Lumen® DDoS and Lumen Defender℠ Deployment Guide

Quick Start Guide to Securing Internet On-Demand in Lumen Connect℠

April 2026

LUMEN®

Table of contents

Why Add Security to Internet On-Demand?

Lumen® Internet On-Demand delivers a consumption-based, programmable internet experience that can be activated and scaled in minutes, giving organizations control over bandwidth, performance, and spend. Built on Lumen's globally interconnected IP backbone, it provides a modern foundation for digital operations that demand speed, flexibility, and scale.

As organizations scale connectivity and expose more applications to the internet, they may also face **volumetric attacks that threaten bandwidth availability**, along with a steady stream of **internet-based threats** such as bots, scanning activity, and command-and-control infrastructure that create noise and operational burden.

Lumen addresses both challenges by offering **network-embedded**, **on-demand security services** that integrate directly with Internet On-Demand:

- **Lumen® DDoS Essentials** helps to protect elastic bandwidth from volumetric DDoS attacks as connectivity scales.
- **Lumen Defender℠** blocks known malicious internet-based threats within the network, designed to reduce noise and improve security efficiency.

Because these services are delivered **within the Lumen network** and enabled through Lumen Connect℠, customers can add protection at the time of ordering Internet On-Demand, or to an existing connection, without deploying hardware or introducing operational complexity.

The following sections walk through how to add:

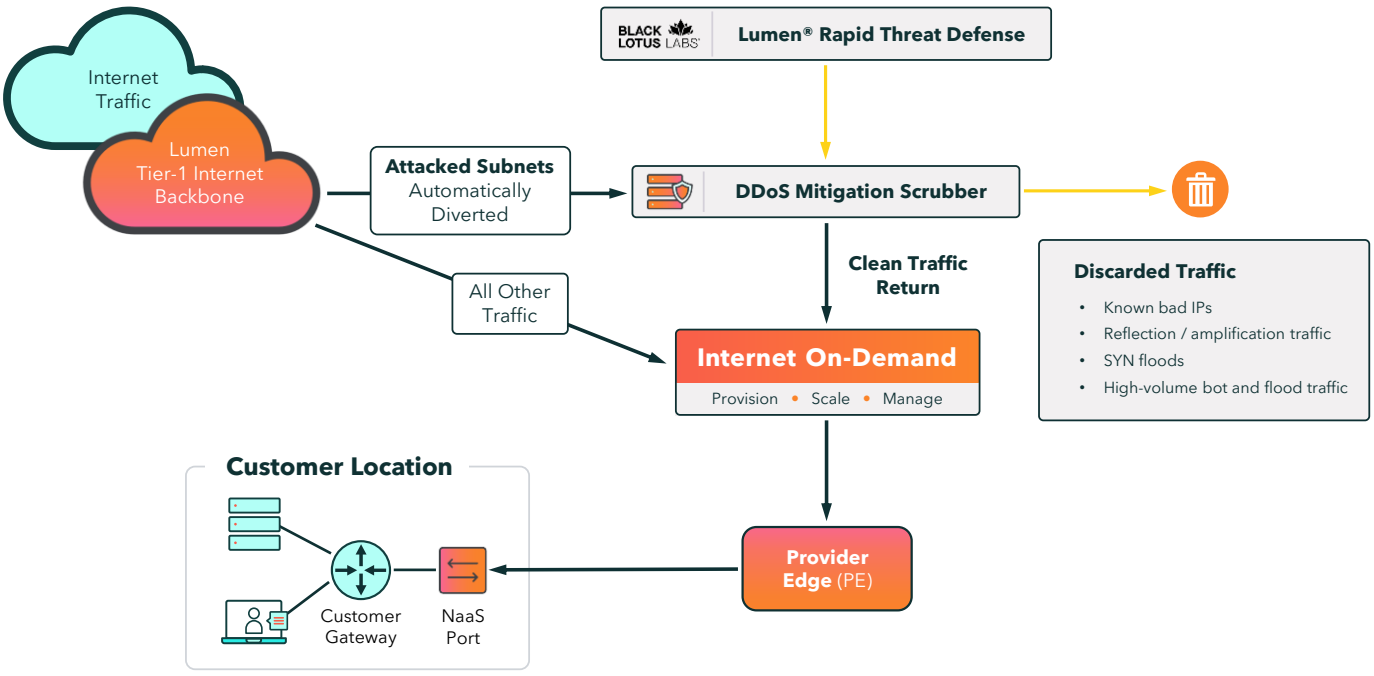
- Lumen® DDoS Essentials
- Lumen Defender℠ Essentials
- Lumen Defender℠ Plus
- Associated Monitoring & Reporting

Adding Lumen® DDoS Essentials to Internet On-Demand

What it does

Lumen® DDoS Essentials provides **automated, network-embedded protection against common volumetric DDoS attacks**, designed specifically for Internet On-Demand. As bandwidth scales dynamically, DDoS Essentials helps protect **elastic, on-demand connectivity** from attacks intended to overwhelm circuits before customer-managed security tools or firewalls ever see the traffic.

Mitigation occurs upstream within the Lumen Tier-1 internet backbone, leveraging threat intelligence from the Lumen global network and **Black Lotus Labs®**. This allows attacks to be detected and scrubbed closer to the source, helping preserve availability, minimize disruption, and reduce operational overhead. Because DDoS Essentials is delivered as an on-demand add-on, protection can be rapidly enabled, without deploying hardware or redesigning the network.



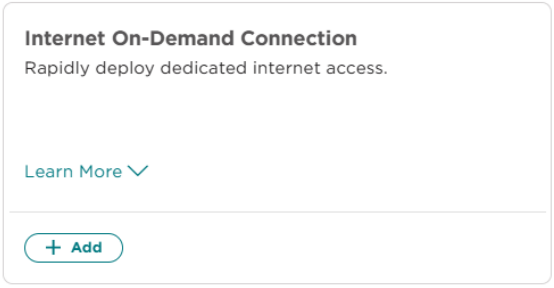
When to add it

- When ordering a **new Internet On-Demand connection** and you want to protect scalable bandwidth from volumetric attacks from day one
- When enhancing protection on an **existing Internet On-Demand connection** as application exposure or bandwidth usage grows

How to add DDoS Essentials to Internet On-Demand

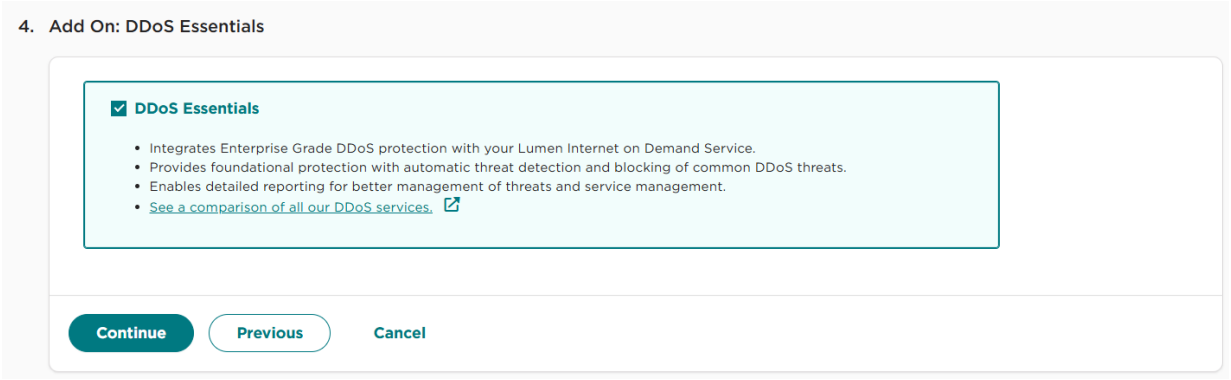
Adding DDoS Essentials to a new Internet On-Demand Connection

1. Sign in to **Lumen Connect℠**
2. Navigate to **Add Services** and select **Add** under Internet On-Demand Connection to add a new Internet On-Demand connection.

