Lumen® DDoS Essentials for Intelligent Internet

Network-embedded, intelligence-driven protection designed to safeguard Intelligent Internet availability from volumetric attacks

Lumen® Intelligent Internet built for scale, resilience, and security

Lumen® Intelligent Internet delivers a **programmable, digital internet experience** that combines term-based cost predictability with elastic capacity that can be activated and scaled in minutes, giving organizations control over bandwidth, performance, and spend. Built on Lumen's global internet backbone, Intelligent Internet gives organizations real-time control over bandwidth, performance, and spend, providing an intelligent foundation for modern digital operations.

As organizations scale bandwidth on demand and expose more applications to the internet, they can also face **large-scale volumetric attacks** designed to overwhelm connectivity itself. These attacks can saturate circuits before customer-managed security tools or firewalls ever see the traffic.

Lumen® DDoS Essentials is a simple, cost-effective security add-on designed to complement Intelligent Internet by protecting elastic bandwidth from volumetric attacks as it scales. Enabled directly through **Lumen Connect®**, it delivers automated, network-embedded protection against common volumetric DDoS attacks, leveraging threat intelligence from the Lumen global network and **Black Lotus Labs®**, with fast time-to-value and minimal operational overhead.

Network-embedded DDoS protection that acts upstream

DDoS Essentials is built to complement Intelligent Internet, not complicate it. Protection is embedded directly into the Lumen tier-1 internet backbone, leveraging one of the world's most connected networks[1] as a **global sensor grid** to detect and mitigate volumetric attacks **upstream, before malicious traffic reaches customer circuits.**

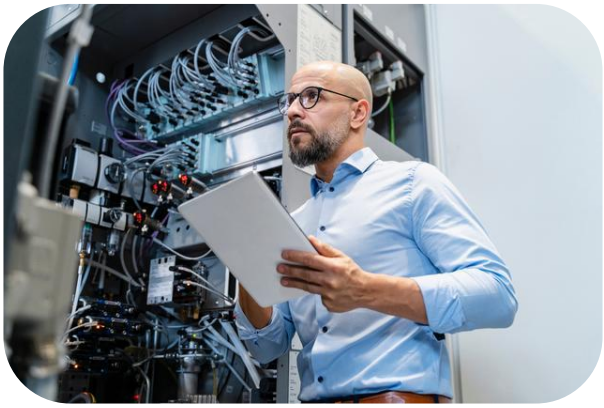
Lumen® Rapid Threat Defense from **Black Lotus Labs®** informs Lumen DDoS mitigation scrubbers with internet-scale threat intelligence, while near real-time behavioral detection is simultaneously applied to automatically protect your network upstream, **without additional appliances, network redesign, or specialized security expertise.**

The expected result is cleaner traffic reaching the customer environment, preserved service availability, and reduced strain on downstream security controls. As the first layer of a holistic security approach, DDoS Essentials is designed to mitigate volumetric floods at the circuit level and **works alongside services like Lumen Defender℠** to block other malicious traffic before it reaches customer environments.

Key benefits

Simple, Scalable Protection:

- **Safeguards Intelligent Internet availability** from common volumetric DDoS attacks
- **Automated, always-on mitigation** driven by network-level threat intelligence, with no customer action required
- **Network-embedded protection that scales** seamlessly with on-demand bandwidth
- **Simple add-on ordering and management** through Lumen Connect
- **Cost-effective protection** designed to reduce operational and security overhead

