Technical FAQ

Lumen® Internet On-Demand with DDoS and Defender℠

This document is intended for organizations evaluating or operating Internet On-Demand with optional Lumen® DDoS Essentials and/or Lumen® Defender℠ security add on services. Service features and functionality described below are provided subject to the applicable service agreements and service descriptions.

High Level Technical FAQs

What security services are available for Internet On-Demand?

- Internet On-Demand supports two optional Lumen network-embedded security services enforced within the Lumen backbone.
- **Lumen DDoS Essentials** – designed to protect availability by mitigating large scale volumetric DDoS attacks upstream within the Lumen Tier-1 Internet Backbone.
- **Lumen Defender℠** – designed to block known malicious internet-based threats based on traffic direction and threat classification. This service is available in the two following service tiers:
  - **Defender Essentials** provides continuous blocking of known severe-risk malicious internet-based threats.
  - **Defender Plus** builds on Essentials by adding enhanced visibility and customer-controlled allow/block lists through Lumen Connect.

Can DDoS Essentials and Lumen Defender be used together?

Yes. These services are designed to be complementary:

- DDoS Essentials helps mitigate high volume floods that overwhelm Internet On-Demand circuits.
- Lumen Defender (Essentials and Plus) is built to block known malicious IPs, bots, and command-and-control infrastructure.

When used together, these services operate in concert to support a layered, upstream security approach, that are designed to reduce unwanted traffic reaching Internet On-Demand connectivity.

What does "network embedded security" mean?

Network embedded security refers to enforcement that occurs within the Lumen Tier-1 Internet Backbone and provider-edge infrastructure, upstream of the customer's Internet On-Demand connection. This approach is intended to complement downstream security controls, appliances, tunnels, or overlays to allow certain threats to be addressed early in the traffic path, and designed to help reduce downstream operational complexity.

Where does security enforcement occur?

Security enforcement occurs within the Lumen Tier 1 Internet Backbone, upstream of the customer edge, using provider edge routing and network embedded security infrastructure.

Is traffic tunneled or redirected to a third party for inspection?

No. Traffic is not tunneled or redirected to third-party service clouds or overlays managed outside the Lumen network. Security enforcement is provided using Lumen-owned and operated infrastructure deployed within the Lumen network. Lumen may use

third-party technology components in delivering the services; however, traffic inspection and mitigation occur within the Lumen network and customer traffic is not shared with external providers. Mitigation and filtering occur within the Lumen network, to preserve routing symmetry and predictable performance.

What happens during a DDoS attack or threat event?

- DDoS Essentials is designed to automatically divert volumetric attack traffic upstream for mitigation to return clean traffic toward the Internet On-Demand connection.
- Lumen Defender is designed to block severe-risk malicious traffic upstream based on threat intelligence and traffic direction.

These services include automatic protections while operating under a shared responsibility model, which may require review and action based on organizational security posture and service configuration.

Does Lumen Defender inspect or decrypt customer traffic?

No. Lumen Defender does not decrypt traffic or inspect application payloads. Filtering decisions are made at the IP and network level using threat intelligence-driven techniques. Encrypted traffic remains encrypted end to end, and modern protocols such as TLS, QUIC, and HTTP/3 are supported.

Are changes required to enable these services?

No. Enabling DDoS Essentials or Lumen Defender does not require IP address changes, routing or BGP changes, on-premises configuration changes, or additional hardware or appliances. For environments using RPKI with Lumen Defender Plus, updates to ROA entries may be required to allow advertisement of routes associated with Lumen's AS 203.

Are there bandwidth or configuration limitations?

Yes, and they vary by service:

- Lumen DDoS Essentials scales dynamically with Internet On-Demand bandwidth and has no fixed bandwidth ceiling.
- Lumen Defender (Essentials and Plus) is supported on Internet On-Demand connections from 100 Mbps up to 1 Gbps.
- Lumen Defender is not currently supported on IPv6 only or dual stack Internet On-Demand configurations.
- Availability may vary by service area and port eligibility.

What visibility do customers have into security activities?

Organizations may have access to logging and summary-level reporting that reflects mitigation or blocking activity. Visibility varies by service:

- DDoS Essentials – high-level insight into mitigation events affecting availability.
- Defender Essentials – summary reporting for automatically blocked severe-risk threats.
- Defender Plus – enhanced logging, visibility, and customer-managed policy controls via Lumen Connect.

Does this replace customer firewalls, SD WAN, or SASE platforms?

