Protezione del lavoro ibrido

Riduci i rischi e aumenta la visibilità per tutti gli utenti, sia all'interno che all'esterno della rete

Proteggi qualsiasi connessione da qualsiasi utente, su qualsiasi dispositivo, in qualsiasi luogo

Il nostro futuro di lavoro da qualsiasi luogo: anni dopo la pandemia globale e con una recessione imminente, il lavoro ibrido sembra qui per restare. I team IT e di sicurezza devono fornire protezione ed esperienze coerenti per tutti gli utenti e i dispositivi, sia remoti che in ufficio, e gli strumenti tradizionali incentrati sulla posizione (come VPN e controlli basati su IP) non riescono a soddisfare il compito.

Sicurezza moderna per una forza lavoro moderna: In risposta, molte organizzazioni stanno reinventando la propria architettura IT e di sicurezza e adottando la sicurezza fornita dal cloud che si adatta alle esigenze della forza lavoro distribuita e segue le best practice Zero Trust.

Cloudflare semplifica la protezione di qualsiasi connessione, in modo che gli utenti su qualsiasi dispositivo o in qualsiasi luogo rimangano al sicuro e produttivi quando accedono alle applicazioni o a Internet.

Cosa riporta Gartner®:

> *Entro il 2026, il 75% dei lavoratori continuerà a dividere il tempo tra casa e uffici tradizionali, in leggero calo rispetto al 77% del culmine della pandemia nel 2021.*[1]

> *I progetti di sicurezza di rete basati su una raccolta di dispositivi di sicurezza perimetrale non sono adatti per soddisfare le esigenze dinamiche ovunque e in qualsiasi momento di un'azienda digitale moderna e della sua forza lavoro digitale ibrida.*[2]

Indice per pagina

Opportunità di modernizzazione della sicurezza

Accesso sicuro alle applicazioni senza VPN

Con gli utenti così dispersi, il backhauling del traffico attraverso dispositivi on-premise come le VPN rallenta le prestazioni e crea il rischio che le minacce si diffondano lateralmente nella rete aziendale.

Invece, riguadagna visibilità per tutte le richieste e applica controlli basati sull'identità forniti più vicino agli utenti per sostenere la produttività. Niente più backhauling.

Sicurezza SaaS semplificata

Oggi più che mai, la forza lavoro si affida ad applicazioni SaaS al di fuori dei controlli delle tradizionali reti aziendali.

In risposta, le organizzazioni necessitano di una visibilità e di un controllo più completi sulle loro applicazioni SaaS per impostare criteri di accesso, applicare controlli di protezione dei dati, mitigare lo shadow IT e scansionare le app alla ricerca di configurazioni errate.

Proteggi utenti e dati dalle minacce Internet

Ransomware, phishing e altre minacce Internet sono sempre presenti e sempre più sofisticate.

L'adozione dell'ispezione e dell'isolamento basati sul cloud per il traffico in uscita protegge gli utenti dal malware. Inoltre, gli amministratori possono applicare controlli per impedire che dati sensibili raggiungano dispositivi locali non gestiti.

Lavoro ibrido per imprese mature

Per le aziende mature, modernizza la sicurezza per il lavoro ibrido in tutta sicurezza

Problema: ambienti complessi e legacy

Le organizzazioni stanno sperimentando modelli di lavoro in ufficio. Ma mantenere protezioni ed esperienze utente coerenti è impegnativo in questi scenari ibridi.

Queste società tendono ad essere più affermate, con investimenti preesistenti (spesso complessi) in loco e legacy più pesanti. Avviare un nuovo progetto di sicurezza di fronte a venti contrari alla recessione può sembrare troppo rischioso e difficile.

Opportunità: percorso più semplice verso la modernizzazione

Le organizzazioni meritano di perseguire la trasformazione digitale al proprio ritmo, senza la necessità di un budget infinito, costose "prove di concetto", complesse fasi di implementazione o servizi collegati a margherita.

Per aiutare queste aziende mature a soddisfare le loro esigenze di lavoro ibrido, Cloudflare è progettato per essere più facile e veloce da implementare rispetto ad altri fornitori di servizi Zero Trust come Zscaler.

