CLOUDFLARE

SINTESI DELLA SOLUZIONE

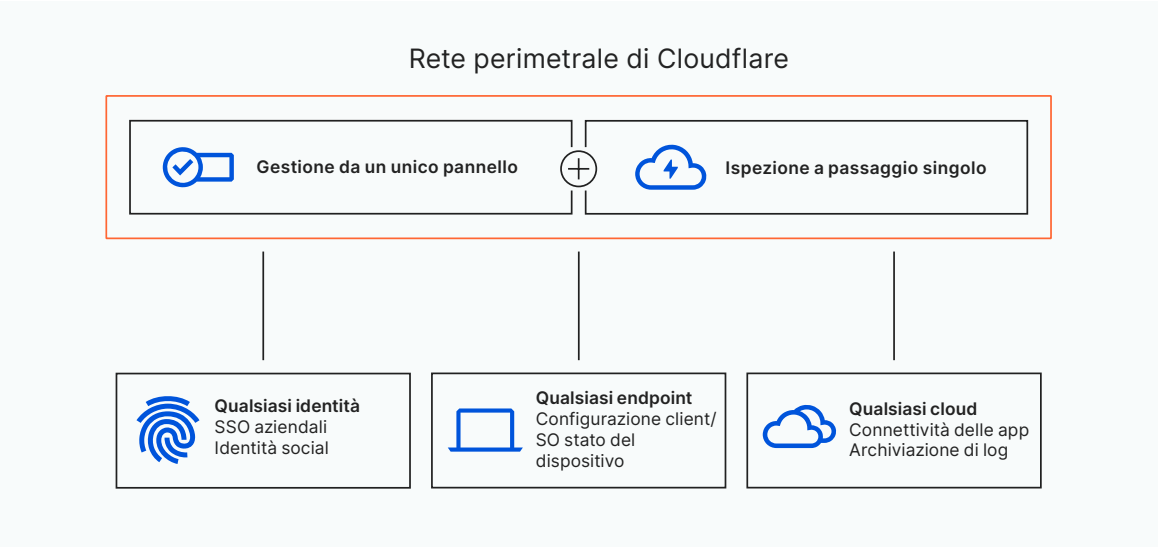
Integrazioni di Zero Trust con Cloudflare

Basati sull'identità, l'endpoint e i fornitori di servizi cloud che già utilizzi

Destreggiarsi tra più provider di identità, endpoint e cloud all'interno di un'organizzazione è inevitabile, ma non deve essere gravoso. In Cloudflare, il nostro obiettivo è fornire alla tua organizzazione la sicurezza più solida nel modo più facile da usare. A differenza di altri fornitori, non abbiamo alcun interesse acquisito nei fornitori specifici in quelle categorie con cui lavori oggi o lavorerai in futuro.

Siamo agnostici. Pertanto, la nostra strategia di lunga data è stata quella di progettare Cloudflare Zero Trust da integrare con quante più altre soluzioni possibili.

Attraverso le integrazioni, Cloudflare aggrega i segnali di più provider e funge da unico pannello di controllo per applicare policy granulari ricche di contesto in tutta la nostra rete globale. Inoltre, queste integrazioni non richiedono la ricerca di una fitta documentazione tecnica; sono pre-costruiti come flussi di lavoro per una gestione più fluida, da un unico riquadro.



Qui, evidenziamo tre principi che seguiamo per incontrare i clienti dove si trovano:

- **Identità agnostica:** autentica gli utenti su più tipi di provider di identità per un accesso agevole a tutti gli utenti senza problemi di configurazione.
- **Endpoint agnostico:** arricchisci i controlli della postura del tuo dispositivo in modi più granulari e adattivi con segnali provenienti sia dai tuoi fornitori di endpoint preferiti che dal nostro client del dispositivo.
- **Cloud agnostico:** proteggi le applicazioni su qualsiasi cloud pubblico o privato (on-premise) per evitare il lock-in del fornitore a lungo termine.

