CLOUDFLARE

Publicación digital

Impedir el tiempo de inactividad: Una guía para los modelos de defensa DDoS

Contenido

Haz clic para saltar a la sección

Introducción: defensa DDoS en un mundo de trabajo híbrido

La empresa promedio usa ahora más de 1400 servicios diferentes en la nube[1] debido a la creciente demanda de aplicaciones y de experiencias del cliente mejores y más rápidas. Sin embargo, una consecuencia de la transformación de la nube es una mayor superficie de ataque: más servicios digitales implican más "puntos de entrada" que pueden vulnerar los atacantes. La superficie de ataque también se ha ampliado con el trabajo híbrido (la combinación de trabajo en la oficina y remoto), necesidad que surge con la pandemia global.

Todos estos factores están aumentando la presión sobre las empresas con pocos recursos. Los equipos de TI y seguridad no solo necesitan ofrecer aplicaciones y redes más resistentes, sino que también necesitan proteger a los usuarios y dispositivos, independientemente de su ubicación, contra amenazas en constante evolución.

Algunas de estas amenazas incluyen ataques distribuidos de denegación de servicio (DDoS) más frecuentes, prolongados y de mayor magnitud. En febrero de 2023, Cloudflare detectó y mitigó el mayor ataque HTTPS DDoS (71 MB/s) registrado. Nuestros datos también muestran aumentos trimestrales en los ataques DDoS hipervolumétricos (ataques superiores a 100 GB/s) en 2022.

Las realidades laborales híbridas y económicas de hoy requieren que las empresas revalúen sus defensas DDoS: el riesgo de inactividad, de robo de datos, de infiltración de la red, y de pérdidas financieras es demasiado grande.

La investigación muestra que más del 60 % de las interrupciones cuestan más de $100 000 dólares y el 15 % de las interrupciones cuestan más de $1 millón de dólares[2]. En un ejemplo, la inactividad debido a una serie de ataques DDoS le costó a una empresa casi $12 millones de dólares[3].

Estas realidades hacen que la defensa contra ataques DDoS sea fundamental para organizaciones de todos los tamaños. Además, los enfoques manuales del pasado ya no son suficientes. Si bien los humanos pueden iniciar los ataques, los bots los ejecutan, y para ganar, debes luchar contra los bots con bots. La detección y la mitigación se deben automatizar tanto como sea posible.

Esta publicación digital explora:

- Diferentes modelos de protección contra ataques DDoS en la nube
- Cómo abordar las limitaciones del fitrado en la nube siempre activo
- Cómo una empresa Fortune Global 500 frustró un ataque de rescate DDoS con Cloudflare

Comprensión de los enfoques de mitigación de DDoS en la nube

Un ataque DDoS es un intento malicioso de interrumpir el tráfico normal de un servidor, servicio o red al sobrecargar el objetivo o la infraestructura que lo rodea con una avalancha de tráfico de Internet. Una solución DDoS eficaz te dirá exactamente cuándo, dónde y cómo se produce este "atasco de tráfico", mientras absorbe y redirige el tráfico malicioso para que no interfiera con el tráfico legítimo. Los destinos con mucho tráfico, junto con las propiedades y redes de Internet desprotegidas, son objetivos comunes.

Si bien los ataques DDoS no son nada nuevo, se necesitan nuevos métodos para detenerlos. Con la migración de las aplicaciones a la nube, el mercado de soluciones DDoS locales también se ha reducido[4]. En su lugar, más organizaciones recurren a la nube para protegerse contra los ataques DDoS.

Un proveedor de servicios en la nube, que cuenta con diversas variedades de protección en la nube, se sitúa frente a las aplicaciones y la infraestructura de una organización y desvía todo el tráfico a un centro de filtrado para que lo "limpie". Solo se devuelve al cliente el tráfico legítimo. Este "filtrado en la nube" se puede activar de dos formas: ***bajo demanda*** o ***siempre activo***.

