CLOUDFLARE

WHITEPAPER

La speranza all'orizzonte: come creare una migliore posizione di sicurezza informatica in tempi di incertezza economica

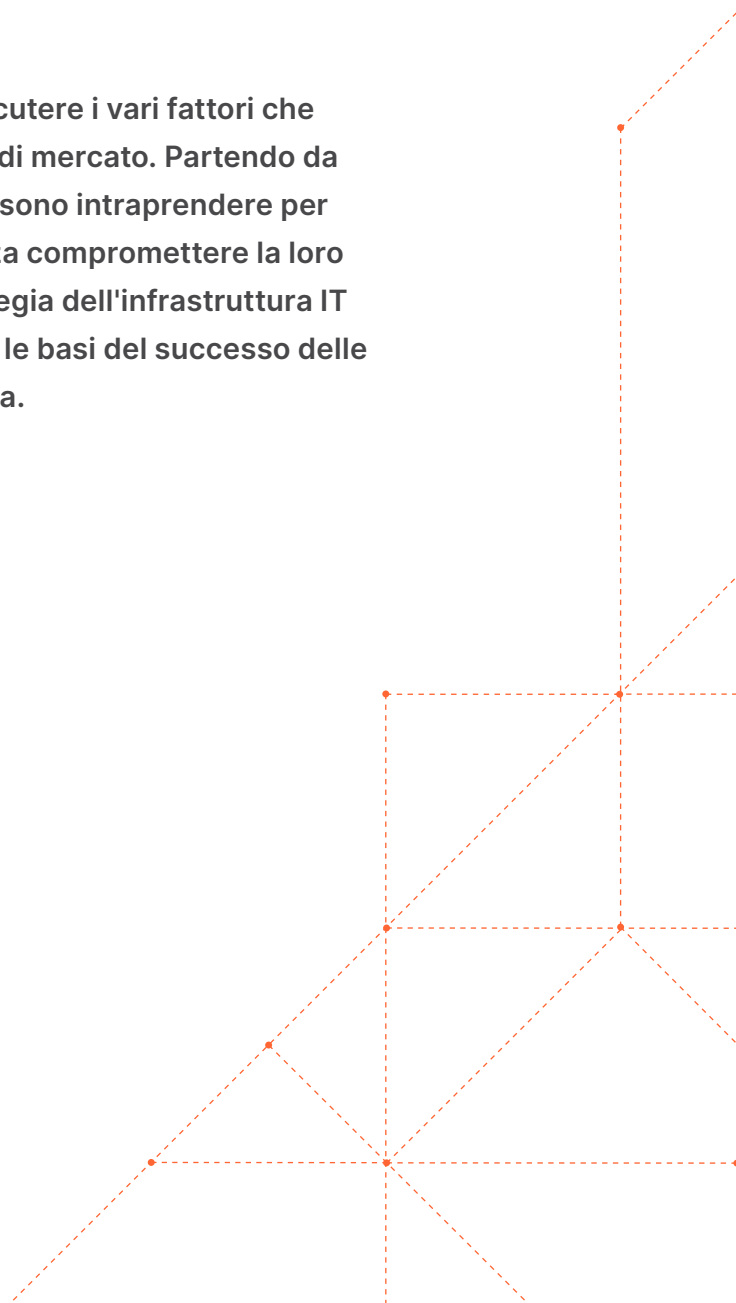
Contenuto

Riepilogo

Le aziende si trovano ad affrontare un periodo di incertezza economica e le prospettive diventano giorno dopo giorno sempre più imprevedibili. Questa incertezza, spesso incarnata da budget in continua contrazione, mette pressione sui CIO e sui responsabili tecnici affinché trovino nuove soluzioni per il futuro.

Fortunatamente, i leader che implementano le giuste strategie per affrontare la tempesta, riallineando i budget, ridefinendo i processi all'insegna dell'efficienza e proseguendo verso la crescita programmata senza un aumento sostanziale delle risorse, potranno ancora trovarsi ben posizionati una volta che le nubi si saranno diradate.

