Zero Trust Network Access

Cloudflare Zero Trust, in particolare Access, migliora la produttività del team e riduce i rischi poiché tutti gli utenti accedono alle tue app self-hosted, SaaS o non Web senza una VPN.

Accesso semplice e sicuro per il lavoro ibrido

Zero Trust Network Access (ZTNA) nativo per Internet

L'ambiente di lavoro distribuito di oggi richiede un approccio distribuito alla sicurezza.Il "perimetro" non esiste più e le tradizionali soluzioni di accesso remoto come le VPN non sono in grado di soddisfare le moderne aspettative di sicurezza o prestazioni.

ZTNA fornisce un accesso semplice e sicuro tra qualsiasi utente e app, su qualsiasi dispositivo, in qualsiasi luogo, controllando continuamente il contesto granulare come l'identità e la posizione del dispositivo risorsa per risorsa. Con un approccio completamente nuovo, non esiste più un "atto di equilibrio" tra sicurezza ed esperienza dell'utente. ZTNA supporta la tua attività migliorando entrambe.

Inoltre, rende le organizzazioni più agili e in grado di affrontare il cambiamento, che si tratti di migrazione al cloud, attività di M&A o di innovazione e scalabilità rapida. Cloudflare è il cuore di una strategia Zero Trust o di modernizzazione della sicurezza, offrendo ZTNA sulla nostra connettività cloud globale programmabile.

80% Riduzione media del tempo impiegato per risolvere i ticket di supporto per l'accesso remoto relativi all'utilizzo di una VPN [1]

72% di tempo risparmiato per la configurazione mensile delle policy rispetto al fornitore precedente [1]

68% Percentuale di chi ha riscontrato un impatto significativo nella semplificazione delle esperienze di autenticazione per dipendenti e collaboratori esterni [1]

Potenzia la tua azienda con un accesso modernizzato

Rafforza l'esperienza utente

Migliora la produttività del tuo team con una sicurezza modernizzata che fa sembrare le app on-premise proprio come le app SaaS. Niente più VPN lente e goffe o lamentele dei dipendenti.

Elimina il movimento laterale

Riduci il rischio informatico e riduci la superficie di attacco concedendo un accesso con privilegi minimi basato sul contesto per risorsa anziché l'accesso a livello di rete.

Scala Zero Trust senza sforzo

Migliora l'efficienza tecnologica proteggendo prima le app critiche o i gruppi di utenti a rischio più elevato, quindi espandendo ZTNA nativo di Internet per proteggere l'intera azienda.

Principali casi d'uso per Access

Lavoro ibrido sicuro

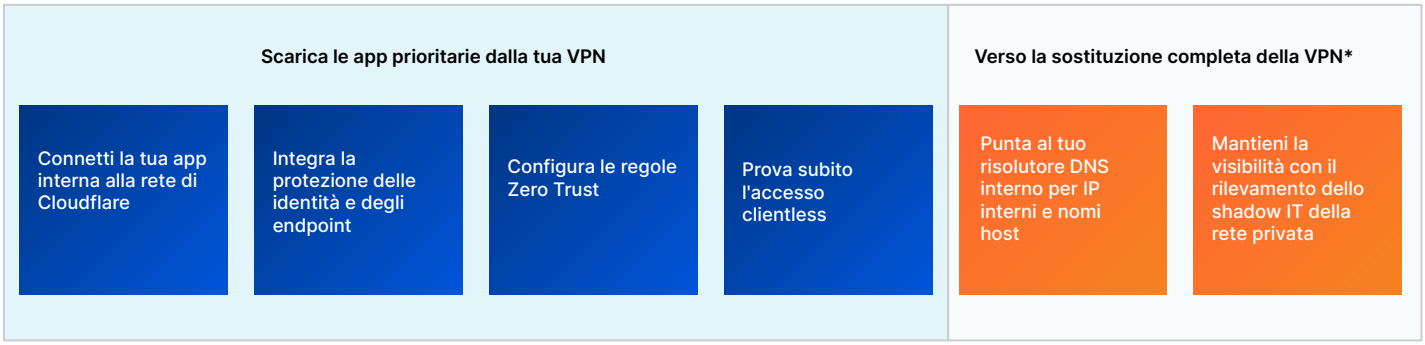
- **Aumento e sostituzione della VPN** : Access è più veloce e sicuro rispetto alle VPN tradizionali. Inizia a scaricare le app critiche per una migliore sicurezza e un'esperienza utente finale.
- **Accesso degli appaltatori** : autentica utenti di terze parti come appaltatori con opzioni clientless, IdP social e altro ancora.
- **Accesso per sviluppatori**: fornisci agli utenti tecnici privilegiati un accesso sicuro all'infrastruttura critica senza compromessi in termini di prestazioni.

