CLOUDFLARE

E-book

Deter o tempo de inatividade: Um guia para modelos de defesa contra DDoS

Conteúdo

Clique para ir para a seção

Sumário

Introdução: defesa contra DDoS em um mundo de trabalho híbrido

A empresa média agora usa mais de 1.400 serviços em nuvem diferentes[1], impulsionada pela crescente demanda por aplicativos e experiências do cliente melhores e mais rápidos. No entanto, um subproduto da transformação para a nuvem é uma superfície de ataque em expansão: mais serviços digitais equivalem a mais "pontos de entrada" para os invasores explorarem. A superfície de ataque também se expandiu com o trabalho híbrido (a combinação de trabalho no escritório e remoto), exigido pelos anos de pandemia global.

Todos esses fatores estão aumentando a pressão sobre as empresas com poucos recursos. As equipes de TI e segurança não precisam apenas fornecer aplicativos e redes mais resilientes, mas também proteger usuários e dispositivos, independentemente da localização, contra ameaças em evolução.

Algumas dessas ameaças incluem ataques de negação de serviço distribuída (DDoS) mais frequentes, mais longos e maiores. Em fevereiro de 2023, a Cloudflare detectou e mitigou o maior ataque DDoS por HTTPS (71 Mrps) já registrado. Nossos dados também mostram aumentos trimestrais em ataques DDoS hipervolumétricos (ataques acima de 100 Gbps) em 2022.

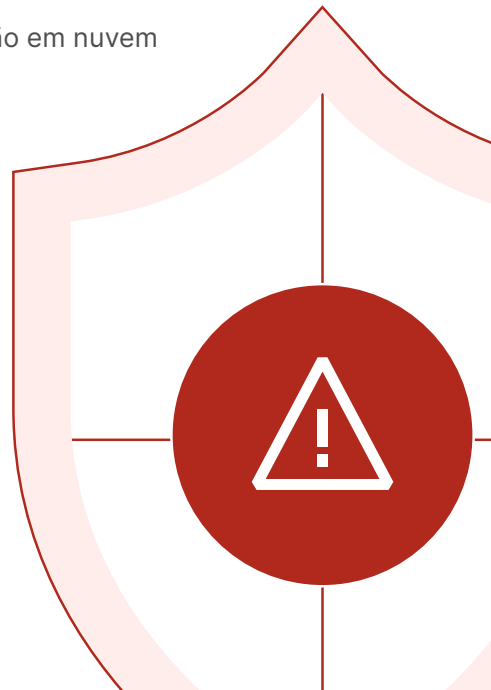
As realidades econômicas e de trabalho híbrido de hoje exigem que as empresas reavaliem suas defesas contra DDoS.
O risco de tempo de inatividade, roubo de dados, infiltração de rede e as perdas financeiras são muito grandes.

A pesquisa mostra que mais de 60% das interrupções custam mais de US$ 100 mil e 15% das interrupções custam mais de US$ 1 milhão[2]. Em um exemplo, o tempo de inatividade devido a uma série de ataques DDoS custou a uma empresa quase US$ 12 milhões[3].

Essas realidades tornam a defesa contra DDoS crítica para organizações de todos os tamanhos. E as abordagens manuais do passado não são mais suficientes. Embora os ataques possam ser iniciados por humanos, eles são executados por bots e para vencer, você deve combater bots com bots. A detecção e a mitigação devem ser automatizadas o máximo possível.

Este e-book explora:

- Diferentes modelos de proteção contra DDoS baseada em nuvem.
- Como superar as limitações da depuração em nuvem sempre ativa.
- Como uma empresa da Fortune Global 500 frustrou um ataque DDoS com pedido de resgate com a Cloudflare.



Entenda as abordagens de mitigação de DDoS baseada em nuvem

Um ataque DDoS é uma tentativa maliciosa de interromper o tráfego normal de um servidor, serviço ou rede de destino, sobrecarregando o alvo ou sua infraestrutura circundante com uma inundação de tráfego da internet. Uma solução eficaz contra DDoS informará exatamente quando, onde e como esse “engarrafamento” está ocorrendo, enquanto absorve e redireciona o tráfego malicioso para que não interfira no tráfego legítimo. Destinos altamente trafegados, juntamente com ativos da internet e redes desprotegidos, são alvos comuns.