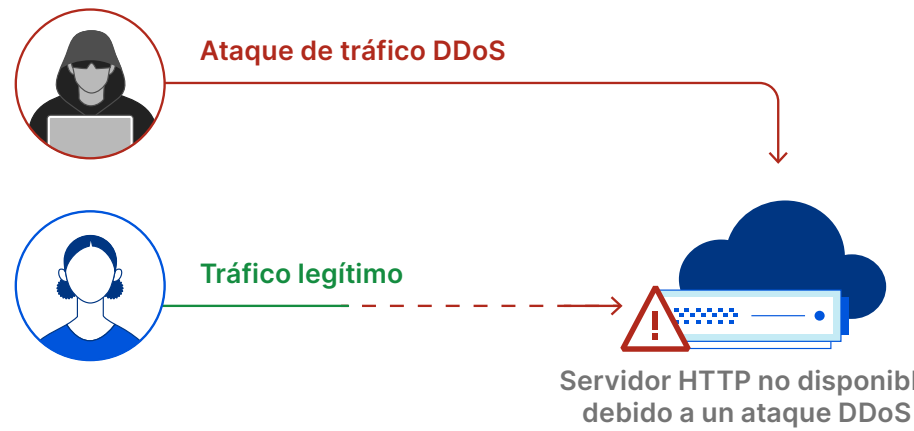
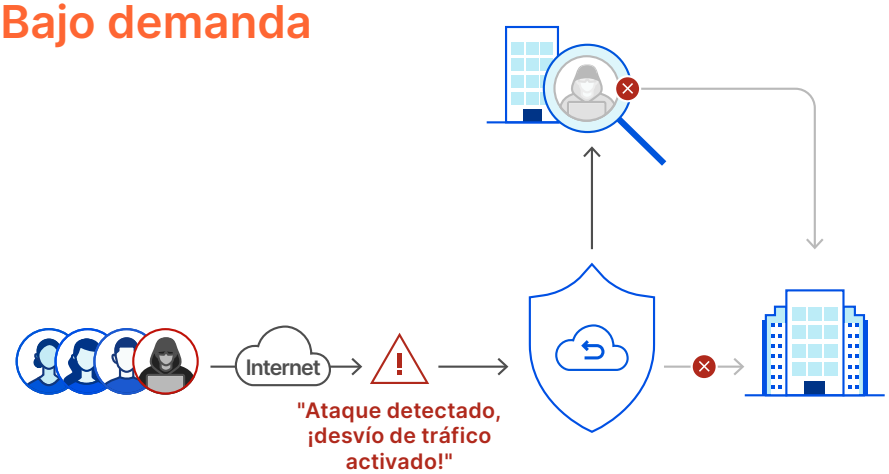


Diagrama de un ataque DDoS a la capa de aplicación que deniega el servicio a los usuarios legítimos

Bajo demanda

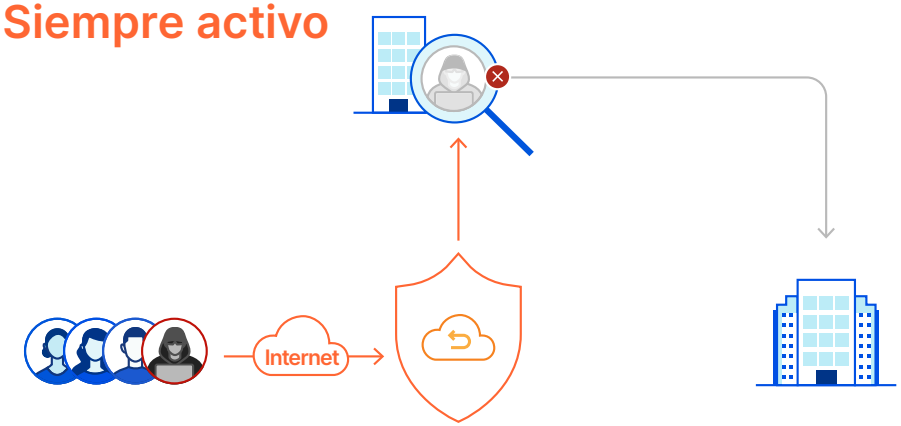


En "tiempos de paz", el filtrado en la nube bajo demanda garantiza que todo el tráfico llegue a las aplicaciones y a la infraestructura sin redireccionamiento. El tráfico solo se desvía al proveedor de filtrado en la nube ante un ataque DDoS activo.

