Lumen℠ DDoS Mitigation

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 research.

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 business and IT/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

Lumen's 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 enterprises 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 (BGP advertisement redirect or DNS redirect) onto Lumen's global scrubbing centers for mitigation and cleansing.

Technical features / capabilities

DDoS Mitigation Service

- Eleven regional scrubbing centers with 4.5 Tbps of attack ingestion capacity
- Customers traffic are on-boarded at closest Lumen POPs
  - Chicago, Dallas, Los Angeles, New York and Washington, D.C.
  - EMEA: Frankfurt, and London
  - LATAM: Sao Paulo
  - APAC: Tokyo, Singapore, Hong Kong
- Volumetric and application-layer attack mitigation
- Mitigates against known forms of layer 3–7 attacks
- Advanced behavioral analytics technology on Proxy service
- Five- to 15-minute Time-to-Mitigate 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" or "On-Demand"
  - Proactive mitigation includes traffic baselining

LUMEN℠

Fixed fee service

Unlimited mitigation with no per-incident fees or overage charges.

GRE option

GRE tunnels over the public internet as a forward path from Lumen global mitigation network to the customer data center for clean traffic. Maximum of 1 Gbps. of peak inbound traffic.

Internet direct option

Clean traffic return over existing Lumen internet service with traffic segmentation and prioritization.

IP VPN direct option

MPLS/IP VPN as a forward path from Lumen 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 origin server(s).

Host level re-routing 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 MyLevel3SM customer portal.

Emergency turn-up

Available for GRE and Proxy services.

Customer initiated mitigation

Available using BGP with GRE, Internet Direct and IP VPN Direct services.

DDoS flow-based monitoring

We provide early detection and notification of attacks by monitoring customer edge routers directly or Lumen's network edge routers if we are the internet provider. 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

Application monitoring and mitigation

Integration with customer-owned premises equipment provides an added layer of defense and efficiency. Signal out to the Lumen scrubbing centers to have attack traffic mitigated in Lumen scrubbing centers.

BGP Flowspec capability for rapid response

BGP Flowspec-based announcements allow for an automated ACL rules delivery to BGP Flowspec capable routers within Lumen network. This highly scalable tool, deployed globally, is managed by the Lumen Security Operations Center to provide rapid response to threats.

Why choose Lumen for DDoS Mitigation?

- **Scalable attack ingestion capacity**
  Lumen currently has eleven global scrubbing centers with 4.5 Tbps of attack ingestion capacity.
- **Multi-layered attack protection**
  Lumen protection extends beyond DDoS scrubbing to include 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**
  Lumen can re-route and scrub all internet connections, not just Lumen on-net capacity.
- **Global footprint and network depth**
  With the ability to access our mitigation network from over 200 POPs globally, Lumen can provide better performance and improved latency of cleansed, returned internet traffic to the customers.
- **Proven attack traffic visibility**
  Lumen's global IP, CDN and DNS networks provide Lumen with extensive visibility into attack traffic and advancing threats.

877-453-8353 | lumen.com