CLOUDFLARE

Ebook

Scoraggiare i tempi di inattività: guida ai modelli di difesa da attacchi DDoS

Contenuto

Fai clic per passare alla sezione

Introduzione: Difesa da attacchi DDoS nel mondo del lavoro ibrido

Un'azienda media oggi utilizza oltre 1.400 servizi cloud distinti[1], spinta dalla crescente domanda di applicazioni ed esperienze dei clienti migliori e più veloci. Tuttavia, un sottoprodotto della trasformazione del cloud è una superficie di attacco in espansione: più servizi digitali equivalgono a più "punti di ingresso" che gli autori di attacchi possono sfruttare. La superficie di attacco si è inoltre ampliata con il lavoro ibrido (la combinazione di lavoro in ufficio e lavoro da remoto), reso necessario da anni di pandemia globale.

Tutti questi fattori stanno aumentando la pressione sulle imprese a corto di risorse. Non solo i team IT e di sicurezza devono fornire applicazioni e reti più resilienti, ma devono anche proteggere utenti e dispositivi, indipendentemente dalla loro posizione, dalle minacce in continua evoluzione.

Alcune di queste minacce includono attacchi DDoS (Distributed Denial of Service) più frequenti, più lunghi e più ampi. Nel febbraio 2023, Cloudflare ha rilevato e mitigato il più grande attacco DDoS HTTPS (71 Mrps) mai registrato. I nostri dati mostrano anche aumenti su base trimestrale negli attacchi DDoS ipervolumetrici (attacchi superiori a 100 Gbps) nel 2022.

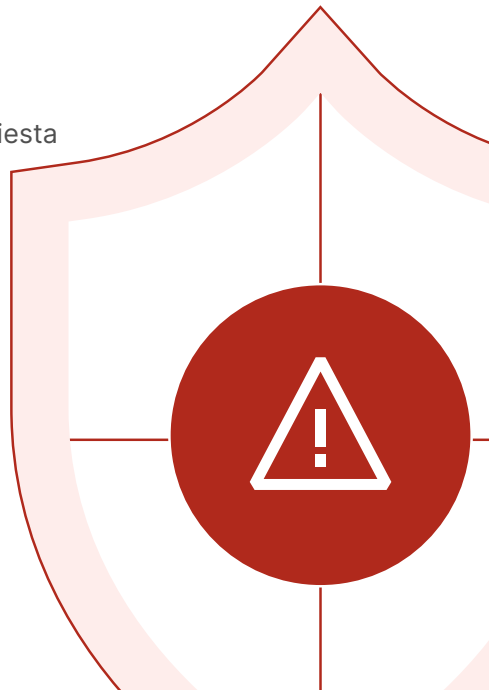
Le odierne realtà lavorative economiche e ibride richiedono alle aziende di rivalutare le proprie difese da attacchi DDoS:
il rischio di tempi di inattività, furto di dati, infiltrazione di rete e perdite finanziarie è troppo elevato.

La ricerca mostra che oltre il 60% delle interruzioni costa più di 100.000 dollari e il 15% delle interruzioni costa più di 1 milione di dollari[2]. In un esempio, i tempi di inattività dovuti a una serie di attacchi DDoS sono costati a un'azienda quasi 12 milioni di dollari[3].

Queste realtà rendono la difesa da attacchi DDoS fondamentale per le organizzazioni di tutte le dimensioni ed è chiaro che gli approcci manuali del passato non bastano più. Sebbene gli attacchi possano essere avviati dagli umani, vengono eseguiti dai bot e per vincere devi combattere i bot con altri bot. Il rilevamento e la mitigazione devono essere automatizzati il più possibile.

In questo ebook si esplora:

- I diversi modelli di protezione da attacchi DDoS basata su cloud
- Come superare i limiti del cloud scrubbing sempre attivo
- Come una società Fortune Global 500 ha contrastato un attacco DDoS con richiesta di riscatto con Cloudflare



Comprensione degli approcci di mitigazione DDoS basati su cloud

Un attacco DDoS è un tentativo dannoso di interrompere il normale traffico di un server, servizio o rete mirato sovraccaricando il bersaglio o l'infrastruttura circostante con un'ondata di traffico Internet. Una soluzione DDoS efficace ti dirà esattamente quando, dove e come si sta verificando questo "ingorgo di traffico", assorbendo e reindirizzando il traffico dannoso in modo che non interferisca con il traffico legittimo. Destinazioni ad alto traffico, insieme a proprietà e reti Internet non protette, sono tutti obiettivi comuni.