Consenti la modernizzazione digitale

- **Accelera fusioni e acquisizioni**: evita del tutto una fusione di rete tradizionale. Integra più IdP e fornisci accesso interno per app durante fusioni e acquisizioni.
- **Migrazione al cloud**: mantieni la continuità aziendale durante i periodi di trasformazione, come la migrazione di app o directory di identità nel cloud.
- **MFA resistente al phishing**: implementa ovunque un'autenticazione forte, come le chiavi di sicurezza conformi a FIDO2.

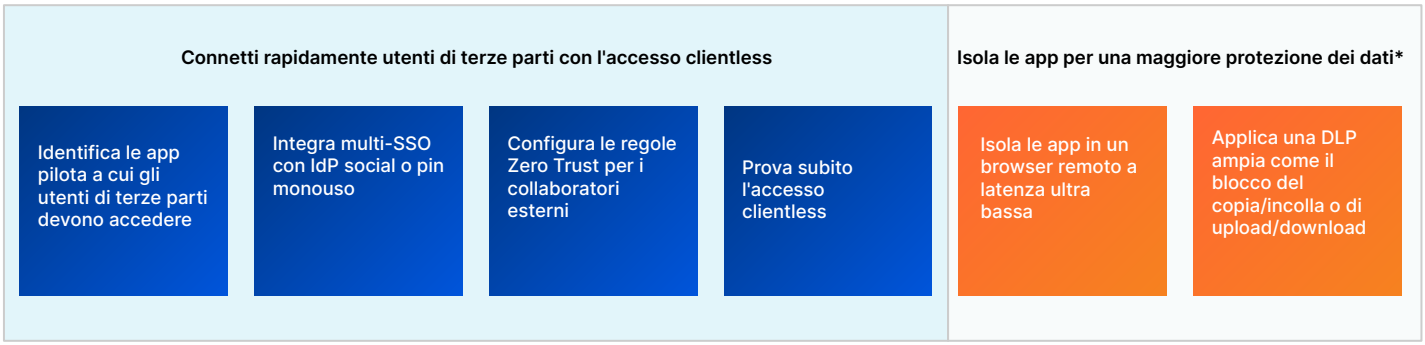
Inizia con l'ampliamento e la sostituzione della VPN

Dai la priorità alle app critiche o agli utenti a rischio per un progetto pilota ZTNA e potenzia la tua VPN. Utilizza l'accesso clientless per le app Web o SSH nel browser per accelerare i test. Adotta funzionalità avanzate nel tempo per procedere verso la sostituzione completa della VPN e mantenere una visibilità dinamica man mano che la tua rete cambia.



Inizia con l'accesso del contraente (terze parti)

Fornisci esperienze utente fluide, mitigando al tempo stesso i rischi derivanti dai dispositivi non gestiti. Configura semplici opzioni di autenticazione per gli appaltatori: non è richiesto alcun software per l'utente finale. Adotta funzionalità avanzate nel tempo per applicare ulteriore protezione dei dati.



