CLOUDFLARE

SINTESI DEL PRODOTTO

Cloudflare Zero Trust

La più veloce piattaforma di navigazione e accesso alle applicazioni Zero Trust

Rischi oltre il perimetro

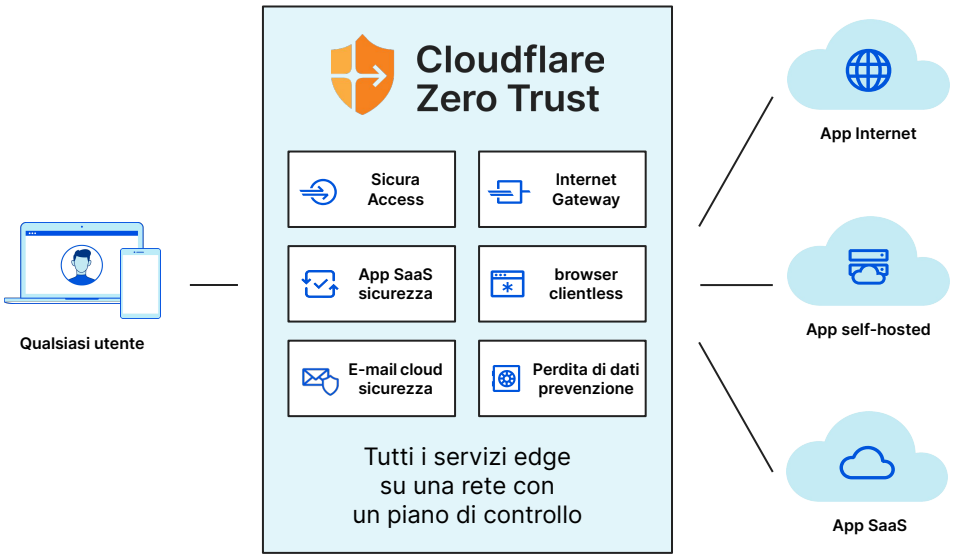
Quando le applicazioni e gli utenti hanno lasciato le pareti del perimetro aziendale, i team di sicurezza hanno dovuto scendere a compromessi su come mantenere i dati al sicuro. I metodi incentrati sulla posizione per la protezione del traffico (come VPN, firewall e proxy Web) sono crollati sotto pressione, lasciando le organizzazioni con visibilità limitata, configurazioni in conflitto e rischi eccessivi.

Con i rischi ormai presenti ovunque, per potersi adattare le organizzazioni si stanno orientando verso Zero Trust fornito nel cloud.

Adotta Zero Trust nativo per Internet

Cloudflare Zero Trust è una piattaforma di sicurezza che aumenta la visibilità, elimina la complessità e riduce i rischi degli utenti remoti e da ufficio che si connettono alle applicazioni e a Internet. In un'architettura a passaggio singolo, il traffico viene verificato, filtrato, ispezionato e isolato dalle minacce.

Opera su una delle reti Anycast più veloci al mondo in più di 275 città in oltre 100 paesi per essere implementato più velocemente e offrire prestazioni migliori rispetto ad altri provider.



Accesso sicuro
Semplifica e proteggi l'accesso per qualsiasi utente a qualsiasi applicazione, su qualsiasi dispositivo, in qualsiasi luogo

Difesa dalle minacce
Proteggi utenti e dati dalle minacce Web, e-mail e multi-canale.

Proteggi con Microsoft
Visibilità e controllo di tutte le suite SaaS su Microsoft, Google e altro

Lavoro ibrido sicuro
Migliora la produttività del team, ridurre il rischio informatico e aumenta l'efficienza tecnologica

Vantaggi aziendali

Riduci l'eccessiva fiducia

Proteggi le app con regole Zero Trust basate su identità e contesto. Blocca phishing, ransomware e altre minacce online. Isola gli endpoint dai rischi tenendo il codice non attendibile lontano dai dispositivi e l'attività degli utenti non attendibili dai dati.

Elimina la complessità

Riduci la dipendenza dai point product legacy e applica controlli di sicurezza standard a tutto il traffico, indipendentemente da come viene avviata la connessione o da dove si trova nello stack di rete.

Ripristina la visibilità

Log completi per attività DNS, HTTP, SSH, di rete e Shadow IT. Monitora l'attività degli utenti su qualsiasi app. Invia i log ai tuoi strumenti di analisi e archiviazione cloud preferiti.