Sebbene gli attacchi DDoS non siano una novità, sono necessari nuovi approcci per fermarli. Con la migrazione delle applicazioni al cloud, anche il mercato delle soluzioni DDoS on-premise si è ridotto[4], ma sempre più organizzazioni si rivolgono al cloud per la protezione da attacchi DDoS.

Con numerose varietà di protezione basata su cloud, un provider di servizi cloud si trova di fronte alle applicazioni e all'infrastruttura di un'organizzazione e devia tutto il traffico verso uno scrubbing center per essere "ripulito". Solo il traffico legittimo viene rispedito al cliente. Questo movimento di "cloud scrubbing" può essere attivato in due modi: ***on demand*** o ***always-on***.

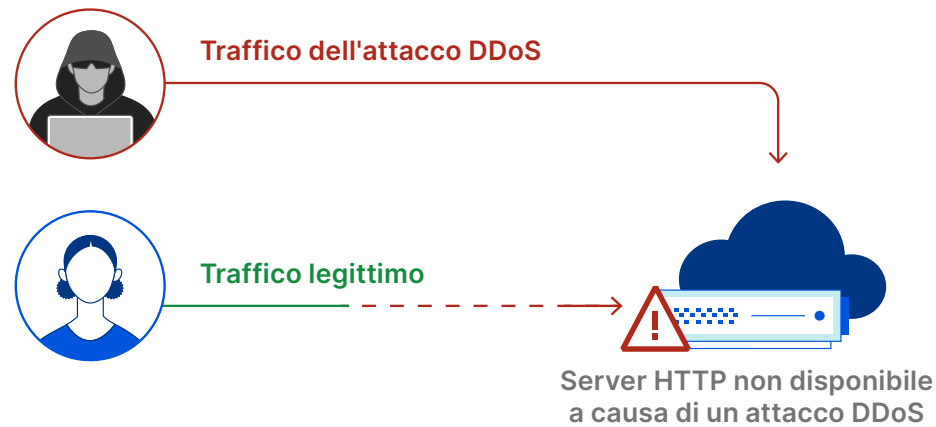
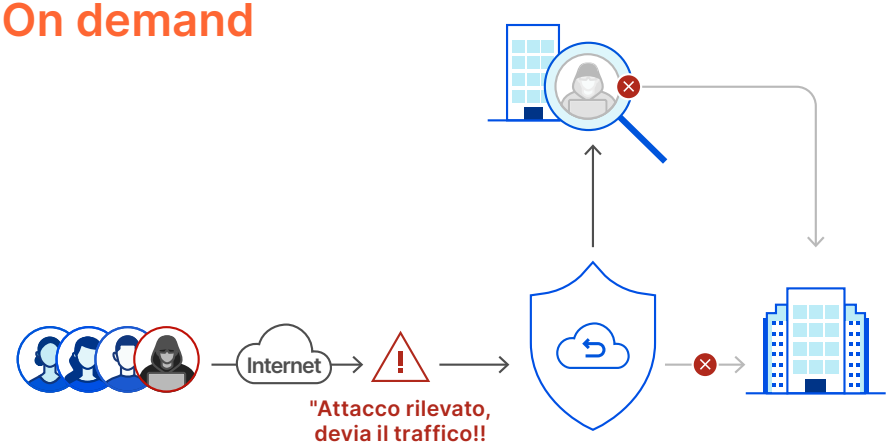


Diagramma di un attacco DDoS a livello di applicazione che nega il servizio agli utenti legittimi

