# Magic WAN

Magic WAN semplifica il percorso verso SASE con una connettività any-to-any

## Evoluzione delle architetture di rete

**Internet è la nuova rete aziendale**

Con il lavoro ibrido ormai diventato la nuova normalità e lo spostamento delle app nel cloud, i team IT sono alle prese con:

- **Complessità della rete:** le soluzioni di provisioning e regolazione MPLS richiedono troppo tempo
- **Lacune di sicurezza:** l'accesso diretto a Internet elude la sicurezza e i criteri di utilizzo accettabile, e mette a rischio gli utenti e i dati
- **Costi elevati:** i collegamenti MPLS e le soluzioni mirate per la sicurezza comportano spese inutili
- **Scarsa esperienza utente:** il backhauling del traffico allo stack di sicurezza di un perimetro introduce latenza

Magic WAN semplifica la connettività di rete da filiali, VPC multi-cloud o datacenter alla piattaforma SASE Cloudflare One, consentendo una connettività sicura, performante ed economica per risolvere le sfide del lavoro ibrido e multi-cloud per i team IT.

A differenza delle rigide e costose reti MPLS o delle complesse distribuzioni SD-WAN basate su firewall on-premise, Magic WAN adotta un approccio "filiale leggera, cloud pesante" per potenziare o sostituire la tua architettura attuale. È più facile da distribuire e si adatta alle mutevoli esigenze aziendali, con sicurezza integrata.

Magic WAN collega posizioni di rete fisiche o virtuali alla piattaforma SASE di Cloudflare. Esempi di sedi fisiche includono filiali, stabilimenti, punti vendita, sedi centrali o datacenter. Esempi di posizioni virtuali includono servizi cloud pubblici come AWS, Azure, GCP e OCI.

**Migliore agilità operativa**

Gestisci centralmente la sicurezza della rete e la connettività da un'unica console amministrativa. Traffico on-ramp in pochi minuti con configurazione zero-touch.

**Sicurezza integrata, non imbullonata**

Ottieni protezione da attacchi DDoS nativa del cloud, firewall di rete, funzionalità SSE e Zero Trust, il tutto profondamente integrato e fornito as-a-service

**Costi di rete ridotti**

Riduci al minimo l'ingombro delle filiali e sposta le funzioni di rete sul cloud per ridurre la dipendenza dai costosi MPLS e abbandonare la SD-WAN.

## Principali casi d'uso per Magic WAN

**Semplifica la connettività di rete**

- **Semplifica la connettività delle filiali**: sostituisci un mosaico di circuiti proprietari e dispositivi di rete per instradare in modo sicuro il traffico tra filiali e datacenter. Facilita la connettività da sito a sito tra sedi con Anycast IPSec.
- **Semplifica la connettività ibrida e multi-cloud**: le organizzazioni dispongono di app in istanze cloud di diversi fornitori (ad esempio, AWS, GCP, Azure, Oracle, IBM) *e* datacenter on-premise. Utilizza controlli centralizzati per instradare e proteggere il traffico attraverso questi ambienti diversificati.

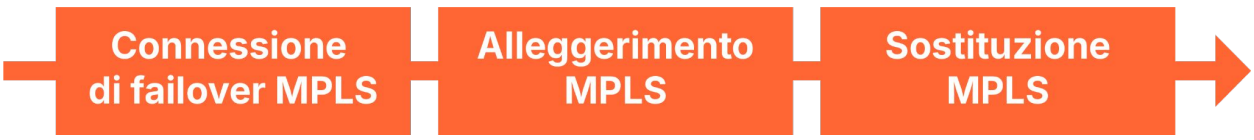
**Aumenta la sicurezza senza sacrificare le prestazioni**

- **Connettività WAN sicura**: connessioni sicure mediante l'applicazione di criteri di sicurezza di rete tra sedi (filiali, datacenter ecc.) con controlli SWG e firewall forniti dal cloud.
- **Dimensiona le prestazioni della WAN**: le distribuzioni MPLS sono costose, poco flessibili e lente. Passare a Cloudflare consente una distribuzione più agile e a costi inferiori con sicurezza integrata.

## Approccio all'implementazione Magic WAN

**La trasformazione della rete è un vero e proprio percorso**

Magic WAN offre prestazioni e affidabilità sulla connettività Internet e aiuta le organizzazioni a migrare dalle architetture di rete legacy. Inizia distribuendo Magic WAN progressivamente implementando una transizione nel tempo. La combinazione "filiale leggera, cloud pesante" di Cloudflare tra connettività dell'ultimo miglio e prestazioni, affidabilità e sicurezza nel miglio intermedio connettere e proteggere meglio il lavoro ibrido. La nostra architettura supporta la distribuzione insieme all'infrastruttura esistente per migrare al tuo ritmo.



