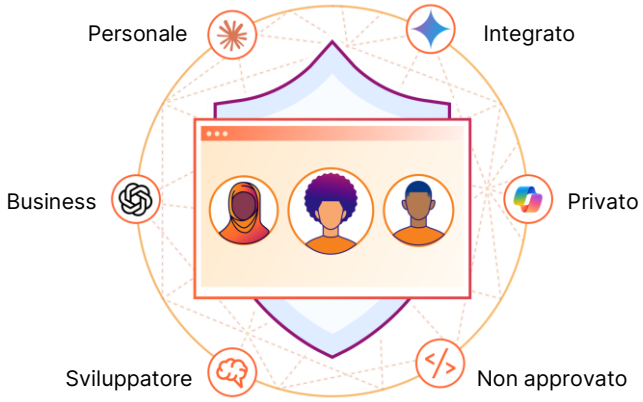
CLOUDFLARE

PANORAMICA DELLA SOLUZIONE

Proteggi l'uso dell'IA generativa e dell'IA agentica da parte della forza lavoro

Consenti ai tuoi team di utilizzare in modo sicuro qualsiasi strumento di intelligenza artificiale con le protezioni applicate dalla piattaforma SASE di Cloudflare.



Riprendi il controllo, aumenta la produttività

La corsa all'adozione dell'intelligenza artificiale sta lasciando dietro di sé una scia di rischi sempre maggiori, tra cui fughe di dati, violazioni normative e una superficie d'attacco in espansione. Bloccare completamente l'intelligenza artificiale significa solo sacrificare il proprio vantaggio competitivo, mentre sperimentare soluzioni puntuali non fa che aumentare la complessità.

Cloudflare salvaguarda l'uso dell'intelligenza artificiale da parte della tua organizzazione estendendo la visibilità, mitigando i rischi e proteggendo i dati in modo olistico negli ambienti di intelligenza artificiale:

- **Scopri la shadow AI** e gestisci i criteri per tutti gli strumenti di intelligenza artificiale autorizzati e non.
- **Rafforza la governance dell'IA** tramite controlli di accesso basati sull'identità e gestione della posizione.
- **Arresta la perdita di dati** bloccando le informazioni sensibili nei prompt utente, applicando misure di sicurezza specifiche ed eseguendo la scansione per individuare configurazioni errate negli strumenti di intelligenza artificiale.

Estendi Cloudflare per adottare l'intelligenza artificiale in modo sicuro, sia che la tua strategia IA preveda di limitarne l'uso ad applicazioni specifiche che di sperimentare una gamma più ampia di strumenti diversi.

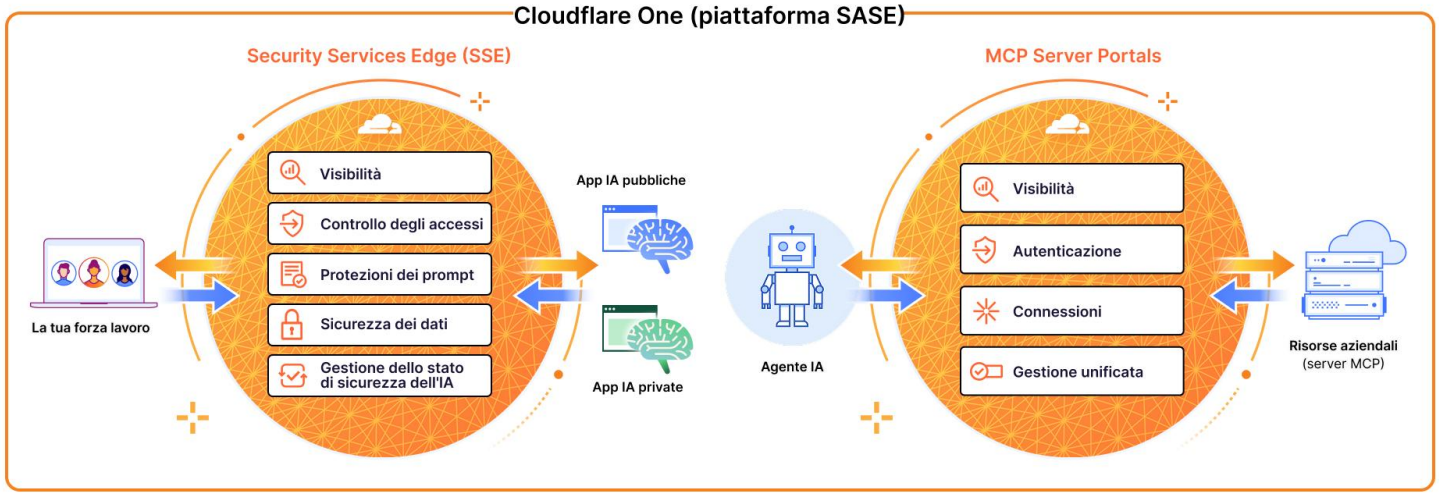
Perché scegliere SASE per proteggere l'uso dell'IA da parte della forza lavoro

La piattaforma Secure Access Service Edge (SASE) di Cloudflare si posiziona tra la tua forza lavoro e gli strumenti di intelligenza artificiale. Ciò la rende un punto di partenza ideale per chi vuole iniziare a utilizzare l'intelligenza artificiale in modo sicuro.

