Lumen Defender℠ for Internet On-Demand

Network-embedded, intelligence-driven threat blocking designed to reduce noise, improve efficiency, and protect Internet On-Demand traffic

Lumen® Internet On-Demand built for scale, resilience, and security

Lumen® Internet On-Demand redefines dedicated internet access by delivering a **consumption-based connectivity experience** that is rapidly activated, and dynamically scalable. Built on Lumen's global internet backbone, Internet On-Demand gives organizations real-time control over bandwidth, performance, and spend, providing an intelligent foundation for modern digital operations.

As organizations scale connectivity on demand and expose more applications to the internet, they can encounter a steady stream of **internet-based threats**: bots, scanning activity, command-and-control infrastructure, and other malicious actors that not only create noise and operational burden, but also increase risk of compromise and downstream security incidents.

Lumen Defender℠ is a simple, network-embedded security add-on designed to complement Internet On-Demand by blocking known malicious internet-based threats at the network edge. Enabled through **Lumen Connect℠**, it delivers automated threat blocking powered by intelligence from the Lumen global network and **Black Lotus Labs®**, enabling reduced risk and operational noise with minimal overhead. Lumen Defender Essentials and Plus offer tiered levels of visibility and control.

Network-embedded protection that acts upstream

Lumen Defender is built directly into the Lumen tier-1 internet backbone, leveraging one of the world's most deeply peered networks[1] as a **global sensor grid**. Informed by threat intelligence from **Black Lotus Labs®,** this visibility enables Lumen to identify known malicious actors with high confidence and enforce protection **upstream within the network**, before traffic impacts customer environments.

Unlike customer-premises firewalls or cloud-only tools that react after traffic arrives, Lumen Defender blocks bad traffic **at the network edge**, helping reduce unwanted traffic delivered to Internet On-Demand connections, **without additional appliances, tunneling, or security infrastructure**.

By removing malicious traffic early, Lumen Defender helps reduce noise and false positives for downstream firewalls, SIEMs, and SOC tools, improving operational efficiency and reducing alert fatigue. When combined with **Lumen® DDoS Essentials, this helps form a more complete network- embedded security posture** by mitigating volumetric attacks and blocking known malicious actors upstream.

Key benefits

Network-embedded threat blocking that is designed to improve security efficiency:

- **Blocks known malicious internet-based threats** before traffic impacts customer environments
- **Helps reduce noise and alert fatigue** by removing known-bad traffic at the network edge
- **Powered by Black Lotus Labs® threat intelligence**, leveraging backbone-level visibility
- **Always-on, automated protection** delivered without additional hardware
- **Simple add-on enablement, configuration, and reporting visibility** through Lumen Connect℠

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

LUMEN® TECHNOLOGIES

Lumen Defender Essentials

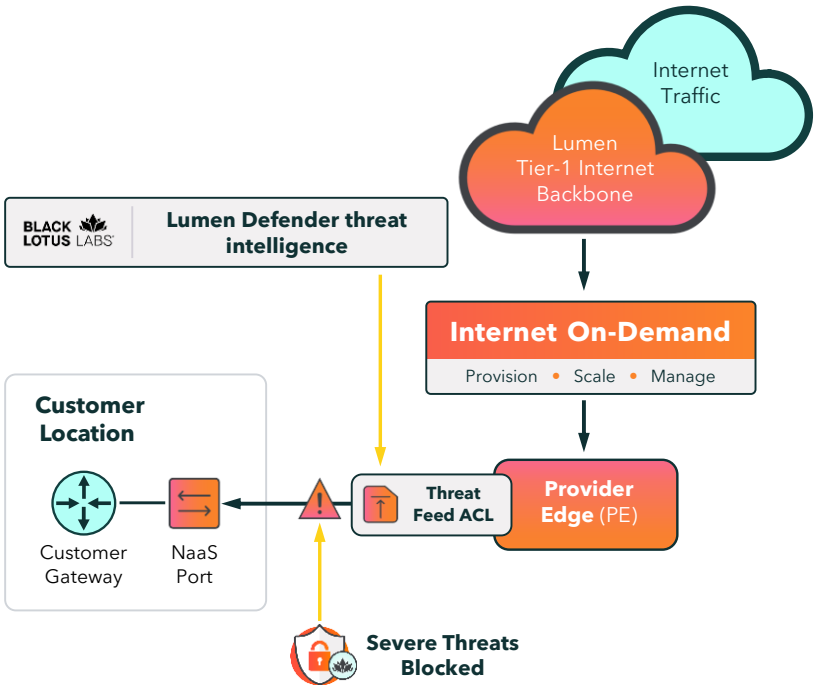
Always-on blocking of severe threats

Lumen Defender Essentials uses the Lumen Provider Edge (PE) routers as a filtering point, applying a **Black Lotus Labs®** tier-1 internet-backbone-derived **severe threat feed** as an ingress access-control list (ACL) on the Internet On-Demand circuit. This prevents customer networks from responding to known severe-risk IPs.

