CLOUDFLARE

SINTESI DELLA SOLUZIONE

Cloudflare AI Security Suite

Proteggi le interazioni dell'IA controllando i dati e gestendo i rischi durante l'intero ciclo di vita dell'IA.

Scala con sicurezza l'IA

I rischi dell'intelligenza artificiale richiedono una sicurezza moderna

I tuoi team utilizzano l'intelligenza artificiale per innovare più velocemente, ma ciò crea rischi critici per la sicurezza. Il vecchio schema di bloccare l'intelligenza artificiale o di aggiungere soluzioni puntuali complesse sta fallendo perché soffoca l'innovazione e ignora la realtà:

- **L'85% dei dipendenti** utilizza strumenti di intelligenza artificiale prima che l'IT possa verificarli.[1]
- **Il 93% ammette** di inserire dati aziendali nell'intelligenza artificiale senza approvazione.[2]
- **Il 63% delle organizzazioni violate** non ha politiche di governance dell'IA.[1]

Impara a potenziare i tuoi team e a sfruttare i vantaggi dell'intelligenza artificiale in termini di produttività, mantenendo al contempo la sicurezza e il controllo di cui la tua azienda ha bisogno.

Una piattaforma unificata per proteggere l'IA agentica e l'IA generativa

Cloudflare fornisce un'unica piattaforma che consente alla tua organizzazione di adottare l'intelligenza artificiale con sicurezza. Diamo ai responsabili della sicurezza gli strumenti per gestire i rischi, ai team tecnologici per aumentare la produttività e agli ingegneri delle piattaforme per creare in modo sicuro, garantendo che tutti possano innovare insieme in tutta sicurezza.

Inizia a utilizzare Cloudflare AI Security Suite

Cloudflare AI Security Suite viene fornito su una piattaforma unificata per garantire l'utilizzo sicuro degli strumenti di intelligenza artificiale e delle applicazioni rivolte al pubblico nell'area di lavoro. Scopri la shadow AI, tutela i modelli dagli abusi, proteggi l'accesso degli agenti e previeni l'esposizione dei dati nei prompt, in modo che la tua azienda possa innovare in modo sicuro ed efficiente, con maggiore visibilità e un controllo più solido.

Estendere la visibilità

attraverso app IA, endpoint API e connessioni di agenti IA.

Mitigare i rischi

con guardrail, controllo dello stato e mitigazione delle minacce in tempo reale

Proteggere i dati

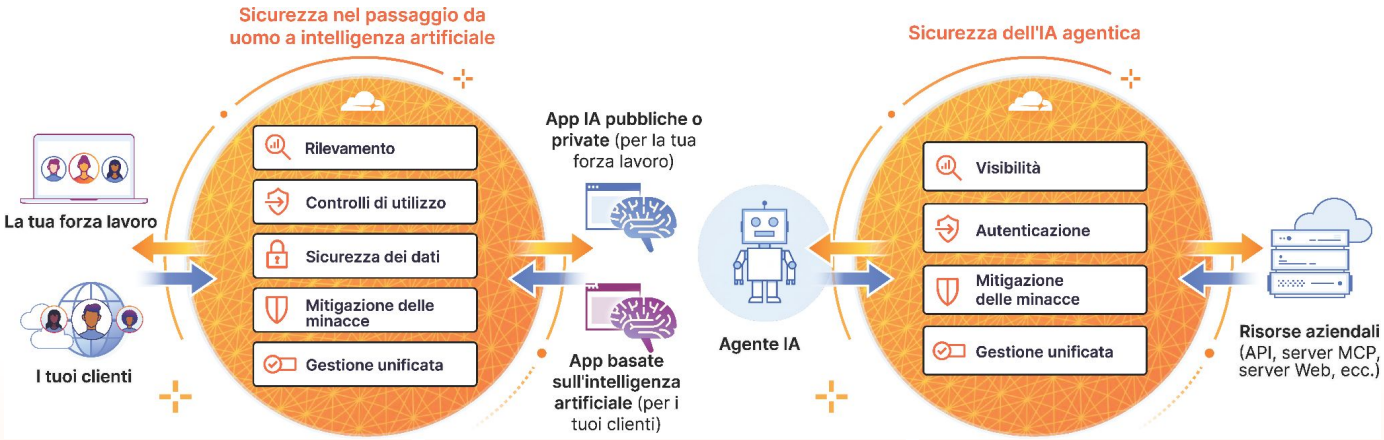
con protezioni dei prompt e controlli di utilizzo per dipendenti e agenti IA.