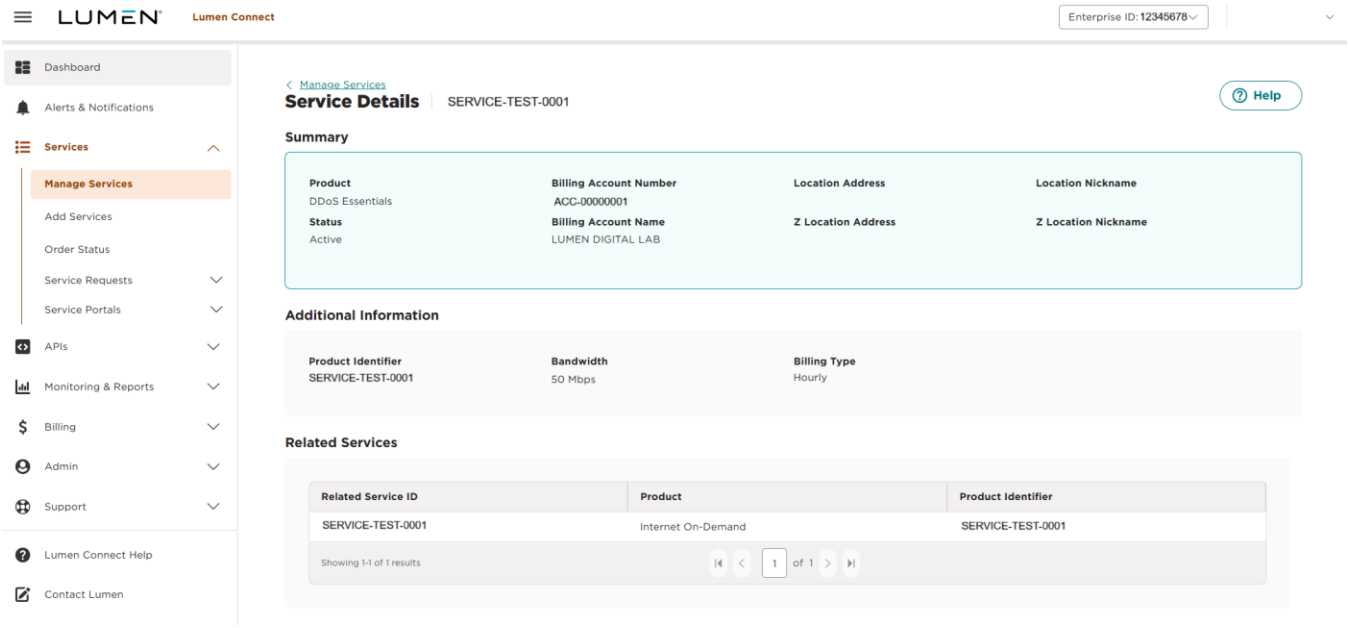


3. Select **DDoS Essentials** in **Step 4** of the Internet On-Demand ordering process to quickly add the service at the time of initial order.

   Note: DDoS Essentials is currently not available for IPv6 and Dual Stack.



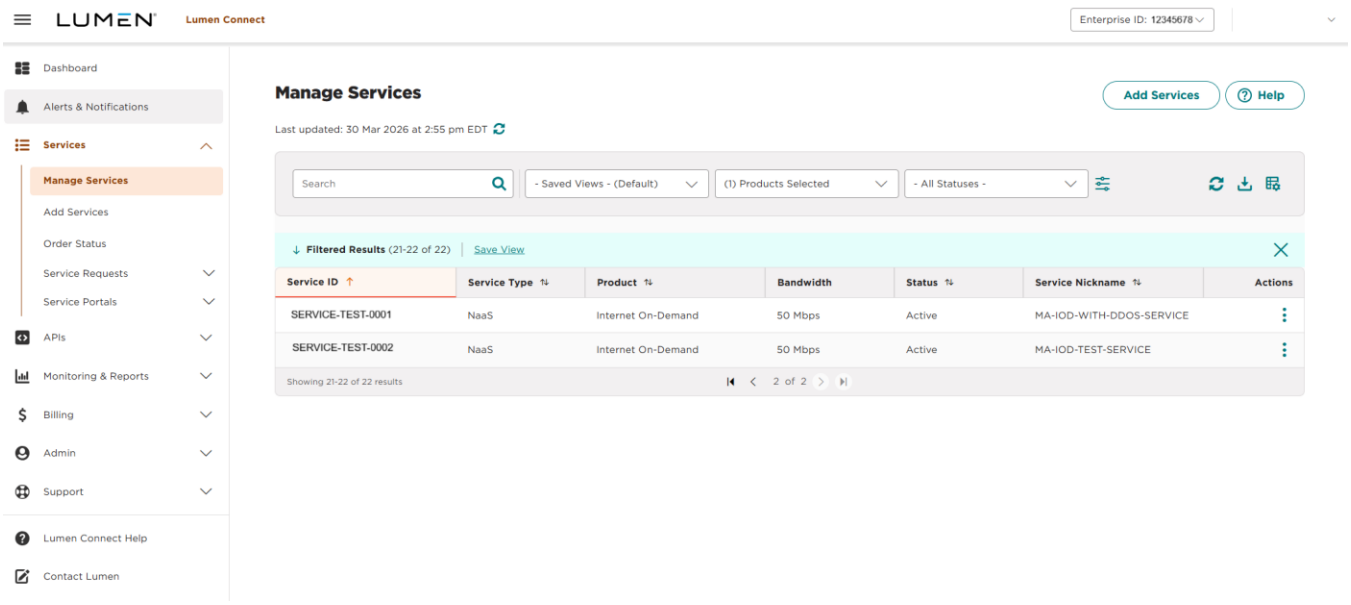
4. Review service details and pricing, **DDoS Essentials** will be in the **Security Add On** section.
5. Submit the Internet On-Demand order to create the service with DDoS Essentials enabled.
6. Once provisioning has been completed, navigate to **Manage Services**, and select the newly provisioned **DDoS Essentials Service** to see the details.



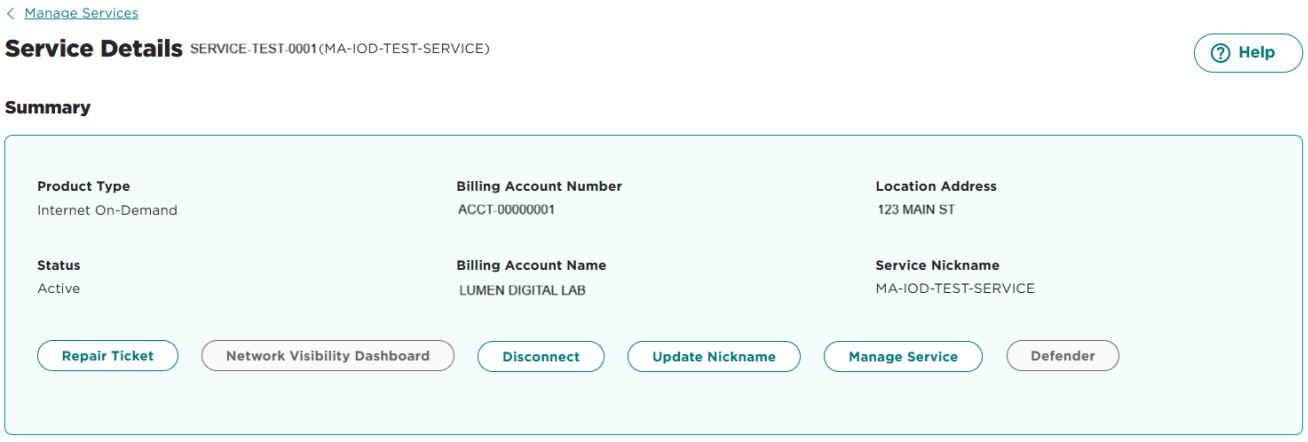
Adding DDoS Essentials to an existing Internet On-Demand Connection

1. Sign in to **Lumen Connect**[SM]

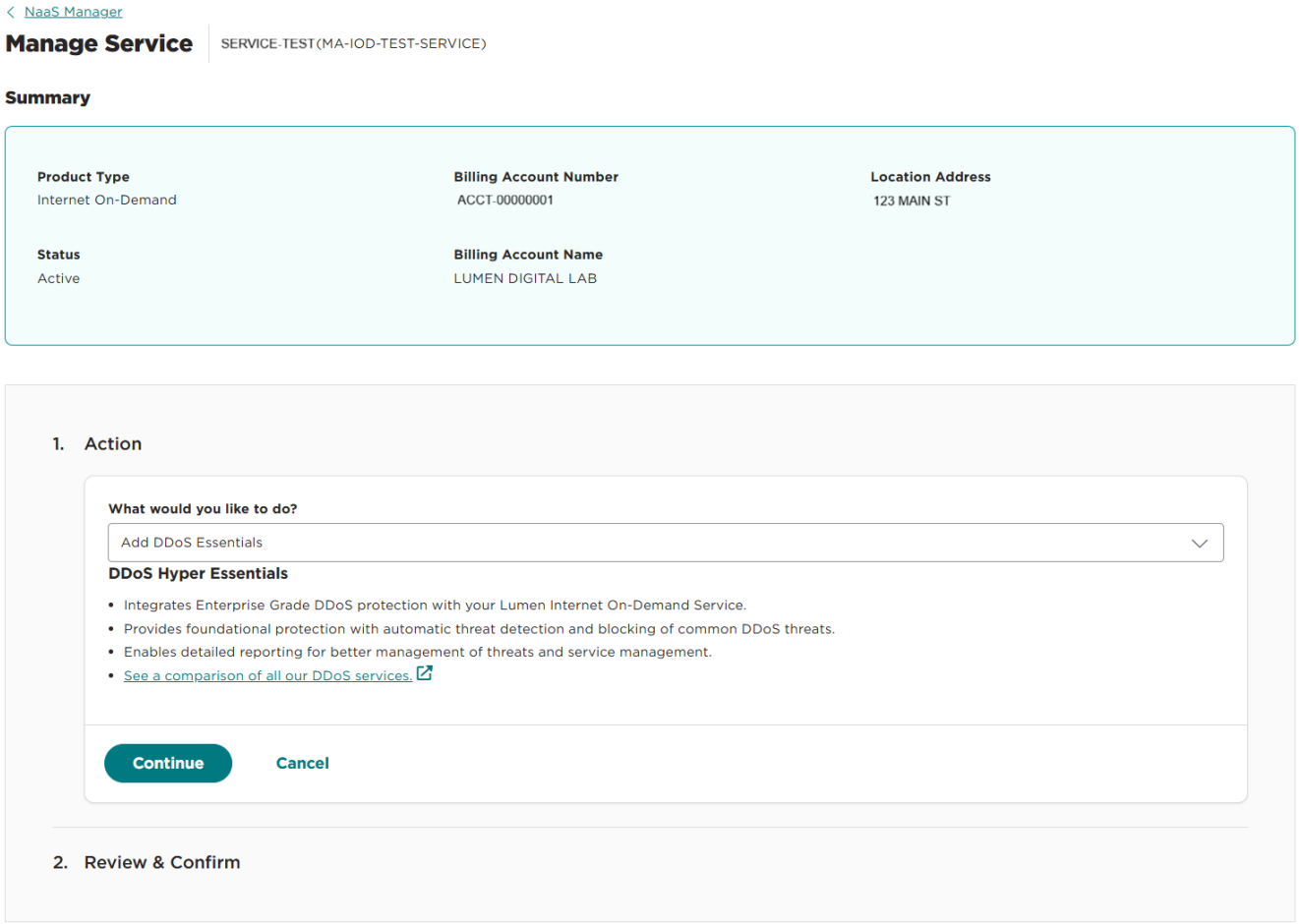
2. Navigate to **Manage Services** and select the specific Internet On-Demand connection to add DDoS Essentials to.