Si el tráfico entrante supera un límite preconfigurado (por ejemplo, el 70 % de la capacidad de conexión) o si se detecta un ataque de gran magnitud, se activa el modo de mitigación en la nube bajo demanda, y el tráfico se desvía al centro de filtrado más cercano para su procesamiento.

frente a

Siempre activo



Este enfoque esencialmente de "no intervención" en el filtrado en la nube siempre dirige el tráfico a través del centro de datos de tu proveedor de servicios en la nube para la inspección de amenazas, incluso en tiempos de paz.

Un modelo siempre activo ayuda a minimizar el tiempo desde la detección hasta la mitigación, sin interrumpir el servicio.

Sin bien las técnicas bajo demanda y siempre activas ofrecen distintas ventajas, cada una de ellas puede presentar limitaciones en distintas circunstancias, como se describe en la siguiente sección.

Limitaciones comunes de los métodos de filtrado en la nube

Desafíos del filtrado en la nube bajo demanda

Retraso en la respuesta a los ataques:

- Un enfoque bajo demanda requiere que el tráfico se redirija al proveedor de servicio en la nube en un ataque DDoS. Este cambio puede tardar varios minutos, además del tiempo que se tarda en responder manualmente al ataque (p. ej., avisar al proveedor para que active el servicio). Si la protección bajo demanda no se activa a tiempo, el impacto puede ser importante.

Mayor costo a largo plazo:

- Los proveedores de servicio en la nube bajo demanda suelen cobrar por byte de tráfico de ataque. Aunque solo pagas por uso, este modelo podría acabar costando más si tu organización sufre ataques DDoS más frecuentes.

Ataques que podrían pasar desapercibidos:

- Los ataques DDoS que no superan el límite de utilización pueden pasar desapercibidos, congestionando las conexiones de red que afectan al tráfico legítimo.
- Las conexiones de red tampoco supervisan los ataques de protocolos de capa superior a nivel SSL y de aplicación.

Desafíos del filtrado en la nube siempre activo

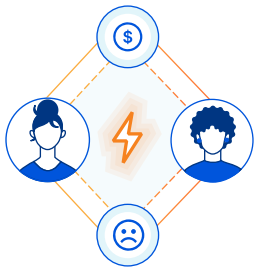
Problemas de latencia que impactan en las experiencias del usuario:

- Muchos proveedores de mitigación DDoS en la nube tienen una serie de centros de datos distantes para filtrar el tráfico de red que están lejos de donde se origina el ataque de tráfico. Una menor cantidad de centros de filtrado equivale generalmente a una mayor latencia. Este redireccionamiento del tráfico también puede añadir latencia y crear retrasos perceptibles.
- Los centros de datos para filtrado DDoS suelen inspeccionar solo la capa de red. En cuanto a las funciones que se alojan en otras capas, como el firewall de aplicaciones web o el almacenamiento en caché de contenidos, este tráfico se suele procesar en un centro de datos alternativo, lo que añade aún más latencia.

Mayor costo total de propiedad:

- Las soluciones de filtrado en la nube siempre activas con capacidad de red limitada pueden trasladar sus limitaciones de ancho de banda a los clientes, en forma de precios más altos. También pueden añadirse tarifas de servicios profesionales.

Cuando el tiempo es oro: cómo la inactividad y la latencia pueden afectar a las empresas

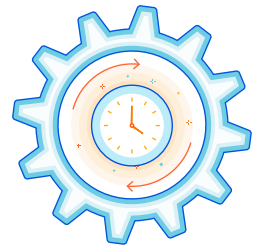


El 91 % de las organizaciones afirman que la **inactividad por hora cuesta hasta 300 000 dólares** debido a la pérdida de oportunidades de negocio, las interrupciones de la productividad y el trabajo de corrección[5]

Para empresas de comercio electrónico conocidas, la inactividad puede suponer una pérdida de hasta **220 000 dólares** por minuto[6]

