DDoS PROTECTION:

5 STEPS FOR GETTING STARTED

TABLE OF CONTENTS

DDoS attacks are complex, employing multiple distributed resources to take down websites and other services. However, there are ways to reduce the chance of being a victim of a DDoS attack, as well as to mitigate damage.

In this eBook are five steps to help you mount a strong defense.

STEP 1:

CREATE A RISK PROFILE

One of the first steps in minimizing your organization's risk of a DDoS attack is to create a risk profile. Start by answering the following questions:

- Why would we be a good candidate to attack?
- Are we in a high-risk industry such as online gaming, software and technology, financial services, etc.?
- What do we have that someone might want?
- What enemies or aggressive competitors do we have?
- What activities are happening on our systems that might make us a target?
- How would a DDoS attack affect our business?
- What are our potential threat vectors and how should they be characterized and prioritized?
- How long could we go without systems affected by a DDoS attack?

An incident response plan can help your organization respond quickly if a DDoS attack occurs. To create one:

+ Identify what your critical systems are and understand how to tell if they are being attacked. Signs of a DDoS attack may include unusually slow network performance when opening files or accessing websites; the unavailability of a website; or a dramatic increase in the number of spam emails.

STEP 2:

DEVELOP AN INCIDENT RESPONSE PLAN

- Request any relevant documentation on DDoS attack mitigation and prevention from your security or firewall vendors or managed security providers.

- Compile a list of people to help in the event of an attack. Include members of your company's executive management team, your internet service provider (ISP), internal and external information security experts, and law enforcement professionals — including from the FBI.

- Determine your strategies for dealing with an attack. Can you shut down services or implement your DR plan? Can your ISP block the traffic? If so, what does it need from you to make it happen?

One of the most important partnerships to forge is with your upstream network service provider. Know what assistance your provider can give in the event of a DDoS attack.

If you experience a DDoS attack, provide the attacking IP addresses to your upstream network service provider so it can implement restrictions at its level.

Keep in mind that DDoS reflection attacks typically originate from legitimate public servers. Determine to whom an IP belongs to when examining network logs during an attack.

Use tools such as the American Registry for Internet Numbers (ARIN) to look up the source IPs involved in the attack. Otherwise, you may block traffic from legitimate networks or servers.

The faster your provider can implement traffic blocks and mitigation strategies at its level, the sooner your services will become available for legitimate users.

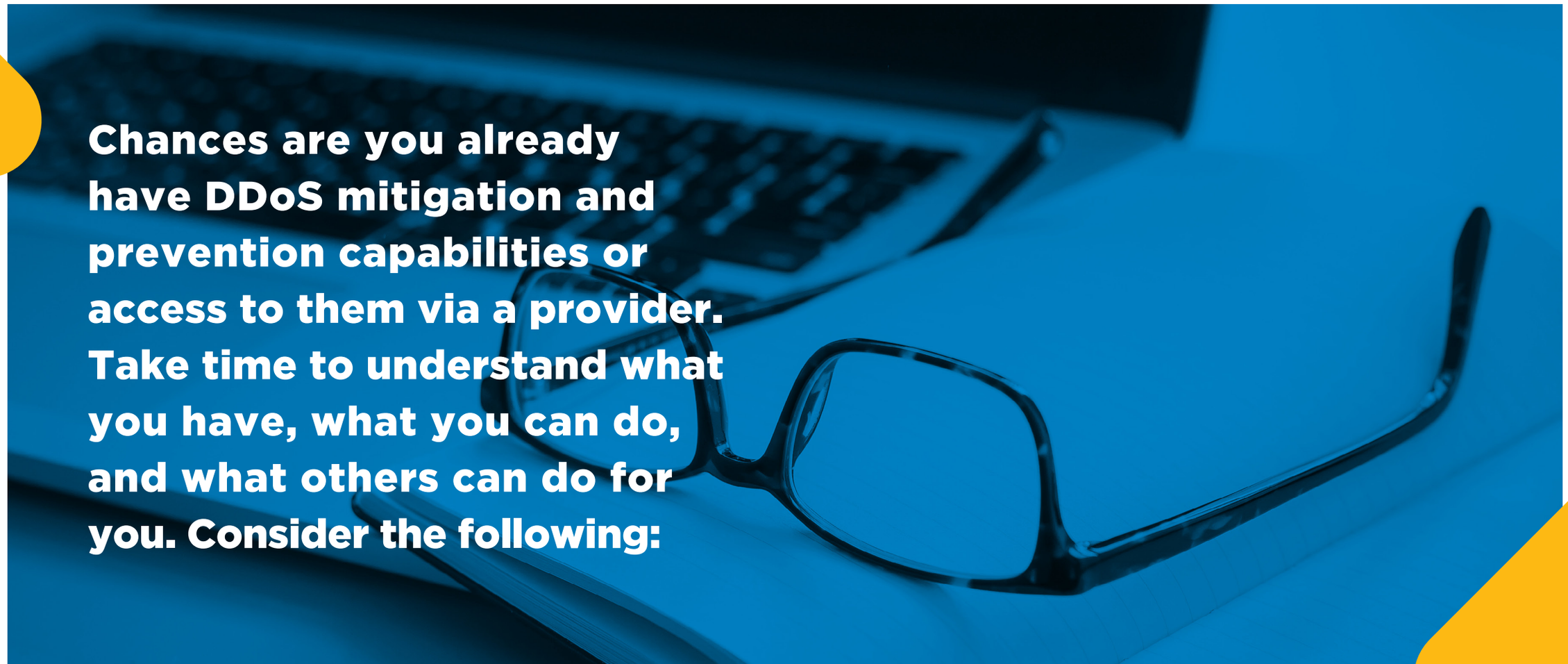
Explore partnerships with technology vendors and IT service providers that can help you mitigate DDoS attacks too.