Embora os ataques DDoS não sejam novidade, novas abordagens são necessárias para detê-los. À medida que os aplicativos migraram para a nuvem, o mercado de soluções contra DDoS no local também encolheu[4]. Em vez disso, mais organizações estão se voltando para a nuvem para proteção contra DDoS.

Com muitas variedades de proteção baseada em nuvem, um provedor de nuvem fica na frente dos aplicativos e da infraestrutura de uma organização e desvia todo o tráfego para um centro de depuração para ser "limpo". Somente o tráfego legítimo é enviado de volta ao cliente. Esse movimento de "depuração em nuvem" pode ser ativado de duas maneiras: ***sob demanda*** ou ***sempre ativo***.

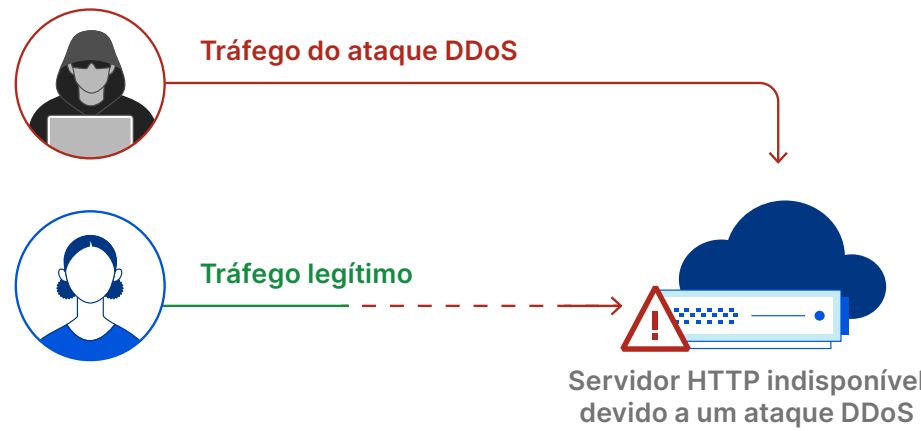
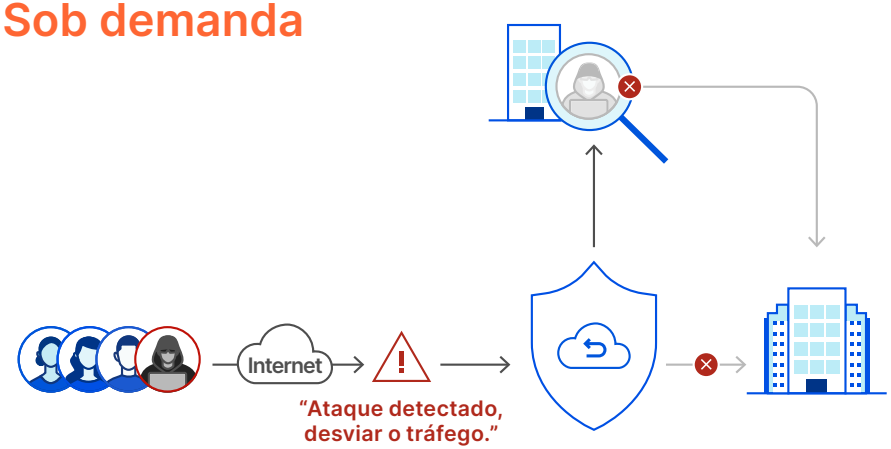


Diagrama de um ataque DDoS na camada de aplicação negando serviços para usuários legítimos