Che i dipendenti chattino con ChatGPT o che gli agenti IA raccolgano informazioni dalle risorse aziendali, la piattaforma SASE di Cloudflare applica controlli di sicurezza coerenti.

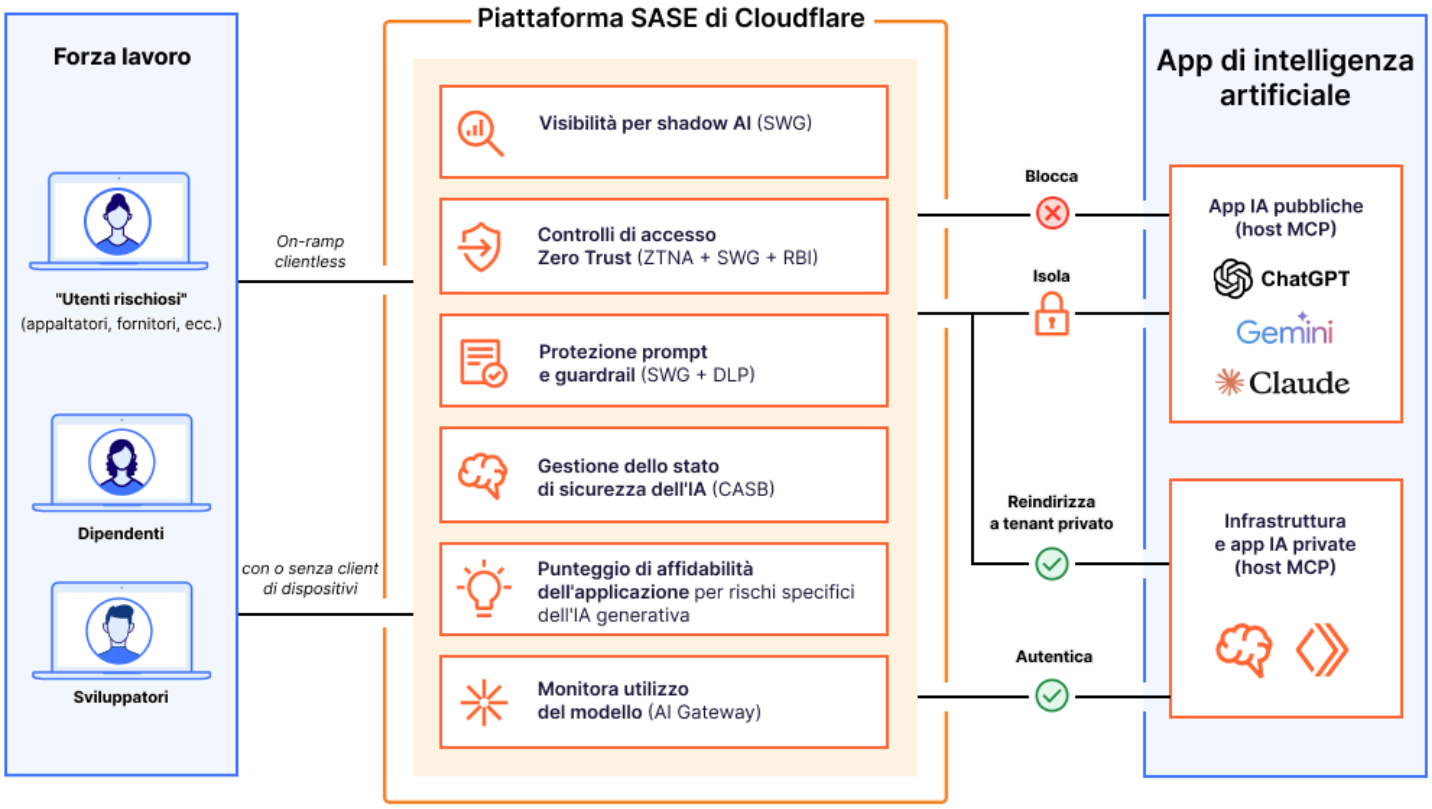
Proteggere la comunicazione dell'IA generativa e dell'IA agentica

La piattaforma SASE di Cloudflare offre un dashboard e un piano di controllo unificati per gestire le interazioni uomo-IA e macchina-macchina all'interno dell'organizzazione.



A differenza di altri fornitori SASE, Cloudflare aiuta anche a connettere e proteggere app e carichi di lavoro abilitati all'IA rivolti al pubblico, come il chatbot IA del tuo sito Web o i motori di raccomandazione.

