CenturyLink® DDoS Mitigation

DATA SHEET

Today's distributed denial of service (DDoS) attacks are growing in size, frequency and complexity. No enterprise is immune to these threats. Application availability, website uptime and infrastructure accessibility are all critical for business continuity. Every minute of downtime can result in lost productivity and revenue.

Scrubbing center mitigation techniques alone are not designed to manage today's massive, highly sophisticated and distributed attacks. To defend against a variety of attack types, it's essential to deploy a multi-layered security approach backed by extensive threat visibility.

CenturyLink provides layers of defense through enhanced network routing, rate limiting and filtering that can be paired with advanced network-based detection and mitigation scrubbing center solutions. Our mitigation approach is informed by threat intelligence derived from visibility across our global infrastructure and data correlation. Tailored for any business and IT or security budget, our flexible managed service can proactively detect and mitigate the threats of today to help ensure business as usual for employees, partners and customers.

Flexible Solutions

CenturyLink internet customers enjoy baseline protection if under attack. Upon request, customers receive basic Internet Protocol (IP) filtering/null routing on malicious IP addresses on a temporary basis. However, we encourage enterprises to invest in a permanent DDoS mitigation solution. DDoS Mitigation Service is a carrier-agnostic solution that pulls customer traffic through either Border Gateway Protocol (BGP) advertisement route redirection or Domain Name System (DNS) redirection onto CenturyLink's global scrubbing centers for mitigation and cleansing.

Technical Features/Capabilities

DDoS Mitigation Service:

- Eleven regional scrubbing centers leveraging 43+ Tbps of FlowSpec-based mitigation on the global backbone
- Customer traffic is onboarded at the closest scrubbing center or at hundreds of CenturyLink internet service or IP VPN point of presence (POP) locations globally
- Volumetric and application layer attack reduction
- Mitigates against known forms of Layer 3–7 attacks
- Advanced behavioral analytics technology on proxy service
- Up to 10-minute time-to-mitigate SLAs for most known forms of attack after traffic is on-ramped through CenturyLink scrubbing centers
- Full range of proactive and reactive mitigation offered
  - Always-On, Always-Routed with Auto-Mitigation or On-Demand
  - Proactive mitigation includes traffic baselining

CenturyLink®

Fixed Fee Service: Unlimited mitigation with no per-incident fees or overage charges.

Flexible Clean Traffic Return Options:

- Generic Routing Encapsulation (GRE) Option: GRE tunnels for clean traffic return over the public internet as a forward path from CenturyLink global mitigation network to customer data centers
- Internet Direct Option: Clean traffic return over existing CenturyLink internet service with traffic segmentation and prioritization
- IP VPN Direct Option: MPLS/IP VPN clean traffic return from CenturyLink global mitigation network to the customer data center for clean traffic
- Proxy Service: DNS-based redirect with a reverse proxy over the public internet for returning traffic to the customer of origin server(s)

Host Level Rerouting and IP Filtering: Less intrusive, providing protection without rerouting entire subnets.

Reporting: Peacetime performance and event reporting with extensive attack visibility and historical data via the customer portal.

Emergency Turn-Up: Available for GRE service option and proxy services.

Customer Initiated Mitigation: Allows customers to be in control and automate starting and stopping mitigation using special BGP announcements.

DDoS Flow-Based Monitoring: Provides early detection and notification of attacks by monitoring customer edge routers directly, or CenturyLink network edge routers, if CenturyLink is the internet provider. Our 24/7 Security Operations Center will detect anomalies in flows, perform impact analyses and notify your personnel of threatening conditions.

- Detects Layer 3 and 4 DDoS attacks and provides alerts
- Analyzes Netflow, Sflow and Jflow data

Application Monitoring and Mitigation: Integration with DDoS mitigation premises equipment provides an additional application layer mitigating controls as well as serving as an added layer of defense that efficiently integrates via cloud signaling with the CenturyLink scrubbing centers.

BGP FlowSpec Capability for Rapid Response: BGP FlowSpec-based announcements allow for an automated access control list (ACL) delivery to BGP FlowSpec-capable routers within the CenturyLink network. This highly scalable tool, deployed globally, is managed by the CenturyLink Security Operations Center to provide rapid response to very large volumetric attacks.

Why Choose CenturyLink for DDoS Mitigation?

Scalable Attack Ingestion Capacity: CenturyLink has 11 global scrubbing centers across four continents and leverages BGP FlowSpec on more than 43 terabits of backbone capacity allowing for rapid threat mitigation across the CenturyLink backbone, shutting down volumetric DDoS attacks and providing a more secure network for our customers.

Multi-Layered Attack Protection: CenturyLink protection extends beyond DDoS scrubbing and includes the ability to control threats through network routing, filtering and rate limiting, providing relief from volumetric and application-based attacks from Layers 3–7.

Carrier-Agnostic Protection and Detection: CenturyLink can reroute and scrub all internet connections, not just CenturyLink on-net capacity.

Global Footprint and Network Depth: With the ability to access the CenturyLink mitigation network from over 200 POPs globally, CenturyLink provides comprehensive performance and improved latency of cleansed, returned internet traffic to customers.

Proven Attack Traffic Visibility: CenturyLink global IP, CDN and DNS networks provide our security experts with extensive visibility into attack traffic and advancing threats.