# Confronto di Cloudflare One con MPLS e SD-WAN

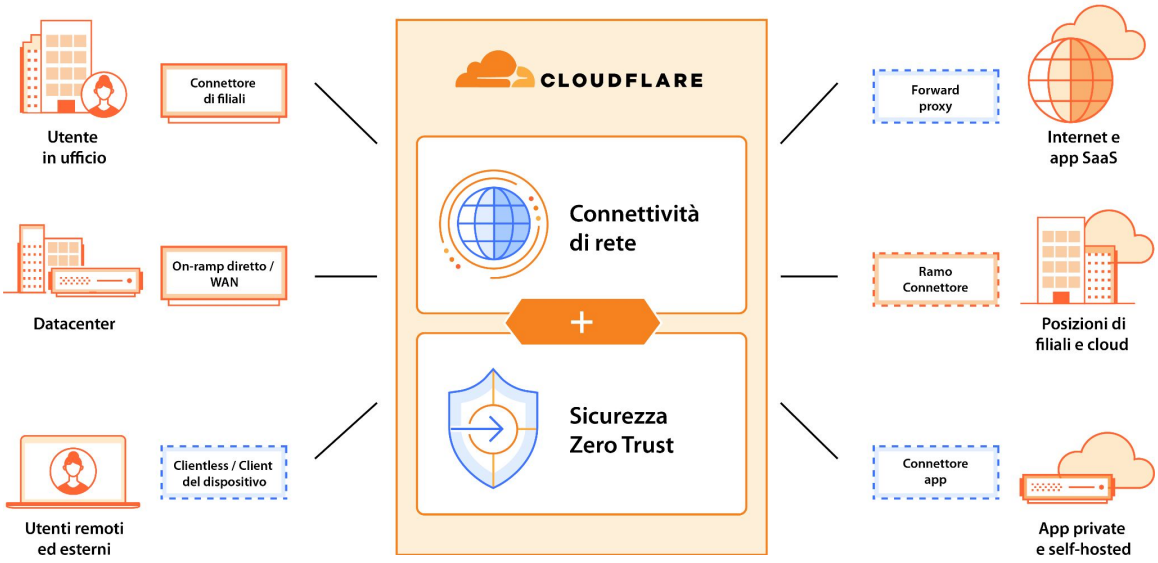
Poiché le applicazioni sono passate al cloud e le organizzazioni adottano un approccio di lavoro ibrido, le architetture di rete tradizionali devono far fronte a livelli di prestazioni e sicurezza in calo. Il traffico di backhauling danneggia le prestazioni e l'esperienza utente. Consentire il breakout locale, invece, danneggia la coerenza e l'efficacia della sicurezza. Nessuno dei due scenari è auspicabile e, di conseguenza, i progetti di rete fanno compromessi che lasciano insoddisfatte le esigenze aziendali e individuali.

Più di recente, SD-WAN ha aggiunto overlay per gestire il traffico nella speranza di offrire un'alternativa a MPLS. Tuttavia, la SD-WAN dipende in gran parte dai dispositivi perimetrali per implementare la sicurezza, lasciando ai team il compito di combinare vari strumenti hardware, virtualizzati e basati su cloud. Di conseguenza, la complessità aggiunta compensa molti dei vantaggi previsti.

La piattaforma SASE di Cloudflare fa convergere rete e sicurezza nella nostra connettività cloud e consente alle organizzazioni di utilizzare la nostra rete come estensione della propria. Gestione semplificata, prestazioni affidabili, sicurezza Zero Trust moderna e costo totale di proprietà ridotto sono possibili simultaneamente solo con un approccio basato su SASE realmente reinventato.

| Criteri | Servizio MPLS/VPN | SD-WAN | SASE con Cloudflare One |
|---|---|---|---|
| **Configurazione**<br>Nuova impostazione, configurazione e gestione del sito | Da MSP tramite richiesta di servizio | Orchestrazione e gestione semplificate tramite controller centralizzato | Orchestrazione automatizzata tramite portale SaaS; pannello di controllo centralizzato |
| **Controllo del traffico dell'ultimo miglio**<br>Bilanciamento del traffico, QoS e failover | Coperto dagli SLA MPLS | Selezione del percorso migliore disponibile nell'appliance SD-WAN | Distribuzione locale minima per controllare il processo decisionale locale |
| **Controllo del traffico del miglio intermedio**<br>Traffico che devia attorno alla congestione del miglio intermedio | Coperto dagli SLA MPLS | "Tunnel Spaghetti" e nessun controllo sul miglio intermedio | Gestione integrata del traffico e controlli della dorsale privata nella stessa interfaccia |
| **Integrazione cloud**<br>Connettività per la migrazione al cloud | Breakout centralizzato | Breakout decentralizzato | Connettività nativa con Cloud Network Interconnect |
| **Sicurezza**<br>Filtra il traffico Internet in entrata e in uscita alla ricerca di malware | Patchwork di controlli hardware | Patchwork di controlli hardware e/o software | Integrazione nativa con strumenti di sicurezza di utenti, dati, applicazioni e rete |
| **Costo**<br>Massimizzare il ROI per gli investimenti di rete | Costo elevato per hardware e connettività | Costi di connettività ottimizzati a scapito di maggiori costi hardware e software | Costi hardware e di connettività ridotti per un ROI massimizzato |