Nelle sezioni che seguono andremo a definire e a discutere i vari fattori che determinano queste circostanze e queste condizioni di mercato. Partendo da questi spunti, definiremo cinque azioni che i capi possono intraprendere per ottenere efficienze nelle loro prassi di sicurezza senza compromettere la loro postura di sicurezza complessiva. Allineando la strategia dell'infrastruttura IT al nuovo contesto economico, i leader possono porre le basi del successo delle proprie organizzazioni anche in una prospettiva futura.



Introduzione

Nel corso degli ultimi anni, i responsabili IT hanno dovuto affrontare una crisi dietro l'altra e l'hanno fatto mentre pianificavano ed implementavano le proprie strategie. Hanno dovuto reagire a una pandemia globale e ai suoi effetti secondari, alle carenze della catena di approvvigionamento, all'escalation del conflitto nell'Europa orientale e a quella che potrebbe rivelarsi una recessione. Nelle parole dell'economista di Stanford Paul Romer, "Una crisi è una cosa terribile da sprecare" (fonte). Le scelte che i CIO hanno fatto per supportare la loro forza lavoro in remoto avranno vantaggi non intenzionali e duraturi nel rendere i luoghi di lavoro ancora più attraenti sotto il profilo del sostegno al lavoro da remoto. Allo stesso modo ora, mentre i dirigenti affrontano un peggioramento delle prospettive economiche, le scelte che fanno in materia di sicurezza, networking, accesso remoto, storage, sviluppo e infrastruttura li aiuteranno a emergere più forti e meglio posizionati per una crescita sicura e sostenibile nel futuro.

L'ascesa del lavoro a distanza è stata accompagnata da un vero e proprio boom di attacchi ransomware e di sofisticate minacce informatiche, che hanno stabilito nuovi parametri di riferimento per l'impatto sui ricavi di questi attacchi, la loro portata e il loro grado di sofisticazione (fonte). La scomparsa di ciò che restava del perimetro di rete, insieme all'aumento storico del turnover dei dipendenti, ha portato alla formazione di lacune nella sicurezza e di ritardi nei progetti IT strategici. Ciò ha costretto le organizzazioni a ripensare non solo il loro approccio verso le politiche di assunzione e di fidelizzazione, ma anche quello verso il controllo dell'accesso ai propri sistemi e alle proprie attrezzature. Sebbene la pandemia abbia dato origine a un drammatico aumento dei crimini informatici (fonte), essa ha anche aperto gli occhi alle organizzazioni e ai loro consigli di amministrazione sull'urgente necessità di un'efficace sicurezza informatica. Per le aziende è giunto il momento per di adottare un approccio più strategico e lungimirante verso l'abilitazione un'infrastruttura di lavoro ibrida sicura, produttiva e disponibile.

Ecco cinque operazioni che è possibile completare per ridurre i rischi della propria azienda con un budget limitato e innalzare la capacità della stessa di gestire le minacce emergenti che si profilano all'orizzonte:

1. Sottoporre a verifica tutti gli strumenti di sicurezza attualmente in uso per mettere a nudo eventuali sovrapposizioni in termini di capacità

