

Mettere in sicurezza i luoghi di lavoro distribuiti

Protezione coerente su un unico piano di controllo unificato per tutte le richieste, da qualsiasi sede

Sposta la sicurezza nel cloud

Riduci la complessità e i rischi per gli uffici con Cloudflare

Con i dipendenti che lavorano in ufficio e in remoto, molte organizzazioni stanno rivalutando il modo in cui proteggono gli uffici oggi, indipendentemente dal fatto che si affidino a dispositivi nei datacenter o consentano un accesso a Internet diretto e non protetto.

Il loro nuovo obiettivo è fornire protezione ed esperienze coerenti tra gli utenti all'interno e all'esterno della rete. Nella maggior parte dei casi, ciò significa spostare i controlli da strumenti disparati come VPN, proxy Web e firewall e verso un'unica piattaforma di sicurezza fornita dal cloud.

Cloudflare vede le organizzazioni modernizzare la sicurezza dell'ufficio con due casi d'uso comuni.

Caso d'uso consigliato:

Proteggi l'accesso alle applicazioni con Zero Trust per sostituire le VPN

Applica criteri granulari e sensibili all'identità per app, invece di consentire lo spostamento laterale attraverso la rete aziendale.

- **Fase 1:** Integrazione con i provider di identità
- **Fase 2:** Proteggi qualsiasi app Web tramite un browser
- **Fase 3:** Proteggi gli ambienti SSH, VNC e RDP tramite un browser



Combina la filiale e l'accesso remoto in un'unica implementazione per garantire criteri coerenti e ridurre al minimo il numero di fornitori richiesti. Distribuisci ZTNA per aumentare o sostituire la VPN legacy per limitare gli investimenti nella tecnologia legacy.¹

Gartner®

Caso d'uso consigliato:

Filtra l'accesso a Internet per una sicurezza coerente con un time-to-value rapido

Proteggi prima gli utenti dell'ufficio con il filtro DNS e, successivamente, ispezioni più complete in tutte le sedi. Niente più backhauling del traffico attraverso dispositivi di sicurezza locali nei datacenter.

- **Fase 1:** Indirizza il traffico DNS verso la rete globale di Cloudflare
- **Fase 2:** Filtro DNS basato sulla posizione per proteggerti da ransomware, phishing e altre minacce Internet
- **Fase 3:** Controlla i flussi di dati applicando regole di isolamento HTTP, di rete e del browser con ispezione TLS 1.3 illimitata.



Come funziona

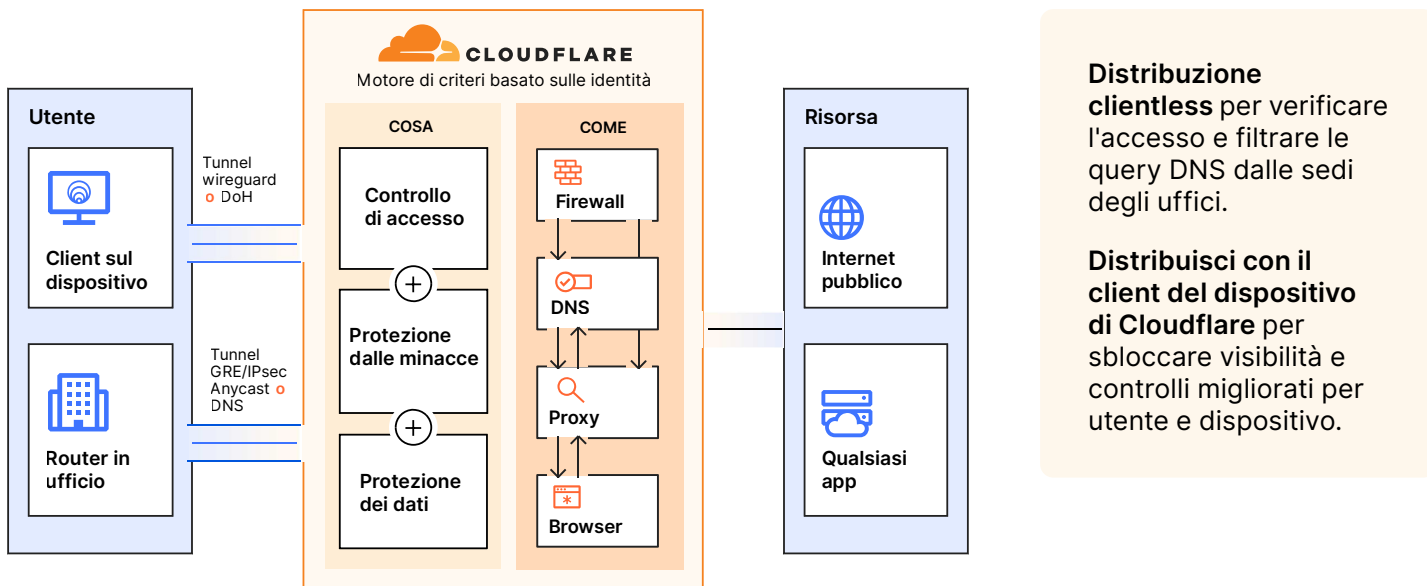


Figura 1: Verifica, filtra, isola e ispeziona il traffico dell'ufficio in un unico passaggio con [Cloudflare Zero Trust](#)

On-ramp flessibili da qualsiasi origine

Inizia utilizzando Cloudflare per la risoluzione DNS tramite router di rete. Nel tempo, invia il traffico L3 alla nostra rete globale tramite i tuoi tunnel GRE o IPsec o utilizza il tuo metodo routing SD-WAN esistente.

In alternativa, distribuisci il client di Cloudflare per il filtraggio e l'ispezione DNS e HTTP sui dispositivi gestiti.

Applicazione rapida dei criteri, progettata per scalare a livello globale

Tutte le funzioni di sicurezza, prestazioni e affidabilità sono progettate per essere eseguite su ogni server in ogni datacenter nelle nostre oltre 275 sedi e in oltre 100 paesi.

La nostra scalabilità della rete significa che le protezioni sono sempre applicate vicino agli uffici e agli utenti finali, ovunque si trovino, ad alta velocità con ispezione a passaggio singolo.

Altri casi d'uso da esplorare nei prossimi sei-dodici mesi



Riprendi il controllo sulle app SaaS

Scopri e mitiga i rischi dello shadow IT che i dipendenti utilizzano in ufficio e a casa.

Previene le fughe di dati e le violazioni della conformità con i criteri CASB abilitati dalla stessa dashboard Cloudflare. [Scopri come.](#)



Scarica il traffico MPLS

Sostituisci le connessioni MPLS private costose, obsolete e lente.

Semplifica l'architettura WAN legacy utilizzando la rete globale di Cloudflare per gestire il traffico tra filiali, datacenter e servizi cloud pubblici. [Scopri come.](#)

1. Gartner Hype Cycle for Network Security, 2021 | GARTNER e HYPE CYCLE sono marchi commerciali registrati e marchi di servizio di Gartner, Inc, e/o delle sue controllate negli Stati Uniti e a livello internazionale, e vengono utilizzati qui previa autorizzazione. Tutti i diritti riservati.