# Deviazione del traffico verso la piattaforma SASE di Cloudflare




Magic WAN Connector semplifica la connessione delle posizioni della tua rete a Cloudflare. Usa il software del connettore di filiale preinstallato e configurato su un dispositivo hardware certificato Cloudflare per una distribuzione semplificata oppure distribuisci il software su dispositivi Linux fisici o virtuali all'interno del tuo ambiente.

### Parte di una famiglia in crescita di on-ramp flessibili

Il primo passo nell'adozione di SASE consiste nel rimanere connessi: stabilendo un percorso sicuro dalla rete esistente alla posizione più vicina dove è possibile applicare le policy di sicurezza Zero Trust. Cloudflare offre un'ampia gamma di "on-ramp" per abilitare questa connettività, comprese opzioni di accesso basate su client e senza client per utenti di lavoro ibridi, tunnel a livello di applicazione stabiliti mediante l'implementazione di connettori software leggeri, connettività a livello di rete con GRE abilitato per Anycast o tunnel IPSec e interconnessione fisica o virtuale sia per datacenter privati che per cloud pubblici.

Per semplificare l'adozione del SASE, Magic WAN Connector può essere distribuito in qualsiasi posizione di rete fisica o cloud per fornire connettività automatica al datacenter Cloudflare ottimale più vicino, sfruttando la connettività Internet dell'ultimo miglio esistente ed eliminando la necessità per i team IT di configurare manualmente l'attrezzatura di rete per connettersi.

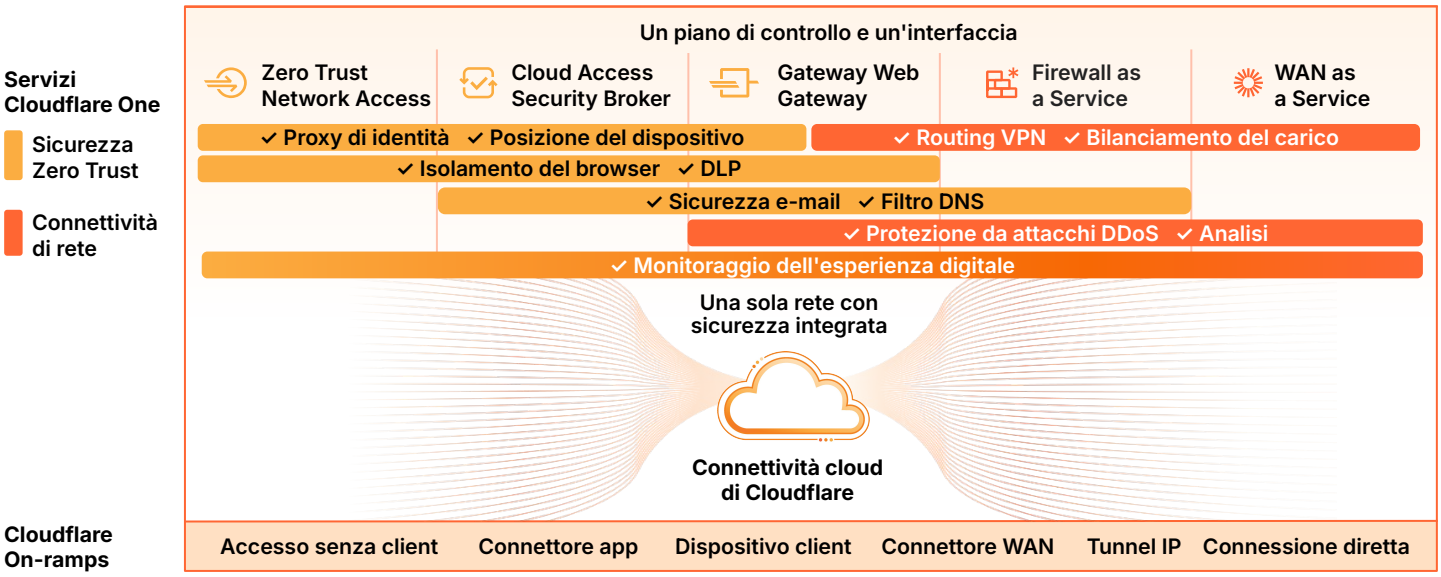
# Funzionalità del software e specifiche hardware