Le organizzazioni hanno molto da guadagnare dalla razionalizzazione dei propri provider di soluzioni per la sicurezza. Sebbene nessuno strumento, preso singolarmente, può diventare quella sorta di "arma risolutiva" che i CISO vorrebbero avere, molti operatori nel campo della sicurezza aziendale ritengono che la loro azienda stia sprecando denaro su un numero eccessivo di strumenti, che tuttavia non offrono ancora una difesa ottimale. Quando si supporta un numero elevato di strumenti forniti da molteplici provider, vuol dire che i dipendenti dedicano tempo prezioso all'approvvigionamento, all'implementazione, alla gestione, alla risoluzione dei problemi e al supporto di un gran numero di sistemi disconnessi, invece di proteggere l'nfrastruttura e i dati aziendali. A tal proposito, un sondaggio condotto nel giugno 2022 in occasione della RSA Conference annuale rilevava che “la metà (53%) delle aziende interpellate riteneva di aver gettato al vento più del 50% del proprio budget per la sicurezza informatica e che non era ancora in grado di opporre un rimedio efficace alle minacce. Il 43% degli intervistati affermava che il problema numero uno nel rilevamento e nella risoluzione delle minacce risiedeva in una sovrabbondanza di strumenti, mentre il 10% delle organizzazioni affermava di non disporre di strumenti efficaci per fronteggiare le minacce alla sicurezza informatica” (fonte). Se si potessero eliminare anche solo una manciata di questi strumenti, si potrebbe migliorare notevolmente la postura di sicurezza, facendo risparmiare tempo prezioso ai dipendenti.

Spostando gli investimenti dalle spese in conto capitale alle spese operative, è possibile inoltre apportare miglioramenti immediati al flusso di cassa a breve termine ed evitare di rimanere bloccati in investimenti di capitale pluriennali che ostacolano l'agilità aziendale. Uno dei modi per semplificare consiste nel ridurre la dipendenza dall'hardware tradizionale. Il passaggio da box legacy a soluzioni as-a-Service può far sì che le iniziative con la massima priorità rimangano sempre finanziate, anche quando i budget si assottigliano. L'adozione di un modello as-a-Service significa inoltre sfruttare i cicli di innovazione intrinsecamente più rapidi del software ed eliminare i fastidi inevitabili legati all'applicazione frequente di patch all'hardware legacy. Il non doversi più preoccupare del fattore innovazione e dell'aggiornamento continuo dei sistemi consente ai team di concentrarsi su attività realmente strategiche per l'azienda. Quando ci si trova ad affrontare periodi di incertezza, la semplificazione strategica e la razionalizzazione possono essere d'aiuto per raggiungere il successo nel lungo periodo.

2. Focalizzarsi sui dati e non solo sugli strumenti

La dirigenza deve valutare di modificare la propria attenzione verso una migliore integrazione non solo degli strumenti, ma anche dei dati, in tutti i loro set di strumenti di sicurezza, in modo da portare meglio alla luce schemi ricorrenti e anomalie. Storicamente, i team di sicurezza hanno continuato ad aggiungere sempre più set di strumenti nel corso del tempo, senza curarsi degli impatti a lungo termine di un numero eccessivo di dataset in un numero eccessivo di luoghi. Spesso, il risultato è un mosaico di prodotti con poca o nessuna interoperabilità e opacità nei dati, che si traducono in informazioni più deboli e con livelli di precisione inferiori e che introducono la possibilità di errore umano. Inoltre, il tempo necessario a un team per estrarre più set di dati, unirli insieme ed eseguire le query non è solo sprecato, ma si accompagna anche a uno spreco di risorse, risorse che potrebbero essere indirizzate verso iniziative di business più strategiche.

Sebbene i team possano essere in grado di trovare soluzioni alternative molto creative per risolvere i problemi di interoperabilità, come l'unione manuale di set di dati o l'importazione e l'esportazione di CSV, è importante considerare che, mettendo da parte il fattore efficienza, il valore degli strumenti di sicurezza risiede nei dati che questi sistemi digeriscono, creano e mettono a disposizione dei difensori. Se i dati sono ovunque e non sono secretati, protetti e gestiti con attenzione, la loro interpretazione potrebbe persino falsare interpretazioni e conclusioni che sarebbero state di eccezionale utilità, se derivate da dati gestiti correttamente. Questo è particolarmente vero per i dati che si trovano in istanze di shadow IT e che potrebbero essere stati completamente tralasciati. Razionalizzando i set di strumenti e considerando attentamente l'interoperabilità del proprio stack di sicurezza, si la possibilità di ridurre gli errori umani e di proteggere meglio i propri dati. Anche se oggi si sono profusi investimenti nei migliori strumenti disponibili sul mercato, la presenza di set di dati isolati e nascosti porta inevitabilmente alla formazione di un quadro della situazione meno aderente alla realtà.