Aggrega più identità su Cloudflare

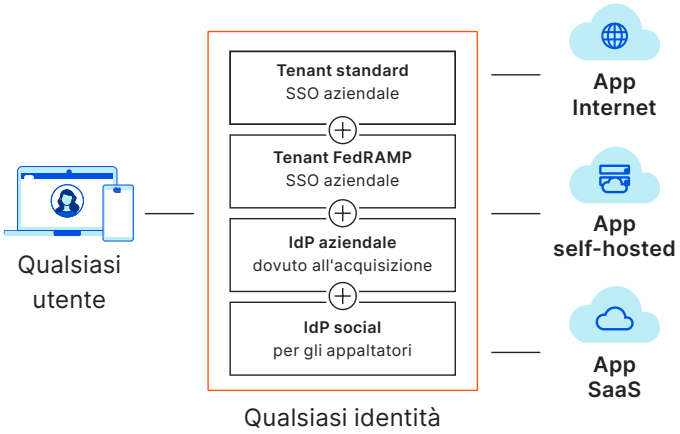
Multi-SSO

Cloudflare ha creato una delle prime soluzioni di accesso Zero Trust per supportare più provider di identità (IdP) contemporaneamente. Oggi ci integriamo con i principali IdP aziendali (come Okta o Azure AD), nonché con identità social (come LinkedIn o Github) e standard open source (come SAML o OIDC). Inoltre, supportiamo più istanze dello stesso IdP: ad esempio, un utilizzo FedRAMP e non FedRamp di Okta.

Federa più identità contemporaneamente

La nostra capacità di federare l'identità tra molti IdP può far ripartire il processo di creazione di policy di riconoscimento dell'identità. Le organizzazioni non hanno più bisogno di creare integrazioni personalizzate tra i loro IdP.

Le organizzazioni in fase di crescita con personale di sicurezza delle informazioni più limitato possono trovare nella federazione uno strumento particolarmente potente per scalare un approccio Zero Trust senza il fastidio di consolidare una singola directory centralizzata.



Funzionalità principali

- Cloudflare si integra con più IdP contemporaneamente, tutti i migliori della categoria
- Federa più provider e più istanze di ciascun provider
- Onboarding più rapido per utenti di terze parti e partner M&A

Caso d'uso:

Far sentire gli utenti di terze parti cittadini di prima classe

L'approccio indipendente dall'identità di Cloudflare è particolarmente utile quando si collabora con terze parti al di fuori dell'organizzazione come appaltatori, aziende acquisite o partner. Le regole di accesso con privilegi minimi possono essere impostate in pochi minuti in base alle identità che questi utenti hanno già messo in campo.

Questa flessibilità semplice evita le inefficienze e i rischi per la sicurezza legati al provisioning di licenze SSO, all'implementazione di VPN o alla creazione di autorizzazioni una tantum.