**utilizzando le funzionalità in altre parti della piattaforma Zero Trust*

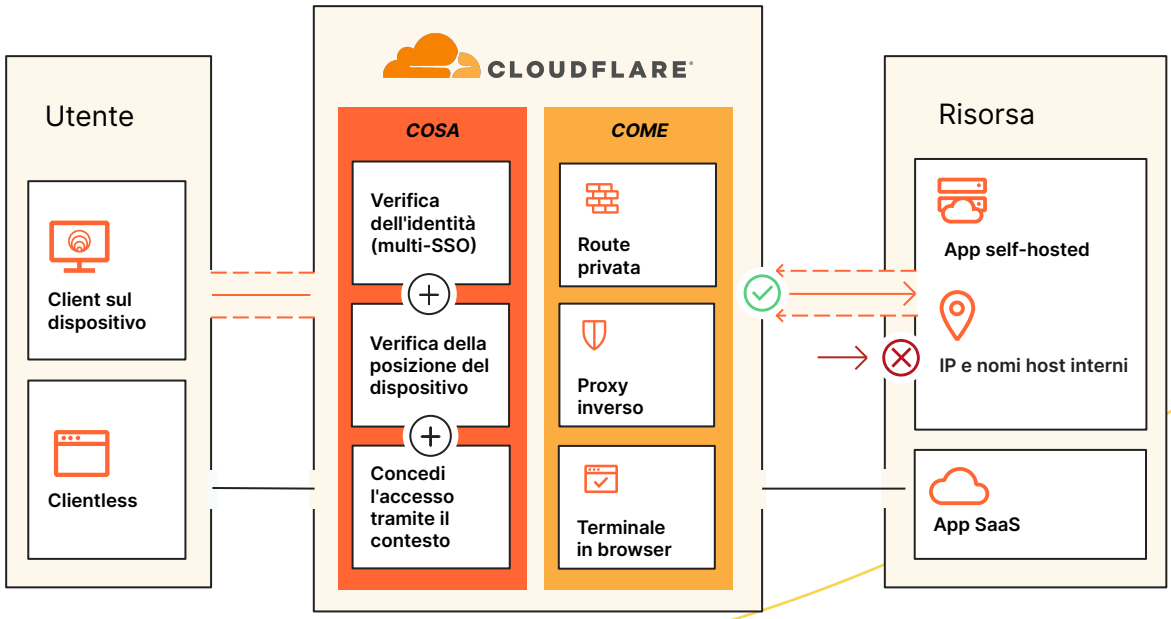
Come funziona Access

Cloudflare Access è un livello di aggregazione flessibile che verifica continuamente il contesto granulare come l'identità e la postura del dispositivo per fornire un accesso semplice e sicuro a tutte le risorse di un'organizzazione individualmente, creando un perimetro definito dal software. Quando un utente esegue l'autenticazione e soddisfa tutti i criteri dei criteri di accesso, Access emette un token Web JSON firmato valido per una durata della sessione specificata. Eseguiamo un'ispezione a passaggio singolo su tutte le richieste degli utenti attraverso la nostra piattaforma componibile e la nostra esperienza di amministrazione centralizzata delle policy profila le modifiche delle policy a livello globale in pochi secondi grazie alla nostra esclusiva architettura di rete Anycast.

Il funzionamento unificato clientless e basato su client gestisce tutti i tipi di dispositivi.Utilizziamo un client dispositivo per tutti i servizi Zero Trust che crittografa il traffico verso la nostra rete per mantenere la privacy dei dati dei nostri clienti. Forniamo inoltre un accesso semplice e sicuro ai dispositivi esterni all'azienda tramite la nostra configurazione clientless. I nostri servizi ZTNA, DNS e WAF e di protezione da attacchi DDoS leader di mercato lavorano insieme per creare e proteggere nomi host pubblici accessibili a utenti di terze parti e una forza lavoro ibrida su qualsiasi dispositivo. Le nostre opzioni di autenticazione userless (token o certificati mTLS) affrontano anche casi d'uso di servizi automatizzati e dispositivi IoT.

Per i controlli Zero Trust, le risorse utilizzano nomi host pubblici per il proxy inverso ad app self-hosted (cloud/on-premise) o SSH/VNC nel browser, proxy di identità per app SaaS o routing privato basato su client/tunnel tramite L4-7 inoltrare il proxy a qualsiasi risorsa Web o non Web (ad esempio, TCP/UDP arbitrario) all'interno di una sottorete privata.La nostra combinazione di software per connettori di rete e app supporta qualsiasi ambiente di elaborazione (cloud pubblico, inclusi Kubernetes e contenitori o risorse di rete locali legacy) senza richiedere l'infrastruttura VM e senza limitazioni di throughput a differenza di altri fornitori Zero Trust.

Identità di terze parti, endpoint, rete on-ramp, registrazione/analisi e strumenti SIEM sono integrati nella nostra dashboard insieme alle opzioni native per il client e l'analisi dei nostri dispositivi, consentendo agli amministratori di rimanere agili e costruire insieme agli strumenti che già utilizzano.