In termini di efficienza, è importante considerare che nell'era di Zero Trust ("mai fidarsi, verificare sempre"), disporre di più strumenti vuol dire anche che i team impiegano più tempo per accedere, autenticarsi e ottenere l'accesso ai sistemi prima ancora che possano anche solo cominciare a svolgere il proprio lavoro. Quanto minore il numero di sistemi coi quali un dipendente dovrà interfacciarsi, tanto maggiore sarà il tempo che risparmierà e che potrà utilizzare per muoversi e lavorare più efficacemente. È di fondamentale importanza considerare che i dati all'interno di questi sistemi, nonché il numero di sistemi a cui i dipendenti devono accedere per completare una determinata attività, sono in definitiva ciò che consentirà o ostacolerà la capacità dei team di rispondere, piuttosto che reagire, alle minacce in un modo tempestivo.

3. Guardare a modelli cloud as-a-Service per massimizzare l'innovazione e ridurre al minimo la complessità

Ogni azienda ha bisogno di innovare per rimanere competitiva. Tuttavia, un'azienda che non opera nel campo della sicurezza informatica semplicemente non ha il tempo, il budget o le risorse per stare al passo con gli ultimi CVE, con le tendenze degli attacchi e con le patch critiche necessarie per mantenere in sicurezza la propria infrastruttura. L'adozione di modelli as-a-Service, ove fattibile, consente alla dirigenza di trarre vantaggio dall'innovazione continua senza doversi preoccupare di scendere a compromessi o dover assumere decisioni difficili in merito al debito tecnico.

È anche importante notare che alcuni servizi di sicurezza addebitano sovrapprezzi considerevoli per il superamento dei limiti di traffico e che alcuni addebitano delle tariffe per l'uso di larghezza di banda. È opportuno esaminare con attenzione ciò che la propria organizzazione sta pagando su base mensile o annuale, per capire se si sta pagando di più di quanto preventivato. Se questo è il caso, è possibile cogliere l'occasione per cercare altre soluzioni che non addebitino sovrapprezzi di alcun genere, non solo per risparmiare denaro, ma anche ad disporre di una spesa più prevedibile a lungo termine, cosa che consentirà ai team aziendali di formulare una pianificazione più efficace per il futuro.

I servizi di questa natura forniti dal cloud danno inoltre alle aziende spazio sufficiente per espandersi e contrarsi in base alle proprie esigenze, senza doversi impegnare nell'acquisto di rack hardware costosi e farsi carico di tutta la fatica della gestione del loro ciclo di vita che ne deriva. In tempi di incertezza, le aziende devono rimanere agili e reattive alle mutevoli condizioni del mercato. Quando il flusso di cassa è un problema, la capacità di ridurre al minimo i costi o eliminarli del tutto è un vantaggio strategico che può fare la differenza tra sopravvivere a malapena e prosperare, indipendentemente dalle condizioni di mercato.