Accesso sicuro (ZTNA)

Un modo più veloce, più facile e più sicuro per connettere qualsiasi utente a qualsiasi applicazione

Problema: Accesso lento, complesso e rischioso

I tradizionali controlli degli accessi basati sul perimetro (come le VPN) sono sempre più un ostacolo. Le prestazioni lente danneggiano la produttività dell'utente finale, gli amministratori hanno difficoltà con la configurazione ingombrante e il movimento laterale è difficile da contenere.

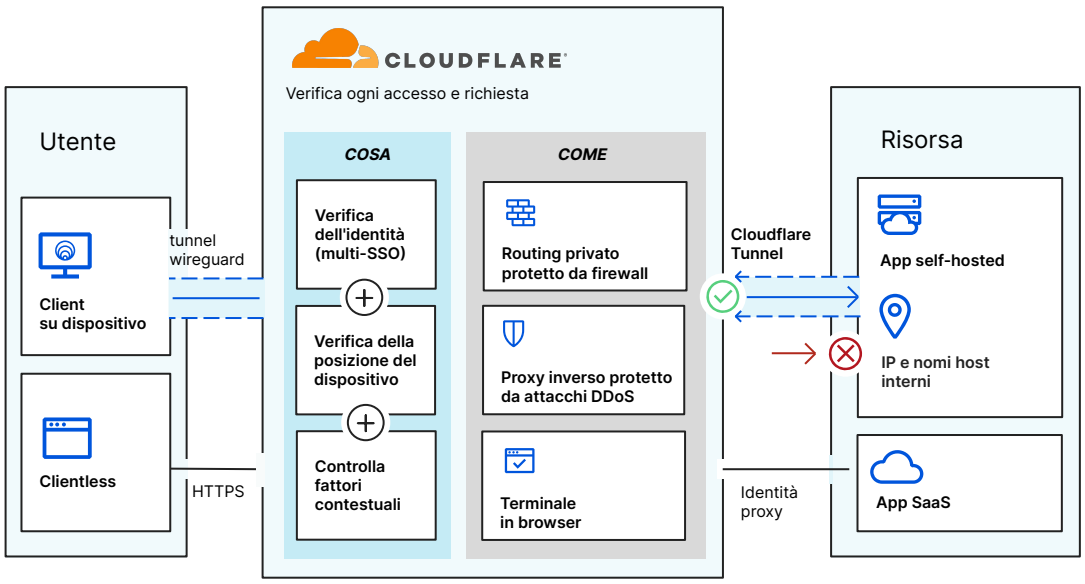
L'adozione accelerata del cloud e il lavoro ibrido hanno ulteriormente esposto questi difetti e reso le VPN più vulnerabili.

Zero Trust Network Access (ZTNA)

Il servizio ZTNA di Cloudflare, Access, aumenta o sostituisce i client VPN proteggendo qualsiasi applicazione, in qualsiasi rete on-premise, cloud pubblico o ambiente SaaS.

ZTNA di Cloudflare collabora con i provider di identità e le piattaforme di protezione degli endpoint per applicare regole Zero Trust di negazione predefinita che limitano l'accesso alle applicazioni aziendali, agli spazi IP privati e ai nomi host.

Come funziona



Distribuzione clientless
per app self-hosted basate su Web, SSH o VNC accessibili tramite browser.

Distribuisci con il client del dispositivo di Cloudflare
per connetterti a IP interni, nomi host e app non Web.

Casi d'uso principali

Supporta il lavoro a distanza e le iniziative BYOD

Verifica l'accesso per tutti gli utenti, ovunque si trovino, in base all'identità, alla posizione del dispositivo, al metodo di autenticazione e ad altri fattori contestuali.

Applica queste politiche Zero Trust per la tua forza lavoro ibrida. Supporta le iniziative BYOD (Bring Your Own Device) proteggendo i dispositivi gestiti o non gestiti.

Semplifica l'accesso di terze parti con flessibilità

Velocizza la configurazione degli accessi per appaltatori, fornitori, agenzie, collaboratori, ecc.

Integra più provider di identità (IDP) contemporaneamente. Imposta le regole del privilegio minimo in base agli IDP già utilizzati.

Evita il provisioning di licenze SSO, la distribuzione di VPN o la creazione di autorizzazioni una tantum.

Semplifica la configurazione amministrativa e il supporto

Aggiungi nuovi utenti, provider di identità o regole Zero Trust in pochi minuti.