I migliori partner per la protezione degli endpoint

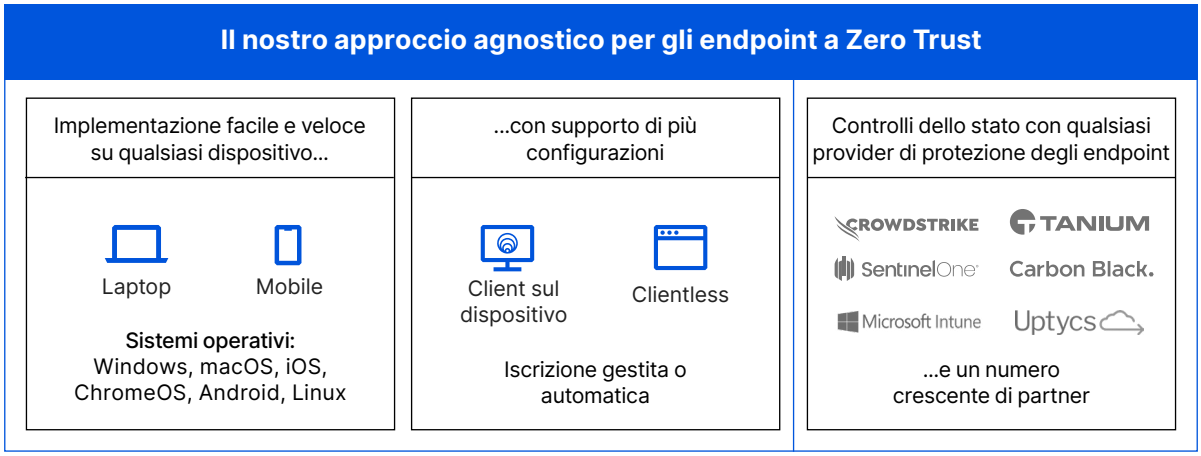
Partnership

Cloudflare collabora con CrowdStrike, SentinelOne, VMware Carbon Black, Tanium, Uptycs e Microsoft Intune.

I clienti possono integrare più provider di protezione degli endpoint contemporaneamente e sfruttare i segnali di sicurezza e le capacità di valutazione del rischio di tali soluzioni.

Configurazione

La configurazione di uno di questi provider richiede solo pochi clic nel dashboard di Cloudflare con flussi di lavoro predefiniti. Una volta configurato, Cloudflare può verificare che i dispositivi eseguano il tuo software endpoint preferito per fornire un monitoraggio continuo contro malware e altre minacce prima di consentire o negare l'accesso a un'applicazione protetta.



Integrazioni potenziate dal nostro client del dispositivo (WARP)

Aumentare il livello di sicurezza spesso richiede un client del dispositivo, che può arricchire i controlli della postura del dispositivo con attributi aggiuntivi. Abbiamo deliberatamente ottimizzato il nostro livello di sicurezza per un'adozione flessibile e senza sforzo.

Distribuisci sulla maggior parte dei sistemi operativi

- Il nostro client aziendale - WARP - funziona su un elenco crescente dei sistemi operativi più diffusi (ad esempio, Windows, macOS, Linux, iOS, ChromeOS e Android).
- La nostra moderna architettura WireGuard richiede solo piccole modifiche al codice specifiche del sistema operativo.
- Il nostro client aziendale ha una versione consumer utilizzata quotidianamente da milioni di persone in tutto il mondo. Testare per così tanti singoli utenti significa che WARP è più pronto per la battaglia rispetto alla maggior parte dei client utilizzati per Zero Trust.

Opzioni di registrazione gestita o automatica

- Per i dispositivi gestiti, documentiamo le distribuzioni con qualsiasi metodo basato su script nei più diffusi software di gestione dei dispositivi mobili (MDM).
- L'autoregistrazione di WARP può essere utile per gli utenti di terze parti e richiede solo pochi minuti per qualsiasi desktop o telefono cellulare.

Evitare il lock-in dei provider di servizi cloud

Problema

Alcuni fornitori più monolitici sono principalmente interessati ad aumentare il consumo dei propri servizi cloud, in particolare a livello di archiviazione e calcolo.

Con sorpresa di nessuno, le loro soluzioni di sicurezza aggiuntive non si integrano perfettamente come dovrebbero con altri fornitori di servizi cloud. Piccoli inconvenienti come documentazione più debole e bug si sommano. Quel blocco dello stack tecnologico rende la vita più difficile ai tuoi team di sicurezza informatica.