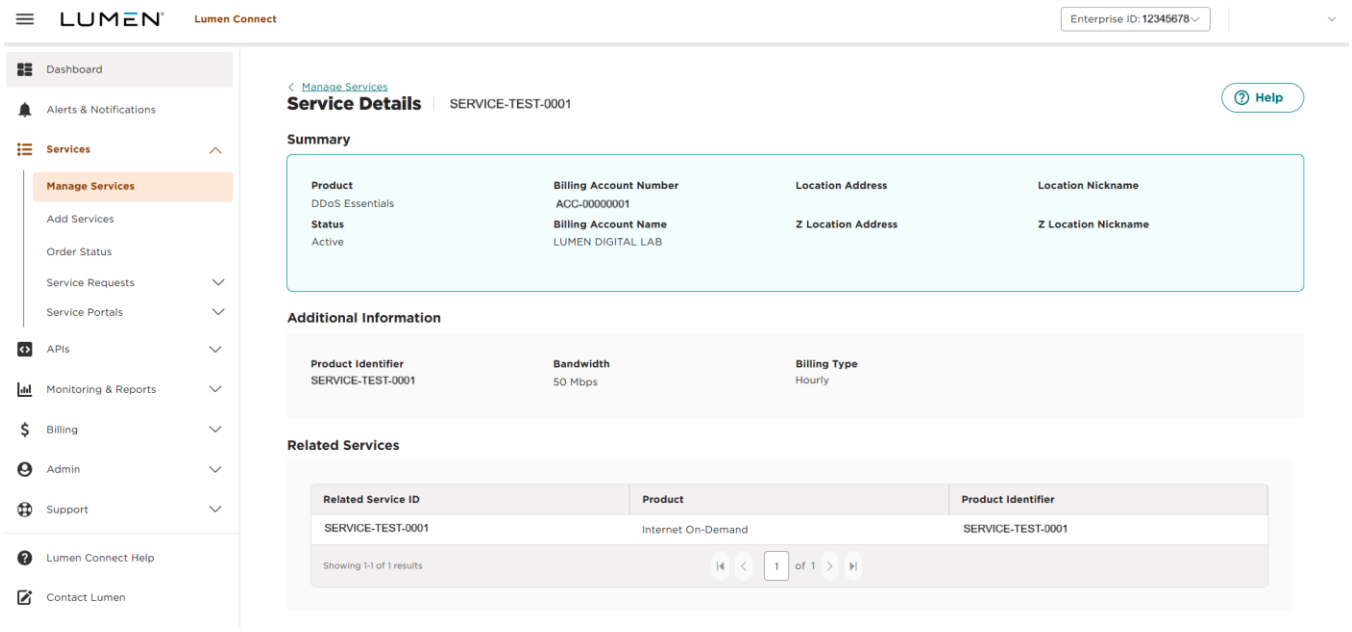
3. Click **Manage Service**.



4. In the Action section, select **Add DDoS Essentials**.
5. Review the notes and cost, then select **Continue**.



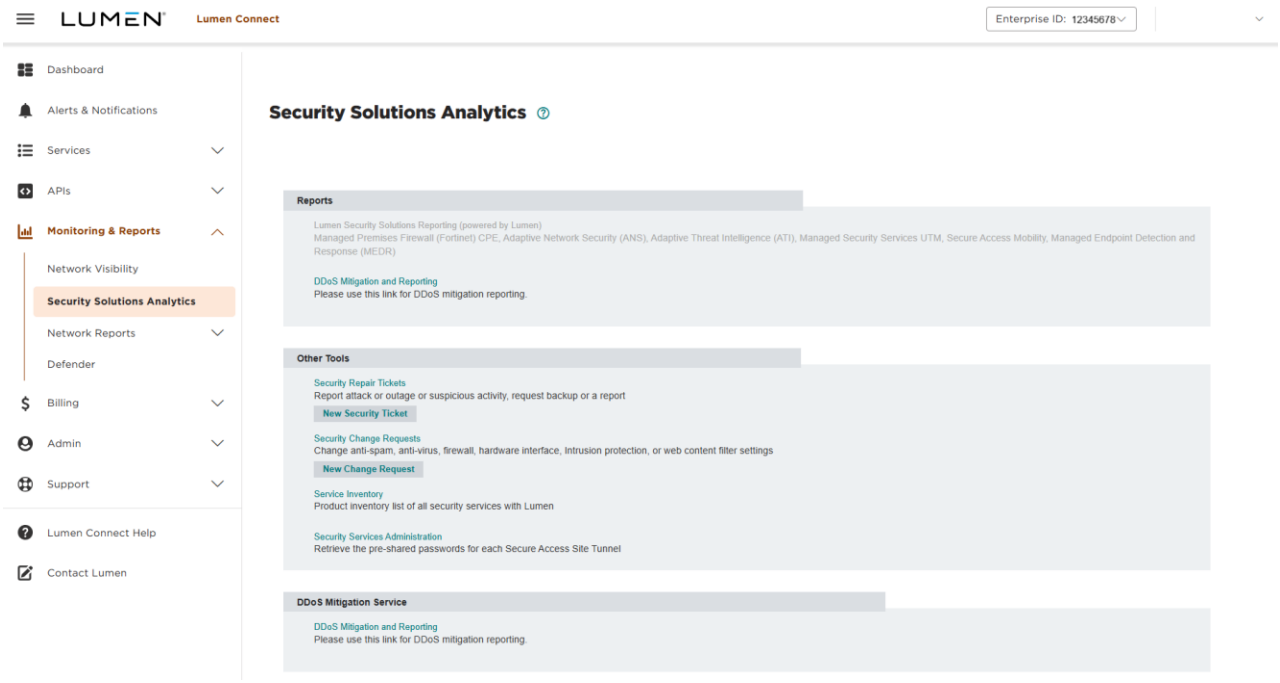
6. Select **Submit Order**.
7. The **Service Details** page for the Internet On-Demand connection will be displayed with activation progress and updated automatically once the new DDoS Essentials service is activated.
8. Once provisioning has been completed, navigate to **Manage Services**, and select the newly provisioned **DDoS Essentials Service** to see the details.



Lumen® DDoS Essentials Monitoring and Reporting

Lumen DDoS Essentials monitoring and reporting capabilities are accessible through **Lumen Connect℠**, providing customers with visibility into internet-based volumetric threats detected and mitigated at the Lumen network edge.

To access DDoS Essentials reporting from Lumen Connect℠, navigate to Monitoring & Reports, **Security Solutions Analytics**, and select **DDoS Mitigation and Reporting**.

