Are you feeling the pressure?

Distributed Denial of Service (DDoS) attacks are increasing in sophistication and continue to exceed an enterprise’s capability to mitigate at scale. Today’s organizations need access to advanced detection and mitigation capabilities to keep up. CenturyLink® DDoS Mitigation Service provides network and application layer protection across multi-vector and mixed application layer attacks to help minimize downtime and maintain performance.

How it works:
The CenturyLink DDoS mitigation solution utilizes multiple layers of defense, including our global internet backbone, intelligent scrubbing centers, extensive peering and Black Lotus Labs threat intelligence. When under attack, customer traffic is re-directed using BGP advertisements to CenturyLink global scrubbing centers for cleansing. Malicious traffic is filtered, and good traffic is returned to the customer via dedicated IP VPN connections, CenturyLink internet connections or GRE tunnels.

DDoS services can be consumed in an On-Demand or Always-On manner and are supported by our eight global SOCs that help customers with attack detection and mitigation. Always-on customers also have an option to start or stop mitigation via automated customer-facing controls. Additional cloud-based WAF/WAAP/Bot management capabilities are available for advanced application layer protection.

We own DDoS defense in depth:
- Advanced scrubbing center technology for enhanced performance
- Black Lotus Labs threat intelligence for botnet identification and takedowns
- Deep global peering for reduced latency
- Expansive global network as a first line of defense

CenturyLink customers reduced mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR) for DDoS attacks by over 75%.

Technical features & capabilities:
- 15 global scrubbing centers leveraging 85+ Tbps of FlowSpec based defense capacity
- 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
- Advanced behavioral analytics technology with DDoS 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 with customer-initiated mitigation controls
  - On-Demand with proactive or auto-mitigation controls
Solution benefits:

- **Global SOC support**: Eight global security operations centers (SOCs) located across North America, Latin America, Asia-Pacific and Europe offer around-the-clock support.

- **Carrier-agnostic protection**: We can re-route and scrub all internet connections, not just CenturyLink internet service. CenturyLink DDoS mitigation supports both IPv4 and IPv6 traffic with options for IP VPN Direct, Internet Direct and GRE clean traffic return path connections.

- **Control in customer hands**: Customer defines when, where, how and what is mitigated, enabling fully automated implementations.

- **Next-generation Web Application Firewall (WAF) and Bot management**: Containerized multi-vendor WAF/Bot/API protection solutions defend public web applications from complex application layer 7 attacks.

- **Global footprint**: Mitigation capabilities deployed across North America, South America, Europe, Asia, and Australia, providing global and regional businesses access to local defenses.

- **Transparent pricing**: Fixed-fee service with no overage charges.

- **Reporting**: Extensive attack visibility and historical data via the customer portal.

- **Emergency turn-up**: Available for GRE service option and proxy services.

- **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.

- **Support for hybrid DDoS deployments**: Ability to integrate DDoS mitigation premises equipment via cloud signaling with CenturyLink DDoS mitigation infrastructure, adding local decryption and more application layer mitigation capabilities.

- **Backbone as defensive barrier**: BGP FlowSpec allows for automated delivery of rules to the CenturyLink backbone, providing highly scalable, global mitigation capabilities against volumetric attacks.

Customers using the CenturyLink DDoS mitigation solution realized a **222% ROI** over three years.

Why CenturyLink for DDoS mitigation?

1. **Scalable attack mitigation capacity**: 15 global, intelligent scrubbing centers backed by 85+ Tb of FlowSpec mitigation capacity to detect and drop attack traffic at our network edge.

2. **Carrier-agnostic protection and detection**: CenturyLink can re-route and scrub all internet connections, not just CenturyLink internet.

3. **Enhanced performance and minimized latency**: More than 9,000+ unique AS interconnects and 120+ Tb of network capacity help maximize performance.

4. **Multi-layered attack protection**: Ability to control threats through network routing, filtering and rate limiting, botnet takedowns, providing mitigation scale for network, protocol and application layer based attacks.

5. **Proven attack traffic visibility**: CenturyLink’s global IP, CDN and DNS networks, combined with Black Lotus Labs threat intelligence, provide CenturyLink with extensive visibility into attack traffic and advancing threats.

---

1. Forrester: The Total Economic Impact Study of CenturyLink DDoS Mitigation Service, April 2020
2. Forrester: The Total Economic Impact Study of CenturyLink DDoS Mitigation Service, April 2020
3. Telegeography, Global Internet Geography Executive Summary, 2018