La sicurezza è integrata
quando si sviluppa l'intelligenza artificiale su Cloudflare.

 | +44 20 3514 6970 | enterprise@cloudflare.com | www.cloudflare.com/it-it/

Proteggere la comunicazione con l'IA generativa e l'IA agentica con Cloudflare AI Security Suite

Proteggi tutte le comunicazioni dell'IA controllando i dati utilizzati dalla tua forza lavoro nell'IA generativa e gestendo i rischi per la sicurezza rappresentati dagli agenti autonomi.

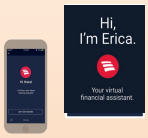


- **La tua forza lavoro:** dipendenti, collaboratori, sviluppatori, ecc.
- **I tuoi clienti:** visitatori dei tuoi siti Web e app

- **App di IA generativa:** autonome o integrate

Gemini ChatGPT Claude Copilot

- **App abilitate all'intelligenza artificiale** ad esempio, il chatbot IA di Bank of America, Erica



- **API** e **server MCP** per qualsiasi applicazione.

Google Workspace

- **Server Web** per l'inferenza e la generazione aumentata dal recupero (RAG)

Accelerare l'adozione dell'IA con la sicurezza integrata fin dalla progettazione durante tutto il ciclo di vita dell'IA

Proteggere l'uso dell'IA per la forza lavoro

Implementa i controlli sull'utilizzo dell'intelligenza artificiale e la gestione dello stato di sicurezza dell'intelligenza artificiale (AI-SPM) per mitigare i rischi e proteggere i dati.

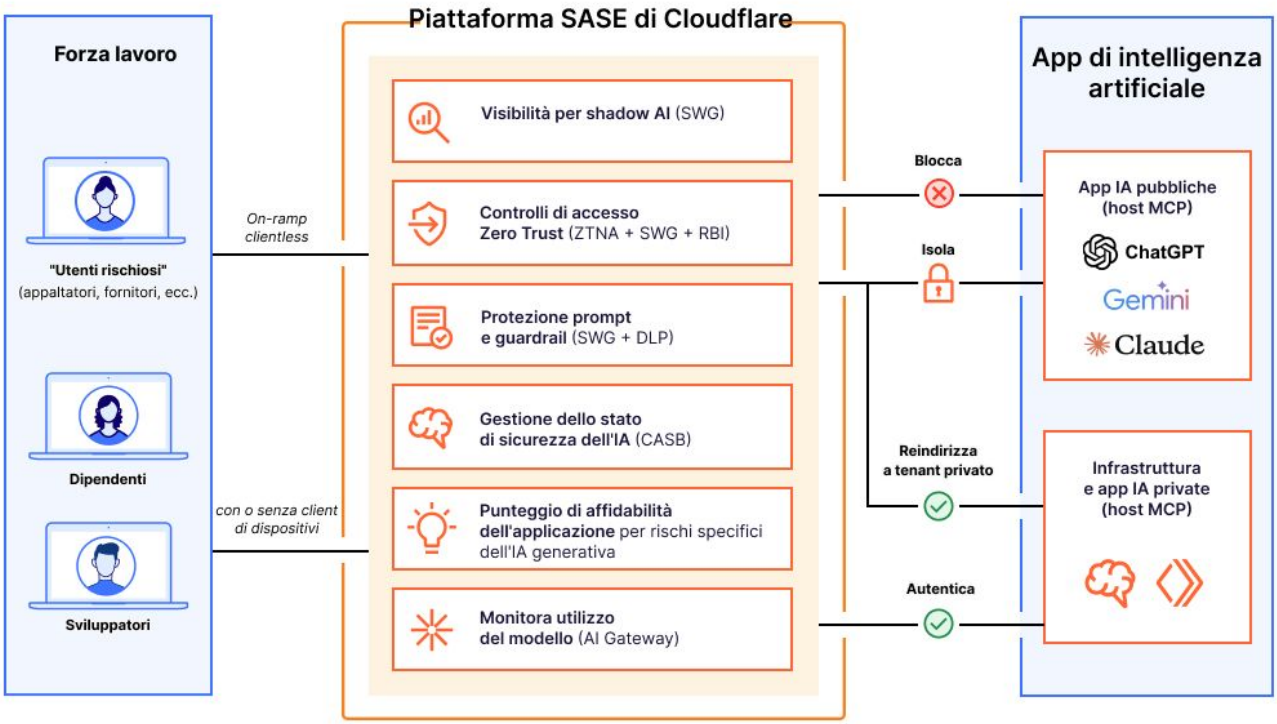
Proteggere le applicazioni basate sull'IA

Proteggi le tue app e API IA dall'inoculazione di prompt e dalle fughe di dati in tempo reale.

