Level 3 COMMUNICATIONS

Connecting and Protecting the Networked World℠

LEVEL 3® 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. It is essential to deploy a multi-layered security approach backed by extensive threat research to defend against a variety of attack types.

Level 3 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

Internet customers of Level 3 enjoy baseline protection if under attack. Customers receive basic IP filtering / null routing of malicious IP addresses on a temporary basis upon request. However, we encourage enterprises to invest in a permanent DDoS mitigation solution.

The Level 3 DDoS Mitigation Service is a carrier agnostic solution that pulls customer traffic through route redirection (BGP configuration or DNS redirect) onto Level 3's global mitigation network scrubbing centers for cleansing.

Technical Features / Capabilities

DDoS Mitigation Service:

- Nine regional scrubbing centers with 4.5 Tbps of attack ingestion capacity
- Customers are on-boarded at closest Level 3 POP
  - Chicago, Dallas, Los Angeles, New York and Washington, D.C.
  - EMEA: Frankfurt, Amsterdam and London
  - LATAM: Sao Paulo
- Volumetric and application layer attack mitigation
- Mitigates against known forms of layer 3 – 7 attacks
- Advanced behavioral analytics technology

Level 3 COMMUNICATIONS

Connecting and Protecting the Networked World℠

- Five- to 15-minute Time to Mitigate SLAs for most known forms of attack after traffic is on-ramped through Level 3 scrubbing centers
- Full range of proactive and reactive mitigation offered
  - "Always-On" or "On-Demand"
  - Proactive mitigation includes traffic base lining
- Fixed fee service with no per incident fees or overage charges with unlimited mitigation
- **Direct Option:** MPLS/IP VPN as a forward path from Level 3 Global Mitigation Network to the customer datacenter for clean traffic
- **GRE Option:** GRE tunnels over the public internet as a forward path from Level 3 global mitigation network to the customer datacenter for clean traffic. Maximum of 1 Gbps. of peak inbound traffic
- **Internet Direct Option:** Clean traffic return over existing Level 3 Internet service with traffic segmentation and prioritization
- **Proxy Option:** DNS based redirect with a reverse proxy over the public Internet for returning traffic to the customer 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 MyLevel3℠ Portal
- **Emergency Turn-Up:** Available for GRE and Proxy services
- **Customer Initiated Mitigation:** Available using BGP with GRE and Direct services

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

Application Monitoring and Mitigation: Integration with customer-owned premises equipment provides an added layer of defense and efficiency. Signal out to the Level 3 scrubbing centers to off-load attack traffic. SSL supported.

BGP Flowspec Capability for Rapid Response: BGP Flowspec based announcements allow for an automated ACL rules delivery to the network. This highly scalable tool, deployed globally, is managed by the Level 3 Security Operations Center to provide rapid response to threats.

Why Choose Level 3 for DDoS Mitigation?

Scalable Attack Ingestion Capacity: Level 3 currently has nine global scrubbing centers across three continents with 4.5 Tbps of attack ingestion capacity.

Multi-Layered Attack Protection: Level 3 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: Level 3 can re-route and scrub all internet connections, not just Level 3 on-net capacity.

Global Footprint and Network depth: With the ability to access our mitigation network from over 200 MPLS POPs globally, Level 3 can help provide increased performance and improved latency of cleansed, returned internet traffic.

Proven Attack Traffic Visibility: Level 3's global IP, CDN and DNS networks provides Level 3 with extensive visibility into attack traffic and advancing threats.

ABOUT LEVEL 3

We operate and take end-to-end responsibility for network solutions that connect you to the world. We put customers first and take ownership of reliability and security across our broad portfolio.

1.877.4LEVEL3 • LEVEL3.COM
INFO@LEVEL3.COM