On demand

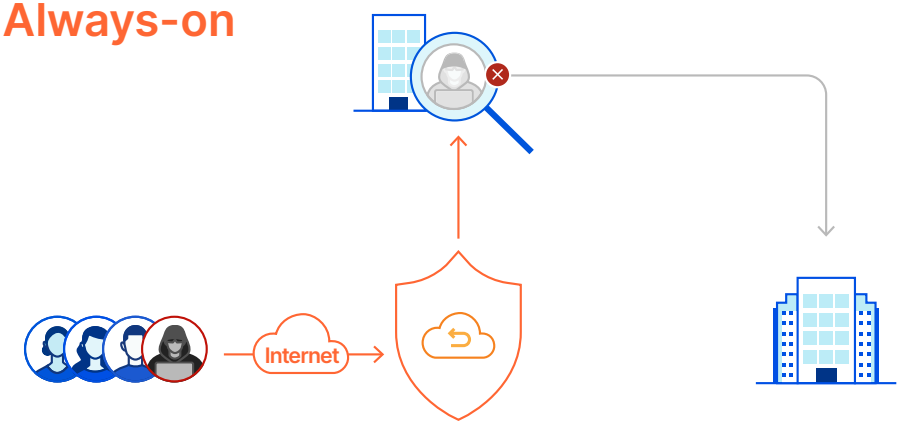


Durante il "tempo di pace", il cloud scrubbing su richiesta garantisce che tutto il traffico raggiunga le applicazioni e l'infrastruttura senza alcun reindirizzamento. Il traffico viene deviato al provider di cloud scrubbing solo in una situazione di attacco DDoS attivo.

Se il traffico in entrata supera una soglia preconfigurata (ad esempio, il 70% della capacità del collegamento) o se viene rilevato un attacco di grandi dimensioni, viene attivata la modalità di mitigazione del cloud su richiesta e il traffico viene deviato al centro di lavaggio più vicino per l'elaborazione.

Rispetto a

Always-on



Questo approccio essenzialmente pratico al cloud scrubbing instrada sempre il traffico attraverso il data center del provider di servizi cloud per l'ispezione delle minacce, anche in tempo di pace.

Un modello sempre attivo aiuta a ridurre al minimo il tempo dal rilevamento alla mitigazione senza alcuna interruzione del servizio.

Sebbene entrambe le tecniche on demand e always-on offrano vantaggi diversi, ognuna può presentare limitazioni in circostanze diverse, come descritto nella sezione successiva.

Limitazioni comuni dei metodi di cloud scrubbing

Problemi di cloud scrubbing in demand

Risposta ritardata all'attacco:

- L'opzione on demand richiede che il traffico venga reindirizzato al provider cloud in caso di attacco DDoS. Possono essere necessari diversi minuti prima che questo passaggio venga completato, oltre al tempo necessario per rispondere manualmente all'attacco (ad esempio, dire al provider di attivare il servizio). Se la protezione on demand non viene attivata in tempo, si può avere un impatto notevole.

Aumento dei costi nel lungo periodo:

- I provider di servizi cloud on demand spesso fanno pagare per byte di traffico di attacco. Mentre paghi solo per ciò che usi, questo potrebbe finire per costare di più se la tua organizzazione subisce attacchi DDoS più frequenti.

Potenziali attacchi mancati:

- Gli attacchi DDoS che non superano la soglia di utilizzo possono passare inosservati, congestionando i collegamenti di rete che influiscono sul traffico legittimo.
- Inoltre, i collegamenti di rete non monitorano gli attacchi di protocollo di livello superiore a livello di SSL e di applicazione.

Problemi del cloud scrubbing always-on

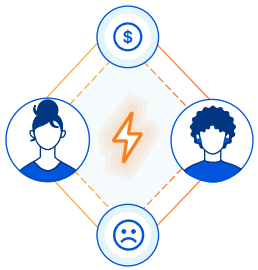
Problemi di latenza che portano a esperienze utente negative:

- Molti provider di mitigazione DDoS nel cloud dispongono di una serie di data center distanti dedicati allo scrubbing del traffico di rete lontano da dove ha origine il traffico di attacco. Un numero inferiore di scrubbing center generalmente equivale a una maggiore latenza. Questo backhaul del traffico può anche introdurre latenza e creare notevoli ritardi.
- I datacenter dedicati allo scrubbing DDoS spesso ispezionano anche solo il livello di rete. Per le funzioni che risiedono su altri livelli, come il firewall dell'applicazione Web o la memorizzazione nella cache dei contenuti, questo traffico viene in genere elaborato in un datacenter alternativo, aggiungendo ancora più latenza.

Costo totale di proprietà più elevato:

- Le soluzioni di cloud scrubbing always-on con una capacità di rete limitata possono trasferire i propri limiti di larghezza di banda ai clienti, sotto forma di prezzi più elevati. Possono essere aggiunte anche le tariffe per i servizi professionali.