Sblocca nuova produttività riducendo il tempo di onboarding dei dipendenti (eTeacher Group) e allontanandoti dalla configurazione degli accessi basata su IP (BlockFi). Non è necessario assumere personale dedicato per gestire le VPN (ezCater).

Difesa dalle minacce (SWG e RBI)

Filtra, ispeziona e isola il traffico diretto a Internet

Problema: il panorama delle minacce in evoluzione

Aumentare il livello di sicurezza mantenendo gli utenti produttivi non è mai stato così complicato. Il lavoro in remoto significa più dispositivi non gestiti che archiviano più dati sensibili in locale. Nel frattempo, ransomware, phishing, shadow IT e altre minacce basate su Internet stanno esplodendo in volume e sofisticatezza.

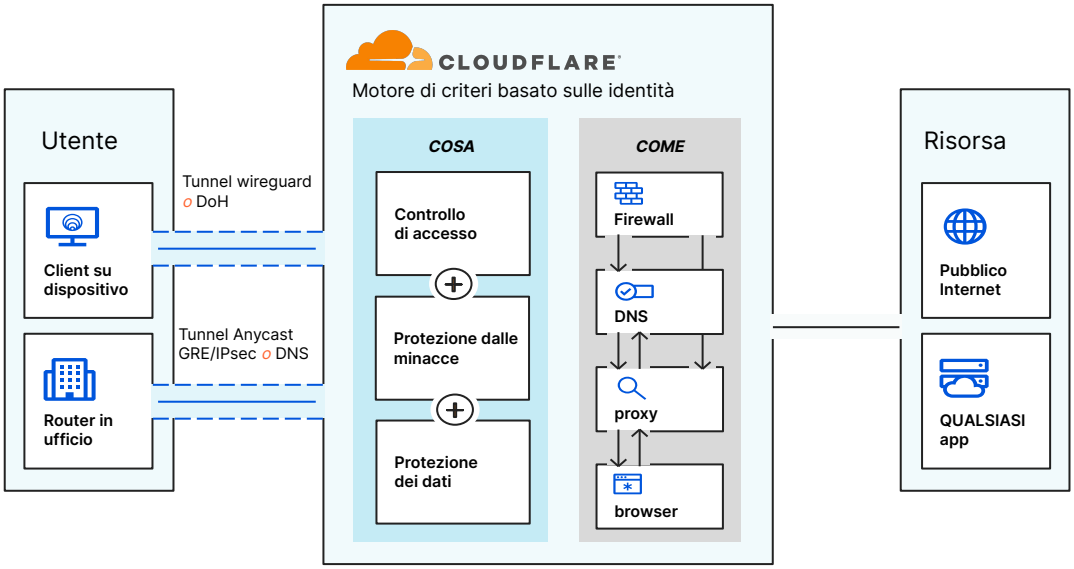
Affidarsi a soluzioni puntuali legacy e backup dei dati è una strategia rischiosa per proteggersi dalle minacce multi-canale.

SWG con navigazione Zero Trust

Cloudflare Gateway, il nostro Secure Web Gateway (SWG), protegge gli utenti con filtri Web basati sull'identità, oltre all'isolamento del browser remoto (RBI) integrato in modo nativo.

Inizia con il filtraggio DNS per ottenere un time-to-value rapido per gli utenti remoti o dell'ufficio. Successivamente, applica un'ispezione HTTPS più completa e, infine, estendi i controlli RBI per abbracciare Zero Trust per tutte le attività Internet.

Come funziona



Niente più backhauling.
Invia traffico L4-7 tramite Cloudflare anziché appliance legacy.

Filtri, ispezione e isolamento possono essere applicati sia al traffico delle risorse interno che a Internet.

Casi d'uso principali

Arresta il ransomware

Blocca siti e domini ransomware in base alla nostra intelligence di rete globale. Isola la navigazione su siti rischiosi per rafforzare la protezione.

Combina il filtro SWG e l'RBI con la negazione predefinita, ZTNA per mitigare il rischio che l'infezione da ransomware si diffonda lateralmente e aumenti i privilegi sulla rete.

Blocca il phishing

Filtra i domini di phishing noti e "nuovi"/"visti di recente". Isola la navigazione per impedire l'esecuzione locale di payload dannosi. Interrompi l'invio di informazioni sensibili su siti di phishing sospetti tramite i controlli di input da tastiera di RBI.

Inoltre, a breve, gli amministratori potranno attivare il filtro e-mail con un solo clic grazie ad Area 1.

