Several years ago, Distributed denial-of-service (DDoS) attacks occurred infrequently, limiting the need for enterprises to focus attention on protecting against them. Today, it’s no secret that DDoS attacks have emerged as the weapon of choice for cyber criminals who target internet-based business sites. As they’ve evolved, their sophistication has advanced. What’s more, launching complex DDoS attacks has become increasingly easy for hacktivists and cyber-criminals. Once launched, these attacks have devastating effects on businesses that are not protected against them. Attacks can result in prolonged outages for services like ecommerce, simple site function, online bill pay and even VoIP telephony.

According to Forrester Research, DDoS attacks are one of the most prevalent cyberassaults in our constantly changing threat landscape. Translation? If your business relies on websites and applications to generate even a small portion of your revenue, the stakes for protecting against malicious attacks have never been higher. Every business must have a strategy for how to protect against DDoS attacks.

**THE SOLUTION**
CenturyLink is an industry-recognized leader for managed security services. Our teams deliver robust mitigation of DDoS attacks far above your infrastructure, from within the CenturyLink network, complemented by optional DDoS appliance that can be deployed on site, in a CenturyLink data center or a third party data center. The core function of CenturyLink’s DDoS mitigation service is to drop DDoS attack traffic prior to reaching your production sites, allowing legitimate traffic to continue to your website with no interruption.
SERVICE FEATURES & CAPABILITIES

DDoS Mitigation service minimizes the impact of distributed denial of service attacks by providing protection far above your infrastructure, at the core-router level and re-routing potential DDoS attack traffic to one or more “cleansing centers.” By addressing attacks quickly, you can reduce downtime and the added cost of bandwidth-spikes commonly associated with DDoS attacks. Because the DDoS mitigation makes use of network-based infrastructure, there is no hardware or software required within your environment, thereby reducing your overall dedicated infrastructure costs. Service options are also available for additional customer-premise based mitigation appliances.

When the service detects a possible DDoS attack, CenturyLink Security Operations Center (SOC) personnel validates the attack and subject to your approval reroutes network traffic for scrubbing in the CenturyLink network to help eliminate the malicious traffic and pass along valid traffic.

CenturyLink DDoS Mitigation service delivers protection on the CenturyLink network as well as any third party network that your business may be leveraging.

ADVANTAGES

- Mitigates DDoS attacks within CenturyLink network and customer premises, minimizing client downtime and potentially reducing costly impacts of attacks
- Ensures business continuity by allowing legitimate transactions to be processed
- Employs a behavioral anomaly capability, to help improve attack-traffic filtering and prevent future DDoS exploits
- Flexible pricing model

Flexible Billing Models

Many DDoS mitigation service providers will charge you a large monthly fee — even if you are never attacked. CenturyLink DDoS Mitigation allows you the flexibility of choosing your billing model. Choose between a pay per use model, or a predictable fixed cost model.

Pay For What You Use:

Priced like an insurance policy, the DDoS Mitigation service is priced to meet the requirements of enterprises who need the peace-of-mind of knowing that a high-capacity DDoS mitigation service is protecting them, but who don’t want to pay a large monthly premium for attack mitigation they may rarely need.

Fixed Cost:

This billing model is available to CenturyLink IQ® Networking Internet Port and Network-Based Security (NBS) customers and provides a fixed monthly charge for the service based on the internet port’s or NBS bandwidth. The cost is fixed regardless of bandwidth utilization or attack duration, delivering a predictable monthly service charge.
Optional CenturyLink DDoS Mitigation Appliance:
As a complement to CenturyLink network-based DDoS Mitigation Service, an optional in-line appliance can be installed at one of CenturyLink data centers, 3rd party data centers or customer premises. The DDoS mitigation appliance works in conjunction with the network-based DDoS solution and provides in-line 24/7 detection and cleansing of DDoS attacks. When traffic through the appliance reaches a preconfigured threshold an alert is sent to the CenturyLink SOC signaling that a network-based mitigation is required. The premises appliance provides for more timely protection of sites with greater than normal need for high availability and gives CenturyLink the ability to provide a proactive DDoS detection and mitigation service to sites on third-party networks.

Optional DDoS Mitigation Appliance service benefits:
• Provides always on detection and mitigation against DDoS attacks
• Provides traffic visibility and DDoS detection on 3rd party networks
• Integrated with network based mitigation capabilities via cloud signaling where the appliance can automatically request help from additional resources from the network
• Can reduce hourly network-based mitigation charges in the pay for what you use model

MONITORING AND REPORTING
CenturyLink’s world-class SOC is staffed by skilled analysts who not only monitor CenturyLink’s network for attack traffic, but also work with you round-the-clock during an attack to help ensure that available countermeasures are deployed and in use to keep your site protected. If you believe that an attack on your site is imminent, you may also contact the SOC and request that your traffic be scrubbed as a precautionary measure.

DDoS Mitigation service provides both CenturyLink network customers as well as third party network customers with a variety of reports that display everything from summary data indicating the effectiveness of the service’s mitigation functionality, to details regarding specific source-IP addresses, which can be used for analysis and future mitigation planning.

For more information about CenturyLink, visit www.centurylink.com/technology.