4. Migliorare l'esperienza dei dipendenti

Secondo Forbes, "Il nostro sondaggio ha rilevato che i processi di accesso complessi strutturati in più fasi generano frustrazione tra i lavoratori, gli fanno perdere tempo, ne ostacolano la produttività e li spingono a rinunciare ad attività lavorative essenziali... Per ironia della sorte, quasi il 40% dei lavoratori ha ammesso di aver procrastinato, delegato o saltato del tutto la configurazione di nuove app per la sicurezza del lavoro a causa di processi di accesso laboriosi. Per analogia, è come proteggere la propria casa con il cancello più robusto, più alto e più sicuro che denaro possa comprare, fortificato con draghi spara-laser, solo per lasciarlo aperto di notte. Non solo è inefficiente e arduo per i difensori tenere traccia di quali tool house svolgono quale funzione, ma disporre di troppe dashboard e di troppi luoghi in cui i dati risiedono sono fattori che possono creare gravi rischi per la sicurezza e gap di visibilità anche nell'azienda più strutturata. Le aziende che vogliono stare al passo con le minacce alla sicurezza informatica devono riflettere sul fatto che ogni singolo clic e ogni singola pressione di un tasto sottrae tempo, energia e attenzione preziosi alla risposta a eventi critici. Al fine di creare un'esperienza dei dipendenti migliore e più snella, è fondamentale che la dirigenza esamini attentamente quanti strumenti devono utilizzare i difensori per svolgere il proprio lavoro in modo efficace e cosa può essere eliminato o razionalizzato per ridurre il tempo necessario a un difensore per rispondere e non solo per reagire, a un evento critico per la sicurezza.

Quando si tratta di dipendenti con mansioni non tecniche o di dipendenti che non ricoprono ruoli di difesa, è anche importante considerare che, poiché i lavoratori in remoto cercano di accelerare la propria produttività personale, essi possono ricorrere a soluzioni di shadow IT o a "scorciatoie" informatiche. Sebbene i controlli Zero Trust stiano tracciando un percorso promettente per la creazione di organizzazioni più sicure, specialmente in un ambiente remoto, è innegabile che non tutti gli approcci Zero Trust sono uguali. Quanto più è complesso per un dipendente ottenere l'accesso a ciò di cui ha bisogno, tanto più è probabile che trovi un modo per aggirare i controlli di sicurezza, piuttosto che rispettarli. La dirigenza deve cercare di capire a fondo non solo l'efficacia dei prodotti di sicurezza, ma anche la loro facilità d'uso, poiché l'ignorare il fattore dell'esperienza vissuta dal dipendente aumenta il rischio organizzativo complessivo.

5. Cercare dei servizi di sicurezza che non richiedano come contropartita una riduzione delle prestazioni di rete.

Non si tratta solo degli strumenti in sé. Ciò che può fare la differenza è il modo in cui li si configura e li si gestisce. È opportuno far svolgere ai team una verifica delle configurazioni e delle personalizzazioni attualmente in uso, per far emergere opportunità che potrebbero contribuire a migliorare le prestazioni. Se non è possibile migliorare le prestazioni, allora il consiglio è prendere in considerazione la ricerca di soluzioni create appositamente per la loro massimizzazione, dato che le soluzioni-tampone adottate in un secondo momento per il miglioramento delle prestazioni raramente raggiungono gli obiettivi che la dirigenza si era prefissata. Quando il discorso cade sulle prestazioni della rete, è importante tenere presente che un'architettura scadente non può essere migliorata con la riscrittura del suo codice. Una volta che le fondamenta di un edificio sono state costruite, è possibile ridisegnarne il progetto soltanto fino a un certo punto. Seguendo lo stesso ragionamento, anche le reti devono essere progettate sin dall'inizio per massimizzare il fattore prestazionale.

Sfruttare la potenza di una rete periferica globale capace di elaborare e gestire i dati più vicino all'origine offrirà alle organizzazioni un vantaggio strategico sia nell'immediato che in futuro. Secondo la MIT Technology Review, “l'elaborazione di grossi volumi di dati può portare a problemi di prestazioni. In risposta, molte organizzazioni si stanno rivolgendo all'edge computing, che elabora i dati vicino all'origine per consentire analisi e risposte rapide e in tempo reale, pur mantenendo i requisiti di privacy e sicurezza" (fonte). Scegliendo in modo strategico soluzioni che si stanno già basando sulle architetture di domani, è possibile offrire ai propri team il vantaggio strategico di disporre di migliori prestazioni di rete senza sacrificare i fattori critici della privacy e della sicurezza.