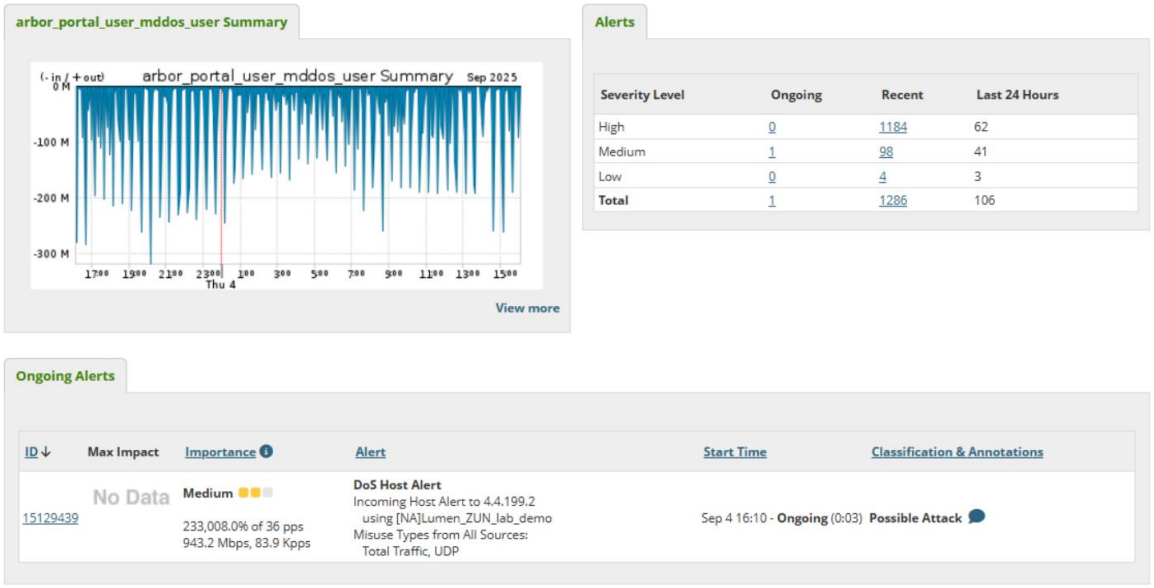


At the top of the landing page, you will see several headers that lead to various sections of the portal that each show different types of information.

- **Status:** Overview and landing page.
- **Alerts:** Focuses on current and previous alerts.
- **Traffic:** Shows various types of flow data that can be used for baselining and tuning thresholds.
- **Mitigation:** All things related to current and previous mitigation events, such as countermeasures applied, volume of traffic diverted, and scrubbing.
- **Administration:** User preferences and administration.

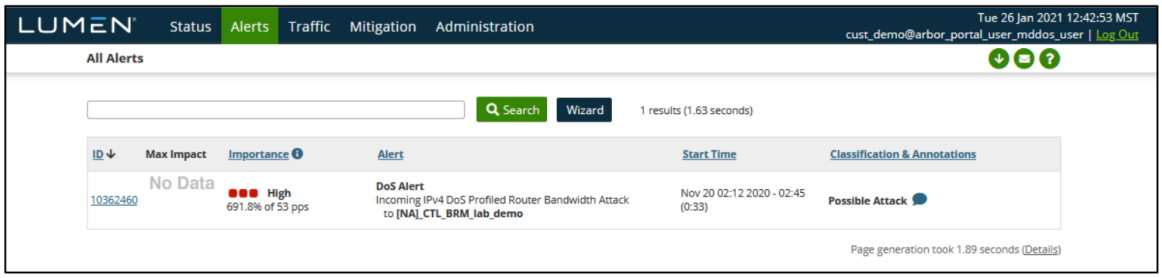
Status Page

The first page presented to the portal user is the DDoS Mitigation Reporting **Status dashboard**, which shows an overview of the flow data volume (used for monitoring and alerting), recent alerts and a list of any ongoing alerts.



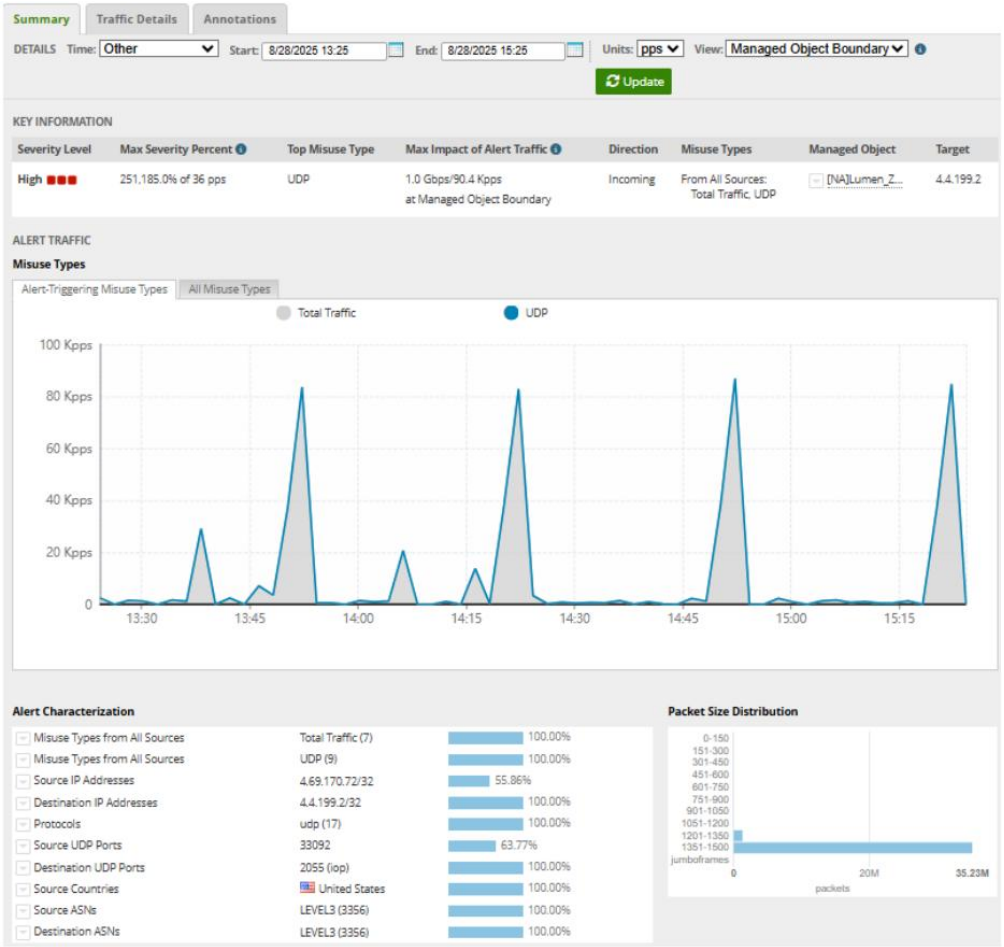
Alert Summary

DDoS Alerts can be viewed under **Alerts**, **All Alerts**, or by clicking on either the number of ongoing or recent alerts on the right side of the status page. Alerts are listed up to 10 per page and can be sorted in various ways by clicking on the column headers. The small graph shows the traffic rates for the affected destination IPs and for the duration of the alert.



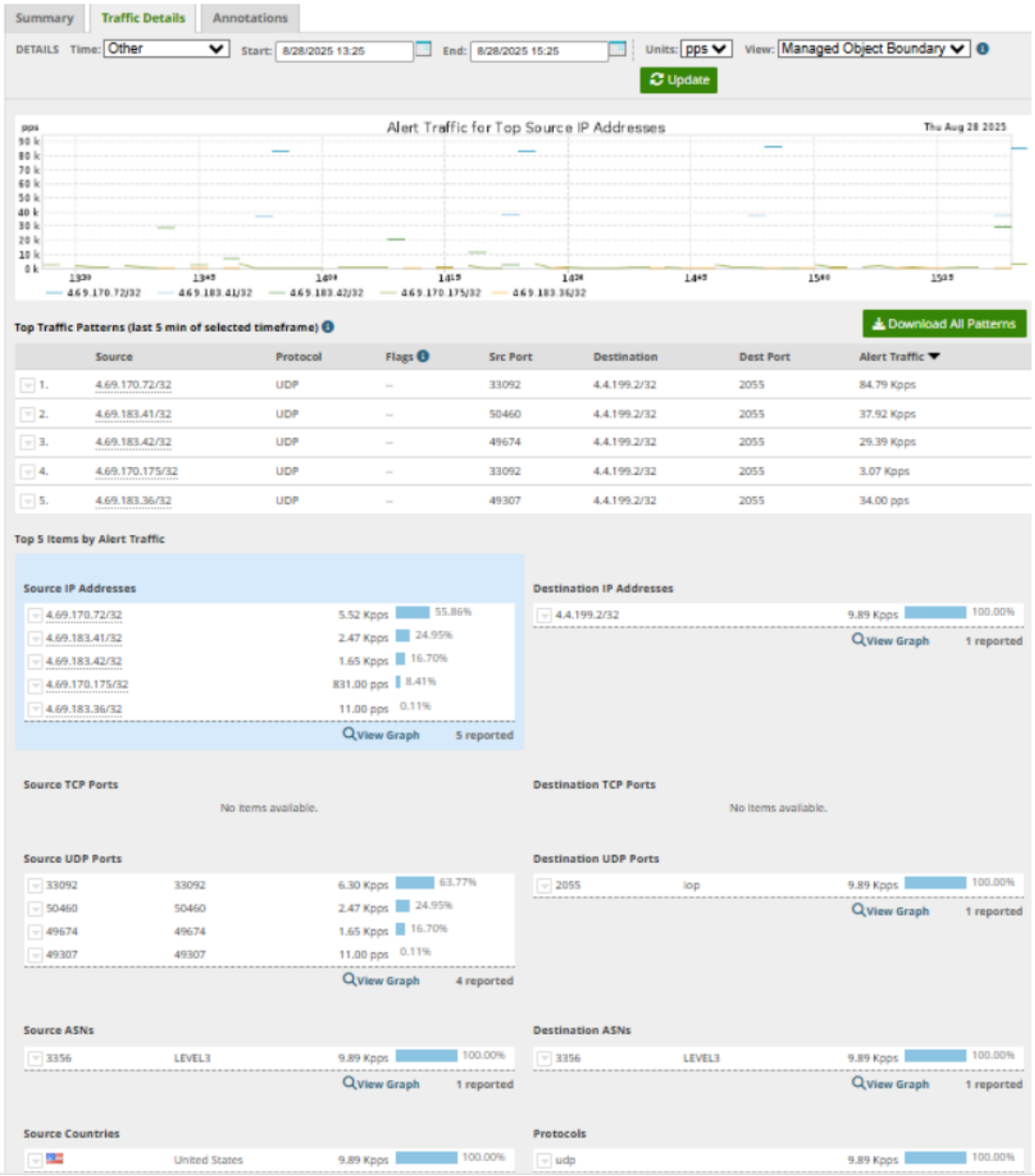
Alert Details

An alert can be inspected by clicking on the alert ID number. The graph shows the total traffic associated with the affected IPs during the alert, along with some information about the alert, such as the data rates, the type of alert, and the affected profile.