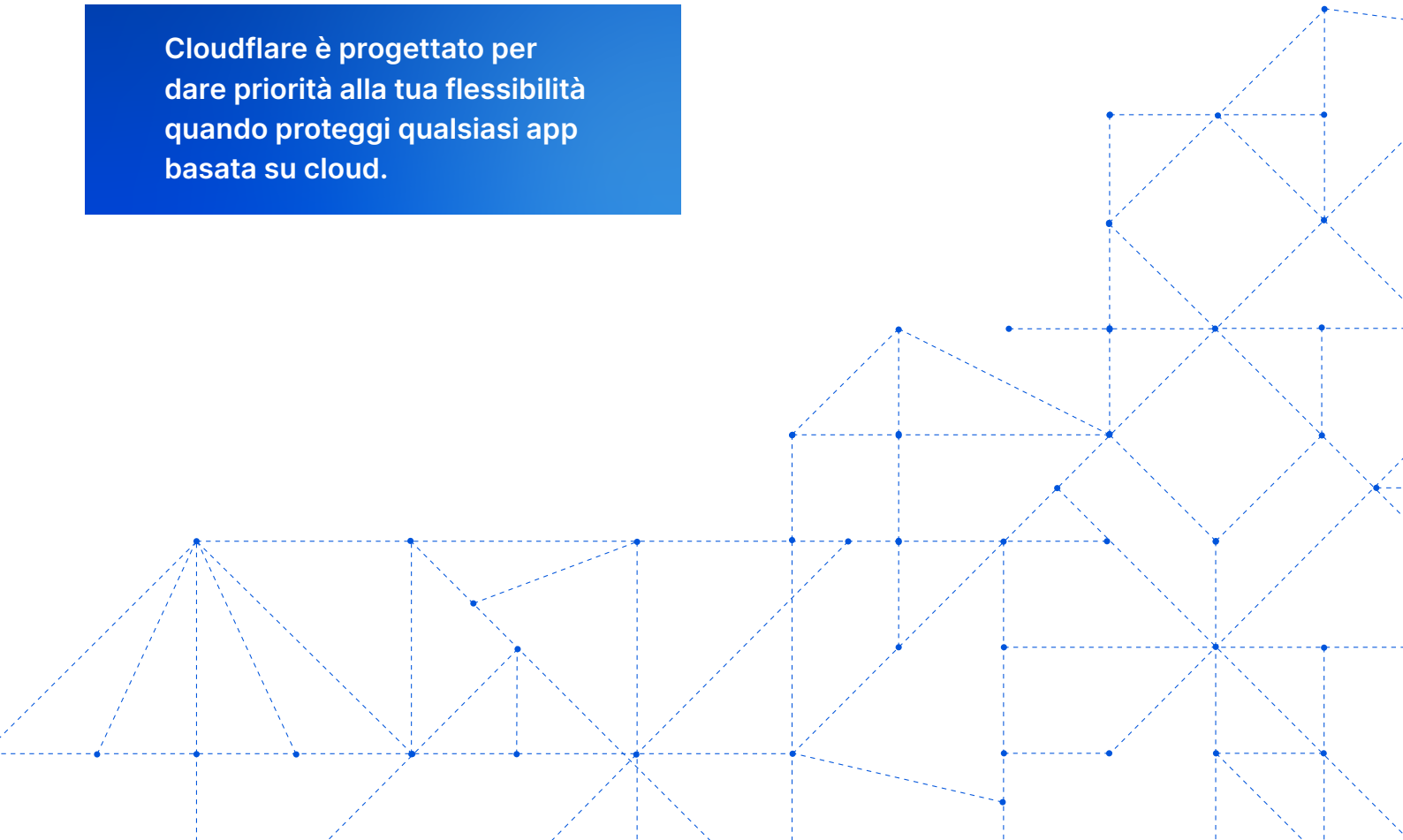
Soluzione

Al contrario, il nostro obiettivo strategico è la tua sicurezza, non il tuo consumo di cloud. Cloudflare è indipendente dal cloud: garantiamo l'accesso a qualsiasi risorsa in qualsiasi ambiente cloud pubblico, privato o SaaS.

Funzionalità principali

- Accesso Zero Trust in ambienti cloud pubblici, privati e SaaS
- Nessun vincolo del fornitore al cloud computing o alle destinazioni di archiviazione
- Connettori per app, partner di rete on-ramp e integrazioni di storage che semplificano l'interazione con le app in qualsiasi cloud

Cloudflare è progettato per dare priorità alla tua flessibilità quando proteggi qualsiasi app basata su cloud.