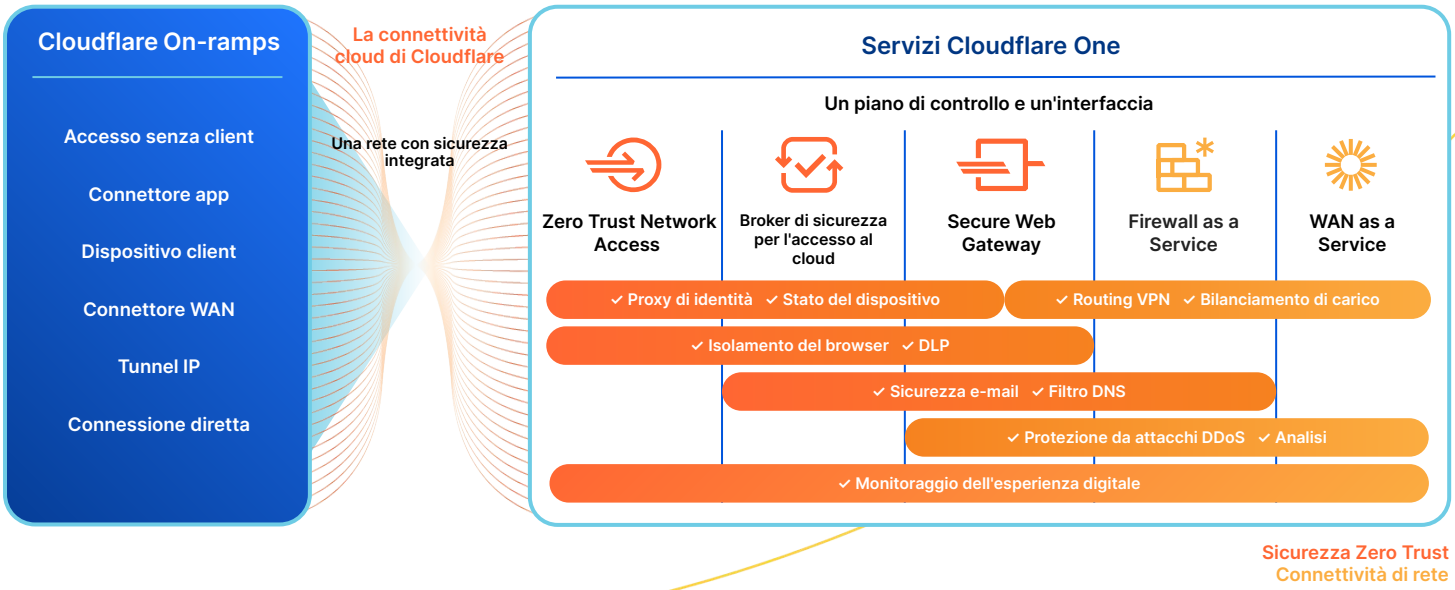
Accesso come parte della piattaforma SSE e SASE di Cloudflare

Mentre SSE e SASE implicano spesso un percorso strategico pluriennale, Cloudflare vede spesso le organizzazioni iniziare con ZTNA perché comporta passaggi attuabili e accessibili per i team IT dimostrando al contempo un significativo valore aziendale a breve termine. I leader IT cercano di proteggere il lavoro ibrido, difendersi dalle minacce e proteggere i propri dati nel percorso verso il consolidamento e scelgono sempre più Cloudflare come partner di fiducia.

La flessibilità di implementazione e l'architettura componibile di Cloudflare consentono a qualsiasi organizzazione di proteggere e accelerare le prestazioni di dispositivi, app e intere reti per mantenere il lavoro ibrido sicuro e produttivo.Per questo supportiamo l'onboarding agentless per gli utenti finali, l'isolamento Web clientless per contenere il traffico non sicuro e un dashboard di gestione unificato che consente la visibilità di tutti i servizi di sicurezza e di rete, indipendentemente da dove si connettono gli amministratori o gli utenti. L'ampiezza della rete globale di Cloudflare consente di applicare la sicurezza più vicino agli utenti finali, riducendo al minimo la latenza e fornendo un'esperienza fluida ai dipendenti. La nostra architettura Anycast aiuta a superare le interruzioni di Internet, mantenendo i team online e contribuendo a garantire la continuità aziendale.