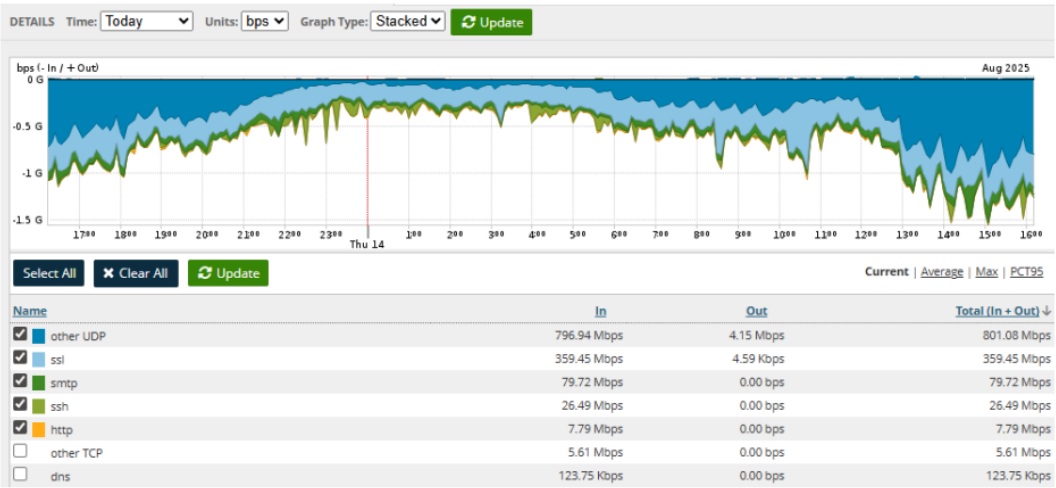
Alert Traffic

More details about the traffic generating a DDoS alert are available on the **Traffic Details** tab. The list of affected interfaces on individual routers is shown on the **Alert Summary** page, and the detail coming from a specific interface is accessed with the **Detail** button for a specific interface.



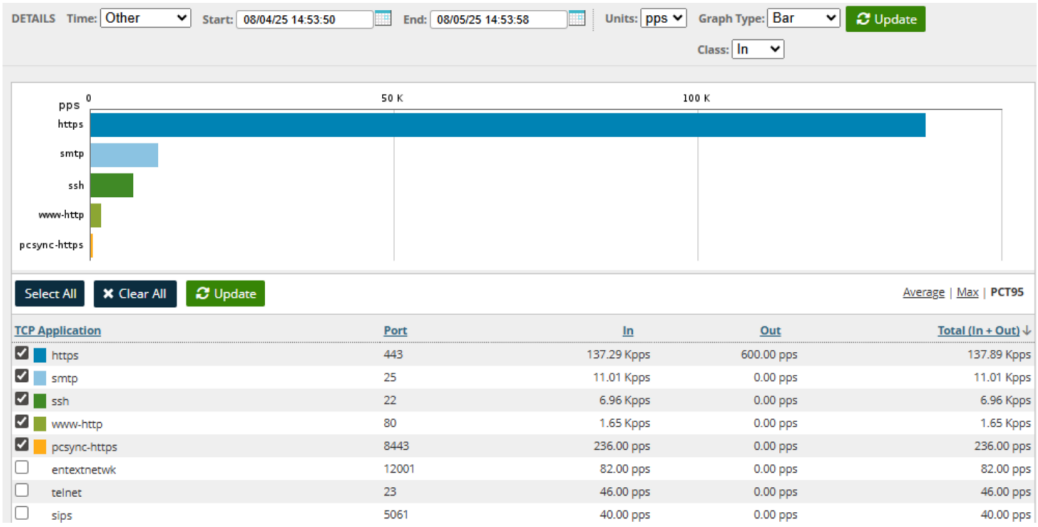
Monitoring: Traffic Summary by Applications

The DDoS Mitigation Reporting portal shows a summary of the traffic, for all monitored networks of the customer, broken down by application.



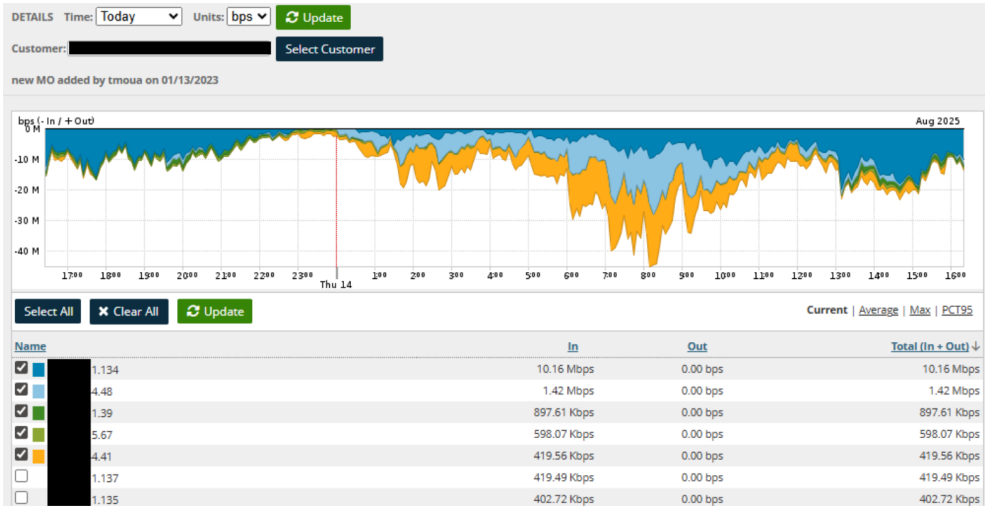
Monitoring: Traffic Summary for TCP & UDP

Similar to the Applications report above, this constrains the report to TCP traffic broken down by TCP. Any selected ports are shown in the graph with a unique color. There is a similar report for UDP ports that looks, and behaves identically, constraining the report to UDP traffic aggregated by UDP port.



Monitoring: Traffic Profiles for Top Talkers

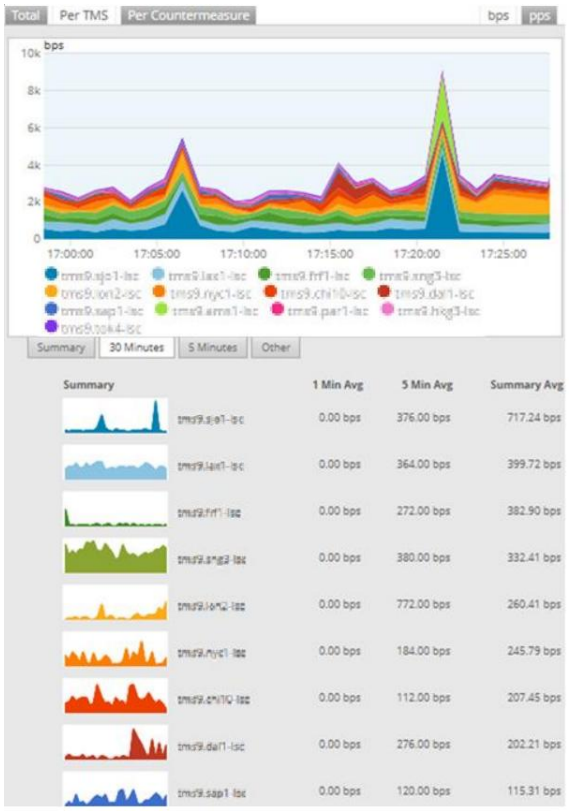
Identifies the systems generating the most traffic that traverses the Lumen network. If the DNS name of host can be resolved, it is shown to the left of the IP address.



