CLOUDFLARE

Accelera l'adozione dell'intelligenza artificiale con la sicurezza fin dalla progettazione

L'intelligenza artificiale è qui e la sicurezza tradizionale è stata abbandonata

98%

Il 98% delle organizzazioni dispone di app non autorizzate, tra cui la shadow AI. Questi punti ciechi rischiano di esporre i dati e violare la conformità.[1]

50%

Tasso di successo del 50% degli attacchi di prompt injection, la principale minaccia alla sicurezza nella classifica OWASP Top 10 per le app LLM.[2]

97%

Il 97% delle organizzazioni che hanno subito incidenti di sicurezza legati all'intelligenza artificiale non disponeva di adeguati controlli di accesso all'IA.[3]

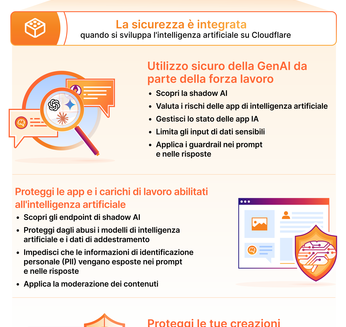
93%

Il 93% dei dipendenti ammette di inserire informazioni negli strumenti di intelligenza artificiale senza approvazione.[4]

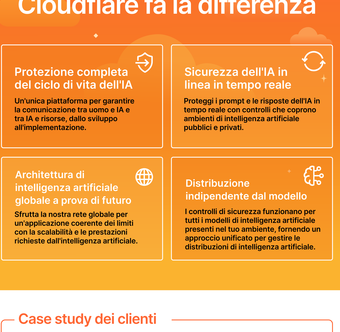
Proteggi il ciclo di vita dell'IA con Cloudflare

attraverso l'IA generativa e l'IA agentica

Sicurezza nel passaggio da uomo a intelligenza artificiale



Sicurezza dell'IA agentica



Estendi la visibilità

attraverso app IA, endpoint API e connessioni MCP e agenti IA

Gestisci il rischio

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

Proteggi i dati

con protezioni dei prompt e controlli di accesso per dipendenti e agenti IA

La sicurezza è integrata

quando si sviluppa l'intelligenza artificiale su Cloudflare

Utilizzo sicuro della GenAI da parte della forza lavoro

- Scopri la shadow AI
- Valuta i rischi delle app di intelligenza artificiale
- Gestisci lo stato delle app IA
- Limita gli input di dati sensibili
- Applica i guardrail nei prompt e nelle risposte

Proteggi le app e i carichi di lavoro abilitati all'intelligenza artificiale

- Scopri gli endpoint di shadow AI
- Proteggi dagli abusi i modelli di intelligenza artificiale e i dati di addestramento
- Impedisci che le informazioni di identificazione personale (PII) vengano esposte nei prompt e nelle risposte
- Applica la moderazione dei contenuti

Proteggi le tue creazioni

- Crea server MCP con autenticazione/autorizzazione integrata
- Registra e limita le richieste/risposte del modello di intelligenza artificiale, l'uso dei token e i costi
- Previeni le interruzioni dei servizi con fallback dei modelli e limitazione della frequenza

Cloudflare fa la differenza

Protezione completa del ciclo di vita dell'IA

Un'unica piattaforma per garantire la comunicazione tra uomo e IA e tra IA e risorse, dallo sviluppo all'implementazione.

Sicurezza dell'IA in linea in tempo reale

Proteggi i prompt e le risposte dell'IA in tempo reale con controlli che coprono ambienti di intelligenza artificiale pubblici e privati.

Architettura di intelligenza artificiale globale a prova di futuro

Sfrutta la nostra rete globale per un'applicazione coerente dei limiti con la scalabilità e le prestazioni richieste dall'intelligenza artificiale.

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.

Case study dei clienti

indeed

Il sito Web di ricerca lavoro numero 1 al mondo

Identifica e controlla la shadow AI

in parallelo con il progetto di modernizzazione dell'accesso remoto

Azienda SaaS abilitata all'intelligenza artificiale

Protegge le informazioni di identificazione personale (PII)

impedendo ai clienti di inviare informazioni sensibili agli endpoint GenAI rivolti al pubblico

Cyndx

Azienda fintech basata sull'intelligenza artificiale

Costi di inferenza ridotti del 95%

adottando Cloudflare per memorizzare nella cache ed eseguire le risposte dei provider di modelli di intelligenza artificiale

Scopri come Cloudflare può proteggere la tua adozione dell'intelligenza artificiale

Esplora i casi d'uso

1. Varonis, 2025 State of Data Security
2. Yi Liu, Gelei Deng, Yuekang Li, Kailong Wang, Zihao Wang, Xiaofeng Wang, Tianwei Zhang, Yepang Liu, Haoyu Wang, Yan Zheng, Leo Yu Zhang, "Prompt Injection attack against LLM-integrated Applications", Y. (2024). Automatic and Universal Prompt Injection Attacks against Large Language Models.
3. IBM, 2025 Cost of a Data Breach
4. ManageEngine, The Shadow AI Surge in Enterprises

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

REVBDES-6376.2025OCT13

CLOUDFLARE