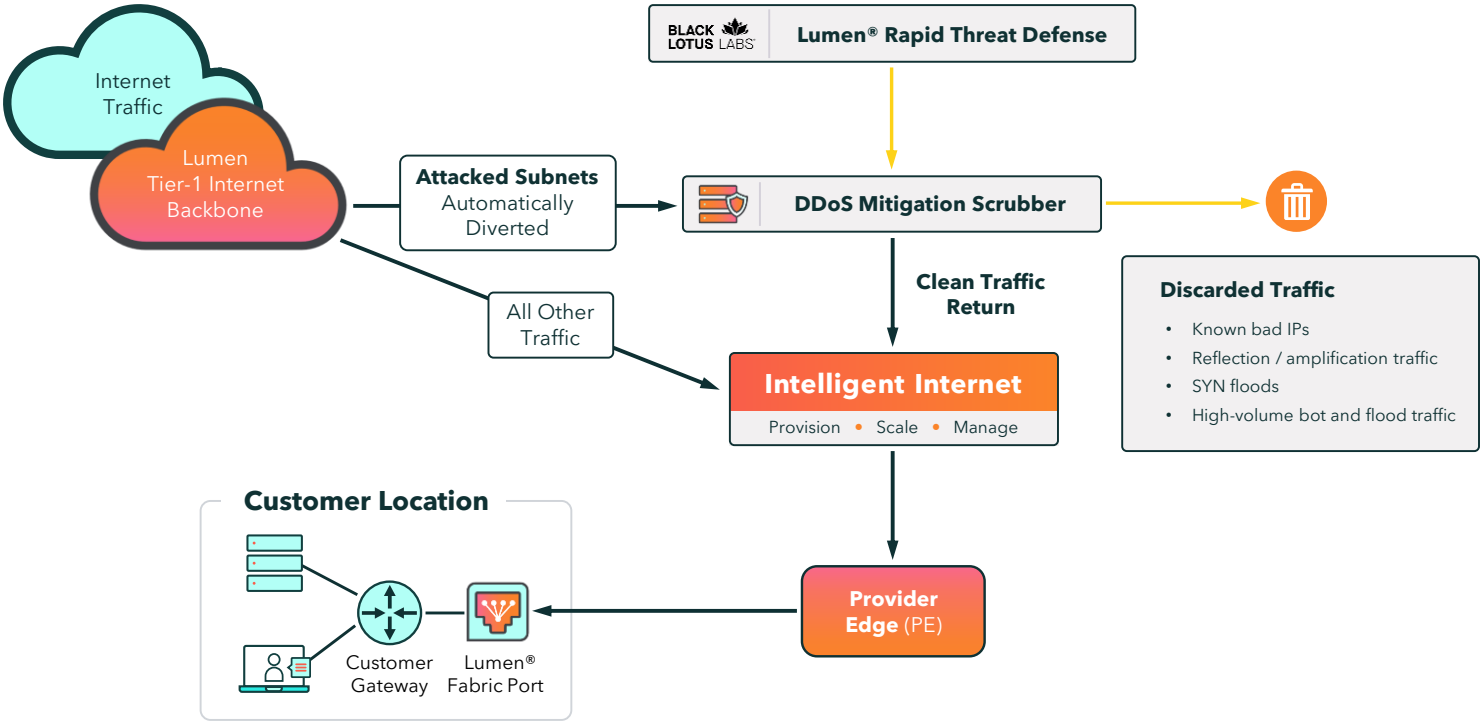


[1] The Center for Applied Internet Data Analysis (CAIDA), AS Rank, January 2025.

LUMEN® TECHNOLOGIES

Lumen® DDoS Essentials for Intelligent Internet

Network-embedded multi-layered volumetric protection powered by Black Lotus Labs® intelligence.



How DDoS Essentials works

Lumen® DDoS Essentials provides **network-embedded volumetric protection** for Intelligent Internet by continuously monitoring traffic within the Lumen tier-1 internet backbone. Using backbone-derived threat intelligence from the **Lumen® Rapid Threat Defense** feed powered by **Black Lotus Labs®**, along with near real-time behavioral analysis of customer traffic, the service identifies abnormal traffic patterns associated with large-scale volumetric DDoS attacks closer to the source, before customer circuits are overwhelmed.

When a volumetric attack is detected on a customer subnet, **affected traffic is automatically diverted upstream within the Lumen network** to DDoS mitigation scrubbers. Automated countermeasures are applied to neutralize the attack, while legitimate traffic is preserved and forwarded.

