CLOUDFLARE

INFOGRAPHIC

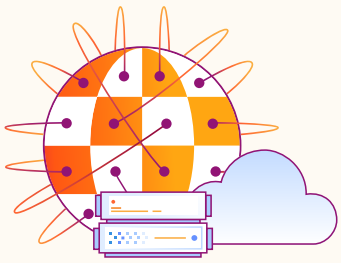
Five questions to ask your DDoS mitigation provider

As DDoS attacks increase in frequency and complexity, selecting the right DDoS mitigation service is essential to protect your networks and users. However, not all services are created equal — and picking the wrong one can lead to unexpected headaches, performance issues, and downtime.

Here are five questions you should consider when evaluating DDoS mitigation providers:

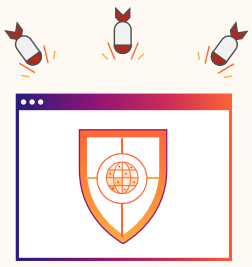
1. Is the service cloud-native?

For a DDoS mitigation service to be effective, it must be cloud-native — not on-premises technology that has been virtualized and hosted in cloud data centers. The difference? Cloud-native mitigation services can scale seamlessly with your business needs without imposing artificial performance bottlenecks, while cloud-hosted virtual appliances still come with the management complexity associated with on-premises hardware.



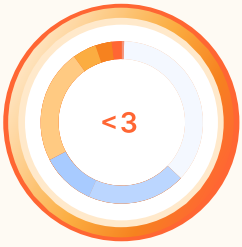
2. How much network capacity does the provider offer?

Large-scale DDoS attacks — like the 2.3 Tbps attack that targeted an AWS customer in 2020 — can overwhelm service providers with insufficient network capacity to absorb DDoS traffic. The largest DDoS attack Cloudflare has detected and mitigated was 2.6 Tbps, in 2023.[1] To combat attacks on this scale, select a provider that offers enough network capacity to withstand attacks without causing downtime or degraded performance.



3. How quickly can the service detect and react to DDoS attacks?

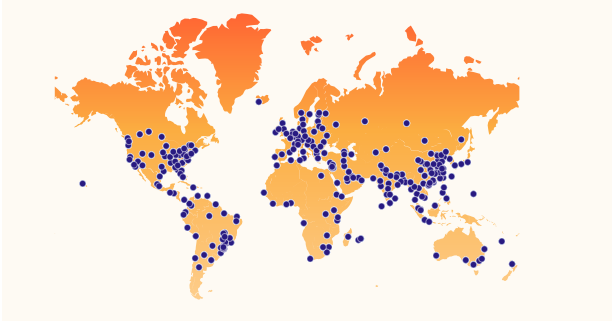
When faced with an attack, a low time to mitigate (the time it takes to detect and mitigate attacks) is crucial. Anything longer than a few seconds of downtime can cause irreversible damage to customer experience, brand reputation, and revenue.



1. Source: https://wiki.cfdata.org/display/COM/Public-Facing+Stats

4. Is the service available in every data center?

When DDoS scrubbing functions are unavailable at every data center, your traffic is forced back through specialized “scrubbing centers” that often add latency and impact application performance. Choose a provider that can offer mitigation services in every data center, while keeping your traffic on the most optimal path.



5. Is the service automated?

A robust DDoS mitigation service should offer automation and self-service ability from a dashboard or API, enabling you to quickly turn on and manage your threat protection. Look for a provider that is easy to contact, quick to respond, and proactive in detecting threats, and mitigating them with no impact to downtime observed on your services.

Cloudflare Magic Transit protects entire IP subnets from DDoS attacks while also accelerating network traffic. Cloudflare’s global network — spanning data centers in over 320 locations — blocks an average of 209 billion threats per day, including some of the largest DDoS attacks in history.

To get started with Magic Transit, request a free demo today.

REV:BDES-6051.2024AUG20