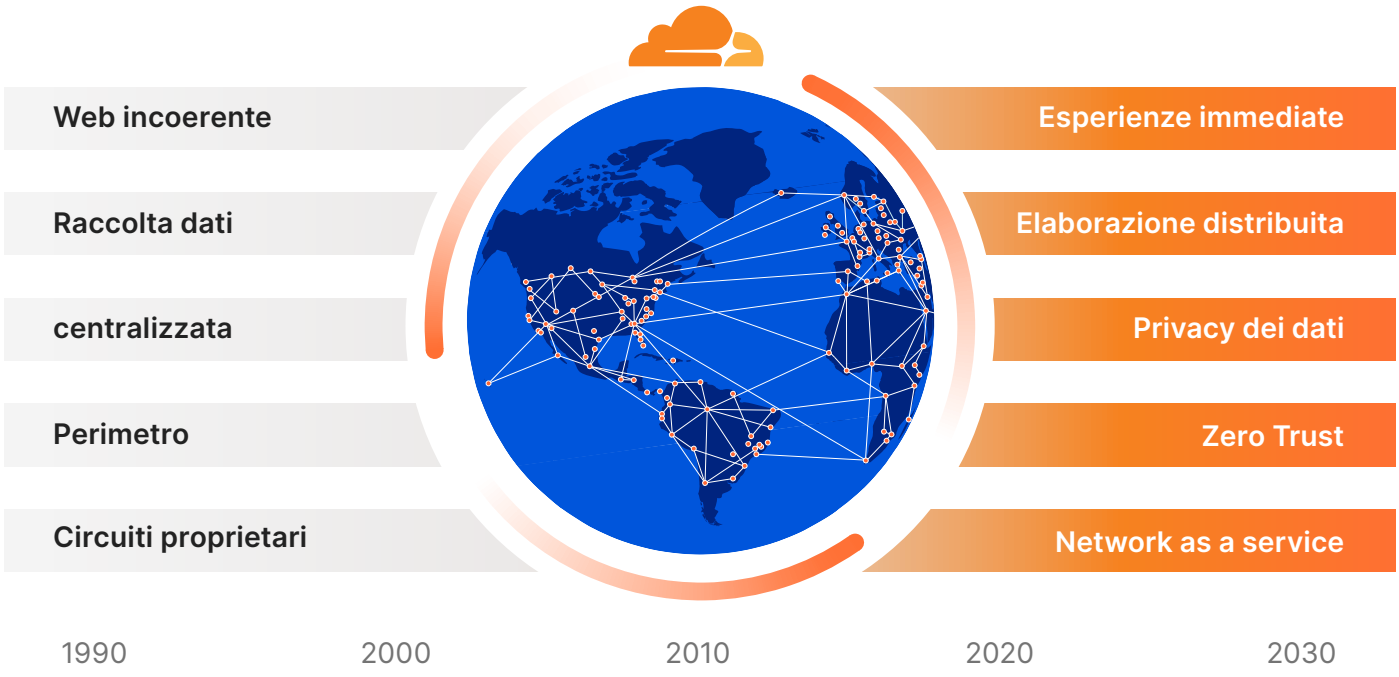
In sintesi, i passaggi che è possibile intraprendere per costruire una postura di sicurezza migliore in tempi caratterizzati da incertezza sono i seguenti:

