US SIGNAL

DDoS PROTECTION

Needs and Wants

Use the following checklist to help determine if your organization should consider a solution to defend against DDoS attacks and what features it should have if you do need one.

1. Your Company Profile

- ☐ Your company relies on its website(s) and/or applications for its business operations.
- ☐ Your company can't afford downtime that disrupts its operations.
- ☐ Your company is in a "high-risk" industry such as government, finance, online gaming, healthcare and others which may have regulatory requirements regarding security, privacy, availability and access.

2. Your Company Situation

- ☐ Your company has adopted a cloud-first strategy.
- ☐ Your company is migrating to the US Signal cloud or will be using one of US Signal's services such as colocation, Disaster Recovery as a Service, or Backup as a Service.
- ☐ Your company could benefit from external expertise and resources to free up internal staff to focus on other IT tasks and initiatives.

3. Your Current DDoS Solution

- ☐ Your company has websites, applications, and/or API's but does not have a DDoS solution in place.
- ☐ Your company has a network-based DDoS solution that relies on expensive scrubbing centers and/or inline hardware.
- ☐ You don't have confidence in your company's current DDoS solution.

4. Your DDoS Protection Needs

- ☐ You have websites and applications that need a WAF (Web Application Firewall) to be PCI or HIPAA compliant.
- ☐ You need protection against volumetric DDoS attacks (Layer 3 & 4).
- ☐ You need a solution that can filter bad traffic, including malicious bots, while keeping server resources free for legitimate traffic.
- ☐ You need a DDoS solution that is always on, filtering threats and mitigating DDoS attacks with no need to failover or activate.
- ☐ You need protection against application layer attacks (Layer 7).
- ☐ You need a DDoS solution that doesn't entail performance tradeoffs.
- ☐ You need predictable, flat-rate pricing.

CHECKLIST

DDoS PROTECTION

Needs and Wants

CHECKLIST

5. Your DDoS Protection Wants

- ☐ You want to protect against known and emerging threats.
- ☐ You want a solution that's proven to work against some of the largest DDoS attacks.
- ☐ You want advanced edge caching to keep keep sites working even if origin servers go down.
- ☐ You want the ability to accelerate performance and reduce bandwidth usage.
- ☐ You want to increase uptime and application availability but reduce the strain on origin infrastructure.
- ☐ You want a DDoS protection solution that doesn't require updates or hardware and/or software investment.
- ☐ You want a solution that stays up to date with emerging DDoS threats and zero-day attacks automatically.
- ☐ You want unlimited and unmetered mitigation of DDoS attacks, regardless of the size of attack at no extra cost.
- ☐ You want a 100% uptime SLA.

THE ANSWER IS:

If you checked any item throughout sections 1-4, your company could benefit from a DDoS protection solution. The items you checked in section 5 gives you an idea of some of the features you may want in that solution.

If you're interested in learning if US Signal's DDoS Protection can meet your needs, start by reading about what it is and how it works at: **https://ussignal.com/it-services/ddos-protection**

Or, call 866.2. SIGNAL or email us at: info@ussignal.com.

Our solution architects will be happy to talk to about DDoS protection and other security issues and create a solution custom tailored to your needs.