5 perguntas para fazer ao seu provedor de mitigação de DDoS

Com o aumento na frequência e na complexidade dos ataques DDoS, escolher o serviço de mitigação de DDoS correto é fundamental para proteger suas Redes e seus usuários. No entanto, nem todos os serviços são criados da mesma maneira — e escolher a opção errada pode dar dor de cabeça, causar problemas de desempenho e tempo de inatividade.

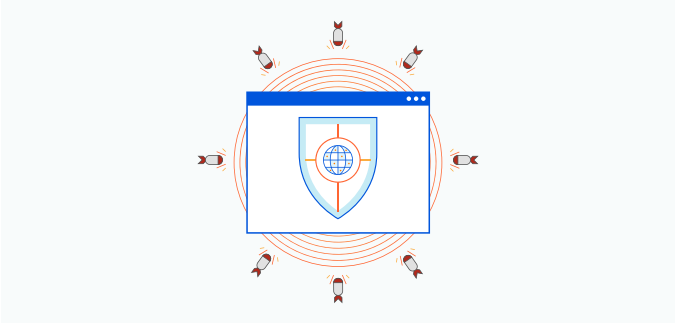
Estas são as cinco perguntas que você deve fazer ao avaliar um provedor de mitigação de DDoS:

1. O serviço é nativo da nuvem?

Para ser eficiente, um serviço de mitigação de DDoS precisa ser nativo da nuvem e não uma tecnologia local virtualizada e hospedada em data centers na nuvem. Qual é a diferença? Os serviços de mitigação nativos da nuvem podem ser dimensionados de acordo com as necessidades do negócio sem impor gargalos artificiais de desempenho, ao passo que os dispositivos virtuais hospedados na nuvem ainda vêm com a complexidade de gerenciamento associada ao hardware local.

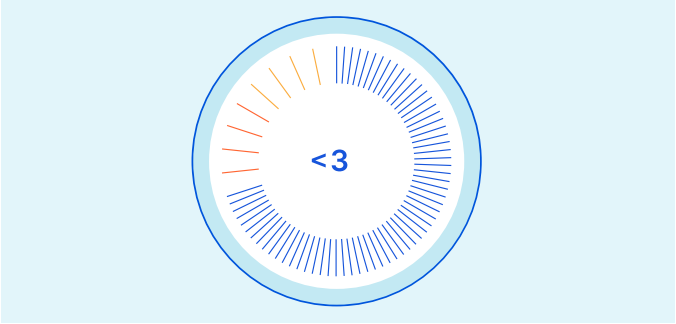
2. Qual é a capacidade de Rede do provedor?

Ataques DDoS de grande escala — como o ataque de 2,3 Tbps a um cliente da AWS em 2020 — podem sobrecarregar um provedor de serviços sem capacidade de Rede suficiente para absorver o tráfego de DDoS. Para combater ataques nessa escala, escolha um provedor que tenha capacidade de Rede suficiente para suportar ataques sem causar tempo de inatividade ou degradar o desempenho.



3. Em quanto tempo o serviço detecta e reage a um ataque DDoS?

É fundamental ter uma reação rápida ao detectar e mitigar um ataque. Alguns segundos de inatividade podem causar um dano irreversível à experiência do cliente, à reputação da marca e à receita.

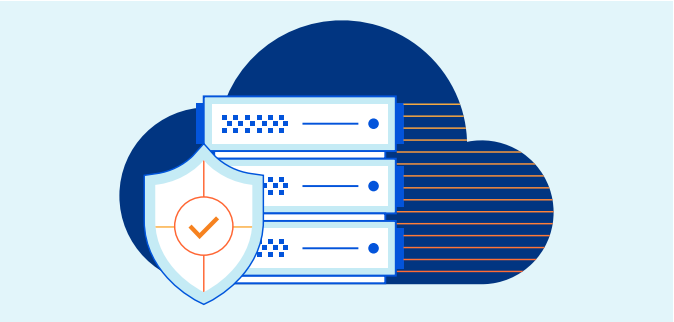


4. O serviço está disponível em todos os data centers?

Quando as funções de DDoS não estão disponíveis em todos os data centers, o tráfego é forçado a voltar por meio de "centros de depuração" especializados, que muitas vezes aumentam a latência e afetam o desempenho do aplicativo. Escolha um provedor que ofereça serviços de mitigação em todos os data centers e mantenha seu tráfego no caminho ideal.

5. O serviço é automatizado?

Um serviço de mitigação de DDoS robusto precisa oferecer automação e automanutenção em um painel ou uma API, para que você ative e gerencie rapidamente a proteção contra ameaças. Procure um provedor que seja fácil de contatar, que responda rapidamente e que seja proativo ao detectar e mitigar ameaças sem causar tempo de inatividade nos seus serviços.



O **Magic Transit da Cloudflare** protege sub-redes IP inteiras contra ataques DDoS e acelera o tráfego de Rede. A Rede global da Cloudflare — abrange data centers em mais de 200 locais — bloqueia uma média de 70 bilhões de ameaças por dia, incluindo alguns dos maiores ataques de DDoS da história.

Solicite uma demonstração gratuita agora para conhecer o Magic Transit.