US SIGNAL

10 TIPS FOR

Mitigating DDoS Attacks

There are several ways to combat DDoS attacks. Here are 10 to consider.

[Education]

Educate your internal teams (IT, Security, Web & Marketing) to spot the signs of DDoS or related application attacks. This can help you identify potential threats faster and respond sooner.

[Monitoring]

Monitor web traffic and setup alerts for suspicious spikes in traffic, especially smaller spikes that hit specific high-risk pages like a login or admin area.

[Incident Response Plan]

DDoS attacks are a persistent threat that businesses must have a plan for. You should have a plan for dealing with a DDoS attack, including an outage due to a persistent attack that lasts for days.

[Use a Cloud-Based DDoS Mitigation Solution]

It is important to protect against volumetric, protocol, and application-layer DDoS attacks with a vendor that covers layer 3, 4, and 7 of the OSI model. Many vendors offer DDoS mitigation that doesn't adequately cover the application layer (layer 7).

[Web Application Firewall]

A good DDoS mitigation solution should include a Web Application Firewall (WAF) that can be used to filter application-level attacks such as credential stuffing or HTTP floods. A WAF uses rules and will filter traffic based on the active rules.

[Separation]

Separate non-critical systems from critical systems and protected assets from unprotected assets. Separation reduces the risk of collateral damage during an attack.

[Firewall]

For DDoS, a cloud-based firewall that offers geo-IP blocking, whitelisting, blacklisting, and more advanced features, such as blocking by ASN, can really help filter out unwanted traffic whether it's DDoS traffic or other malicious threats.

[Rate Limiting]

Rate limiting end users is especially effective for login pages and form fill out pages. By creating a limit for how many requests can be made on those pages, you can thwart many application attacks that could cripple your servers or network.

[Redundancy]

Building redundancy into a system to reduce choke points and failure points is smart for dealing with DDoS and other malicious attacks. For example, having two separate Internet connections from diverse providers reduces the risk of one failing and your site being offline.

[Get Help]

Prevention and mitigation for DDoS and related attacks takes up a lot of time and resources and not everyone has the time or expertise to manage a DDoS mitigation. If you've looked through this list and wonder where to start, perhaps it's time to contact a Managed Service Provider like US Signal.

Need more suggestions? Call 866.2.SIGNAL or email us at: info@ussignal.com.

201 Ionia Avenue SW Grand Rapids, MI 49503 866.2.SIGNAL www.ussignal.com