Con la nostra piattaforma SSE e SASE unificata, il contesto condiviso tra le nostre politiche ZTNA, CASB, DLP e SWG aiuta a rafforzare il livello di sicurezza semplificando al tempo stesso l'implementazione attraverso un flusso di lavoro amministrativo coerente. Gli stessi attributi di identità e postura del dispositivo possono informare sia le policy di accesso per ZTNA e CASB sia le policy SWG, semplificando la gestione delle policy tra le organizzazioni.

ZTNA, RBI e la sicurezza della posta elettronica possono anche essere utilizzati insieme per fornire accesso condizionato alle risorse isolando gli utenti dai contenuti dannosi (collegamenti, allegati) a cui sono esposti attraverso gli strumenti di posta elettronica e di collaborazione. Agli appaltatori e agli utenti su dispositivi non gestiti può essere fornito un accesso limitato alle risorse aziendali con interazioni utente (ad esempio,upload/download, copia/incolla, input da tastiera) disabilitate per impedire la compromissione dei dati ed è possibile applicare altri criteri DLP L7 per rilevare dati sensibili.



Cosa dicono i clienti

"Cloudflare Access è un'alternativa straordinaria alle VPN tradizionali.Gli utenti devono semplicemente aprire il proprio browser ed effettuare il login, senza dover scaricare e configurare software aggiuntivo".

- **Platzi**, Head of Cloud Engineering

"Access è molto più semplice e sicuro di una VPN per limitare l'accesso alle risorse interne. Lo attiviamo semplicemente e aggiungiamo utenti.Funziona e basta!"

- Bitpanda, CTO e cofondatore

"Cloudflare è diventato disponibile appena in tempo per impedirci di dover affrontare la seccatura di implementare una VPN. È stata una scelta facile per noi ed è stato incredibilmente semplice da implementare".

- **ezCater**, Head of Security

"Prima di implementare Cloudflare, la preparazione di un'applicazione per un'implementazione sicura richiedeva dalle due alle quattro settimane. Con Cloudflare Zero Trust, risparmiamo quasi il 90% di quel tempo".

- **Creditas**, Network Engineering Team Lead

Il parere degli analisti

IDC

Cloudflare nominato Leader nel 2023 IDC MarketScape per Zero Trust Network Access (ZTNA)

IDC cita la "strategia di prodotto aggressiva di Cloudflare per supportare le esigenze di sicurezza aziendale". Riteniamo che il nostro riconoscimento convalidi il nostro approccio per aiutare le aziende di qualsiasi dimensione a iniziare con Zero Trust e garantire l'accesso per qualsiasi utente a qualsiasi risorsa, senza VPN.

kuppingercole ANALYSTS

Cloudflare nominato Leader nel 2022 KuppingerCole Leadership Compass per ZTNA

Attraverso la sua analisi di mercato ZTNA del 2022, KuppingerCole Analysts AG ha citato diversi punti di forza di Cloudflare come la nostra piattaforma di sicurezza sviluppata organicamente e completamente integrata, la grande infrastruttura cloud globale e la massiccia presenza sul mercato.

