CLOUDFLARE

Libro electrónico

Cómo evitar el tiempo de inactividad: guía de los modelos de protección contra ataques DDoS

Contenido

Haz clic para pasar a cada sección

Introducción: Protección contra DDoS en el mundo del trabajo híbrido

Hoy día, la empresa media usa más de 1400 servicios en la nube diferentes,[1] debido a la exigencia cada vez mayor de mejorar y acelerar las aplicaciones, y las experiencias de los clientes. Sin embargo, una de las consecuencias de la transformación de la nube es el incremento de la superficie de ataque. Más servicios digitales equivalen a más "puntos de entrada" para potenciales ataques. La superficie de ataque también se ha expandido con el trabajo híbrido (la combinación de trabajo presencial y remoto) a raíz de años de pandemia global.

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

Algunas de estas amenazas incluyen ataques de denegación de servicio distribuido (DDoS) más frecuentes, de mayor duración y tamaño. En febrero de 2023, Cloudflare detectó y mitigó el mayor ataque DDoS HTTPS (71 millones de solicitudes por segundo) registrado. Nuestros datos también muestran aumentos intertrimestrales en los ataques DDoS hipervolumétricos (ataques superiores a 100 GB/s) en 2022.

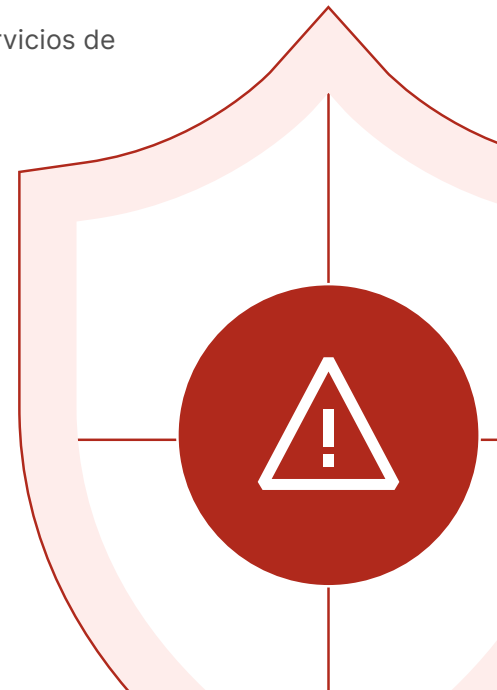
La realidad económica y el entorno de trabajo híbrido de hoy día requieren que las empresas revalúen sus sistemas de protección DDoS. Los riesgos del tiempo de inactividad, el robo de datos, la filtración de red y las pérdidas financieras son demasiado grandes.

Algunos estudios muestran que más del 60 % de las interrupciones cuestan más de 100 000 dólares y el 15 % de las interrupciones originan pérdidas superiores a más de 1 millón de dólares[2]. A modo de ejemplo, el coste del tiempo de inactividad de una empresa debido a una serie de ataques DDoS fue casi de 12 millones de dólares[3].

Estas realidades hacen que la protección contra los ataques DDoS sea fundamental para organizaciones de todos los tamaños. Además, los enfoques manuales del pasado ya no son suficientes. Los ataques los pueden iniciar personas, pero también los pueden ejecutar bots y, para ganar, debes combatir los bots con bots. La detección y la mitigación se deben automatizar tanto como sea posible.

Este libro electrónico analiza:

- Diferentes modelos de protección contra ataques DDoS basados en la nube.
- Cómo superar las limitaciones de los servicios de filtrado en la nube "siempre activos".
- Cómo una empresa de la lista Fortune Global 500 evitó un ataque DDoS de rescate con Cloudflare.



Enfoques de la mitigación de DDoS basados en la nube

Un ataque DDoS es un intento malicioso de interrumpir el tráfico normal de un servidor, servicio o red específico, abrumando al objetivo o su infraestructura circundante con una avalancha de tráfico de Internet. Una solución DDoS eficaz te informará exactamente de cuándo, dónde y cómo se está produciendo esta "congestión de tráfico", al tiempo que absorberá y redirigirá el tráfico malicioso para que no interfiera con el tráfico legítimo. Los destinos con mucho tráfico, al igual que las propiedades y las redes de Internet sin protección, son objetivos comunes.

Si bien los ataques DDoS no son nada nuevo, se necesitan nuevos enfoques para detenerlos. Conforme las aplicaciones han migrado a la nube, el mercado de soluciones DDoS locales también se ha reducido[4]. En su lugar, más organizaciones están recurriendo a la nube para protegerse contra los ataques DDoS.

