LUMEN® DDOS HYPER℠ FAQ

Get answers to the most frequently asked questions about our self-service DDoS mitigation solution, now available in our customer portal, Control Center.

Overview

Q **What is Lumen® DDoS Hyper?**

A Distributed Denial of Service (DDoS) attack occurs when an attacker sends traffic to a targeted organization's network with the intent of disrupting or making unavailable that organization's internet connection(s), web-facing systems or web-facing applications. Attack methods may vary, but the goal is always to achieve disruption or make internet-facing resources unavailable. The carrier-agnostic Lumen® DDoS Hyper mitigation solution helps solve this problem by pulling customer traffic through BGP route redirection onto Lumen global scrubbing centers for cleansing. Attack traffic is filtered out and good traffic is sent back to the customer via GRE tunnel. The service can be subscribed to protect both Lumen and third-party internet circuits. Flow-Based Monitoring provides proactive monitoring and alerting of potential attacks.

Q **What is Lumen® DDoS Hyper used for?**

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. Lumen® DDoS Hyper provides network and application layer protection across multi-vector and mixed-application layer attacks to help minimize downtime and maintain performance.

Q **How is Lumen® DDoS Hyper delivered?**

Lumen® DDoS Hyper 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 Lumen global scrubbing centers for cleansing. Malicious traffic is filtered, and good traffic is returned to the customer via GRE tunnels.

LUMEN®

DDoS services can be consumed On-Demand and Always-On and are supported by our eight global SOCs that help customers with attack detection and mitigation.

Lumen also offers advanced DDoS mitigation features, clean traffic return via dedicated IP VPN connections or integrated with Lumen internet service, and additional cloud-based WAF/WAAP/ Bot Management capabilities for increased application layer protection.

To learn more, please visit the DDoS and Web Application web page.

Q **What is included with Lumen® DDoS Hyper?**

Lumen® DDoS Hyper includes:

- On-Demand or Always-On DDoS attack mitigation
- Over-the-top protection on Lumen or third-party internet services
- Up to 10 Gbps of clean traffic return
- Up to 10 GRE tunnels and 10 Flow-Based Monitoring instances
- Optional designated professional security consultant for runbook development, analysis and reporting tailored to your business needs

Lumen also offers advanced DDoS mitigation features, clean traffic return via dedicated IP VPN connections or integrated with Lumen internet service, and additional cloud-based WAF/WAAP/Bot Management capabilities for increased application layer protection.

Ordering and deployment

Q **How do I order Lumen® DDoS Hyper?**

Lumen® DDoS Hyper can be ordered online using Control Center, our customer self-service portal. To be eligible for the service, you must have a router* (CPE) capable of GRE tunnel termination and able to support the GRE throughput requirement for your service, BGP advertisements, NetFlow generation and, for internet service that is not provided by Lumen, IP address space of at least /24 or larger. If you have Lumen internet service, the minimum size of address space does not apply.

Once you accept the terms of the service, you will be redirected to a microapp where the technical parameters to provision your service will be gathered. This includes the IP address space that is to be protected, the IP address(es) of the GRE tunnel(s), version of NetFlow you will send to Lumen from your CPE, etc.

*Not currently supported with Lumen Managed Router.

Q **What happens once I order? How is Lumen® DDoS Hyper installed?**

You can track the status of your order in our customer self-service portal, Control Center. The service is provisioned in near real time. Once the service is provisioned, we will notify you and provide you with configuration parameters for your CPE to make it work with Lumen® DDoS Hyper service.

Q **How do I get help with my purchase/service activation?**

If you need help or have questions, dedicated support with chat and call options is available in our customer self-service portal, Control Center. The portal will provide regular updates, and our support team is available to guide you through the process.

Additional features

Q **Can I combine Lumen® DDoS Hyper with Lumen Internet?**

You can order Lumen® DDoS Hyper online, which includes over-the-top clean traffic return on Lumen or third-party internet. We also offer advanced DDoS mitigation features, clean traffic return via dedicated IP VPN connections or Lumen internet connections, and additional cloud-based WAF/WAAP/Bot Management capabilities for increased application layer protection.

Q **Does Lumen® DDoS Hyper protect IPv6?**

Lumen® DDoS Hyper supports IPv4 protection. IPv6 protection is included in our advanced set of DDoS mitigation features.

Q **What is the SLA for Lumen® DDoS Hyper?**

The service is monitored 24/7 by Lumen SOCs with alerts and mitigations backed by up to 10-minute time-to-mitigate SLAs for most known forms of attack after traffic is on-ramped through Lumen scrubbing centers.

Attack response

Q **What happens if an attack occurs?**

On-Demand customers have multiple options for how to set up their service:

- The Lumen SOC automatically detects the attack, notifies the customer and begins mitigating the attack once customer approval is given.
- The Lumen SOC, subject to customer pre-approval, sets up auto-mitigation of attacks, which allows mitigation to occur automatically when detected.
- For customers that want complete control over initiating mitigation, they may choose the option to contact the Lumen SOC when an active attack occurs to request the start of mitigation. The Lumen SOC can be contacted directly by calling (866) 254-5210.
- For Always-On customers, whose traffic is always routed through Lumen Mitigation infrastructure, Lumen automatically detects and begins mitigating attacks. If attack countermeasures require any fine-tuning, Always-On customers can contact the SOC directly by calling (866) 254-5210.
- Always-On customers also have the option of a customer-initiated mitigation feature to start and stop mitigation through automated mechanisms the customer controls.

If there is a need to escalate a potential DDoS attack or a trouble ticket issue to the Lumen Security Operations Center management team, the escalation path can be found on page 2 of the "Managed Security" section on the Lumen Service Assurance Escalation Matrix website http://lumen.com/repairescalations.

To learn more about Lumen® DDoS Hyper, please visit the https://www.lumen.com/login/ or contact your sales representative.