STEP 3:

ESTABLISH EFFECTIVE PARTNERSHIPS

STEP 4:

EMPLOY YOUR EXISTING SECURITY CAPABILITIES



Chances are you already have DDoS mitigation and prevention capabilities or access to them via a provider. Take time to understand what you have, what you can do, and what others can do for you. Consider the following:

- The security appliances you currently use may have features to assist with DDoS detection and prevention. Know what they are and how they work. Enable them if they aren't already on.

- Configure firewalls and intrusion detection/prevention devices to alert you to traffic anomalies. Make sure firewalls only accept traffic detailed in your organization's security policy as required for business purposes.

- Set firewalls to block, at a minimum, inbound traffic sourced from IP addresses that are reserved (0/8), loopback (127/8), private (RFC 1918 blocks 10/8, 172.16/12, and 192.168/16), unassigned DHCP clients (169.254.0.0/16), multicast (224.0.0.0/4) and otherwise listed in RFC 5735. Request this configuration at the ISP level as well.

- Enable firewall logging of accepted and denied traffic to determine where the DDoS may be originating.

- Take hosts offline or move them to disaster recovery facilities to mitigate issues.

- If possible, shed services under attack to protect services that aren't. It requires triaging your services and knowing which ones are the most important.

Take steps to better defend your company against DDoS attacks. Among them:

+ Implement a routing protocol like Border Gateway Protocol (BGP), so you can block or re-route traffic yourself. This will allow you to send routing information to your service provider dynamically and have more control over the situation.

+ Tap the expertise of others. Attend local ISC2 events and speak with other companies about what works and what doesn't. Involve your network service providers in your planning, testing, and event management. Work with law enforcement, including the FBI. The InfraGard program, a partnership between the FBI and members of the private sector, provides resources to help you stay abreast of attack events and learn about emerging solutions without vendor bias.

STEP 5:

PLAN YOUR DEFENSE

+ Move your security perimeter as far from your network as possible, into your services providers' colocation data center or to a security solution hosted by your provider if possible. This transfers the problem of DDoS attacks into the provider's network.

+ Move web-based services to the cloud. Most cloud services employ DDoS mitigation technologies and best practices. They also have more internet bandwidth available, so they are better able to absorb larger DDoS attacks than end users can.

With the initial steps outlined in this eBook, you're off to a good start in terms of DDoS protection.

Now bolster your defenses by protecting against DNS-based volumetric and multi-vector attacks.

Scalable, cloud-based and provided as a managed service, US Signal's DDoS Protection is available for websites and applications hosted on on-premise, colocated, and cloud-hosted servers. You get unmetered DDoS attack mitigation backed by a 100% uptime SLA. The solution also includes advanced analytics reporting on data utilization and more. Two service levels are available: standard and premium.

To learn more, call 866.2.SIGNAL or email US Signal at: info@ussignal.com.

NEXT STEPS

US SIGNAL®