5 Questions to Ask About Pricing for DDoS Protection

DDoS protection pricing is all over the map and can be fairly complex. However, paying attention to certain criteria can help you ensure that you're not paying too much while also gaining comprehensive protection.

DDoS protection vendors come in all shapes and sizes, from dedicated DDoS mitigation providers or content delivery network (CDN) vendors that add website DDoS protection to internet service providers (ISPs) that sell DDoS protection as an add-on. As a result, the quality and cost of such services can vary wildly, and many customers end up purchasing protection packages that are either inadequate or too large for their needs, resulting in unnecessary costs.

Here are five questions to ask your DDoS mitigation vendor, to make sure that you're getting the protection you need without overpaying.

1 Are You Paying to Monitor Bad Traffic?

The biggest pitfall – and arguably the main reason overpaying occurs – is buying protection packages that are too large.

DDoS protection packages are usually sold in price tiers according to traffic volume. The package you purchase should correspond to the volume of legitimate traffic your website handles on a regular basis.

If you're not sure about how much traffic you need to monitor, you can find out by looking at traffic statistics on your routers or web servers and verify how much traffic you normally see.

2 How Much Traffic Do You Need to Monitor?

Next, you should determine which type of traffic you're paying to have monitored. When under a DDoS attack, traffic volumes increase exponentially within a short time frame. Therefore, it is important to know whether you are paying for legitimate traffic or attack traffic.

Legitimate traffic is the normal user traffic that is supposed to reach your website. A legitimate traffic payment model ensures that you pay to monitor only legitimate user traffic. Attack traffic, on the other hand, is malicious traffic created by hackers that is intended to overwhelm your website. An attack traffic payment model means that you pay to monitor all traffic reaching your website, legitimate or not.

Paying to monitor attack traffic is particularly a concern if you rely on your CDN provider, your ISP, or your public cloud host for DDoS protection, because these providers charge customers based on overall traffic volumes. In these cases, you will essentially be paying your provider to be attacked, which can quickly escalate to tens of thousands of dollars (or more) per attack.

To protect yourself against such surcharges, it is important to make sure you have cost protection in case of a DDoS attack. Depending on the provider, such price protections might be called “cost protection,” “unmetered DDoS protection” or “legitimate traffic payment model.”

3 Does the Package Include Application-Layer DDoS Protection?

Broadly speaking, DDoS attacks are divided into network-layer attacks and application-layer attacks. Network-layer attacks are based on Layer 3 and Layer 4 protocols, such as TCP and IP, and include attack vectors such as TCP SYN Floods, UDP Floods, IP fragmentation attacks, and others. Application-layer attacks refer to Layer 7 DDoS attacks such as HTTP Floods or low-and-slow DDoS attacks.

Many DDoS protection vendors – especially ISPs and public cloud providers – provide protection only against network-layer attacks and do not protect against application-layer attacks at all. Others – particularly CDN-based DDoS vendors – require that you subscribe to expensive add-on services to receive application-layer protection.

Modern DDoS protection requires that you be protected against both network- and application-layer attacks. Neglecting application-layer defenses will leave you exposed to attack, particularly for public-facing web applications.

4 Are You Protected Against SSL-Based DDoS Attacks?

As more web traffic is encrypted, SSL- and TLS-based DDoS attacks are increasing in frequency. SSL-based DDoS attacks are particularly potent because they demand large amounts of computing resources from target servers. A single SSL request can require up to 15 times more resources from the target server than from the origin computer. As a result, a small attack can result in crippling damage.

Protection against SSL-based DDoS attacks is increasingly important. However, there are still some DDoS vendors that do not provide this type of protection. Other vendors – in particular, CDN vendors – charge extra fees for SSL traffic (thereby increasing the cost) and require that customers share their full SSL keys (thereby compromising user privacy) and decrypt all SSL traffic in the cloud (thereby creating much latency).

It is imperative for organizations to make sure they are protected against this potent form of DDoS attack and that the protection offered does not impede regular user traffic.

5 Are You Aware of Hidden Costs in the Public Cloud?

It is important to ensure there are no hidden costs if you use public cloud infrastructure for your web applications.

As more organizations migrate workloads to the cloud, it is increasingly popular to leverage ancillary cloud DDoS protection services such as load balancing, CDN, storage and databases. Many of these services are charged based on the amount of traffic or number of requests. If there is a DDoS attack, the traffic that goes through these services will skyrocket, as will their associated cost.

Some cloud providers provide limited cost protection against network-level DDoS attacks, but that usually does not include application-level DDoS attacks (such as HTTP Floods) or ancillary services. If there is an attack, these hidden costs can add up to a significant amount.

The best approach is to block malicious traffic before it ever reaches the public cloud, so you aren't charged for cloud infrastructure services. Check the terms to see if you're covered against such attacks, and consider how you can protect yourself.

WHAT TO LOOK FOR IN A DDOS PROTECTION PACKAGE

Ultimately, effective protection means that organizations receive the best coverage, tailored to their needs, at a price point they can afford. Robust defenses must protect against both network-layer and application-layer DDoS attacks, as well as provide protection against increasingly common SSL- and TLS-based DDoS attacks.

To control costs, organizations should make sure that they are not paying to monitor more traffic than they need to, that they are paying for legitimate traffic only, and that they are not paying any hidden costs, especially if using public cloud infrastructure. Examine your DDoS protection package to make sure that this is indeed the case.