Un proveedor de nube, que cuenta con numerosas soluciones de protección diferentes basadas 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". El cliente solo recibe el tráfico legítimo. Este movimiento de "filtrado en la nube" se puede activar de dos formas: ***bajo demanda*** o ***siempre activo***.

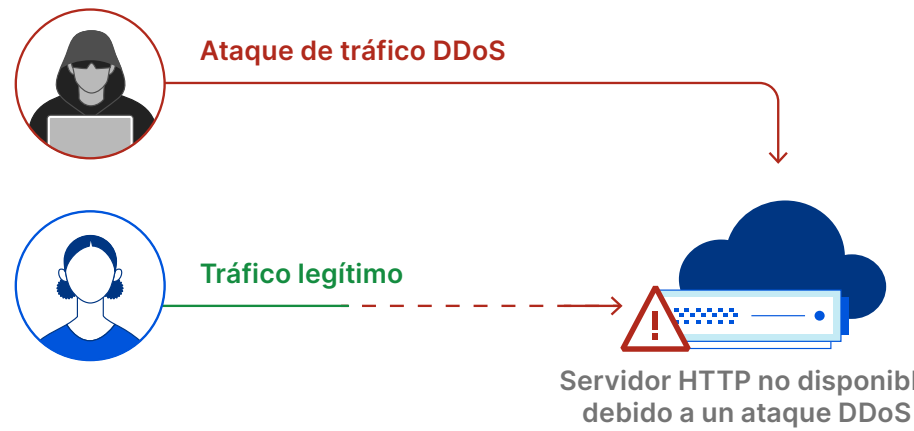
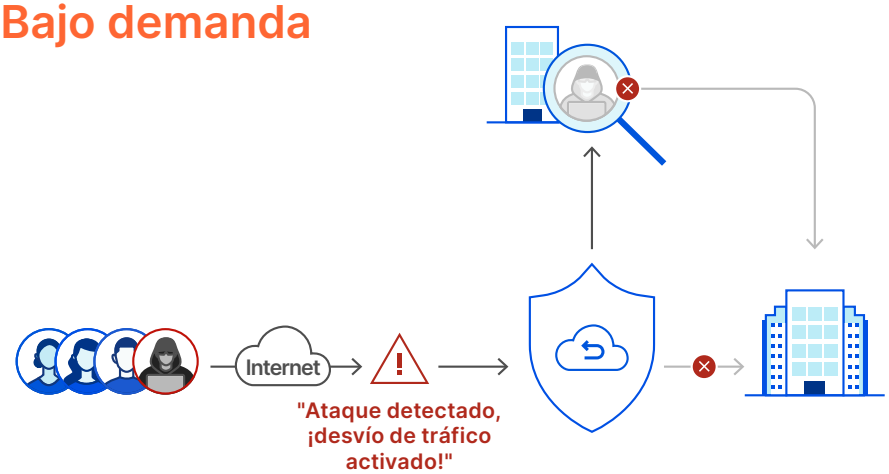


Diagrama de un ataque DDoS a la capa de aplicación que deniega el servicio a los usuarios legítimos

Bajo demanda

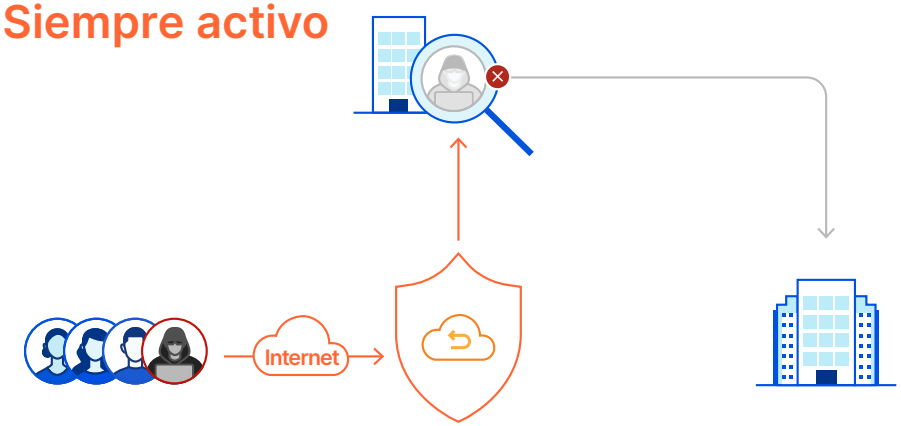


En "tiempos de paz", el filtrado en la nube bajo demanda garantiza que todo el tráfico llegue a las aplicaciones y a la infraestructura sin redireccionamiento. El tráfico solo se desvía al proveedor de filtrado en la nube cuando un ataque DDoS está activo.