Casi d'uso campione

Telecomunicazioni

Situazione: Oltre 100 anni di società di telecomunicazioni europee con un fatturato annuo di oltre 20 miliardi di dollari volevano che un unico fornitore implementasse il filtraggio Internet e autenticasse l'accesso alle app legacy che erano state migrate di recente in più ambienti cloud.

Soluzione: L'azienda ha scelto Cloudflare per consolidare i servizi e utilizzare una piattaforma unificata per proteggere sia l'applicazione che l'accesso a Internet tra i suoi oltre 100.000 dipendenti.

Governo federale

Situazione: Dipartimento per la sicurezza interna degli Stati Uniti (DHS) sta conducendo investimenti nella protezione dalle minacce Internet in uffici, sedi e infrastrutture federali.

Soluzione: DHS ha selezionato Cloudflare e Accenture Federal Services per sviluppare una soluzione congiunta per filtrare le query DNS verso destinazioni dannose e rischiose che verranno utilizzate dalle agenzie federali.

Media e pubblicità

Situazione: Il conglomerato dei media (oltre 10 miliardi di dollari di entrate e oltre 100.000 dipendenti a livello globale) affronta attacchi informatici all'infrastruttura interna, inclusa una richiesta di riscatto.

Soluzione: Cloudflare protegge centinaia di app Web e non Web con regole Zero Trust basate sull'identità. L'azienda implementa la protezione per 50.000 dipendenti entro 3 mesi e prevede di espandersi a tutta la forza lavoro entro 9 mesi.

Energia

Situazione: Il fornitore di gas naturale Fortune 500 ha cercato una maggiore protezione dalle crescenti minacce informatiche rivolte al settore sia per i suoi data center distribuiti che per oltre 1.500 dipendenti.

Soluzione: L'azienda ha scelto Cloudflare per sostituire Zscaler, citando una migliore affidabilità e coerenza nella protezione dell'applicazione e dell'accesso a Internet e un percorso più semplice per adottare controlli avanzati con isolamento remoto del browser.

TESTIMONIANZE DEI CLIENTI

> *Cloudflare è un moltiplicatore di forza nel nostro viaggio verso Zero Trust.*

John McLeod
CISO, National Oilwell Varco

> *Cloudflare ha consentito a Ziff Media Group di fornire in modo semplice e sicuro la nostra suite di strumenti interni ai dipendenti di tutto il mondo su qualsiasi dispositivo, senza la necessità di complicate configurazioni di rete.*

Josh Butts
SVP Product & Technology,
Ziff Media Group

> *Con Cloudflare, siamo riusciti a ridurre la nostra dipendenza dalle VPN e dagli elenchi di indirizzi IP consentiti per gli ambienti di sviluppo.*

Alexandre Papadopoulos,
Direttore della sicurezza informatica,
INSEAD

Forza lavoro da remoto per nativi digitali

Per i nativi digitali, dai la priorità alla sicurezza agile per supportare la flessibilità del lavoro remoto

Problema: scalare e automatizzare la sicurezza del cloud

Molte organizzazioni stanno adottando l'assunzione a distanza. Spesso tendono ad essere i primi e i più giovani ad adottare il cloud con un'infrastruttura locale limitata e con modelli di business basati su servizi digitali sicuri, veloci e affidabili.

Consentire la flessibilità del lavoro da qualsiasi luogo può essere un fattore di differenziazione, ma richiede strumenti di sicurezza che siano ugualmente flessibili man mano che gli utenti si spostano e fanno affidamento sui dispositivi personali.

Opportunità: sicurezza componibile adatta alla scalabilità

Con meno IT legacy da deprecare, questi nativi digitali possono sfruttare la nostra architettura nativa di Internet e la flessibilità di distribuzione per rimanere agili nella loro modernizzazione della sicurezza.

I nostri servizi componibili, la progettazione API-first e la gestione a riquadro singolo semplificano l'avvio e l'adattamento della sicurezza. La velocità, la scalabilità e l'affidabilità della nostra rete globale soddisfano le esigenze di una forza lavoro completamente remota.