Key characteristics:

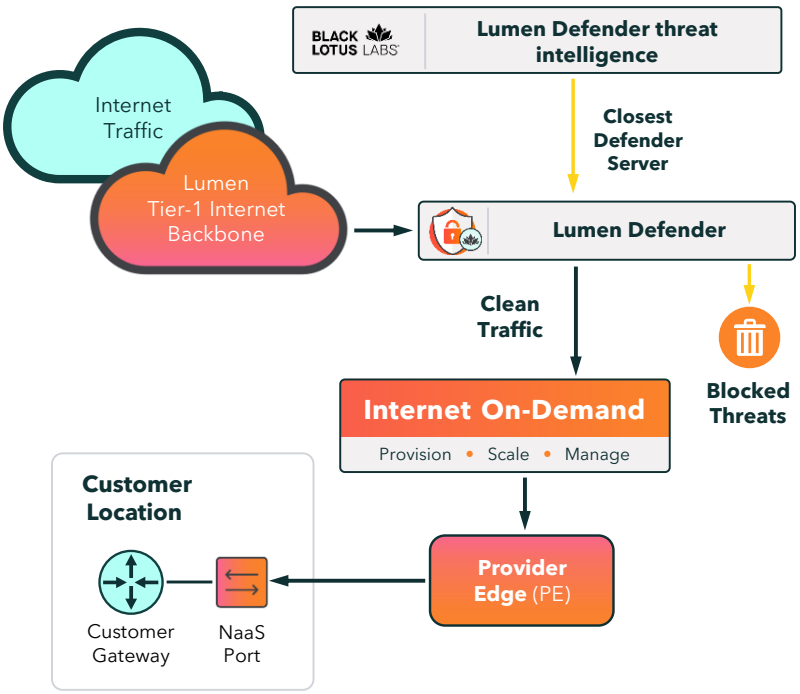
- Blocks **severe-risk threat actors**
- Always on, fully automated
- No customization required
- Block lists are updated approximately every fifteen minutes

Defender Essentials is ideal for customers who want simple, baseline threat blocking designed to reduce noise and risk of compromise with minimal operational effort.



Lumen Defender Plus

Advanced, customizable threat filtering with clean-return architecture



Lumen Defender Plus provides deeper protection by diverting inbound traffic to the closest **Lumen Defender Servers** deployed within the Lumen network. These network-embedded resources intercept internet traffic, automatically block threats, and return filtered traffic over a **clean return network**.

Key characteristics:

- Filters inbound traffic **before it reaches the customer**
- **Supports multiple threat-severity thresholds** (severe, very high, high)
- Customer-controlled allow, block, and monitor lists
- More frequent threat feed updates (approximately every five minutes)

Defender Plus is ideal for customers who want **greater visibility, control, and operational insight** into what is being blocked, without deploying customer-side security infrastructure.

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

LUMEN® TECHNOLOGIES

Why Black Lotus Labs®

See more. Stop more.®

At the foundation of Lumen Defender is **Black Lotus Labs®**, a dedicated threat research and intelligence organization. Backbone-level telemetry is continuously analyzed across the Lumen-operated global network, using large-scale flow data, machine learning, and expert investigation to identify and classify malicious infrastructure.

This intelligence assigns risk scores to internet-based IP addresses and feeds **high-confidence threat intelligence** directly into Lumen Defender. Because this analysis is derived from the network itself, **Lumen can identify bad actors earlier and with greater confidence** than solutions that rely only on endpoint or application-level signals.

For customers, this means fewer false positives and more effective blocking of **traffic that has no legitimate reason to reach their network**.

What Lumen Defender protects against

Lumen Defender focuses on **known malicious internet-based threats** that generate risk, noise, and operational burden for Internet On-Demand customers. These threats often bypass volumetric controls and overwhelm downstream security tools if not addressed upstream, including:

- **Bots and automated attacks:** Infrastructure used to generate malicious traffic, probe networks, or participate in coordinated attack campaigns.
- **Proxy and anonymization services:** Hosts commonly used to obscure attacker identity and evade traditional perimeter controls.
- **Malware and command-and-control (C2) infrastructure:** Systems associated with malware distribution, botnet coordination, and remote attacker control.
- **Phishing, spam, and scanning activity:** Internet-based threats that generate constant background noise, reconnaissance attempts, and unnecessary alerts.

Who should add Lumen Defender

Lumen Defender is a **network embedded security add-on designed for Internet On-Demand customers** who:

- Want to reduce malicious traffic before it impacts customer environments
- Operate lean IT or security teams and prefer automated, zero-touch protection
- Struggle with alert fatigue and inefficient downstream security tools
- Want network-embedded security as part of a broader security strategy and posture

Delivered as a native capability of the Lumen network and informed by Black Lotus Labs® threat intelligence, Lumen Defender is easy to add, simple to operate, and designed to scale as connectivity and exposure grow.

Why Lumen?

Lumen delivers Internet On-Demand, 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 Defender℠** operationalize this intelligence within the network, delivering automated, upstream identification and blocking of threats as a native extension of Internet On-Demand. The result is a simplified, intelligence-driven security posture that protects availability as bandwidth scales, without added infrastructure, configuration, or operational complexity.

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

LUMEN® TECHNOLOGIES