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 a large amount of traffic to a targeted organization's network with the goal of disrupting internet connections, systems or applications or making them unavailable.

Lumen® DDoS Hyper can solve this problem by rerouting customer traffic through our global scrubbing centers for cleaning. Attack traffic is filtered out and legitimate traffic is sent back to the customer via GRE tunnel or an integrated Lumen Internet connection via Internet Direct. The service can protect both Lumen and third-party internet circuits. Additional 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, duration and frequency 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.

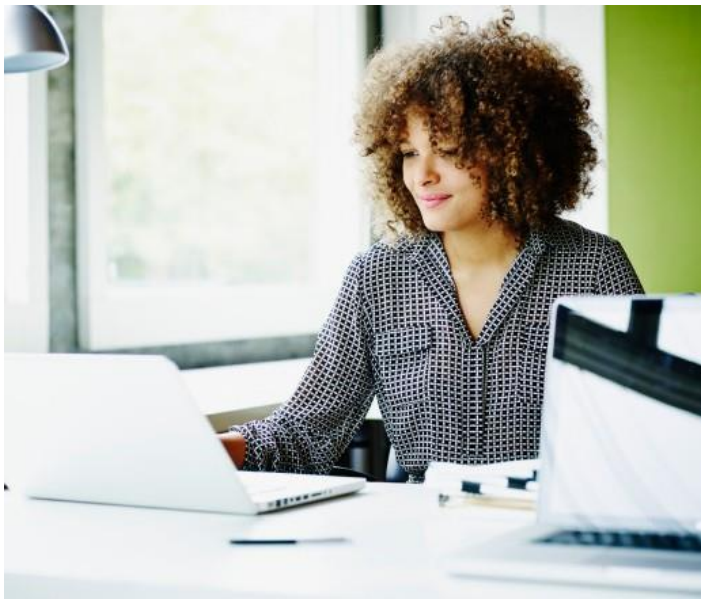
Q **How is Lumen® DDoS Hyper delivered?**

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 clean traffic is returned to the customer via GRE tunnels or, for Lumen Internet customers, via Internet Direct.

DDoS services can be consumed On-Demand and Always-On and are supported by our nine 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 third-party internet services
- Clean traffic return via Internet Direct for Lumen DIA customers
- Up to 100 Gbps of clean traffic return
- Up to 10 clean traffic return paths and 10 Flow-Based Monitoring instances; up to 50 CTRPs and FBM for an additional charge
- Optional SOC Advanced Support Services for an additional charge, providing run book 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 when internet is not provided by Lumen, 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 IP address space of at least /24 or larger.

If you have eligible Lumen Internet Service, DDoS Hyper requires a router with either BGP static or directly connected configuration. Lumen can protect subnets smaller than /24 when provided by Lumen.

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) or Lumen Internet circuits and information needed to collect Netflow from your CPE or Lumen edge router.

*Support for DDoS Hyper with the Lumen Managed Router is available only with On-Demand DDoS Hyper service using Internet Direct clean traffic return with either BGP or static WAN IP routing configuration.

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.

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

Do all Lumen Internet service options work with Lumen® DDoS Hyper?

Lumen offers an integrated clean traffic return delivery option with DDoS Hyper when using Lumen Internet. This advanced capability is available on a subset of Lumen Internet services. For Lumen Internet services that do not support an integrated clean traffic return delivery, you use a carrier agnostic method such as GRE for clean traffic return. The exceptions below are a few reasons why Internet Direct may not be currently available for the selected return path and the GRE clean traffic return may be a good temporary option.

- Change order in progress
- Return path is a public BGP peer with anything other than AS3356
- You have a Lumen managed router that requires Always-On DDoS mitigation instead of an On-Demand model.

For the below exemptions you can contact your account team for manual installation options or select to use the GRE method.

- Managed Router with Aways-On mitigation or managed router with On-Demand on the selected DIA service with other than BGP or static routing (requires manual installation)
- IPv4 not on the selected circuit (requires manual installation)
- Lumen Internet with BGP or static routing or directly connected with a WAN interface other than /27 though /31

What is Web Application Firewall (WAF) and why should I add it onto my DDoS Hyper service?

A: Lumen Application Protection provides layer 7 protection designed to protect your web facing assets against bot attacks, API abuse, vulnerability exploit attacks, and more. By bundling WAF with your DDoS Hyper service, you enable holistic web protection.

For additional information, view our DDoS Hyper + Application Protection brochure.

How quickly does Lumen® DDoS Hyper mitigate attacks?

The service is monitored 24/7 by Lumen global SOCs with most known forms of attack being mitigated in seconds after the 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 this is the first mitigation, the customer will need to contact the SOC for initial set-up. 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 DDoS and Web Application web page or contact your sales representative.

Ready to get started?

Log in to Control Center to make a purchase, track orders or call/chat with our dedicated customer support.

Visit Control Center
https://www.lumen.com/login