



Can Web Hosts Up Their DDoS Game?

Distributed denial-of-service attacks are among the most prevalent types of cyber threats, which even hobby hackers can implement. Over the years, the threats have evolved from volumetric attacks, meant to make websites offline, into more malicious and complex issues. That said, we should question the part that web hosts play in making the threat less severe. That mitigation is up to all web hosts, including [shared server hosting](#) service providers, and internet providers.

Without effective DDoS protection or mitigation in its services, a web host may deliver possibly harmful and useless traffic across its customer networks. When folks decline to pay a public utility for the contaminated water it offers, why do several companies pay for a comparable situation in their web hosting and other services?

An issue with web traffic is that customers cannot correctly visualize the whole traffic that flows across their networks. Analyzing that much traffic is too significant a task for staffers. A sub-saturating DDoS attack is designed to compromise or explore some aspects of your network. Another form of DDoS attack is an attempt to make the entire place offline. Either way, customers cannot force web hosts to explain the issue in pretty much the same manner, notwithstanding the substandard service that they are perhaps getting.

During a possible DDoS attack, web hosts' legacy solution was to send their traffic to a non-existing IP location. However, that would also deliver the good web traffic portion to that location, which would make legitimate users unable to access the website or service that they were expecting to. For the attackers involved, it would make the site inaccessible even when the attack becomes subsided.

Today's tools have gone ahead of hackers in terms of their capabilities. There are technological innovations with live mitigation software installed in line with the network peering point. That makes it possible to protect customer traffic as the traffic travels across a company's network. Such creations make web hosts better positioned as compared to the past to offer customers effective protection as well as ensure that applications and websites stay operational without any interruption.

Companies, including the [best dedicated server providers](#), are beginning to use that technology as an element of their website hosting packages to protect customers, besides automating the newest solutions and making those scalable. That minimizes human intervention while maximizing efficiency, which should serve as a remedy for past DDoS attack-induced headaches.