Quando il tempo è denaro: in che modo i tempi di inattività e la latenza possono influire sulle aziende

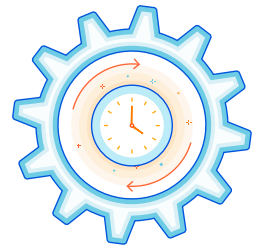


Il Il 91% delle organizzazioni afferma **che i tempi di inattività orari costano fino a 300.000 dollari** a causa di interruzioni di attività, interruzioni della produttività e sforzi correttivi [5]

Per le note società di e-commerce, i tempi di inattività possono costare fino a **220.000 dollari** al minuto[6]

Il 90% degli acquirenti abbandonerà un sito se non si carica "in un tempo ragionevole" e il **57% se ne andrà e acquisterà da un rivenditore simile**[7]

Il **44% dei giocatori** che sperimentano la latenza rispondono **abbandonando il gioco a cui stanno giocando** per riprovare più tardi, mentre il **24% inizierà a giocare a qualcos'altro**[8]



Il **64% dei decisori IT** indica che la necessità di offrire un'esperienza cliente più rapida e semplice è un **"onere significativo o importante per la loro infrastruttura tecnologica"**[9]

Garantisci la difesa da attacchi DDoS basata su cloud e proteggiti dalla perdita di entrate causata dalle interruzioni

Ecco come la nostra piattaforma cloud unificata, alimentata da una rete globale intelligente, protegge dalle minacce DDoS:

Il cloud scrubbing on demand si basa sull'intervento umano, aggiungendo tempo alla risposta di mitigazione. Al contrario, la protezione DDoS cloud always-on è più completa, tuttavia, molti fornitori DDoS cloud sempre attivi si affidano a scrubbing center distanti che aggiungono latenza all'esperienza dell'utente.

Cloudflare affronta queste limitazioni con una piattaforma di sicurezza unificata, che include tre livelli di protezione da attacchi DDoS (livelli 3, 4 e 7) e accelerazione del traffico per reti on-premise, ospitate nel cloud e ibride. Il traffico degli attacchi viene mitigato vicino alla fonte, in modo che i tuoi utenti finali vivano un'esperienza fluida e performante.

Sicurezza basata sulla rete

Cloudflare ha **datacenter in più di 285 città** e una **capacità di rete pari a 197 Tb/s** (per contro, un noto servizio di mitigazione DDoS sempre attivo ha meno di 40 scrubbing center e 20 Tb/s di capacità di rete).

Gli attacchi vengono assorbiti automaticamente dalla nostra rete prima che raggiungano la tua e la maggior parte del traffico dannoso viene bloccato in **meno di 3 secondi**, senza che sia necessario alcun backhauling.

Usabilità, visibilità e self-service

La protezione da attacchi DDoS di Cloudflare viene fornita as-a-Service, il che significa che non è richiesto alcun investimento CapEx o gestione del ciclo di vita dell'hardware.

In più, è **self-service** con funzionalità di configurazione personalizzata in **un singolo pannello di controllo**.

Intelligence delle minacce su larga scala

Vedi di più, proteggi di più: quasi il 20% del Web viene eseguito su Cloudflare. I nostri clienti beneficiano delle dimensioni e dell'intelligenza della nostra rete globale, che **blocca oltre 112 miliardi di minacce informatiche al giorno**.

I modelli avanzati di machine learning migliorano continuamente le nostre difese, così possiamo stare al passo con le minacce emergenti per tuo conto.

Difesa da attacchi DDoS riconosciuta nel settore

Cloudflare è stato riconosciuto come **Leader nel report GigaOm Radar per la protezione da attacchi DDoS del 2022**. Il report ha valutato nove diversi fornitori e Cloudflare si è classificato al primo posto in assoluto. Cloudflare è stato nominato **'Leader' anche nel The Forrester Wave™: DDoS Mitigation Solutions, Q1, 2021**.