Casi d'uso campione

SaaS B2B

Situazione: La piattaforma di progettazione grafica australiana Canva (del valore di $ 40 miliardi nel 2021) ha implementato Cloudflare prima della pandemia per semplificare l'accesso per utenti di terze parti ed evitare il fastidio dell'implementazione di una VPN.

Soluzione: Nel tempo, Canva ha implementato criteri di accesso alle applicazioni Zero Trust in tutta la sua forza lavoro in crescita, oltre a estendere il filtraggio e l'ispezione di Internet.

Fintech e blockchain

Situazione: BlockFi, una piattaforma di gestione patrimoniale di serie D basata sulla tecnologia blockchain, necessaria per aumentare la sicurezza di fronte alle minacce informatiche contro le sue crescenti risorse gestite e la forza lavoro remota.

Soluzione: Cloudflare ha consentito a BlockFi di passare all'autenticazione basata sull'identità per l'accesso alle applicazioni e lontano dai lunghi controlli basati su IP.

Social media

Situazione: La piattaforma di social media globale ha subito una violazione di alto profilo sfruttando l'accesso alle applicazioni interne e le configurazioni VPN.

Soluzione: In risposta, l'azienda ha deciso di rivedere il suo approccio di accesso remoto adottando la soluzione Zero Trust Network Access (ZTNA) di Cloudflare per 13.000 dipendenti e appaltatori e ritirando le sue implementazioni VPN.

e-commerce

Situazione: La piattaforma di e-commerce globale ($ 4 miliardi di entrate e oltre 15.000 dipendenti) ha cercato una migliore protezione per gli utenti remoti che navigano in Internet e accedono ad app SaaS sensibili mentre sono fuori rete.

Soluzione: L'azienda implementa Cloudflare per stratificare funzionalità di protezione dalle minacce come il filtraggio DNS fornendo al contempo una maggiore visibilità sull'utilizzo delle applicazioni SaaS.

TESTIMONIANZE DEI CLIENTI

"Noi di Delivery Hero ci impegniamo molto per offrire ai nostri clienti un'esperienza straordinaria. Cloudflare ci aiuta a fare lo stesso per i nostri team interni: offrendo loro un ambiente di lavoro sicuro in tutto il mondo e un modo semplice per creare applicazioni veloci, affidabili e rispettose della privacy."

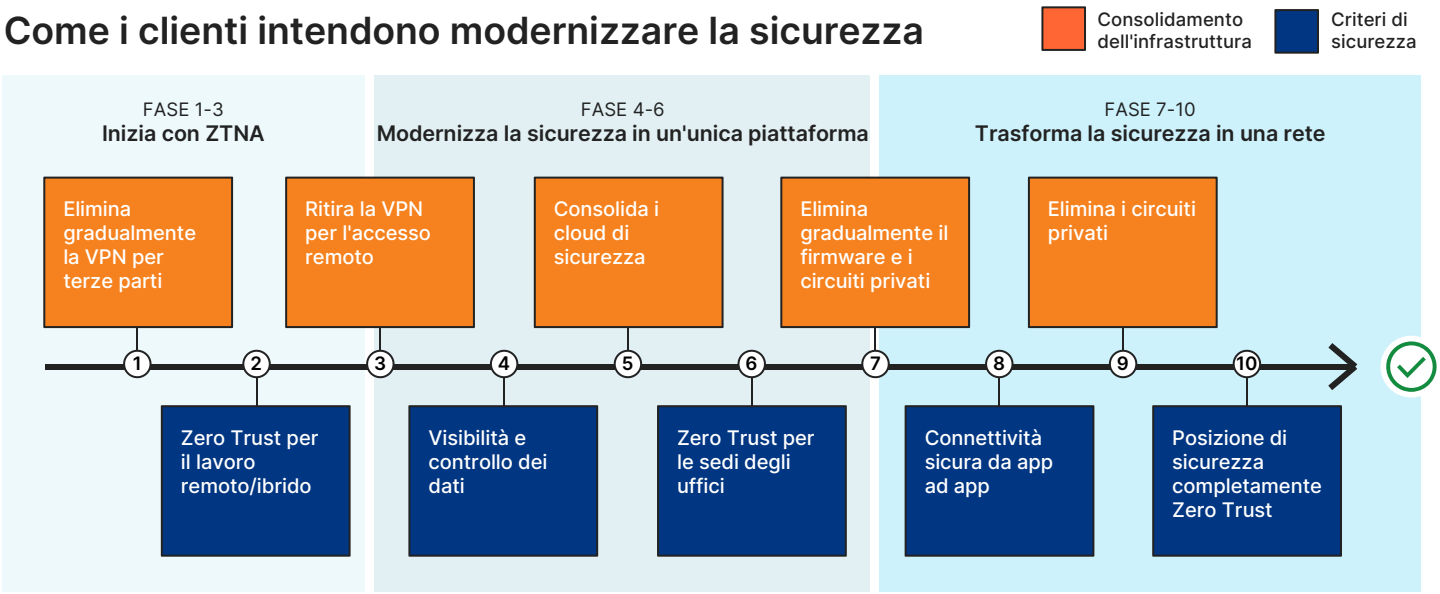
Christina von Hardenberg
CTO, Delivery Hero