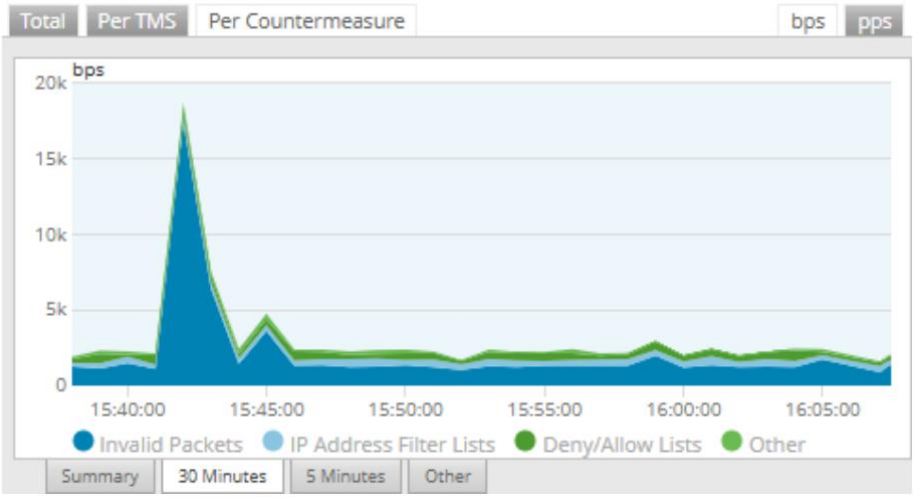
Mitigation Events

Shows details about any ongoing or recent mitigations. The details provided include countermeasures used and how much traffic was passed or dropped by each event.

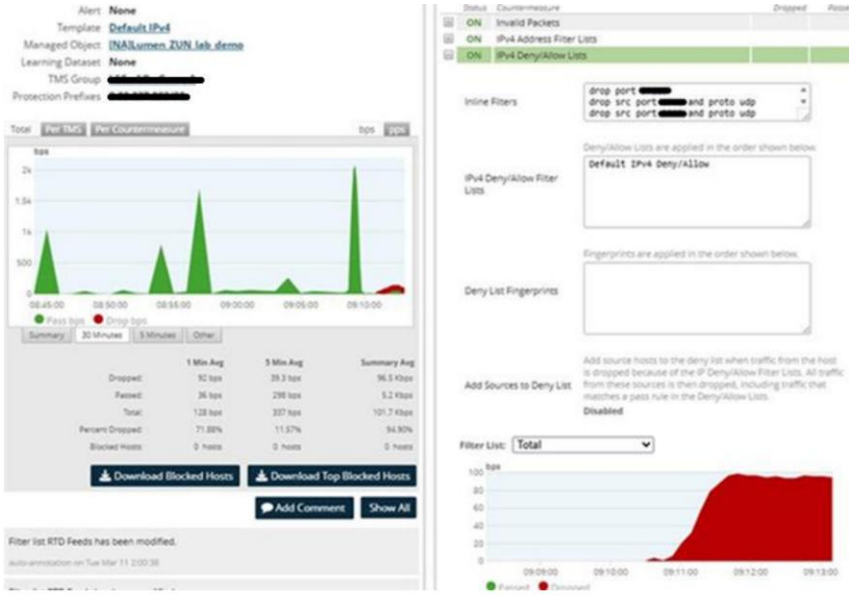
The Per TMS tab will show how much volume each scrubbing center handled:



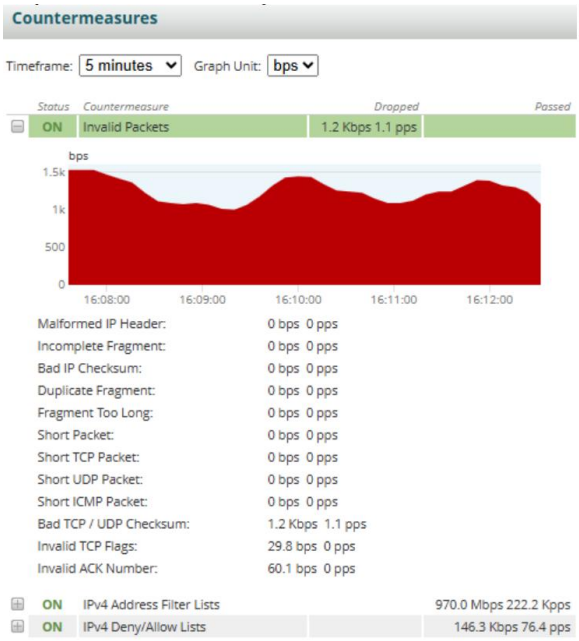
While the **Per Countermeasure** tab shows what all countermeasures were used and how much volume was matched to each of them:



Expanding the groupings under the **countermeasure section the right side of the page** allows for seeing how much of the attack volume was dropped by each countermeasure:



Finally, each countermeasure may also contain multiple filters that handle similar violations. For example, an Invalid packet includes packets with an invalid ACK Number, TCP Flag, bad TCP/UDP Checksum and many more, as shown in this example:

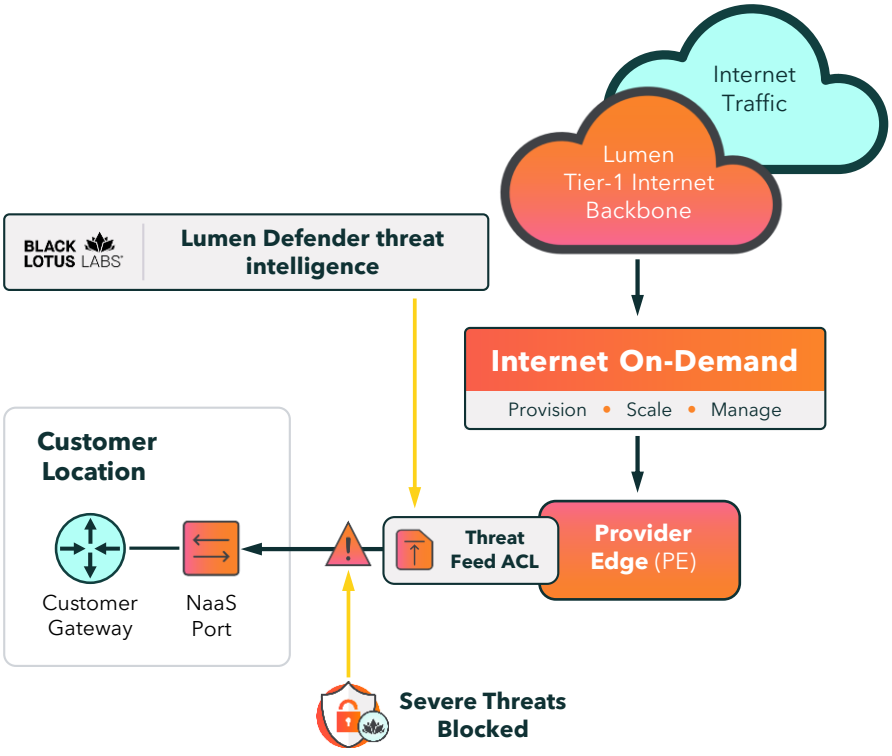


Adding Lumen Defender℠ Essentials to Internet On-Demand

What it does

Lumen Defender Essentials provides **always-on, network-embedded threat blocking** for Internet On-Demand by automatically blocking responses to severe-risk internet-based threats before customer environments become impacted. Protection occurs upstream within the Lumen network, helping to reduce malicious noise that can overwhelm downstream firewalls, SIEMs, and security teams.

Powered by **Black Lotus Labs®** threat intelligence, Lumen Defender Essentials leverages backbone-level visibility across the Lumen global network to identify known bad actors with high confidence. Because blocking is applied within the network, customers gain immediate protection without deploying hardware, configuring appliances, or managing policies, making Lumen Defender Essentials a simple way to improve security efficiency as Internet On-Demand exposure scales.



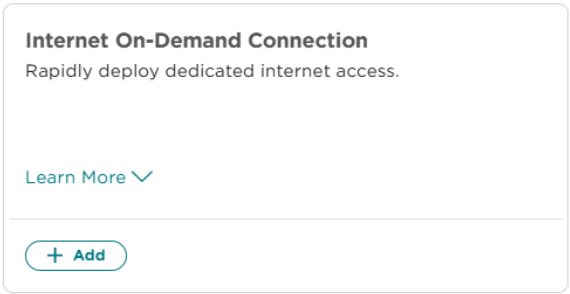
When to add it

- When ordering a **new Internet On-Demand connection** and you want always-on protection from known malicious internet-based threats from day one
- When enhancing protection on an **existing Internet On-Demand connection** to reduce alert fatigue and operational burden as application exposure grows

How to add Lumen Defender℠ Essentials to Internet On-Demand

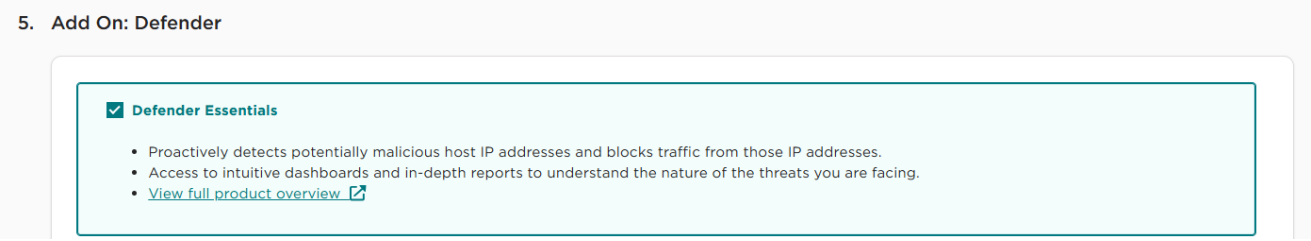
Adding Lumen Defender℠ Essentials to a new Internet On-Demand Connection