1. **Sottoporre a verifica tutti gli strumenti di sicurezza attualmente in uso per mettere a nudo eventuali sovrapposizioni in termini di capacità**
   - Razionalizzare i tool che si sovrappongono
   - Spostare gli investimenti dal CapEx all'OpEx
2. **Focalizzarsi sui dati e non solo sugli strumenti**
   - L'interoperabilità degli strumenti conduce a data set migliori e più precisi
   - Disporre di dataset e report più accurati permette di acquisire una visione più realistica della situazione, un fattore fondamentale per raggiungere gli obiettivi aziendali
3. **Guardare a modelli cloud as-a-Service per massimizzare l'innovazione e ridurre al minimo la complessità**
   - Se non si opera nel campo della sicurezza informatica, si ha molto da guadagnare dal trasferire le operazioni di patching, manutenzione e aggiornamento a una soluzione as-a-Service
   - I modelli cloud e as-a-Service offrono la flessibilità necessaria per essere agili in un ambiente economico fluttuante
4. **Migliorare l'esperienza dei dipendenti**
   - Troppi strumenti in troppi posti possono creare punti ciechi nella sicurezza e generare frustrazione nei dipendenti: razionalizzandoli e semplificandoli, anche l'esperienza del dipendente uscirà migliorata
   - L'ottimizzazione delle soluzioni sotto il profilo della loro facilità d'uso per i dipendenti aumenterà la fidelizzazione di questi ultimi e li scoraggerà dal rivolgersi a soluzioni IT non approvate per portare a termine il proprio lavoro
5. **Cercare i costi nascosti e le opportunità di miglioramento delle prestazioni nel proprio stack di cybersecurity**
   - Sottoporre a verifica gli strumenti esistenti per scoprire eventuali possibilità di miglioramenti prestazionali, tenendo a mente che non è però possibile ottimizzare un'architettura scadente
   - L'adozione di strumenti costruiti su scala globale e ubicati più vicino a dove si prevede che si troveranno i propri clienti consentirà all'azienda di offrire un'esperienza cliente sicura e di qualità superiore

In che modo Cloudflare può essere d'aiuto

Cloudflare è stato lanciato nel 2010, nel periodo immediatamente successivo alla crisi finanziaria del 2008, per guidare la trasformazione dall'infrastruttura on-premise al cloud. Abbiamo costruito la piattaforma di Cloudflare da zero con un obiettivo ambizioso: aiutare a costruire un Internet migliore. La suite di prodotti di Cloudflare è in grado di proteggere e accelerare qualsiasi applicazione Internet senza dover aggiungere altro hardware, installare software o modificare anche una sola riga di codice.

L'intero traffico delle proprietà Internet che si affidano a noi viene distribuito sulla nostra rete globale intelligente, che diventa sempre più efficace richiesta dopo richiesta. Aiutiamo i nostri clienti a lavorare in modo più intelligente, creare meglio, funzionare più velocemente e crescere in modo sicuro. Oggi Cloudflare protegge e accelera milioni di proprietà Internet.



Controllo

Acquisisci tutta la potenza di una rete globale integrata che offre connettività, sicurezza ed elaborazione complete lasciandoti il pieno controllo delle policy.