Funzionalità di Access

Creazione/modifica di policy Zero Trust per l'accesso sicuro	
Politiche di accesso granulari e personalizzate	Esperienza di gestione delle policy centralizzata. Le app L7 sono protette a livello di sottodominio e percorso con supporto per carattere jolly e nomi multi-host, e supportano richieste CORS. I cambiamenti delle politiche proliferano a livello globale in pochi secondi. Include un tester delle politiche.
Ampiezza delle risorse: cosa possiamo proteggere e come	Le risorse utilizzano nomi host pubblici per il reverse proxy su app self-hosted (cloud/on-premise) o SSH/VNC in browser, proxy di identità su app SaaS o routing privato basato su client/tunnel tramite forward proxy* L4-7 a qualsiasi risorsa Web/non Web (TCP/UDP arbitrario) all'interno di una sottorete privata.
Identità	Autenticazione tramite tutti i principali provider di identità (IdP) aziendali e sociali, inclusi più IdP contemporaneamente. Può utilizzare i connettori generici SAML e OIDC. Supporta (e può applicare) qualsiasi metodo AuthN fornito dall'IdP, AuthN temporaneo, giustificazione dello scopo, intervalli di re-AuthN su base globale o per sessione per app e opzione di revoca immediata della sessione per app o per utente.
Posizione del dispositivo	Verifica la posizione del dispositivo utilizzando il client dispositivo e le integrazioni Endpoint Protection Platform (EPP) di terze parti. Utilizza le integrazioni da servizio a servizio per inserire i punteggi di rischio EPP nelle politiche Zero Trust.
Segnali contestuali per le politiche	Configura segnali quali gruppi di e-mail, intervalli IP, geolocalizzazione, metodo di accesso (ad esempio, tipo MFA, tipo IdP), certificato mTLS o SSH valido, token di servizio, elenco di numeri di serie, attributi di posizione del dispositivo, client dispositivo installato, durata della sessione, applicazione delle regole SWG o segnali da chiamate API esterne. Può anche fare riferimento direttamente ai criteri di accesso condizionale di Microsoft Entra ID (Azure AD).
Altro supporto correlato	• **SCIM:** effettua il provisioning/deprovisioning automatico degli utenti per app self-hosted e SaaS (esempi per Okta e Azure AD) • **DNS interno:** configura il fallback di dominio locale e risolvere le richieste della rete privata • **Split tunnels:** includi/escludi gli IP per reti private o in esecuzione insieme a una VPN • **Autenticazione mTLS:** autenticazione basata su certificato per IoT e altri casi d'uso mTLS • **Isolamento delle app:** con una singola casella di spunta, isola le app nel nostro velocissimo browser remoto*
On-ramp e off-ramp	
Connettore app	La semplice orchestrazione del nostro velocissimo connettore di app (Cloudflare Tunnel) accelera la connessione delle risorse a Cloudflare, senza richiedere l'infrastruttura VM e senza limitazioni di throughput. Include funzionalità di monitoraggio, reti virtuali (per sovrapposizioni di IP) e ridondanza e failover.
Client dispositivo: Quando utilizzarlo	• **Clientless:** estendi le politiche Zero Trust a utenti di terze parti su dispositivi non gestiti; inoltre funziona bene con RBI clientless e politiche DLP L7*. L'accesso clientless supporta app Web e SSH/VNC in-browser. • **Basato su client:** il nostro client per dispositivi (Cloudflare WARP) estende l'accesso sicuro alle reti private, consente integrazioni del comportamento dei dispositivi da servizio a servizio ed è indipendentemente dalla posizioneper applicare politiche su misura per gli utenti on-premise. Può anche connettere due o più dispositivi a cui è in esecuzione WARP per creare reti private. Gli utenti possono registrarsi automaticamente oppure possono distribuire la soluzione tramite MDM.
Estendibilità e visibilità	
Personalizzazione delle pagine	Carica HTML personalizzato per schermate di blocco e di avvio app adatte al tuo marchio o trasmetti istruzioni di accesso specifiche per semplificare l'esperienza dell'utente finale.
Registrazione	Registrazione completa per tutte le richieste, gli utenti e i dispositivi. Può utilizzare logpush o le API per l'integrazione con strumenti SIEM, di orchestrazione e di analisi esistenti. Per le risorse sconosciute, il nostro shadow IT per l'infrastruttura interna cataloga passivamente il traffico unico che emerge da tutte le origini.
Automazione	Le API intuitive e il provider Terraform sono disponibili per gestire a livello di programmazione tutti gli aspetti di un'implementazione Zero Trust. Offre anche supporto per token di servizio userless per i servizi automatizzati.

**utilizzando le funzionalità in altre parti della piattaforma Zero Trust*

Perché Cloudflare?

Configurazione e gestione facilitate

Semplifica radicalmente la configurazione e il funzionamento del traffico in rampa verso le risorse private con il software del connettore delle app e l'orchestrazione del tunnel.

Esperienza always-on continua

Raggiungi le massime prestazioni degli utenti finali e la resilienza alle interruzioni di rete con la tecnologia Anycast globale di Cloudflare, garantendo affidabilità.

Innovazione rapida e precoce

Resta al passo con l'evoluzione di Internet stessa con un provider che innova costantemente i suoi concorrenti per rendere l'accesso alle app più veloce e più sicuro.

Parliamo di un accesso semplice e sicuro per la tua organizzazione

Richiedi un workshop

CLOUDFLARE

Non sei ancora pronto per una conversazione dal vivo?

Scopri di più sulla [piattaforma SSE e SASE di Cloudflare]

1. Sondaggio 2023: techvalidate.com/product-research/cloudflare/charts