1. Sign in to **Lumen Connect℠**
2. Navigate to **Add Services** and select **Add** under Internet On-Demand Connection to add a new Internet On-Demand connection

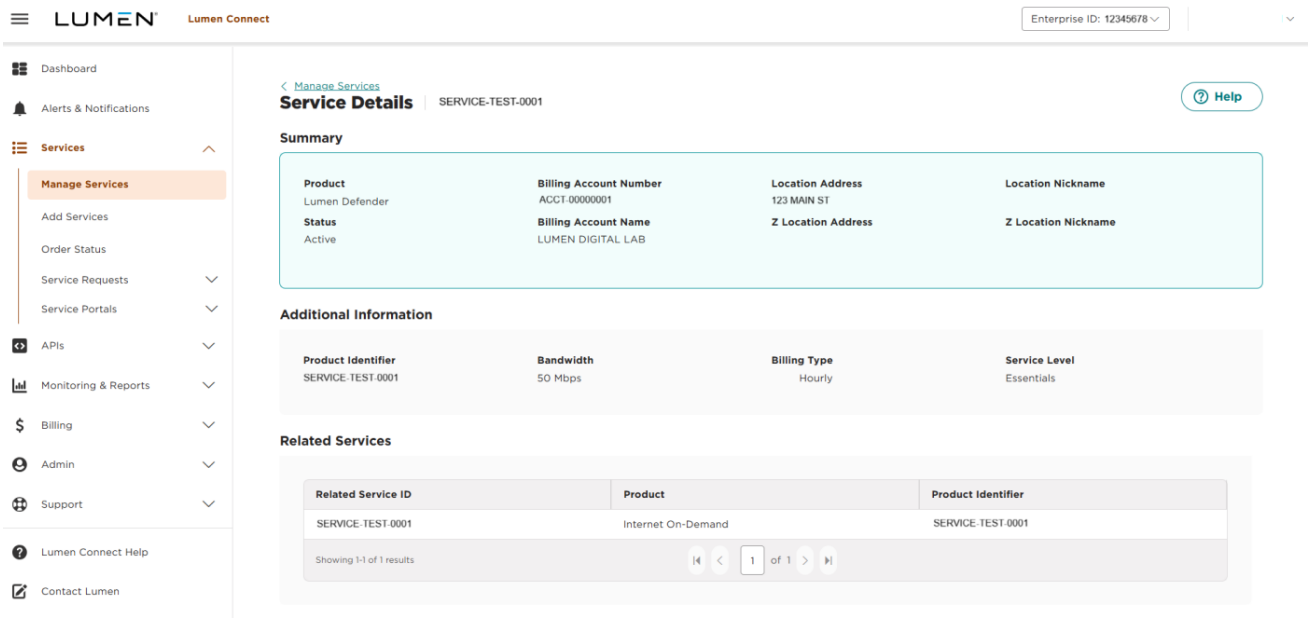


3. Select **Defender Essentials** in **Step 5** of the Internet On-Demand ordering process to quickly add the service at the time of initial order.

   Note: Lumen Defender is currently not available for IPv6 and Dual Stack.

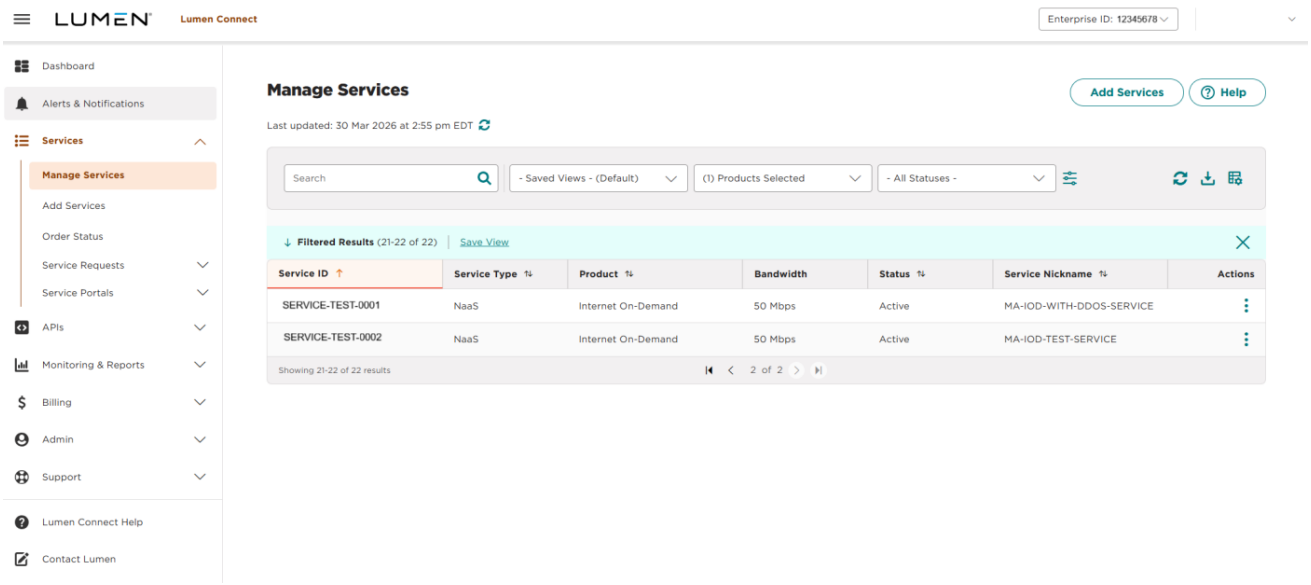


4. Review service details and pricing, **Defender Essentials** will be in the **Security Add On** section.
5. Submit the Internet On-Demand order to create the service with Lumen Defender Essentials enabled.
6. Once provisioning has been completed, navigate to **Manage Services**, and select the newly provisioned **Lumen Defender Essentials Service** to see the details.