Si el tráfico entrante supera un umbral preconfigurado (por ejemplo, el 70 % de la capacidad del vínculo) o si se detecta un ataque a gran escala, 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.

VS.

Siempre activo



Este enfoque básicamente de "no intervención" durante el proceso de filtrado en la nube siempre dirige el tráfico a través del centro de datos de tu proveedor de 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 ninguna interrupción del 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 al ataque:

- Un enfoque "bajo demanda" requiere que el tráfico se redirija al proveedor de nube en un ataque DDoS. Este cambio puede tardar varios minutos en producirse, 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, pueden tener un impacto importante.

Mayor coste a largo plazo:

- Los proveedores de nube bajo demanda suelen cobrar por byte de ataque de tráfico. 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 umbral de utilización pueden pasar desapercibidos, congestionando las conexiones de red que afectan al tráfico legítimo.
- Las conexiones de red tampoco supervisan los ataques a protocolos de capa superior a nivel SSL y de aplicación.

Desafíos del filtrado en la nube "siempre activo"

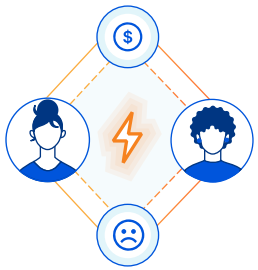
Problemas de latencia que impactan en las experiencias de los usuarios:

- Muchos proveedores de mitigación DDoS en la nube tienen un conjunto de centros de datos distantes, dedicados a filtrar el tráfico de red, que están lejos de donde se origina el ataque de tráfico. Un menor número 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 dedicados al 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 coste 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 se pueden añadir tarifas de servicios profesionales.

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

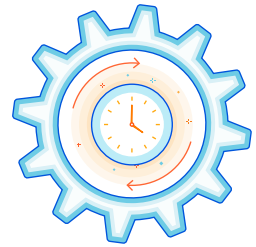


El 91 % de las organizaciones afirman que el **tiempo de inactividad por hora cuesta hasta 300 000 dólares** debido a la pérdida de oportunidades de negocio, las interrupciones de la productividad y el trabajo de corrección.[5]

Para conocidas empresas de comercio electrónico, el tiempo de inactividad puede suponer pérdidas 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 % se irá y comprará en un comercio similar.**[7]

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



El 64 % de los responsables de TI a cargo de la toma de decisiones sostiene que la necesidad de ofrecer experiencias de cliente más rápidas y sencillas es un **"problema significativo o importante para su infraestructura tecnológica".**[9]

Consigue protección DDoS basada en la nube, y evita 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 ataque de tráfico se mitiga cerca del origen, para que la experiencia de tus usuarios finales sea sencilla 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 del hardware.

Además, se proporciona en forma de **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

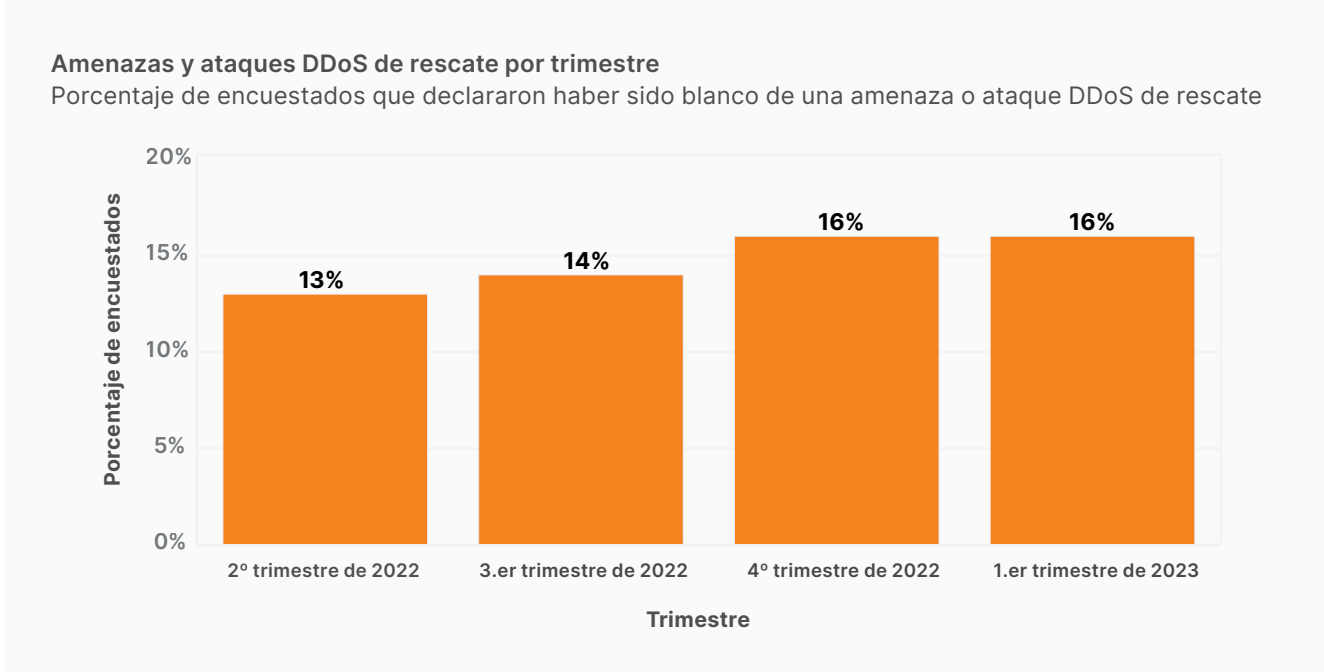
Cloudflare ha sido reconocida como empresa **líder en el informe "GigaOm Radar 2022 for DDoS Protection**, que evaluó a nueve proveedores diferentes, y Cloudflare obtuvo la mejor clasificación general. Cloudflare también ha sido reconocida como empresa **"líder" en el informe "The Forrester Wave™: DDoS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