El 90 % de los compradores abandonará un sitio si la página no se carga "en un tiempo razonable", y el **57 % lo abandonará y comprará en un comercio similar**[7]

El 44 % de los jugadores que experimentan latencia **abandonan el juego que están jugando** para volver a intentarlo más tarde, mientras que el **24 % lo abandonará para jugar otra cosa**[8]



El 64 % de los responsables de TI a cargo de la toma de decisiones sostienen que la necesidad de ofrecer una experiencia más rápida y sencilla al cliente es un **"problema significativo o importante para su infraestructura tecnológica"**[9]

Haz realidad la promesa de la defensa DDoS en la nube, y protégete de la pérdida de ingresos causada por las interrupciones

A continuación, te mostramos cómo nuestra plataforma unificada en la nube, basada en una red global inteligente, protege contra las amenazas DDoS:

El filtrado en la nube bajo demanda depende de la intervención humana, lo que añade tiempo a la respuesta de mitigación. En cambio, la protección DDoS en la nube siempre activa es más completa, aunque muchos de los proveedores que ofrecen este enfoque dependen de centros de filtrado distantes que añaden latencia a la experiencia del usuario.

Cloudflare aborda estas limitaciones con una plataforma de seguridad unificada, que incluye tres capas de protección DDoS (capas 3, 4 y 7) y aceleración del tráfico para redes locales, alojadas en la nube y entornos híbridos. El tráfico de ataque se mitiga cerca del origen, para que la experiencia de tus usuarios finales sea perfecta y eficaz.

Seguridad impulsada por la red

Cloudflare tiene **centros de datos en más de 285 ciudades** y una **capacidad de red de 197 TB/s** (en cambio, un conocido servicio de mitigación de DDoS siempre activo tiene menos de 40 centros de filtrado y una capacidad de red de 20 TB/s).

Nuestra red absorbe automáticamente los ataques antes de que lleguen a la tuya, y la mayor parte del tráfico malicioso se bloquea **en menos de 3 segundos**. Sin redireccionamientos.

Facilidad de uso, visibilidad y autoservicio

La protección DDoS de Cloudflare se ofrece como servicio, lo que significa que no se necesita invertir ni gestionar el ciclo de vida útil del hardware.

Además, es **autoservicio** con funciones de configuración personalizadas **en un único panel de control**.

Información sobre amenazas a escala

Mayor visibilidad, mayor protección: casi el 20 % de la web utiliza Cloudflare. Nuestros clientes se benefician de la escala y la información de nuestra red global, que **bloquea más de 112 000 millones de ciberamenazas al día**.

Los modelos avanzados de aprendizaje automático mejoran continuamente nuestras defensas, para que podamos adelantarnos a las amenazas emergentes en tu nombre.