No. These services are designed to complement—not replace customer managed firewalls, SD WAN, SASE, or other downstream security controls by reducing unwanted or malicious traffic before it reaches those systems.

Does this architecture impact latency or throughput?

Under normal conditions, latency impact is expected to be negligible. Because enforcement occurs upstream in the backbone and does not require tunneling or customer side processing, traffic follows optimized network paths. During attacks, clean return paths remain within the backbone to preserve predictable performance for legitimate traffic.

What happens if a security component becomes unavailable?

DDoS Essentials and Defender Plus are delivered over a redundant, distributed network architecture. If an individual enforcement node, location, or system becomes unavailable, traffic is automatically handled by other enforcement points within the Lumen network to support service availability and continuity.

What is this security model not designed to do?

This model is not designed to:

- Perform Layer 7 application inspection
- Replace customer firewalls, WAFs, or endpoint security
- Provide SLA-backed mitigation guarantees
- Support customer-tuned or manually-triggered mitigation workflows

Use cases requiring these capabilities should evaluate advanced DDoS mitigation or application-level security services.

Persona Specific Technical FAQs (Additional Questions by Role)

CIO / CISO FAQs

How are Internet On-Demand security services (DDoS Essentials and Lumen Defender) designed to reduce enterprise risk?

By applying baseline DDoS mitigation and threat-blocking controls at the internet access layer, certain attack types are addressed upstream, supporting availability and to reduce unnecessary malicious traffic reaching Internet-facing connectivity.

Who is accountable during incidents?

Security services operate under a shared responsibility model. Lumen is responsible for operating and maintaining Internet On-Demand, DDoS Essentials, and Defender services as defined in the applicable service documentation. Responsibility for application-level security, identity controls, and policy decisions remains with the organization.

IT & Network Operations FAQs

Who operates and maintains the security services?

Lumen operates and maintains the DDoS Essentials and Defender platforms, including infrastructure operations, threat intelligence updates, and service monitoring. Policy configuration and response workflows may apply for Defender Plus deployments.

What should operations teams do if an application is unreachable?

Application health and configuration should be validated first, followed by review of relevant security indicators. Lumen support may be engaged if network-level security involvement is suspected.

Cloud Architect FAQs

How do security services for Internet On-Demand fit into hybrid and multi-cloud designs?

Security services for Internet On-Demand are enforced at the network level within the Lumen backbone, upstream of the Internet On-Demand connection. This approach supports consistent protection for internet-facing traffic used by hybrid, multi-cloud, SaaS, and API-based architectures regardless of workload location.

Is security enforced at the network level rather than relying on cloud specific or cloud native security services?

Yes. Security enforcement occurs at the network level within the Lumen backbone, upstream of the Internet On-Demand connection, rather than relying on cloud specific or cloud native security services. This enables consistent protection across single cloud, hybrid, and multi-cloud deployments.

Application Owner FAQs

Will legitimate users be blocked?

Blocking is focused on severe-risk malicious traffic classifications and is designed to minimize impact to legitimate users. Defender Plus provides additional visibility and policy controls for managing higher-risk but non-severe traffic categories.

Do customer application changes need to be coordinated?

No customer application changes or deployment coordination are required.

Software Developer FAQs

Do applications require code changes?

No. These services do not modify payloads, inject headers, or depend on application frameworks.

Does this affect CI/CD pipelines or deployment workflows?

No. Because traffic handling occurs at the network layer, application deployment processes are unaffected.

Procurement & Sourcing FAQs

How are Internet On-Demand and its security services priced?

Internet On-Demand uses a consumption-based pricing model. DDoS Essentials and Lumen Defender are add-on services priced per Internet On-Demand connection or port, as specified in the applicable service order, with predictable tier-based pricing and no per-attack or surge charges.

Are there risks of unexpected costs during attacks?

No. Costs for DDoS Essentials and Lumen Defender do not increase during attack events or traffic spikes.

Compliance, Risk & Audit FAQs

Does this expand compliance scope for regulated workloads?

Because traffic is not decrypted, stored, or inspected at the application layer, these services generally do not expand compliance scope. Customers remain responsible for application-level security and compliance controls.

How should this be documented for audits?

These services may be documented as upstream, network level protective controls that improve availability without accessing application data.

Why Lumen?

Lumen is unleashing the world's digital potential. We ignite business growth by connecting people, data, and applications – quickly, securely, and effortlessly. As the trusted network for AI, Lumen uses the scale of our network to help companies realize AI's full potential. From metro connectivity to long-haul data transport to our edge cloud, security, managed service, and digital platform capabilities, we meet our customers' needs today.

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