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

Caso práctico: Empresa de la lista Fortune Global 500, blanco de un ataque DDoS de rescate

Un ataque DDoS de rescate (RDDoS), también conocido como ataque de extorsión DDoS, 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 a lo largo de 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.er trimestre de 2023.

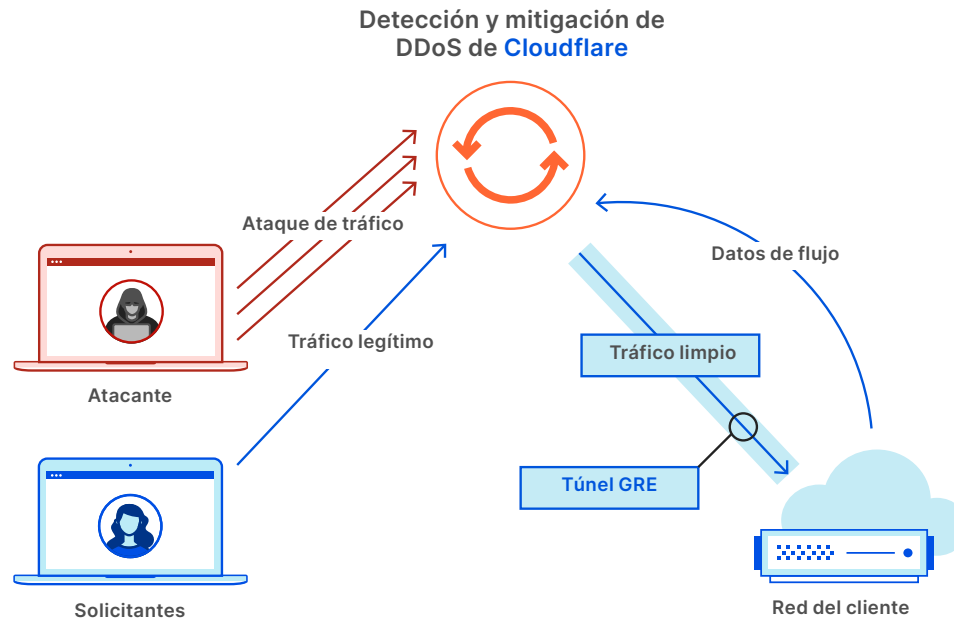
Aunque a menudo se confunden con los ataques de ransomware, los ataques DDoS de rescate funcionan de forma diferente y son más fáciles de ejecutar. No requieren engañar a la víctima para que abra un correo electrónico o haga clic en un enlace, ni necesitan irrumpir en la red o un punto de apoyo en los 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 antes de utilizar los servicios de mitigación de DDoS de 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 bitcóin 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 de 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 a 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

Conforme los ataques DDoS aumentan en frecuencia y complejidad en la era pospandemia, es importante mantener el flujo de tráfico legítimo para ayudar a proteger tus resultados. La capacidad de proteger contra ataques de forma rápida y fácil, sin los problemas de latencia ni los elevados costes que suelen asociarse a otros proveedores, permite a Cloudflare facilitar 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 saber más sobre nuestra red global única con funciones integradas de Zero Trust, mitigación de DDoS, firewall de red y aceleración del tráfico, haz clic aquí.

Referencias

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

+34 518 880 290 | enterprise@cloudflare.com | www.cloudflare.com/es-es/

CLOUDFLARE