| Funzionalità del software Magic WAN[1] | |
|---|---|
| **Configurazione di WAN Connector** | Dispositivi CPE plug-and-play con provisioning zero-touch, gestiti centralmente tramite dashboard/API di Cloudflare. Configura automaticamente tunnel e percorsi IPSec per indirizzare il traffico alla rete Cloudflare per funzioni di connettività e sicurezza. Aggiornamenti software automatici (entro la finestra di servizio definita dal cliente). |
| **Configurazione del sito WAN Connector** | Supporto WAN/LAN per configurazioni IP statiche o DHCP.<br>Supporto per VLAN e segmentazione della rete locale. |
| **Approccio "filiale leggera, cloud pesante"** | Connettore WAN leggero ad alta disponibilità con bilanciamento del carico e failover su più circuiti WAN in base ai controlli di integrità. Servizi di sicurezza come firewall e funzionalità SSE Zero Trust forniti dalla connettività cloud di Cloudflare. |
| **Integrazione di terzi** | Configura gli endpoint del tunnel Anycast IPsec o GRE con i tuoi VPC cloud esistenti come Amazon AWS Transit Gateway o apparecchiature locali del cliente come dispositivi SD-WAN, firewall e router.Configura percorsi statici con l'inoltro dei pacchetti ECMP alla rete Cloudflare. |
| **Sicurezza integrata** | Firewall L3 integrato e rilevamento delle intrusioni; integrazione perfetta con altre funzionalità SSE/sicurezza e rampe di on-ramp come gateway Web sicuro L4-7, client dispositivo, connettore app, ecc. |
| **Visibilità e controllo** | Rilevamento e routing del traffico basati su app. Controllo della larghezza di banda.<br>Visibilità/analisi per tunnel, traffico e parametri dei dispositivi disponibili tramite dashboard, API, log o GraphQL. Gestisci tramite il dashboard di Cloudflare, l'API o Terraform. |
| **Magic WAN Connector: specifiche dell'opzione hardware[2]** | |
| **Specifiche del dispositivo** | • **Porte:** (6× 1G Copper RJ45) + (2× 10G SFP+) + (2x USB 3.0 Tipo A)<br>• **Dimensioni:** 20,6×20×5 cm; 1.5RU; **Peso:** 1,3 Kg<br>• **Opzioni di montaggio:** posizionamento su scrivania, montaggio a parete o montaggio su rack (con vassoio)<br>• **TPM:** 2.0, in tutto il mondo tranne in Cina<br>• **CPU:** Denverton 4 Core C3558<br>• **Unità:** M.2 120 SSD con 16G eMMC Flash<br>• **RAM:** 8 GB DDR4<br>• **Wi-Fi e Bluetooth:** 802.11ac, 2×2 MIMO, massimo tasso di phy: 866.7 Mbps<br>• **Ventola:** una |

[1] Tutta la documentazione della funzionalità Magic WAN è disponibile in Cloudflare Docs
[2] Hardware certificato Cloudflare con software Magic WAN preinstallato: Dell VEP 1425 venduto tramite partner (viene fornito con supporto per rack)

# Connettività di rete e percorso verso SASE

**La connettività cloud di Cloudflare fornisce la semplicità di implementazione, la resilienza della rete e la velocità di innovazione necessarie per rimanere all'avanguardia mentre si consolidano prodotti specifici e si converge su una strategia IT unificata.**




Cloudflare One sta consentendo alle organizzazioni di tutte le dimensioni di realizzare la transizione verso SASE: connettere qualsiasi sorgente e destinazione di traffico a una rete globale sicura, veloce e affidabile in cui tutte le funzioni di sicurezza vengono applicate e il traffico è ottimizzato lungo il percorso verso la sua destinazione, sia all'interno di una rete privata che su Internet pubblico.

Sia che la tua organizzazione stia scaricando il traffico da distribuzioni MPLS o SD-WAN mature o che si stia avvicinando per la prima volta alla modernizzazione della rete, Magic WAN può aiutarti a semplificare il processo. Cloudflare One offre sia la sicurezza Zero Trust che la WAN-as-a-service per realizzare un SASE con un unico fornitore, ma può anche integrare una strategia multi-fornitore per assisterti nel tuo percorso verso l'adozione di SASE.

## Parliamo della connettività di rete per la tua organizzazione

Richiedi un workshop

CLOUDFLARE

Pensi non sia ancora arrivato il momento di avere una conversazione dal vivo?

Scopri di più sulla nostra architettura di riferimento SASE.