Sob demanda

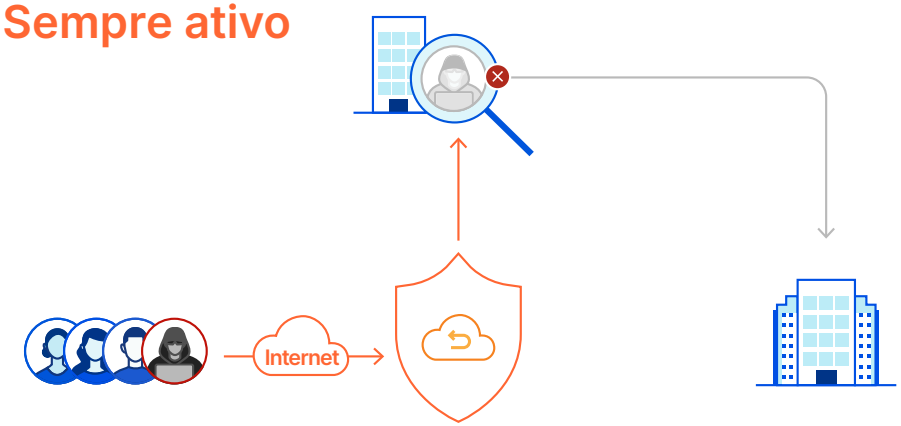


Durante o "tempo de paz", a depuração em nuvem sob demanda garante que todo o tráfego chegue a aplicativos e infraestrutura sem qualquer redirecionamento. O tráfego só é desviado para o provedor de depuração em nuvem em uma situação de ataque DDoS ativo.

Se o tráfego de entrada ultrapassar um limite pré-configurado (por exemplo, 70% da capacidade do link) ou se um grande ataque for detectado, o modo de mitigação em nuvem sob demanda será ativado e o tráfego será desviado para o centro de depuração mais próximo para processamento.

Versus

Sempre ativo



Essa abordagem essencialmente prática para depuração em nuvem sempre direciona o tráfego através do data center do seu provedor de nuvem para inspeção de ameaças mesmo em tempos de paz.

Um modelo sempre ativo ajuda a minimizar o tempo desde a detecção até a mitigação sem nenhuma interrupção do serviço.

Embora as técnicas sob demanda e sempre ativa ofereçam benefícios diferentes, cada uma delas pode apresentar limitações em diferentes circunstâncias, conforme descrito na próxima seção.

Limitações comuns dos métodos de depuração em nuvem

Desafios de depuração em nuvem sob demanda

Resposta ao ataque com atraso:

- Sob demanda exige que o tráfego seja redirecionado para o provedor de nuvem em um ataque DDoS. Pode levar vários minutos para que essa troca ocorra, além do tempo necessário para responder manualmente ao ataque (por exemplo, diga ao provedor para ativar o serviço). Se a proteção sob demanda não for ativada a tempo, o ataque pode causar um grande impacto.

Custo aumentado no longo prazo:

- Os provedores de nuvem sob demanda geralmente cobram por byte de tráfego de ataque. Embora você pague apenas pelo que usa, isso pode acabar custando mais se sua organização sofrer ataques DDoS mais frequentes.

Possíveis ataques não detectados:

- Ataques DDoS que não ultrapassam o limite de utilização podem passar despercebidos, congestionando os links de rede o que afeta o tráfego legítimo.
- Os links de rede também não monitoram ataques de protocolo de camada superior no SSL e no nível do aplicativo.

Desafios de depuração em nuvem sempre ativa

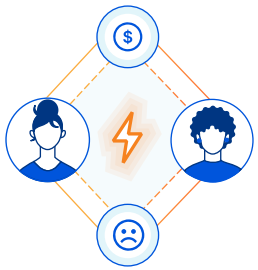
Problemas de latência que levam a experiências do usuário negativas:

- Muitos provedores de mitigação de DDoS em nuvem têm um conjunto de data centers distantes dedicados a depurar o tráfego de rede que estão longe de onde o tráfego de ataque se origina. Menos centros de depuração geralmente equivalem a maior latência. Esse backhaul de tráfego também pode introduzir latência e criar atrasos perceptíveis.
- Os data centers dedicados à depuração de DDoS também inspecionam frequentemente apenas a camada de rede. Para funções que residem em outras camadas, como firewall de aplicativos web ou armazenamento em cache de conteúdo, esse tráfego é normalmente processado em um data center alternativo, adicionando ainda mais latência.