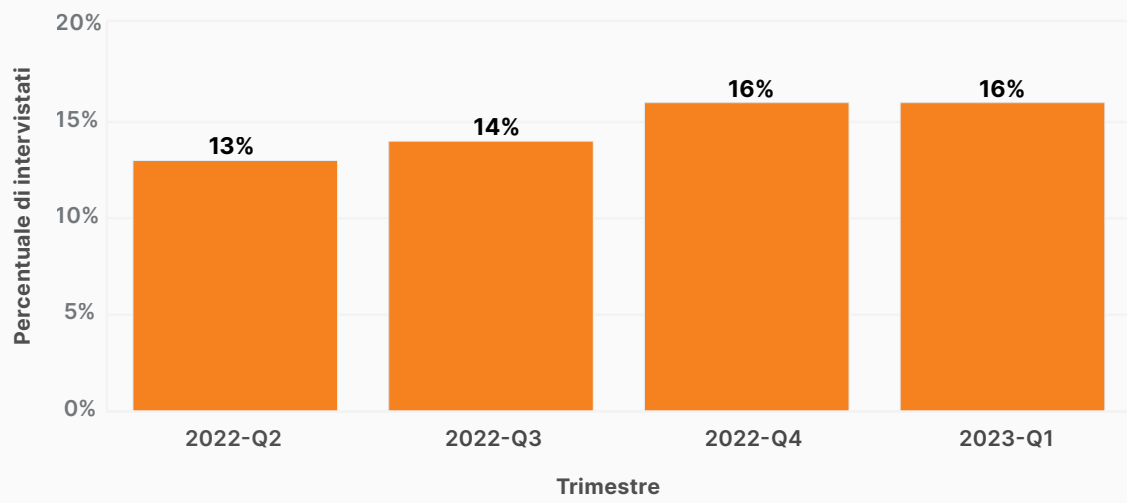
Cloudflare ha ricevuto i punteggi più alti possibili in 15 criteri, inclusi i centri operativi di sicurezza, l'automazione della risposta, le prestazioni e altro ancora.

Case study: Società Fortune Global 500 presa di mira da un attacco DDoS con richiesta di riscatto

Un attacco DDoS con richiesta di riscatto (RDDoS), noto anche come estorsione con riscatto, è quando le parti malintenzionate tentano di estorcere denaro minacciando un individuo o un'organizzazione con un attacco DDoS. Il numero di tentativi di riscatto DDoS è aumentato costantemente nel corso del 2022 e oltre il 16% dei clienti Cloudflare ha ricevuto una minaccia o una richiesta di riscatto come parte di un attacco DDoS nel primo trimestre del 2023.

Anche se spesso confusi con gli attacchi ransomware, gli attacchi DDoS con richiesta di riscatto funzionano in modo diverso e sono più facili da eseguire: non richiedono di indurre la vittima ad aprire un'e-mail o a fare clic su un collegamento, né richiedono un'intrusione nella rete o un punto d'appoggio nelle risorse aziendali. La crescente disponibilità di ransomware-as-a-service ha anche reso il riscatto DDoS un'opzione a basso sforzo e a basso rischio per gli autori di attacchi.

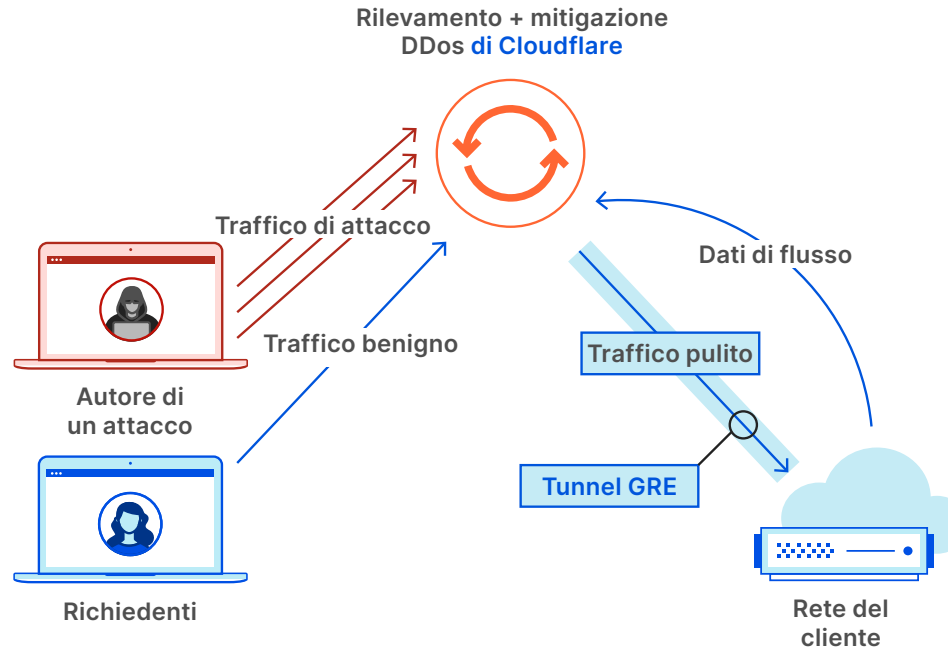
Attacchi DDoS con richiesta di riscatto e minacce per trimestre
Percentuale di intervistati che hanno riferito di essere stati presi di mira o minacciati da un attacco DDoS con richiesta di riscatto