Once mitigation is in place, **clean traffic is automatically returned to the customer's Intelligent Internet connection**, protecting valuable bandwidth and performance without customer intervention. All other non-impacted traffic continues to flow normally.

DDoS Essentials operates as the **first layer of a layered, network-embedded security approach**, stopping volumetric floods before they reach customer circuits and **complementing services like Lumen Defender℠**, which block known malicious actors that generate noise and operational burden for security teams downstream.

866-352-0291 I lumen.com I info@lumen.com

LUMEN® TECHNOLOGIES

Why Black Lotus Labs®

See more. Stop more.®

Black Lotus Labs® is Lumen's dedicated threat research and intelligence organization, uniquely embedded within the Lumen-operated global network. Because Lumen owns and operates one of the world's most deeply peered networks,[1] Black Lotus Labs can observe threat activity at internet scale with unmatched visibility.

That intelligence is fed directly into Lumen's **network-embedded security services**, including **DDoS Essentials**, enabling automated, upstream detection and mitigation of malicious traffic **before it reaches customer environments**. The expected result is faster response, reduced disruption, and lower operational overhead for Intelligent Internet customers.

What DDoS Essentials mitigates

DDoS Essentials mitigates common Layer 3 and Layer 4 volumetric attack types that can overwhelm internet links and disrupt service availability, focusing on attacks that must be stopped upstream of the customer edge:

- **UDP reflection and amplification attacks:** High-bandwidth floods generated by abusing open internet services (for example, DNS or NTP), designed to saturate network capacity. These attacks are detected and blocked upstream to prevent circuit exhaustion before traffic reaches downstream controls.
- **TCP SYN floods:** Connection-exhaustion attacks that overwhelm servers or network devices with incomplete TCP handshakes, exhausting connection-tracking resources and impacting availability.
- **Traffic from known malicious sources:** IP addresses and infrastructure identified through network-wide backbone visibility by **Black Lotus Labs®** threat intelligence are automatically dropped when mitigation is active, **enabling faster suppression than approaches limited to individual customer traffic patterns**.

Who should add DDoS Essentials

DDoS Essentials is a **network embedded security add on designed for Intelligent Internet customers** who want to protect internet availability as they scale without adding infrastructure or operational complexity.

It is well suited for:

- Any critical application where consistent on-demand connectivity is needed
- Lean IT or security teams that prefer automated, always on protection
- Organizations seeking affordable, upstream DDoS mitigation for common volumetric attack scenarios

Delivered as a native capability of the Lumen network and informed by Black Lotus Labs® threat intelligence, DDoS Essentials is always on, automated, and scales seamlessly with Intelligent Internet bandwidth, making it easy to add, simple to operate, and cost effective.

Why Lumen?

Lumen delivers Intelligent Internet, as part of a **Network-as-a-Service (NaaS) platform**, built on one of the world's most deeply embedded and highly peered IP networks. That global network foundation gives customers the scale, reach, and performance to provision and scale internet connectivity in minutes, while maintaining control as demand changes.

Security is embedded directly into that foundation. By operating the network itself, Lumen can observe traffic patterns at internet scale and act on threats **upstream, before they reach customer environments**. This capability is powered by **Black Lotus Labs®,** Lumen's dedicated threat research organization, which continuously analyzes backbone-level telemetry to identify and classify malicious activity.

Services like **Lumen® DDoS Essentials** operationalize this intelligence within the network, delivering automated, upstream mitigation of volumetric attacks as a native extension of Intelligent Internet. The result is a simplified, intelligence-driven security posture that protects availability as bandwidth scales, without added infrastructure, configuration, or operational complexity.

[1] The Center for Applied Internet Data Analysis (CAIDA), AS Rank, January 2025.

866-352-0291 I lumen.com I info@lumen.com

LUMEN® TECHNOLOGIES