Custo total de propriedade mais alto:

- Soluções de depuração em nuvem sempre ativas com capacidade de rede limitada podem passar suas limitações de largura de banda para os clientes, na forma de preços mais altos. Taxas de serviços profissionais também podem ser adicionadas.

Quando tempo é dinheiro: como o tempo de inatividade e a latência podem afetar as empresas

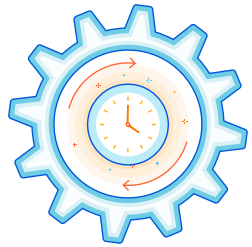


91% das organizações dizem **que o tempo de inatividade por hora custa até US$ 300 mil** devido a negócios perdidos, interrupções de produtividade e esforços de remediação.[5]

Para empresas de comércio eletrônico conhecidas, o tempo de inatividade pode custar até **US$ 220 mil** por minuto.[6]

90% dos compradores abandonarão um site se ele não carregar "em um tempo razoável" e **57% sairão e comprarão de um varejista semelhante.** [7]

44% dos jogadores que experimentam latência respondem **encerrando o jogo que estão jogando** para tentar novamente mais tarde, enquanto **24% param para jogar outra coisa.**[8]



64% dos tomadores de decisão de TI dizem que a necessidade de oferecer uma experiência de cliente mais rápida e fácil é uma **"carga significativa ou importante em sua infraestrutura de tecnologia".** [9]

Entenda todo compromisso da defesa contra DDoS baseada em nuvem e proteja-se contra a perda de receita causada por interrupções

Veja como nossa plataforma em nuvem unificada, alimentada por uma rede global inteligente, protege contra ameaças DDoS:

A depuração em nuvem sob demanda depende da intervenção humana, adicionando tempo à resposta de mitigação. Por outro lado, a proteção contra DDoS em nuvem sempre ativa é mais abrangente. No entanto, muitos fornecedores dessa proteção contam com centros de depuração distantes que adicionam latência à experiência do usuário.

A Cloudflare aborda essas limitações com uma plataforma de segurança unificada, que inclui três camadas de proteção contra DDoS (camadas 3, 4 e 7) e aceleração de tráfego para redes no local, hospedadas em nuvem e híbridas. O tráfego de ataque é mitigado perto da origem, para que seus usuários finais tenham uma experiência perfeita e de alto desempenho.

Segurança alimentada pela rede

A Cloudflare possui **data centers em mais de 285 cidades** e uma **capacidade de rede de 197 Tbps** (em comparação, um conhecido serviço de mitigação de DDoS sempre ativa tem menos de 40 centros de depuração e 20 Tbps de capacidade de rede).

Os ataques são absorvidos automaticamente por nossa rede antes mesmo de atingirem a sua, e a maior parte do tráfego malicioso é bloqueado em **menos de 3 segundos**. Sem necessidade de backhaul.

Usabilidade, visibilidade e autoatendimento

A proteção contra DDoS da Cloudflare é fornecida como serviço, o que significa que não é necessário nenhum investimento CapEx ou gerenciamento do ciclo de vida do hardware.

Além disso, **possui autoatendimento** com recursos de configuração personalizados em **um único painel**.

Inteligência contra ameaças em escala

Veja mais, proteja mais: quase 20% da web é executada na Cloudflare. Nossos clientes se beneficiam da escala e da inteligência de nossa rede global, que **bloqueia mais de 112 bilhões de ameaças cibernéticas por dia**.

Modelos avançados de aprendizado de máquina aprimoram continuamente nossas defesas, para que possamos ficar à frente das ameaças emergentes em seu nome.

Defesa contra DDoS reconhecida pelo setor

A Cloudflare foi reconhecida como **Líder no GigaOm Radar Report for DDoS Protection de 2022**. O relatório avaliou nove fornecedores diferentes e a Cloudflare foi classificada na posição mais alta no geral. A Cloudflare também foi nomeada **"Líder" no The Forrester Wave™: DDoS Mitigation Solutions, do T1 de 2021**.