"Cloudflare è essenziale per proteggere la nostra forza lavoro remota in rapida crescita. L'adozione di Zero Trust per l'accesso alle applicazioni ha offerto ai nostri amministratori una maggiore visibilità e controlli granulari che non avrebbero mai potuto ottenere con i precedenti strumenti legacy."

Marccio Alcaide
Head, IT Security, Facily

Tabella illustrativa del lavoro ibrido

Come i clienti intendono modernizzare la sicurezza



Roadmap per la modernizzazione della sicurezza

La roadmap sopra illustra l'approccio adottato dalle organizzazioni durante la modernizzazione della propria sicurezza per adattarsi al lavoro ibrido. Questa roadmap ha due obiettivi principali:

1) **Riga in alto (in arancione):** per consolidare la connettività e l'infrastruttura di sicurezza dai prodotti e dall'hardware specifici a un'unica piattaforma cloud-native.
2) **Riga in basso (in blu):** per ottenere visibilità e controlli per adottare la sicurezza Zero Trust tra utenti e risorse su qualsiasi dispositivo, in qualsiasi luogo.

Fasi 1-5: Protezione dell'app e dell'accesso a Internet

Per molti, adattarsi al lavoro ibrido significa innanzitutto modernizzare il modo in cui la forza lavoro raggiunge le risorse aziendali.

Fase 1: spesso il primo passo è iniziare a scaricare il traffico VPN e passare ai controlli nativi di Internet per utenti selezionati, come appaltatori, sviluppatori, partner o team di nuova acquisizione. Cloudflare rende particolarmente facile proteggere le app self-hosted accessibili tramite un browser senza la necessità di distribuire alcun software sugli endpoint.

Fase 2: questi strumenti moderni consentono la visibilità necessaria per creare policy per-app basate su ruolo, requisiti MFA e hard key, identità e posizione del dispositivo.

Fase 3: man mano che i team acquisiscono fiducia in questo approccio, si spostano per ritirare completamente la propria VPN e proteggere le reti private legacy e non Web con Zero Trust.

Fase 4: l'attenzione si sposta quindi sul miglioramento della visibilità e dei controlli per le app SaaS, inclusa la mitigazione dell'IT ombra, la gestione dei tenant e la prevenzione dell'esfiltrazione dei dati.

Fase 5: con le app interne e SaaS ora gestite da un'unica piattaforma, le organizzazioni cercano di espandere i controlli per l'accesso a Internet in uscita e consolidare gli strumenti di protezione dalle minacce come i filtri DNS e i gateway Web sicuri.

Fasi 6-10: Spostare la connettività al cloud

Le restanti fasi della roadmap sono in fase di pianificazione per la maggior parte delle organizzazioni, ma la loro aspirazione è spostare tutta la connettività e la sicurezza della rete su un'unica rete cloud unificata.

Fase 6: qui, le organizzazioni cercano di estendere Zero Trust coerente a qualsiasi posizione di rete come quartier generale, filiale, data center e uffici satellite per supportare il lavoro ibrido.