Protección DDoS reconocida en el sector

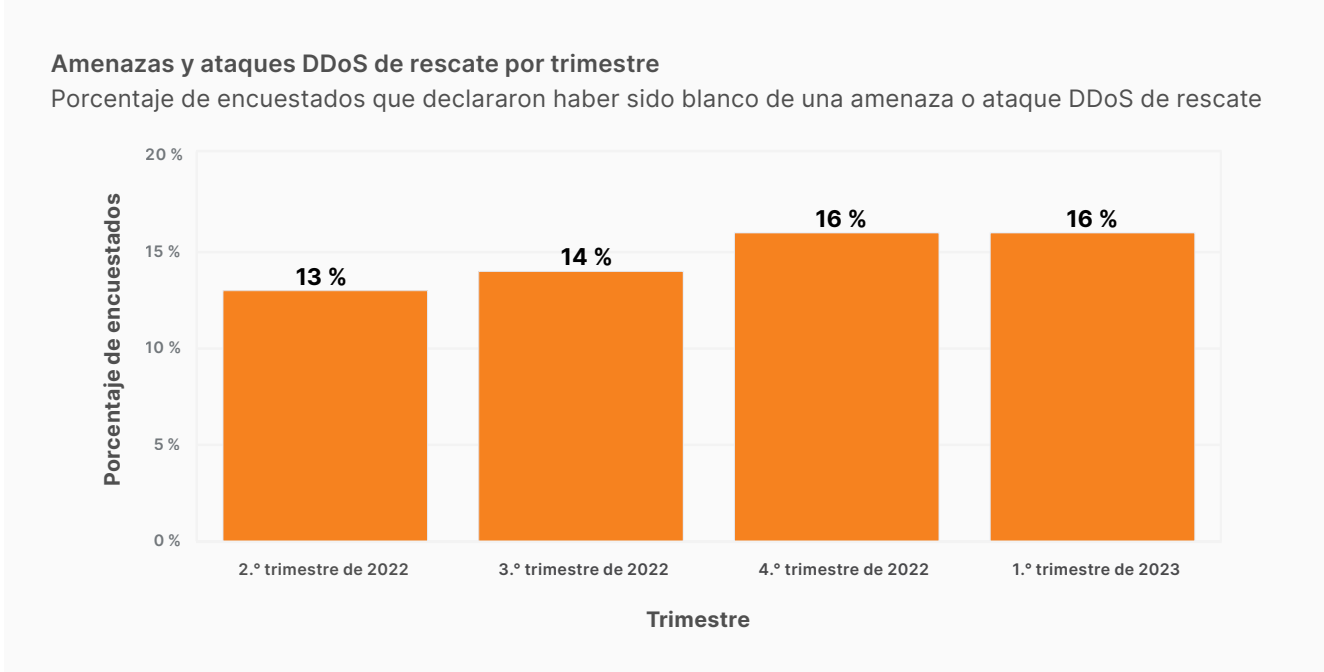
Cloudflare ha sido reconocida como empresa **líder en el informe "GigaOm Radar 2022 for DDoS Protection**. Dicho informe evaluó a nueve proveedores diferentes, y Cloudflare obtuvo la mejor clasificación general. Cloudflare también ha sido reconocida como empresa **"líder" en el informe "The Forrester Wave™: DDoS Mitigation Solutions, 1.º trimestre de 2021"**.

Cloudflare recibió las puntuaciones más altas posibles en función de 15 criterios, incluidos los centros de operaciones de seguridad, la automatización de la respuesta, el rendimiento, etc.

Caso práctico: una empresa Fortune Global 500 objetivo de un ataque DDoS de rescate

Un ataque DDoS de rescate (RDDoS), también conocido como ataques de extorsión y rescate, se produce cuando los ciberdelincuentes intentan extorsionar a través de una amenaza a una persona u organización con un ataque DDoS. El número de intentos de DDoS de rescate aumentó de forma constante durante 2022, y más del 16 % de los clientes de Cloudflare recibieron una amenaza o exigencia de rescate como parte de un ataque DDoS en el 1.º trimestre de 2023.

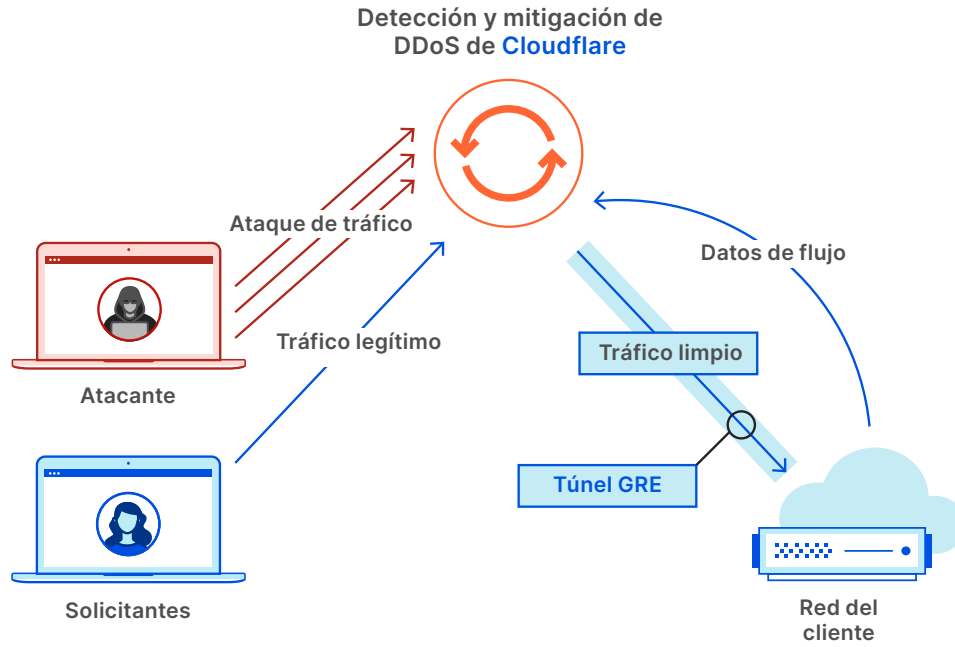
Aunque a menudo se confunden con los ataques de ransomware, los ataques DDoS de rescate funcionan de forma diferente y son más fáciles de ejecutar. No requieren engañar a la víctima para que abra un correo electrónico o haga clic en un enlace, ni necesitan irrumpir en la red o un punto de apoyo en los activos corporativos. La creciente disponibilidad de ransomware como servicio también ha convertido este tipo de ataques en una opción cuyo esfuerzo y riesgo para los atacantes son mínimos.