Previeni la perdita dei dati

Implementa la prevenzione della perdita di dati (DLP) con controlli sui tipi di file in grado di impedire agli utenti di caricare file sui siti.

Distribuisci la navigazione Zero Trust per controllare e proteggere i dati che risiedono all'interno delle app basate sul Web. Controlla le azioni dell'utente all'interno del browser, come download, caricamento, copia-incolla, input da tastiera e funzionalità di stampa.

Proteggi con Microsoft (CASB)

Semplifica la sicurezza SaaS per una maggiore visibilità e controllo, con meno spese generali

Problema: Proliferazione delle app SaaS

La forza lavoro moderna si affida alle applicazioni SaaS come Microsoft 365 ora più che mai. Ma ogni app SaaS richiede considerazioni di sicurezza diverse e opera al di fuori delle salvaguardie del perimetro tradizionale.

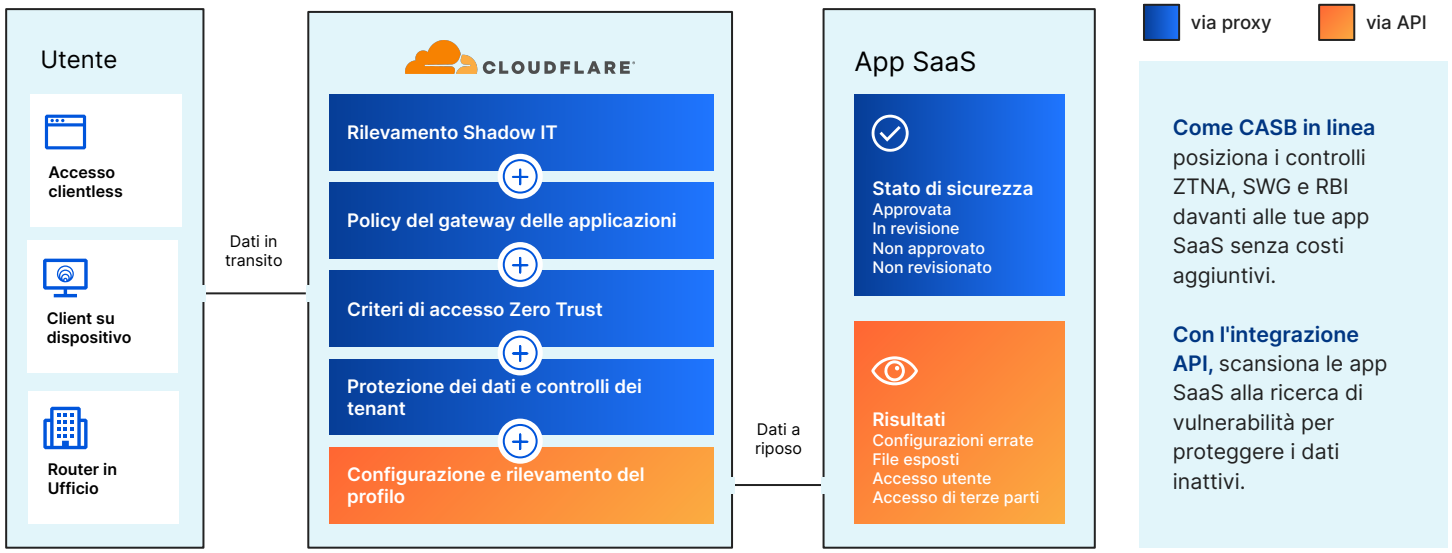
Poiché le organizzazioni adottano decine di app SaaS, diventa sempre più difficile mantenere sicurezza, visibilità e prestazioni coerenti.

Cloud Access Security Broker (CASB)

Il servizio CASB di Cloudflare offre visibilità e controllo completi sulle app SaaS, in modo da poter prevenire facilmente fughe di dati e violazioni della conformità.

Blocca le minacce interne, lo shadow IT, la rischiosa condivisione dei dati e i soggetti ostili. Registra ogni richiesta HTTP per rivelare applicazioni SaaS non autorizzate. Scansiona le app SaaS per rilevare configurazioni errate e attività sospette.

Come funziona



Casi d'uso principali

Applica i controlli sulla protezione dei dati e del tenant

Applica il controllo del tenant tramite i criteri del gateway HTTP per impedire agli utenti di accedere e archiviare i dati nelle versioni sbagliate delle app SaaS più diffuse, inavvertitamente o in modo dannoso.