Flessibilità

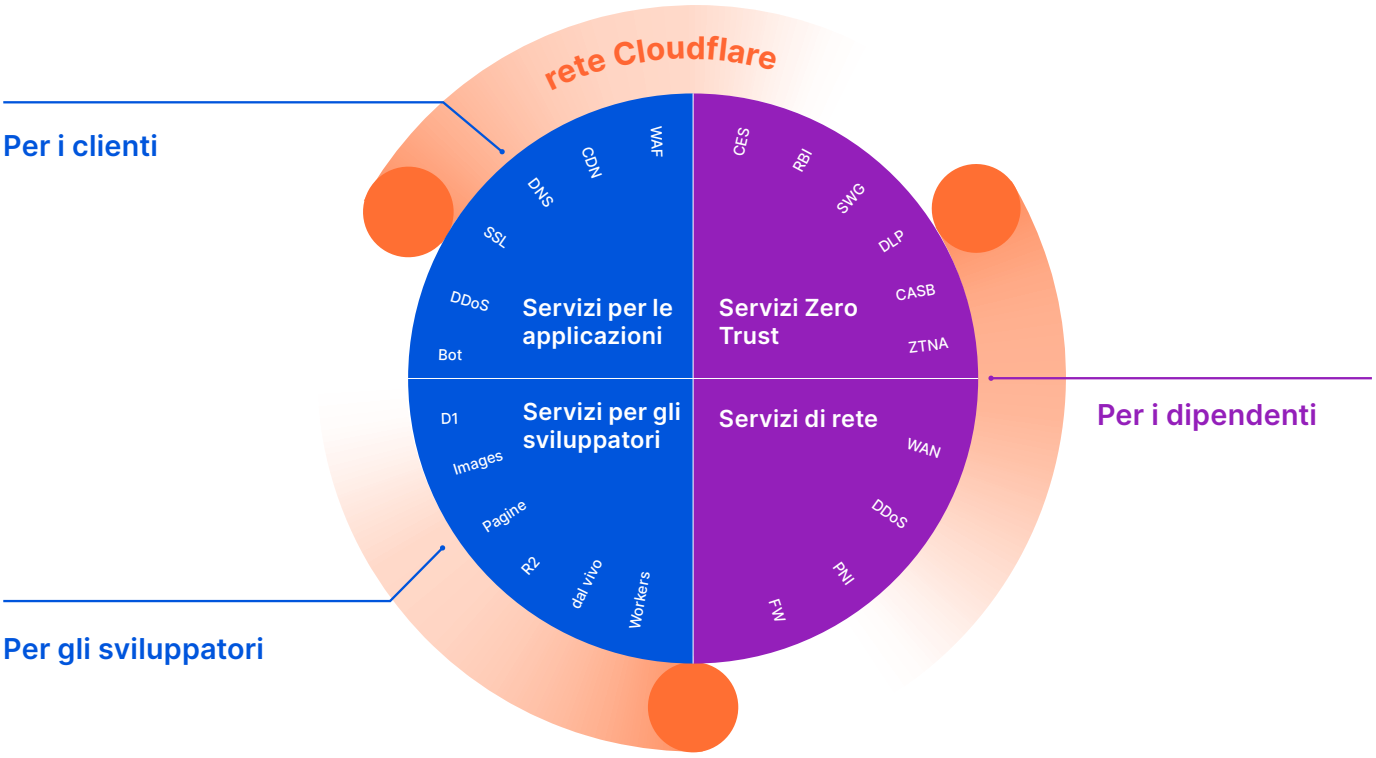
I servizi cloud native non richiedono investimenti in conto capitale anticipati. Il loro utilizzo può essere ampliato o ridotto in linea con le fluttuazioni del business.

Prevedibilità

Fatturazione prevedibile, senza costi inattesi come tariffe di uscita non forfettarie. Nessun bisogno di consumare spese in conto capitale per hardware che verrà consegnato l'anno prossimo.

La rete globale di Cloudflare rende tutto ciò che connetti a Internet sicuro, privato, veloce e affidabile.

- **Proteggi** i tuoi siti Web, API e applicazioni Internet.
- **Proteggi** le reti, i dipendenti e i dispositivi aziendali
- **Scrivi** e **distribuisci** codice che viene eseguito sul perimetro della rete



La nostra piattaforma

Informazioni su Cloudflare

Cloudflare è stato lanciato nel 2010 per guidare la trasformazione dall'infrastruttura on-premise al cloud. Abbiamo costruito la piattaforma di Cloudflare da zero con una piena comprensione del nostro piano audace: aiutare a costruire un Internet migliore. La suite di prodotti di Cloudflare è in grado di proteggere e accelerare qualsiasi applicazione Internet senza dover aggiungere altro hardware, installare software o modificare anche una sola riga di codice.

L'intero traffico delle proprietà Internet che si affidano a noi viene distribuito sulla nostra rete globale intelligente, che diventa sempre più efficace richiesta dopo richiesta. Aiutiamo i nostri clienti a lavorare in modo più intelligente, costruire meglio, funzionare più velocemente e crescere in modo sicuro. Oggi Cloudflare protegge e accelera milioni di proprietà Internet.

Per saperne di più, visita www.cloudflare.com/it-it/

CLOUDFLARE

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

REV:BDES-4327.2023MAR10