Costruire l'IA in modo sicuro

Consenti agli sviluppatori di proteggere le app IA con funzionalità di osservabilità integrate, limitazione della frequenza e sistemi di protezione IA in linea.

Proteggi l'utilizzo di app e carichi di lavoro IA da parte della forza lavoro con la piattaforma SASE di Cloudflare



SSE per proteggere la comunicazione da uomo a intelligenza artificiale

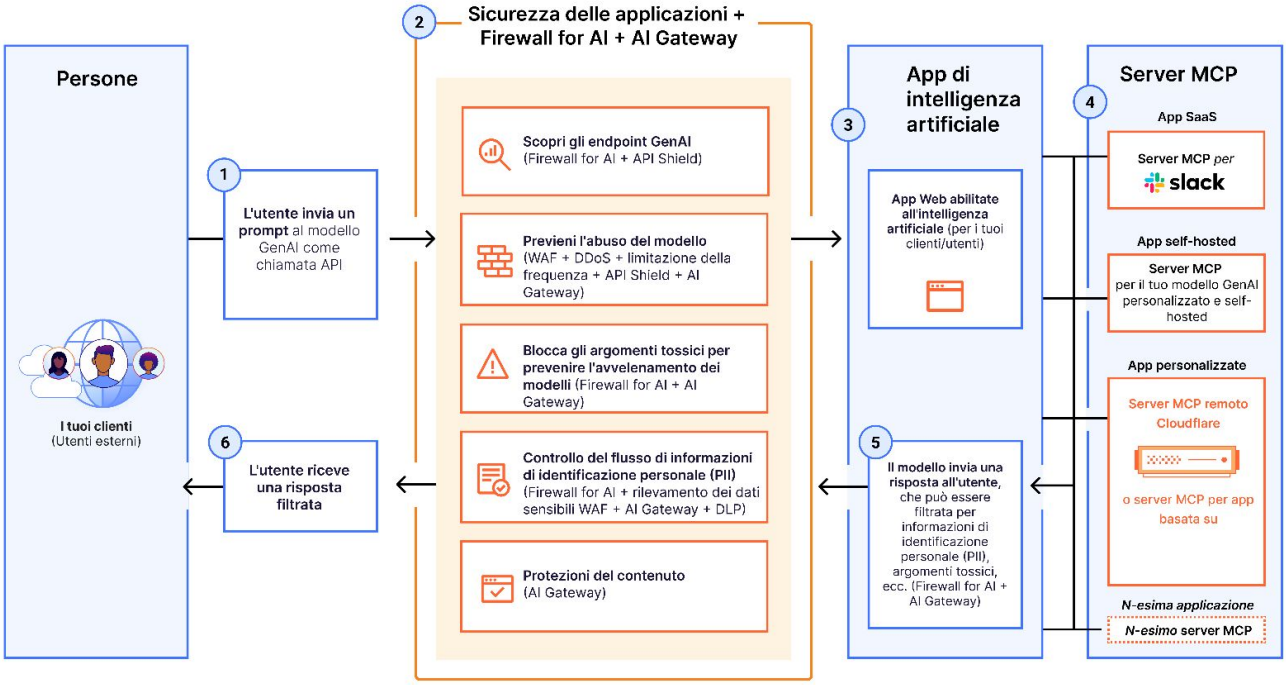
- **Visibilità:** scopri e analizza l'uso della shadow AI tramite l'ispezione del traffico in linea. Valuta i rischi posti da tali app di intelligenza artificiale con punteggi trasparenti.
- **Controlli degli accessi:** blocca, isola, reindirizza o consenti le connessioni utente. Applica regole Zero Trust basate sull'identità per app.
- **Protezione dei prompt e guardrail**: rileva e blocca i prompt degli utenti in base all'intento (ad esempio, tentativi di jailbreak, abuso di codice, richieste di informazioni di identificazione personale).
- **Sicurezza dei dati:** impedisci l'esposizione di dati sensibili con rilevamenti di prevenzione della perdita di dati (DLP) basati sull'IA per informazioni di identificazione personale (PII), codice sorgente e altro.
- **Gestione dello stato di sicurezza IA:** integra gli strumenti di GenAI tramite API per la scansione di configurazione errate con il nostroCloud Access Security Broker (CASB). Disponibile ora per ChatGPT, Claude, e Google Gemini.

MCP Server Portals per proteggere la comunicazione tra IA e risorse

- **Visibilità:** aggrega tutti i log delle richieste del Model Context Protocol (MCP) per audit e analisi. Verifica e approva ciascun server MCP prima di aggiungerlo al portale.
- **Autenticazione:** autentica l'accesso degli utenti al portale in base all'identità. Limita l'accesso ai server MCP in base al principio del privilegio minimo.
- **Connessioni:** connetti tutti i server MCP accessibili con un singolo URL, invece di configurare singolarmente ogni server MCP.
- **Gestione unificata:** applica gli stessi criteri di accesso granulari per le tue connessioni IA come fai per i tuoi utenti umani.