Proteggi la comunicazione degli utenti con app di intelligenza artificiale generativa con controlli di utilizzo dell'intelligenza artificiale sulla piattaforma SASE di Cloudflare



- **Visibilità:** scopri e analizza la 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 le 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 GenAI tramite API (disponibile ora per ChatGPT, Claude e Google Gemini) per la scansione di errori di configurazione tramite il nostro Cloud Access Security Broker (CASB).

Risultati del cliente

indeed

Sito Web di ricerca lavoro numero 1 al mondo

Identifica e controlla la shadow AI

parallelamente al progetto di sostituzione della VPN

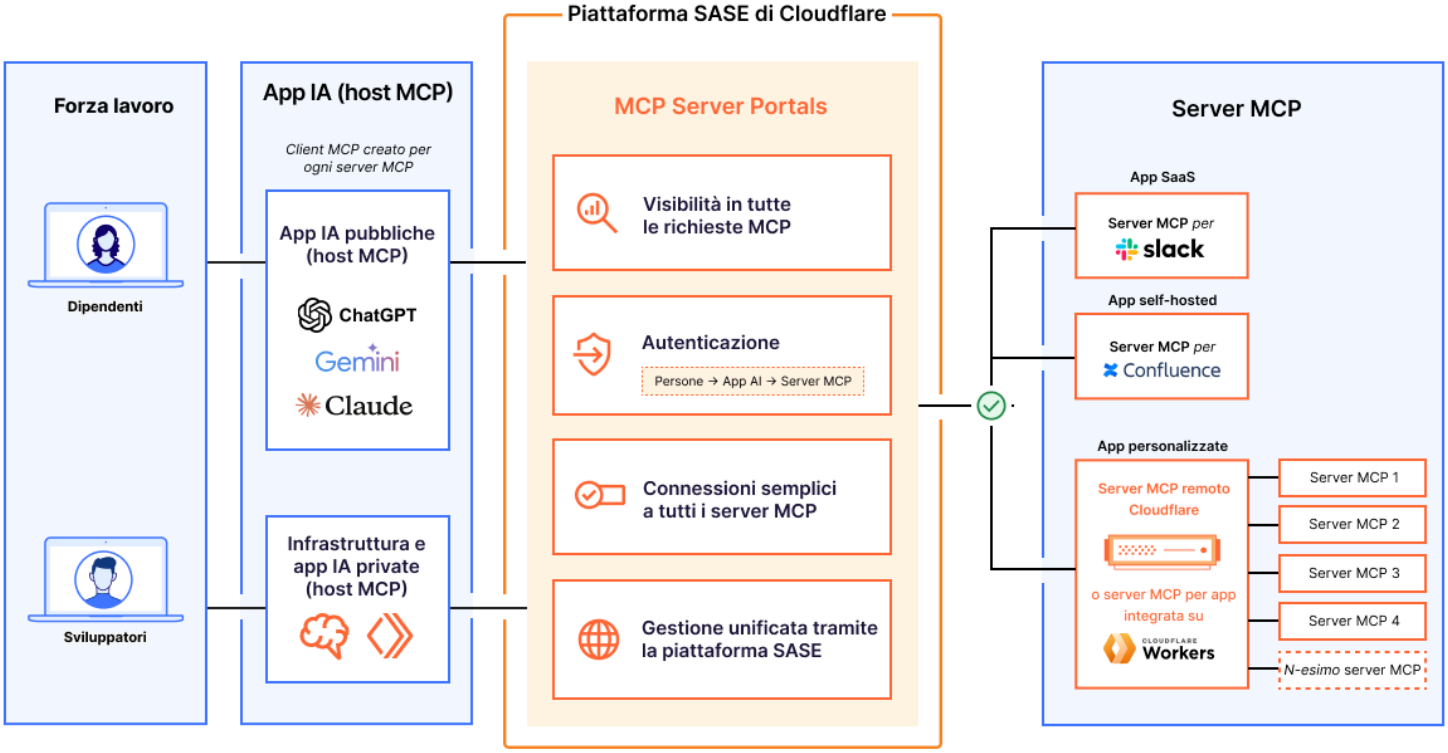
APPLIED

Tecnologia assicurativa

Isola gli strumenti GenAI pubblici come ChatGPT

per bloccare il copia-incolla di dati sensibili

Comunicazione sicura dell'IA agentica (da IA a risorsa)
con MCP Server Portals sulla piattaforma SASE di Cloudflare



- **Visibilità:** aggrega tutti i log delle richieste 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 connessioni IA come fai per gli utenti umani.
- **Personalizza gli strumenti per il portale:** scegli strumenti e modelli di prompt specifici resi disponibili per ogni utente.

Nota: MCP Server Portals di Cloudflare supporta qualsiasi server MCP incluso, ma non solo, qualsiasi server MCP remoto creato o distribuito su Cloudflare. Questa funzionalità è disponibile come controllo Zero Trust Network Access (ZTNA).

Scopri di più sulla nostra visione in questo blog.

Sei pronto a scoprire come Cloudflare può proteggere il tuo utilizzo dell'IA?

Richiedi un workshop

