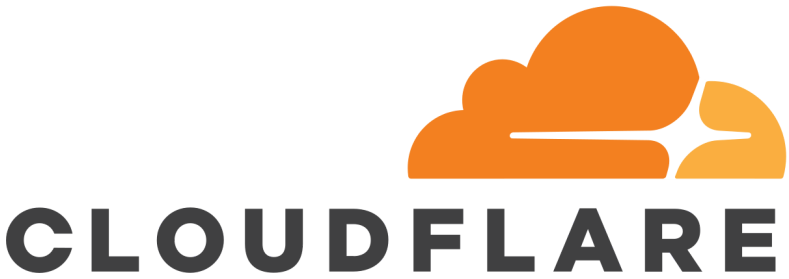
Don't Panic: Some Services to The Rescue!

Now, if all this talk about DDoS has scared you, I have some good news! There are very large internet companies that offer DDoS protection services at a reasonable price tag. Let's look at them in this lesson.

We'll cover the following

Cloudflare



Cloudflare definitely champions this space, as their free tier offers DDoS protection against layer 3, layer 4, and layer 7 attacks. Their more expensive tiers don't command an unreasonable price tag either, from $20 to $200 a month you can raise the wall in front of your webserver. The Pro plan offers enhanced security through a WAF, and their Business plan includes a 100% uptime guarantee.

I've been both a Business and Enterprise customer of Cloudflare (enterprise pricing is quoted differently to each customer, though it's quite a steep increase from the less expensive plans) and I must admit their plans seem to be worth the price tag.

In addition, Cloudflare attaches additional services to their package, such as CDN, free SSL, and enhanced performance, so they can really be thought of as an all-in-one web server platform.

Cloud infrastructures

Chances are that your cloud infrastructure provider also offers some sort of DDoS protection service off-the-shelf. AWS, Azure, and GCP all have developed services to help their customers out when under attack.

AWS

AWS Shield, for example, protects your AWS-hosted resources from the most frequent network and transport layer DDoS attacks, while a higher level of defense can be deployed by enabling the AWS Shield Advanced tier.

Azure

I wanted to mention Azure DDoS protection as it takes an interesting approach to a couple of features. First, it offers advanced analytics while the attack is ongoing, and provides a detailed report once it's over. On the other end, Azure is committed to refund costs incurred as a result of a documented attack, definitely an interesting combination.

Cloud Armor

Finally, Cloud Armor, a service currently in Beta for GCP users, is Google's own DDoS and application-layer attacks.

It is relatively new and still under testing, but fairly promising. Their Rich Rules Language allows the creation of creative, dynamic, and custom firewall rules that can use many inputs, such as L3 to L7 parameters or geolocation data from your visitors.

In addition, Cloud Armor is built on top of Google's massive infrastructure which has fought attacks on the largest highly-available sites in the world, such as `google.com` and `youtube.com`.

We'll conclude this chapter with the next lesson.