Controlla le azioni utente (ad esempio, copia/incolla, download, stampa, ecc.) all'interno di applicazioni SaaS basate sul Web per ridurre al minimo il rischio di perdita di dati.

Mitiga e controlla lo Shadow IT

Riduci al minimo i rischi introdotti da applicazioni SaaS non approvate.

Cloudflare aggrega e classifica automaticamente tutte le richieste HTTP nel nostro registro attività in base al tipo di applicazione. Gli amministratori possono quindi impostare lo stato e tenere traccia dell'utilizzo delle app approvate e non approvate nell'organizzazione.

Identifica nuove minacce e configurazioni errate

Connettiti alle app SaaS più diffuse (Google Workspace, Microsoft 365, ecc.) tramite API e cerca i rischi.

Offri ai tuoi team IT e di sicurezza visibilità su autorizzazioni, configurazioni errate, accesso improprio e problemi di controllo che potrebbero mettere a rischio i loro dati e dipendenti.

Protezione dal phishing (CES)

Estendi Zero Trust alle e-mail per una protezione completa dalle minacce

Problema: I messaggi e-mail sono il principale vettore di minaccia

L'e-mail è il principale modo con cui i team comunicano, ma anche il principale modo con cui gli autori di attacchi riescono a cavarsela. In effetti, uno studio recente lo ha rilevato che il 91% di tutti gli attacchi informatici iniziano con un'e-mail di phishing.

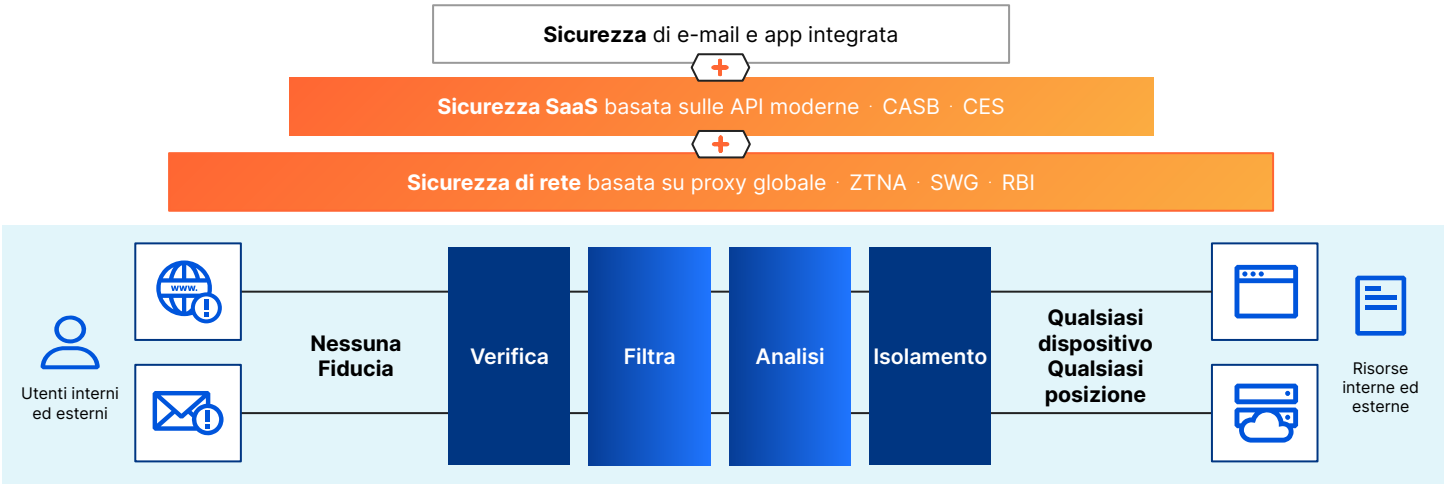
Gli autori di attacchi prendono spesso di mira e sfruttano con successo l'alto livello di fiducia che spesso viene dato alla comunicazione e-mail.

Integrazione della sicurezza e-mail nativa per il cloud

L'aggiunta di Area 1 Cloud Email Security (CES) come parte di una strategia Zero Trust completa rimuove la fiducia implicita dalla posta elettronica per fermare preventivamente gli attacchi di phishing e BEC (Business Email Compromise).

Tutto il traffico degli utenti, compresa la posta elettronica, viene verificato, filtrato, ispezionato e isolato dalle minacce note e sconosciute. Area 1 aiuta i clienti a bloccare le minacce trasmesse tramite e-mail, adottare una posizione di sicurezza proattiva e ridurre del 90% i tempi di risposta agli incidenti di phishing.