A finales de 2020, antes de utilizar Cloudflare para la mitigación de DDoS, una importante empresa de la lista Fortune Global 500 fue objeto de un intento de DDoS de rescate por parte de individuos que afirmaban ser el grupo Lazarus (un grupo de ciberdelincuentes supuestamente dirigido por el gobierno de Corea del Norte). Los atacantes enviaron inicialmente un correo electrónico exigiendo bitcoin y les dieron una semana para "pagar", o de lo contrario se produciría un segundo ataque de mayor envergadura, y el rescate aumentaría.

Tras recibir la nota de rescate y observar un aumento significativo del tráfico hacia uno de sus centros de datos globales, la empresa se puso en contacto con su servicio del centro de filtrado bajo demanda. Tardaron más de 30 minutos en activar el servicio del proveedor y redirigir el tráfico al centro de filtrado. La activación del servicio bajo demanda también provocó fallos en la red y dio lugar a numerosos incidentes.

Tras el ataque inicial y los problemas con su proveedor bajo demanda, la empresa decidió incorporar Cloudflare Magic Transit, la protección permanente de Cloudflare contra ataques DDoS en la capa de red. Aunque los atacantes prometieron un segundo ataque a gran escala, nunca llegó a producirse.



Cloudflare Magic Transit para proteger la capa de red contra ataques DDoS

"Una diferencia básica es el análisis de ataques y tráfico que observamos y que nuestro proveedor tradicional no podía proporcionarnos. Tenemos visibilidad sobre cómo se mitigan automáticamente ataques de los que no teníamos ni idea".

Equipo de respuesta a incidentes y análisis forense
Empresa de la lista Fortune Global 500

Conclusión

A medida que los ataques DDoS aumentan en frecuencia y complejidad después de la pandemia, es importante mantener el flujo de tráfico legítimo para proteger resultados. Con la capacidad de proteger contra ataques de forma rápida y fácil, sin los problemas de latencia ni los elevados costos que suelen asociarse a otros proveedores, Cloudflare facilita la opción de una estrategia en la nube siempre activa.

Para obtener más información sobre la protección contra ataques DDoS a la red con Cloudflare, solicita una demostración.

Para obtener más información sobre una única red global con función Zero Trust integrada, mitigación de DDoS, firewall de red y aceleración del tráfico, haz clic aquí.

Fuentes

1 Langrock, Sam. “The Cloud has Complicated Attack Surface Management.” Recorded Future, 3 de abril de 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 de junio de 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 de noviembre de 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 de marzo de 2021

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

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

7 Crets, Stephanie. “Most consumers abandon a slow-loading ecommerce site.” DigitalCommerce360, 21 de agosto de 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 de octubre de, 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, noviembre de 2019. https://hazelcast.com/resources/infinity-data-report

+55 (11) 3230 4523 | enterprise@cloudflare.com | www.cloudflare.com

CLOUDFLARE