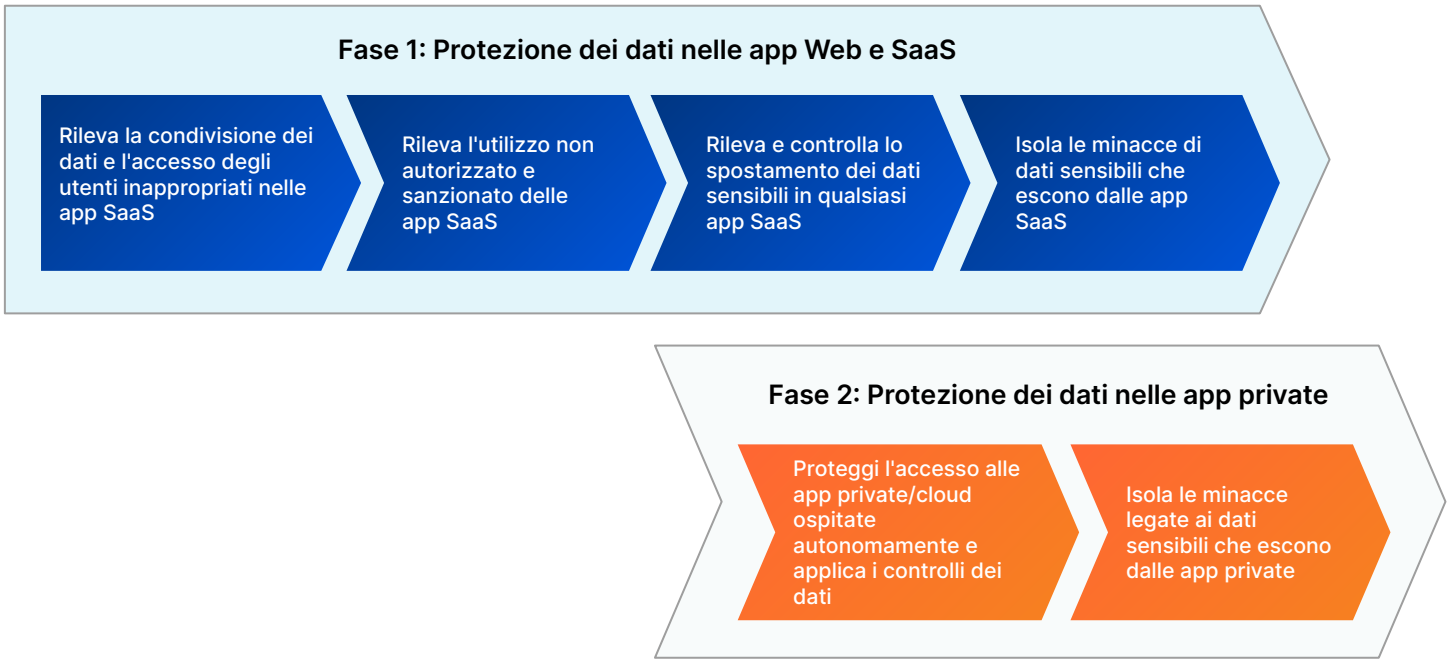
Applied Systems

Leggi il case study

Altri casi d'uso

- **Azienda di gas naturale inclusa nella lista Fortune 500** per proteggere l'accesso degli appaltatori ai dati
- **Importante sito di lavoro statunitense** per la protezione del codice e delle informazioni personali
- **Compagnia aerea regionale statunitense** per mitigare i rischi di esposizione dei dati dei clienti
- **Azienda sanitaria australiana** per proteggere i dati medici regolamentati
- **Produttore statunitense di dispositivi medici** per semplificare la conformità HIPAA

Percorsi di adozione comuni



Introduzione

SCOPRI...

come escalare i rischi dei dati in questa infografica

IMPEGNATI...

come funziona la piattaforma in questa demo

DIMOSTRA...

il valore richiedendo un workshop di consulenza

1. Report Costo di una violazione dei dati 2023, IBM
2. United Nations Conference on Trade & Development
3. International Association of Privacy Professionals (IAPP)
4. Report 2023 "Stato del CISO"