Fase 7: poiché il traffico dell'ufficio viene inviato sempre più spesso a Cloudflare per motivi di sicurezza, le organizzazioni possono eliminare gradualmente i tradizionali firewall on-premise e altri dispositivi di rete privati.

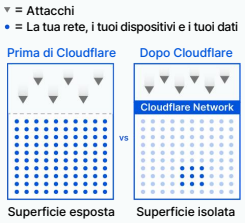
Fase 8: Questi casi d'uso avanzati si concentrano sulla protezione della connettività da app a app in ambienti multi-cloud ibridi, che preparano il team dell'infrastruttura di rete a terminare i contratti MPLS di telecomunicazione nella **Fase 9**.

Fase 10: sebbene la modernizzazione non sia mai veramente finita, l'aspirazione è che Zero Trust ora si estenda a tutti gli utenti, dispositivi, dati, applicazioni e ambienti.

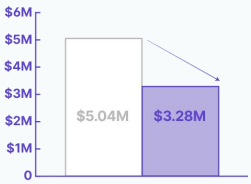
Risultati aziendali e di sicurezza

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

Riduci la superficie d'attacco
91% ↓

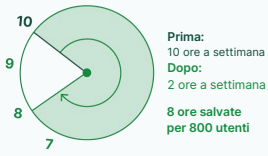


Riduci violazioni elevate
35% ↓



Accelera l'onboarding dei dipendenti
60% ↑

Riduci sovraccarico dei ticket IT
80% ↓



Riduci Utente latenza
39% ↓

Altri driver di business

Sblocca la produttività della forza lavoro

Per gli amministratori

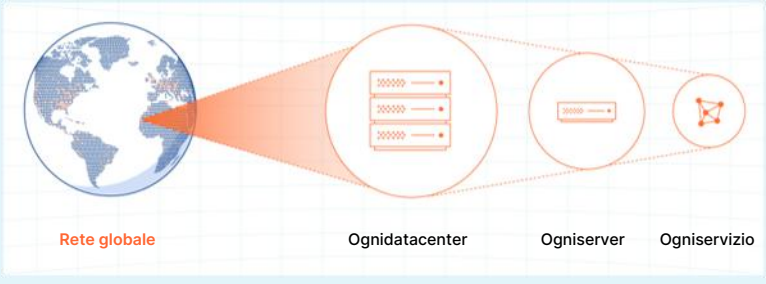
- Semplifica la configurazione con un'unica interfaccia di gestione per impostare i criteri nell'applicazione e nell'accesso a Internet
- Configura tutte le integrazioni con provider di identità, protezioni endpoint, provider cloud e rampe di rete dalla stessa interfaccia di gestione

Per gli utenti finali

- Autenticazione senza attriti ed esperienze di navigazione nativa con una sicurezza che rimane fuori mano

Riduci i costi sui servizi legacy

- Sostituisci o aumenta i tuoi dispositivi di rete privata virtuale (VPN) e adotta invece Zero Trust Network Access (ZTNA)
- Transizione da proxy Web o firewall in loco a servizi di sicurezza L3-L7 nativi del cloud
- Scarica i casi d'uso dall'infrastruttura del desktop virtuale con Remote Browser Isolation (RBI)
- Sostituisci il tradizionale gateway di posta elettronica sicuro con la moderna sicurezza della posta elettronica nel cloud



Velocità e scalabilità costanti per proteggere tutti gli utenti remoti o dell'ufficio

Tutte le funzioni di sicurezza, prestazioni e affidabilità sono progettate per funzionare su ogni singolo server in ogni data center Cloudflare sulla nostra rete che oggi copre oltre 275 città.

Accelera la tua roadmap Zero Trust — Provalo ora — Contattaci

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

REV: PMM-2022JJUL

[1] *Top Network Practices to Support Hybrid Work,* Gartner, Karen Brown, Andrew Lerner, Mike Toussaint, 08/04/2022
[2] *2022 Strategic Roadmap for SASE Convergence,* Gartner, Neil MacDonald, Andrew Lerner, John Watts 24/06/2022