A Cloudflare recebeu as pontuações mais altas possíveis em 15 critérios, incluindo centros de operações de segurança, automação de resposta, desempenho e muito mais.

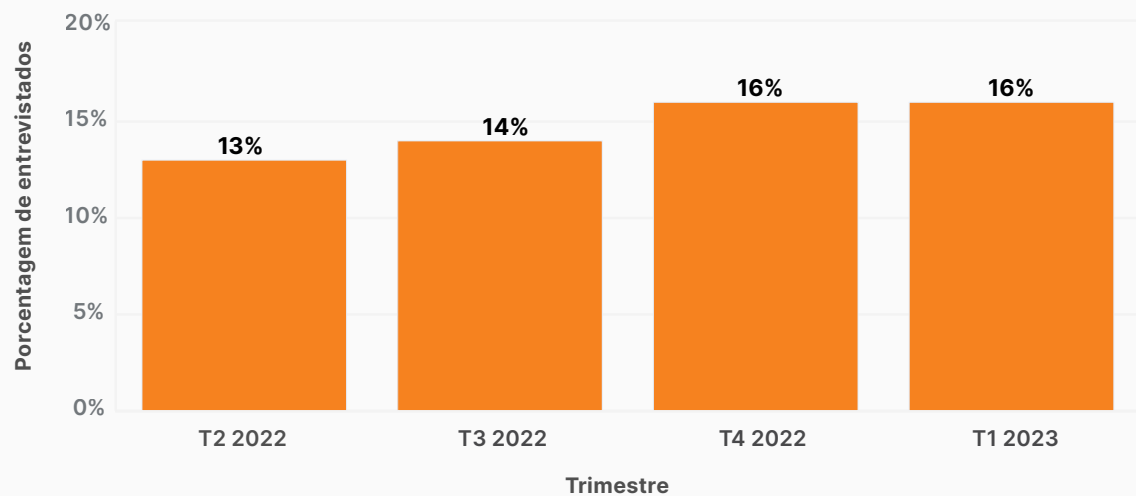
Estudo de caso: empresa da Fortune Global 500 alvo de um ataque DDoS com pedido de resgate

Um ataque DDoS com pedido de resgate (RDDoS), também conhecido como extorsão de resgate, ocorre quando partes maliciosas tentam extorquir dinheiro ameaçando um indivíduo ou organização com um ataque DDoS. O número de tentativas de DDoS com pedido de resgate aumentou constantemente ao longo de 2022 e mais de 16% dos clientes da Cloudflare receberam uma ameaça ou pedido de resgate como parte de um ataque DDoS no primeiro trimestre de 2023.

Embora muitas vezes confundidos com ataques de ransomware, os ataques DDoS com pedido de resgate funcionam de maneira diferente e são mais fáceis de executar: eles não exigem enganar a vítima para abrir um e-mail ou clicar em um link, nem exigem uma invasão de rede ou uma posição em ativos corporativos. A crescente disponibilidade de ransomware como serviço também tornou o DDoS com pedido de resgate uma opção de baixo esforço e baixo risco para os invasores.