Alla fine del 2020, prima di utilizzare Cloudflare per la mitigazione degli attacchi DDoS, un'importante azienda Fortune Global 500 è stata presa di mira da un tentativo di RDDoS da parte di parti che affermano di essere il Gruppo Lazarus (un gruppo criminale informatico presumibilmente gestito dal governo della Corea del Nord). Gli aggressori inizialmente hanno inviato un'e-mail chiedendo bitcoin e hanno concesso loro una settimana per "pagare", altrimenti sarebbe arrivato un secondo attacco più grande e il riscatto sarebbe aumentato.

Dopo aver ricevuto la richiesta di riscatto e aver notato un aumento significativo del traffico verso uno dei propri datacenter globali, l'azienda ha contattato il proprio servizio di scrubbing center su richiesta. Ci sono voluti più di 30 minuti per attivare il servizio del fornitore e reindirizzare il traffico allo scrubbing center. Anche l'attivazione del servizio on-demand ha causato errori di rete e più incidenti.

Dopo l'attacco iniziale e le sfide con il proprio fornitore on-demand, l'azienda ha deciso di integrare Cloudflare Magic Transit, la protezione sempre attiva di Cloudflare contro gli attacchi DDoS a livello di rete. Sebbene gli autori dell'attacco avessero promesso un secondo, enorme attacco, non è mai avvenuto.



Cloudflare Magic Transit per la protezione da attacchi DDoS a livello di rete

"Una delle principali differenze è l'analisi degli attacchi e del traffico che vediamo che il nostro fornitore storico non è in grado di fornirci. Stiamo assistendo ad attacchi di cui non sapevamo che sarebbero stati mitigati automaticamente".

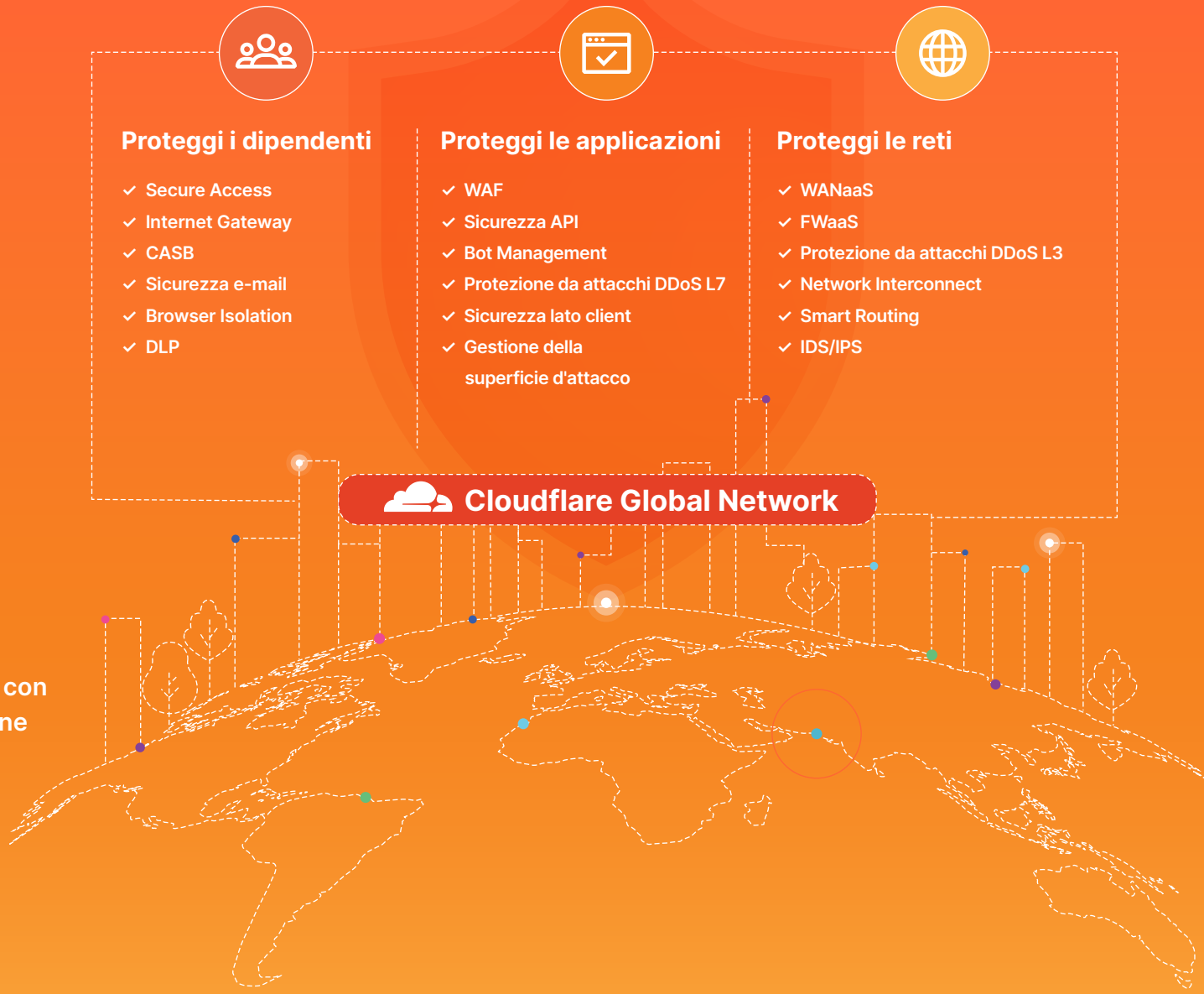
Team di risposta agli incidenti e forense
Società Fortune Global 500

