Lumen® DDoS Mitigation for Government

Today's Distributed Denial of Service (DDoS) attacks are growing in size, frequency, and complexity. These attacks can prevent access to a government agency's public-facing websites, applications, and other assets, having substantial impact on operations. Opposition to legislation and political activism often serve as motivation for government attacks, and no agency, department or branch is immune to these threats. Application availability, website uptime and infrastructure accessibility are all critical for mission success. Every minute of downtime can result in lost productivity, inability to serve citizens and a tarnished reputation. Scrubbing center mitigation techniques alone are not sophisticated enough to manage today's massive, widely distributed attacks. It is essential to deploy a multi-layered security approach leveraging scale from a global network and backed by extensive threat research to defend against a variety of threat types.

Lumen 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 organization and IT/security budget, our flexible managed service can proactively detect and mitigate the threats of today so you can stay focused on your agency's core mission.

Flexible solutions

Lumen internet customers enjoy baseline protection if under attack. Upon request, customers receive basic IP filtering/null routing on malicious IP addresses on a temporary basis. However, we encourage agencies to invest in a permanent DDoS mitigation solution. The Lumen DDoS Mitigation Service is a carrier-agnostic solution that pulls customer traffic through route redirection (using BGP advertisement redirect or DNS redirect) into Lumen global scrubbing centers for mitigation and cleansing.

Technical features/capabilities

DDoS Mitigation Service

- Available on several contract vehicles including WITS 3, Networx, NASPO ValuePoint Cloud Solutions and MiCTA.
- 15 global scrubbing centers leveraging 85+ Tbps of FlowSpec based defense capacity.
- Customer traffic is on-boarded at the closest scrubbing center. The clean traffic is returned via the options of GRE tunnels, at hundreds of Lumen Internet Service or IP VPN point of presence (POP) locations globally.
- Mitigates against known forms of layer 3–7 attacks.
- Competitive SLAs for most known forms of attack after traffic is on-ramped through Lumen 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

Lumen customers reduced mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR) for DDoS attacks by

over 75%

Forrester: The Total Economic Impact Study of Lumen DDoS Mitigation Service, April 2020

LUMEN®

Solution benefits

- **IP VPN Direct option**
  Private MPLS/IP VPN as a forward path from Lumen Global Mitigation Network to the customer datacenter for clean traffic.

- **GRE option**
  GRE tunnels over the public Internet as a forward path from Lumen global mitigation network to the customer datacenter for clean traffic return.

- **Internet Direct option**
  Clean traffic return over existing Lumen Internet service.

- **Host Level Re-routing and IP Filtering**
  Less intrusive, providing protection without rerouting entire subnets when on the Lumen network.

- **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 multivendor WAF/Bot/ API protection solutions defend public web applications from complex application layer 7 attacks.

- **Reporting**
  Peacetime performance and event reporting with extensive attack visibility and historical data via the Lumen® Security Services portal.

- **Emergency turn-up**
  Available for GRE service option.

- **DDoS Flow-Based Monitoring**
  Early detection and notification of attacks by monitoring customer edge routers directly. Our 24/7 Security Operations Center will detect anomalies in volumetric 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

- **Support for hybrid DDoS deployments**
  Ability to integrate DDoS mitigation premises equipment via cloud signaling with Lumen 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 Lumen backbone, providing highly scalable, global mitigation capabilities against volumetric attacks.

Why Lumen for DDoS mitigation?

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

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

3. Enhanced performance and minimized latency
More than 9,000+ unique AS interconnects* and 120+ Tbps 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 layer 3, layer 4 volumetric to layer 7 application based attacks

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

6. Trusted Government Partner
Lumen is a trusted provider of choice for government entities around the globe.Government agencies and departments rely on our advanced, geographically resilient, scalable network for secure end-to-end solutions

*Telegeography, Global Internet Geography Executive Summary, 2018

Customers using the Lumen DDoS mitigation solution over three years realized a

222% ROI

Forrester: The Total Economic Impact Study of Lumen DDoS Mitigation Service, April 2020

LUMEN®