Ataques DDoS com pedido de resgate e ameaças por trimestre

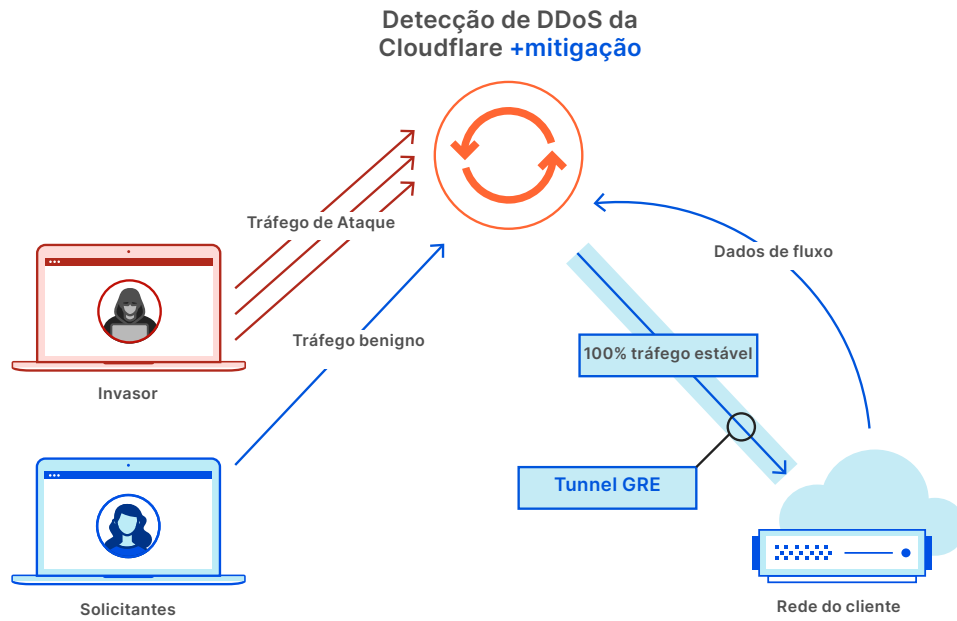
Porcentagem de entrevistados que relataram ter sido alvo ou ameaçados por um ataque DDoS com pedido de resgate.



No final de 2020, antes de usar a Cloudflare para mitigação de DDoS, uma grande empresa da Fortune Global 500 foi alvo de uma tentativa de RDDoS por partes que alegavam ser o Lazarus Group (um grupo de crimes cibernéticos supostamente administrado pelo governo da Coreia do Norte). Os invasores inicialmente enviaram um e-mail exigindo bitcoin e deram a eles uma semana para "pagar", ou então um segundo ataque maior aconteceria e o resgate aumentaria.

Depois de receber a nota de resgate e perceber um aumento significativo no tráfego para um de seus data centers globais, a empresa contatou seu serviço de centro de depuração sob demanda. Eles levaram mais de 30 minutos para ativar o serviço do fornecedor e redirecionar o tráfego para o centro de depuração. A ativação do serviço sob demanda também causou falhas de rede e resultou em vários incidentes.

Após o ataque inicial e os desafios com seu provedor sob demanda, a empresa decidiu integrar a proteção sempre ativa do Cloudflare Magic Transit, a proteção contra ataques DDoS na camada de rede sempre ativa da Cloudflare. Embora os invasores prometessem um segundo ataque enorme, isso nunca aconteceu.



Cloudflare Magic Transit para proteção contra DDoS na camada de rede

"Uma das principais diferenças é a análise de ataque e tráfego que vemos que nosso provedor atual não poderia nos fornecer. Estamos vendo ataques que nunca soubemos que eram mitigados automaticamente."

Equipe de Resposta a Incidentes e Forense
Empresa da Fortune Global 500

Conclusão

À medida que os ataques DDoS aumentam em frequência e complexidade na era pós-pandemia, é importante manter o tráfego legítimo para ajudar a proteger seus resultados. Com a capacidade de proteger contra ataques de forma rápida e sem esforço, sem problemas de latência ou altos custos comumente associados a outros provedores, a Cloudflare facilita a opção por uma estratégia em nuvem sempre ativa.

Para saber mais sobre proteção contra ataques DDoS em rede com a Cloudflare, solicite uma demonstração.

Para saber mais sobre uma rede global única com funcionalidade Zero Trust, mitigação de DDoS, firewall de rede e aceleração de tráfego integrados, clique aqui.

Fontes

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 junho 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, 1º de novembro 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, T1 de 2021,” Forrester, 3 de março de 2021

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

6 “The Cost of Downtime for the Top US Ecommerce Sites,” Gremlin, acessado em 8 de maio 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 outubro 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, novembro de 2019. https://hazelcast.com/resources/infinity-data-report

+55 (11) 3230 4523 | enterprise@cloudflare.com | www.cloudflare.com/pt-br/

CLOUDFLARE