Conclusioni

Con l'aumentare della frequenza e della complessità degli attacchi DDoS nell'era post-pandemia, è importante mantenere attivo il traffico legittimo per proteggere i profitti. Con la capacità di proteggere rapidamente e senza sforzo dagli attacchi, senza i problemi di latenza o i costi elevati comunemente associati ad altri fornitori, Cloudflare rende facile optare per una strategia cloud sempre attiva.

Per saperne di più sulla protezione dagli attacchi DDoS di rete con Cloudflare, richiedi una demo.

Per saperne di più su un'unica rete globale con funzionalità Zero Trust integrate, mitigazione DDoS, firewall di rete e accelerazione del traffico, fai clic qui.



del traffico

1 Langrock, Sam. “The Cloud has Complicated Attack Surface Management.” Recorded Future, 3 aprile 2023, https://www.recordedfuture.com/the-cloud-has-complicated-attack-surface-management

2 “Uptime Institute’s 2022 Outage Analysis Finds Downtime Costs and Consequences Worsening as Industry Efforts to Curb Outage Frequency Fall Short.” Uptime Institute, 8 giugno 2022, https://uptimeinstitute.com/about-ui/press-releases/2022-outage-analysis-finds-downtime-costs-and-consequences-worsening

3 Cimpanu, Catalin. “Bandwidth.com expects to lose up to $12M following DDoS extortion attempt.” The Record, 1 novembre 2021, https://therecord.media/bandwidth-com-expects-to-lose-up-to-12m-following-ddos-extortion-attempt

4 Holmes, David and Blankenship, Joseph, et al. “The Forrester Wave™: DDoS Mitigation Solutions, Q1 2021,” Forrester, 3 marzo 2021

5 Didio, Laura. “The Cost of Enterprise Downtime,” TechChannel, September 30, 2021. https://techchannel.com/IT-Stratgy/09/2021/cost-enterprise-downtime

6 “The Cost of Downtime for the Top US Ecommerce Sites,” Gremlin, accesso 8 maggio 2023, https://www.gremlin.com/ecommerce-cost-of-downtime

7 Crets, Stephanie. “Most consumers abandon a slow-loading ecommerce site.” DigitalCommerce360, 21 agosto 2020. https://www.digitalcommerce360.com/2020/08/21/most-consumers-abandon-a-slow-loading-ecommerce-site

8 Duperre, Mathieu. “44 percent of gamers respond to latency by quitting their games — what can we do to stop this?” PocketGamer.biz, 24 ottobre 2022, https://www.pocketgamer.biz/asia/comment-and-opinion/79974/44-per-cent-of-gamers-respond-to-latency-by-quitting-their-games-what-can-we-do-to-stop-this

9 “Infinity Data and the battle to conquer latency.” Hazelcast and Intel, November 2019. https://hazelcast.com/resources/infinity-data-report

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

CLOUDFLARE