Punti di forza di Cloudflare

Estendi le connessioni alle app in qualsiasi cloud

Il nostro connettore per app leggero funziona in ogni cloud

- Esegui lo strumento della riga di comando come servizio su Linux e altri sistemi operativi
- Preconfezionato come container Docker
- Supporto della replica per i moderni ambienti Kubernetes
- Il tunnel può essere configurato e monitorato tramite l'interfaccia utente

Ampie interconnessioni con i provider di servizi cloud

- Connessioni veloci per gli utenti rese possibili da 11.000 interconnessioni tra la nostra rete e altri provider cloud, 50 delle quali sono interconnessioni private con i datacenter di Microsoft, Amazon e Google

Diversi partner di rete onramp che non sono specifici del cloud

- Connetti facilmente qualsiasi ambiente cloud pubblico e privato alla nostra rete utilizzando il tuo metodo di routing SD-WAN esistente (ad es. VMware) o interconnettiti privatamente presso oltre 1600 sedi di provider di colo (ad esempio, Equinix)

Invia i dati di log a qualsiasi cloud

I dati di log possono essere archiviati su cloud o inviati direttamente ai provider di analisi

- Supporto integrato per una o più destinazioni di archiviazione contemporaneamente, tra cui AWS, Azure, Google Cloud e qualsiasi API compatibile con S3 (ad esempio, Digital Ocean Spaces)
- Integrazioni integrate con strumenti di analisi e SIEM come Sumo Logic, Splunk e Datadog

Sicurezza su qualsiasi cloud pubblico o privato

Elenco dei partner di integrazione Zero Trust

Nel corso del tempo, Cloudflare aggregherà i segnali provenienti da un elenco ancora più ampio dei tuoi fornitori preferiti, il tutto supportato dall'intelligenza della nostra piattaforma Zero Trust e della nostra rete globale.

Provider di identità

SSO aziendali

- Centrify
- Citrix ADC
- Google Workspace
- Jumpcloud
- Microsoft Azure Active Directory (AD)
- Okta
- OneLogin
- Ping Identity

Identità social

- Facebook
- GitHub
- Google
- LinkedIn
- Yandex

Open source

- OIDC
- SAML 2.0

Provider di endpoint

Provider di protezione endpoint

(per lo stato di sicurezza del dispositivo)

- Crowdstrike
- Microsoft Endpoint Manager
- SentinelOne
- Tanium
- Uptycs
- VMWare Carbon Black

Provider di gestione endpoint

(per la distribuzione dei client)

- Hexnode
- Ivanti
- Jamf
- Jumpcloud
- Kandji
- Microsoft Intune

Network Onramp Partners

Physical Interconnect Partners

- 365 Data Centers
- BBIX
- CoreSite
- Cyxtera
- Databank
- Digital Realty
- EdgeConneX
- Equinix
- Netrality Data Centers
- Teraco
- Zayo

Fabric Interconnect Partners

- Console Connect / PCCW
- CoreSite
- Epsilon Infiny
- Equinix Fabric
- Megaport
- PacketFabric

SD-WAN

- Aruba (Silverpeak)
- Cisco
- VMWare (Velocloud)

Provider di servizi cloud

Destinazioni di archiviazione cloud

- AWS S3
- Google Cloud Storage
- Microsoft Azure Blob Storage
- Altri fornitori con un'API compatibile con S3

Cloud Analytics e SIEM Partners

- Azure Sentinel
- Data Dog
- Elastic
- Google Cloud
- Graylog
- IBM QRadar
- Looker
- New Relic
- Splunk
- Sumo Logic

Per saperne di più su Cloudflare Zero Trust e richiedere una demo o un POC a un rappresentante di vendita, visita il sito all'indirizzo: https://www.cloudflare.com/products/zero-trust.

CLOUDFLARE

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

REV:BDES-3795.2022SEP26