Come funziona: Zero Trust per tutto il traffico e-mail, Web e di rete



Casi d'uso principali

Previeni BEC e frodi basate su e-mail

Ferma gli attacchi BEC (Business Email Compromise) sofisticati e le acquisizioni degli account dei fornitori attraverso l'analisi del sentiment, la rappresentazione grafica dei social partner, la classificazione dei messaggi e l'analisi dell'origine della campagna.

Blocca, metti in quarantena e intensifica automaticamente le comunicazioni finanziarie fraudolente.

Proteggiti dagli attacchi multi-canale

Blocca facilmente le campagne di attacco che prendono di mira le persone attraverso più canali di comunicazione, come e-mail e Web, consentendo agli utenti di caricare in modo sicuro collegamenti sospetti o sconosciuti in un browser remoto e isolato.

Cattura gli attacchi di phishing posticipati che trasformano i link in un'arma dopo la consegna con la classificazione dei link in base al tempo del clic.

Accelera il triage e la risposta al phishing

Libera i cicli di indagine sulla sicurezza, ottieni informazioni utili sul tuo ambiente di posta elettronica e riduci i tempi di risposta con risorse dedicate che potenziano il tuo team esistente per neutralizzare rapidamente le minacce di phishing.

Ottieni ulteriore supporto e competenza in materia di sicurezza con i servizi di sicurezza della posta elettronica gestiti.

Lavoro ibrido sicuro: la differenza di Cloudflare

Sicurezza moderna per una forza lavoro moderna

Semplicità di distribuzione

Cloudflare offre una piattaforma uniforme e componibile per una facile configurazione e operazioni. Con connettori solo software e integrazioni una tantum, i nostri servizi Cloudflare on-ramp e edge funzionano tutti insieme.

Ciò porta a un'esperienza migliore per i professionisti IT e gli utenti finali.

Resilienza di rete

La nostra automazione del traffico end-to-end garantisce una connettività di rete affidabile e scalabile con una protezione coerente da qualsiasi luogo.

Con Cloudflare, a differenza di altri provider di sicurezza, ogni servizio perimetrale è progettato per essere eseguito in ogni posizione di rete, disponibile per ogni cliente.

Velocità di innovazione

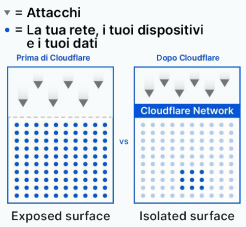
La nostra architettura all'avanguardia ci aiuta a costruire e fornire molto rapidamente qualcosa su cui abbiamo stabilito una solida reputazione.

Che si tratti della nostra rapida adozione di nuovi standard Internet e di sicurezza o della creazione di casi d'uso guidati dai clienti, la nostra storia di abilità tecnica parla da sé e la nostra base offre un'estrema possibilità di scelta.

5 modi in cui Zero Trust fa risparmiare tempo e denaro alla tua azienda

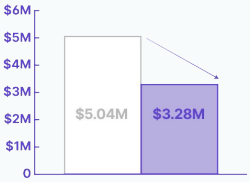
Riduci attacco superficie

91% ↓



Riduci violazione elevati

35% ↓

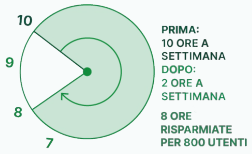


Accelera onboarding dei dipendenti

60% ↑

Riduci Ticket IT sovraccarico

80% ↓



Riduci Utente latenza

39% ↓

Ottimizzato per l'usabilità

Una sola interfaccia di gestione

Semplifica la configurazione con un pannello di controllo creato in modo nativo per le politiche di accesso a Internet e alle applicazioni.

Utilizza un pannello di controllo per l'integrazione con provider di identità, protezioni degli endpoint e on-ramp di rete.

Una piattaforma consolidata

Sostituisci un patchwork di client VPN, firewall locali e altre soluzioni di sicurezza dei punti con una piattaforma e un piano di controllo.

Riduci i costi e la complessità spostando la sicurezza al limite.

Esperienza utente senza eguali

Cloudflare è più vicino ai tuoi utenti e servizi e indirizza le richieste più velocemente utilizzando un routing ottimizzato e basato sull'intelligence attraverso la nostra vasta rete Anycast,
con oltre 275 sedi in più di 100 paesi in tutto il mondo.

Accelera il tuo percorso verso Zero Trust — Provalo ora — Contattaci