Nota: MCP Server Portals supporta qualsiasi server MCP inclusi, ma non solo, i server MCP remoti creati o distribuiti su Cloudflare. Questa funzionalità è disponibile come controllo Zero Trust Network Access (ZTNA).

Proteggere le app e i carichi di lavoro abilitati all'IA con la sicurezza in linea indipendente dal modello di Cloudflare



Proteggere l'intelligenza artificiale rivolta al pubblico con la sicurezza delle applicazioni e Firewall for AI per

- **Rilevare gli endpoint GenAI:** individua automaticamente tutti i modelli IA e le API nelle tue proprietà Web.
- **Proteggere i modelli di IA dagli abusi:** utilizza il nostro Firewall for AI appositamente progettato per bloccare la prompt injection, l'avvelenamento dei modelli, l'utilizzo eccessivo e altre minacce che potrebbero aggirare le tradizionali protezioni di sicurezza.
- **Controllare il flusso di informazioni di identificazione personale (PII):** scansiona i prompt degli utenti e le risposte dei modelli per bloccare l'esposizione di dati sensibili, mantenendo la conformità.
- **Guardrail dei contenuti:** blocca i prompt non sicuri o tossici utilizzando modelli integrati come Llama Guard. Crea regole WAF personalizzate per bloccare o registrare facilmente le interazioni sospette dell'IA.

Proteggere l'IA creata con la piattaforma per sviluppatori e AI Gateway

- **Piano di controllo IA unificato:** gestisci tutte le tue app IA da un unico dashboard. Instrada le richieste, memorizza le risposte nella cache, controlla i costi e monitora le prestazioni.
- **Proteggere le credenziali sul perimetro:** archivia in modo sicuro chiavi API e segreti sul perimetro, prevenendo l'esposizione lato client e semplificando la rotazione delle chiavi tra i provider.
- **Applicare le protezioni di sicurezza dei contenuti:** identifica e blocca oppure oscura automaticamente i contenuti dannosi e le informazioni di identificazione personale (PII) nei prompt e nelle risposte.

Cloudflare è l'unico fornitore in grado di proteggere sia gli ambienti IA pubblici che quelli privati

Implementa le giuste misure di sicurezza per adottare l'intelligenza artificiale con sicurezza, assicurandoti che acceleri l'innovazione, non la ostacoli.

- **Protezione unificata dell'ecosistema IA:** gli stack di sicurezza complessi aumentano il rischio. Utilizza un'unica piattaforma per proteggere i dati e garantire la conformità durante l'intero ciclo di vita dell'IA.
- **Architettura globale a prova di futuro:** previeni oggi le problematiche di domani con una rete post-quantistica sicura, scalabile per qualsiasi volume di traffico, in grado di adattarsi costantemente alle nuove minacce e programmabile per nuovi casi d'uso.
- **Sicurezza basata sull'IA:** le nostre difese basate sull'IA analizzano prompt e risposte per il rilevamento delle minacce in tempo reale.
- **Leadership comprovata nel campo dell'IA:** innova con sicurezza su una piattaforma scelta dall'80% delle prime 50 aziende GenAI.
- **Distribuzione indipendente dal modello:** i controlli di sicurezza funzionano per tutti i modelli di intelligenza artificiale presenti nel tuo ambiente, fornendo un approccio unificato per gestire le distribuzioni di intelligenza artificiale.

Cosa dicono i clienti

indeed

Sito Web di ricerca lavoro numero 1 al mondo
Leggi il case study

Identificare e controllare la shadow AI

In parallelo con il progetto di sostituzione della VPN

APPLIED

Tecnologia assicurativa
Leggi il case study

Isola strumenti di IA generativa pubblici come ChatGPT

per impedire il copia-incolla di dati sensibili

Azienda SaaS abilitata all'intelligenza artificiale

Proteggere le informazioni di identificazione personale (PII)

impedendo ai clienti di inviare informazioni sensibili a endpoint GenAI pubblici

Cyndx

Fintech basata sull'IA

Costi di inferenza ridotti del 95%

adottando Cloudflare per memorizzare nella cache ed eseguire le risposte dai fornitori di modelli di IA

Vuoi discutere delle tue esigenze di sicurezza dell'IA?

Parla con un esperto

1. Ricerca Manage Engine 2025: Fonte
2. 2025 IBM, report Cost of a Data Breach report: Fonte