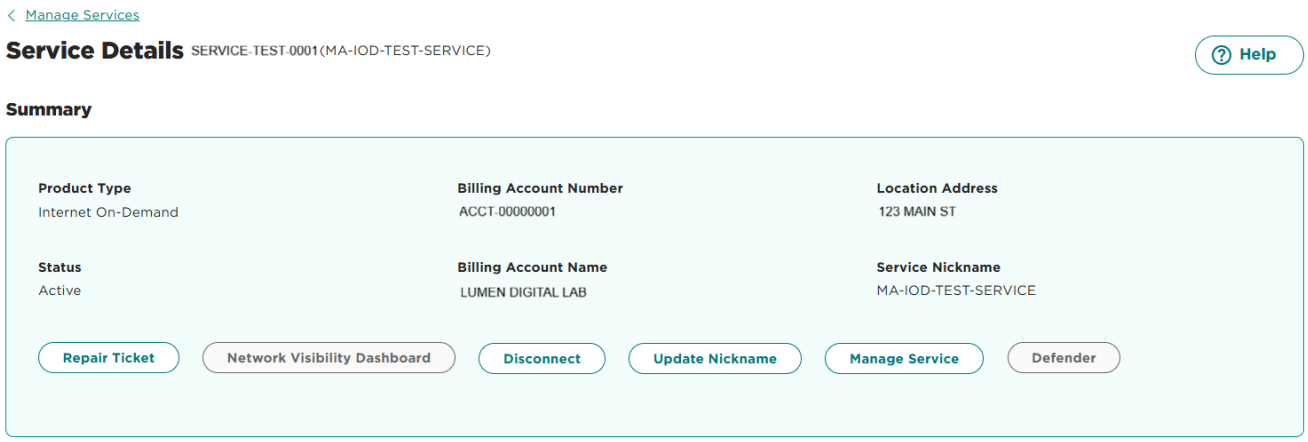


Adding Lumen Defender℠ Essentials to an existing Internet On-Demand Connection

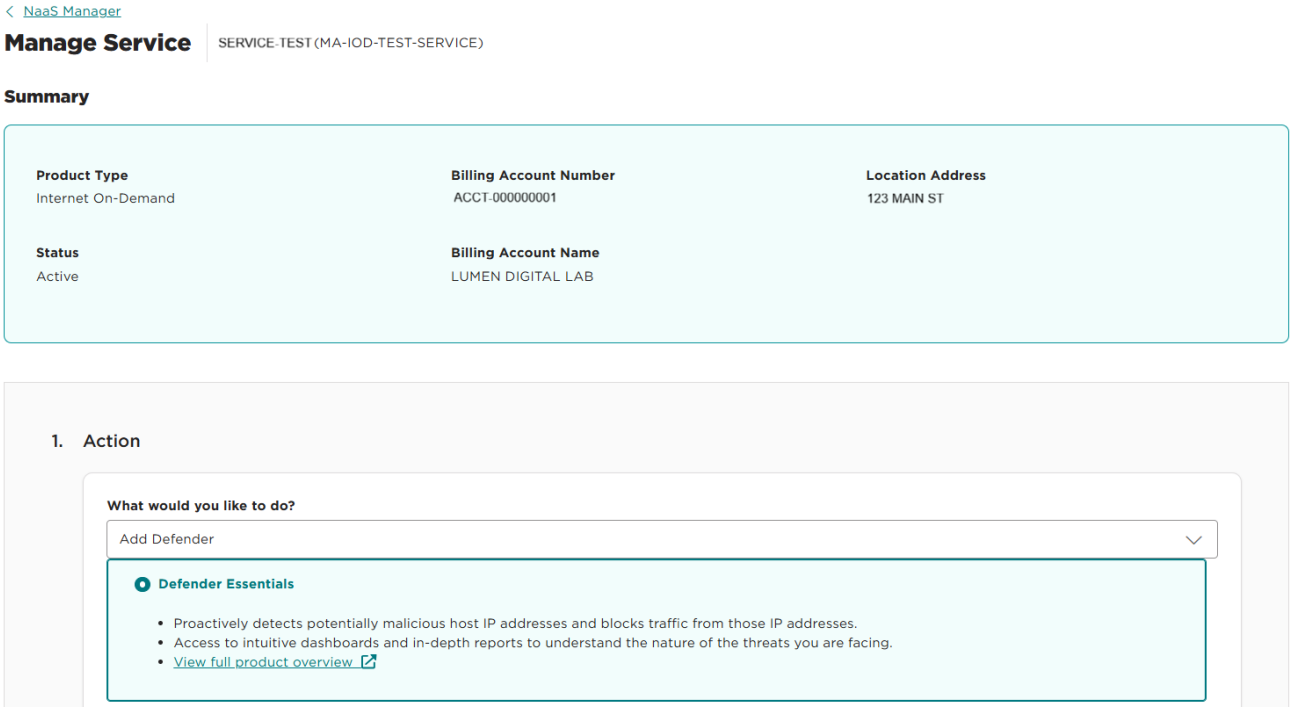
1. Sign in to **Lumen Connect℠**
2. Navigate to **Manage Services** and select the specific Internet On-Demand connection to add Lumen Defender Essentials to.



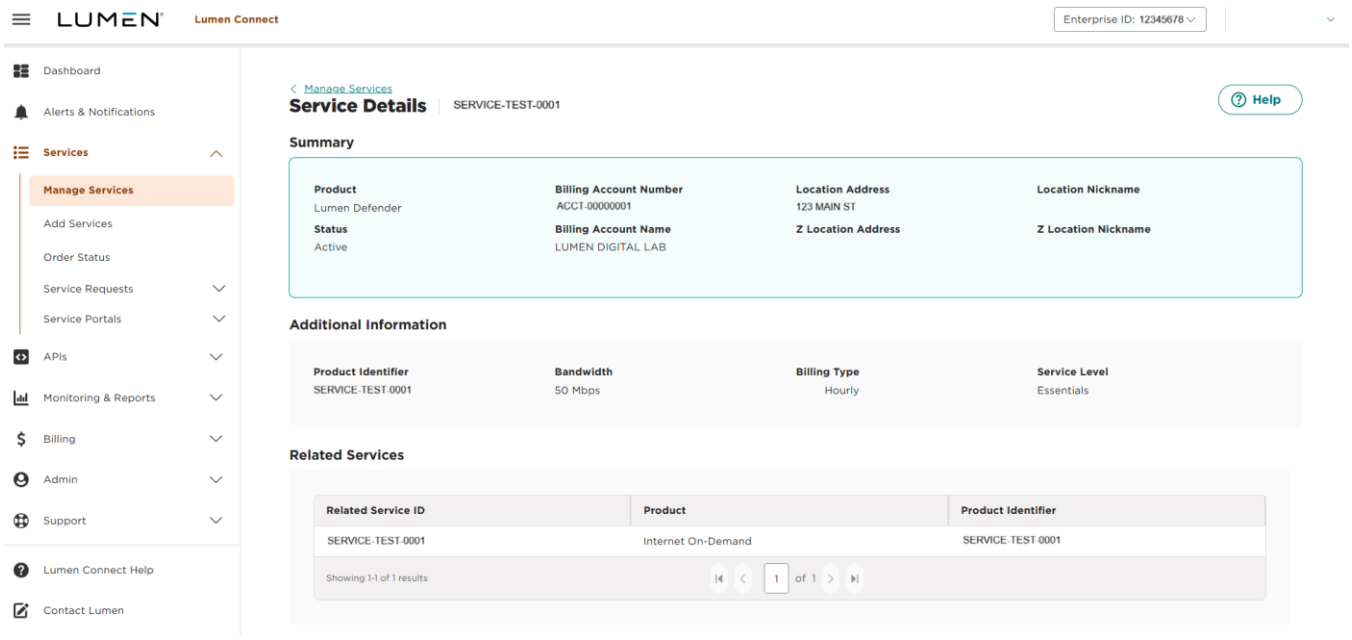
3. Click **Manage Service**.



4. In the Action section, select **Add Defender**.
5. Review the notes and cost, then select **Continue**.



6. Select **Submit Order**.
7. The **Service Details** page for the Internet On-Demand connection will be displayed with activation progress and updated automatically once the new Lumen Defender Essentials service is activated.
8. Once provisioning has been completed, navigate to **Manage Services**, and select the newly provisioned **Lumen Defender Essentials Service** to see the details.



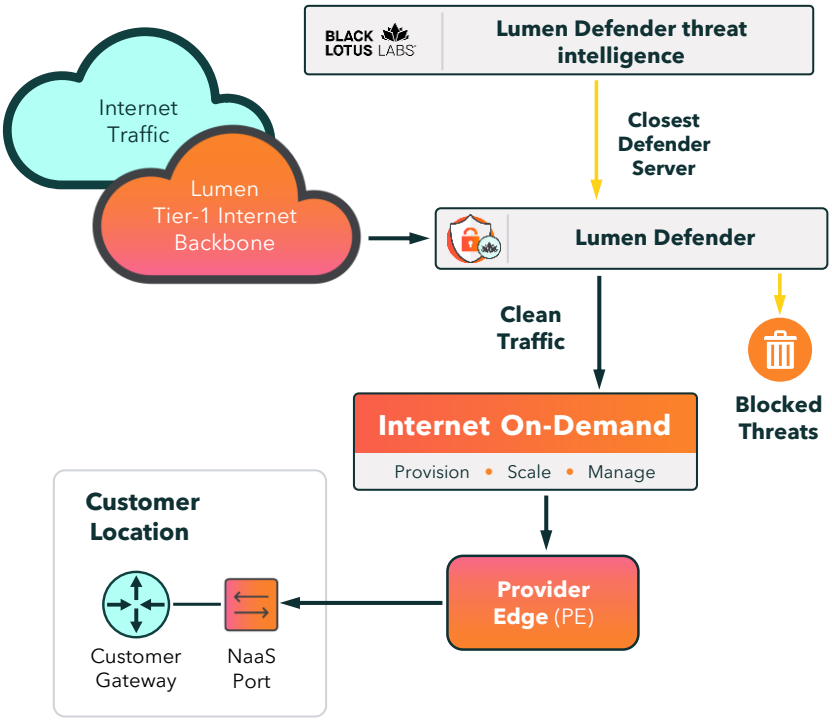
Adding Lumen Defender℠ Plus to Internet On-Demand

What it does

Lumen Defender Plus extends network-embedded threat protection for Internet On-Demand by combining **upstream threat blocking** with **enhanced visibility, reporting, and customer control**. In addition to blocking severe-risk threats, Lumen Defender Plus allows customers to apply blocking across multiple threat-severity levels and gain deeper insight into the malicious activity targeting their internet-facing applications.

Powered by **Black Lotus Labs®** threat intelligence and enforced within the Lumen network, Lumen Defender Plus intercepts known malicious internet-based threats such as bots, malware, command-and-control infrastructure, and proxy activity **before traffic reaches customer environments**. Clean traffic is returned automatically, helping reduce noise, false positives, and operational burden on downstream security tools.

Lumen Defender Plus provides a richer operational experience through Lumen Connect℠, including detailed threat reporting, IP-level visibility, and the ability to allow, block, or monitor specific threats without deploying customer-side security infrastructure.



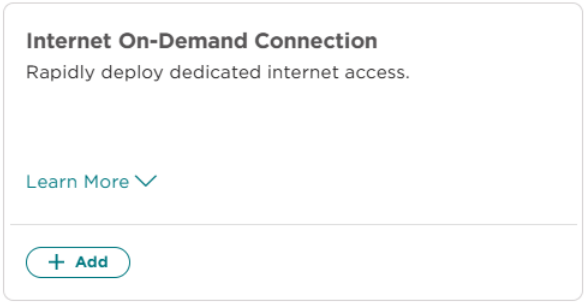
When to add it

- **When ordering a new Internet On-Demand connection** and you want network-embedded threat blocking with enhanced visibility and control from day one
- **When enhancing protection on an existing Internet On-Demand connection** or when **upgrading from Lumen Defender Essentials** to gain deeper insight into threats, expanded severity controls, and reporting
- **When security teams want to reduce alert fatigue** while retaining the ability to review, monitor, and manage blocked threats

How to add Lumen Defender℠ Plus to Internet On-Demand

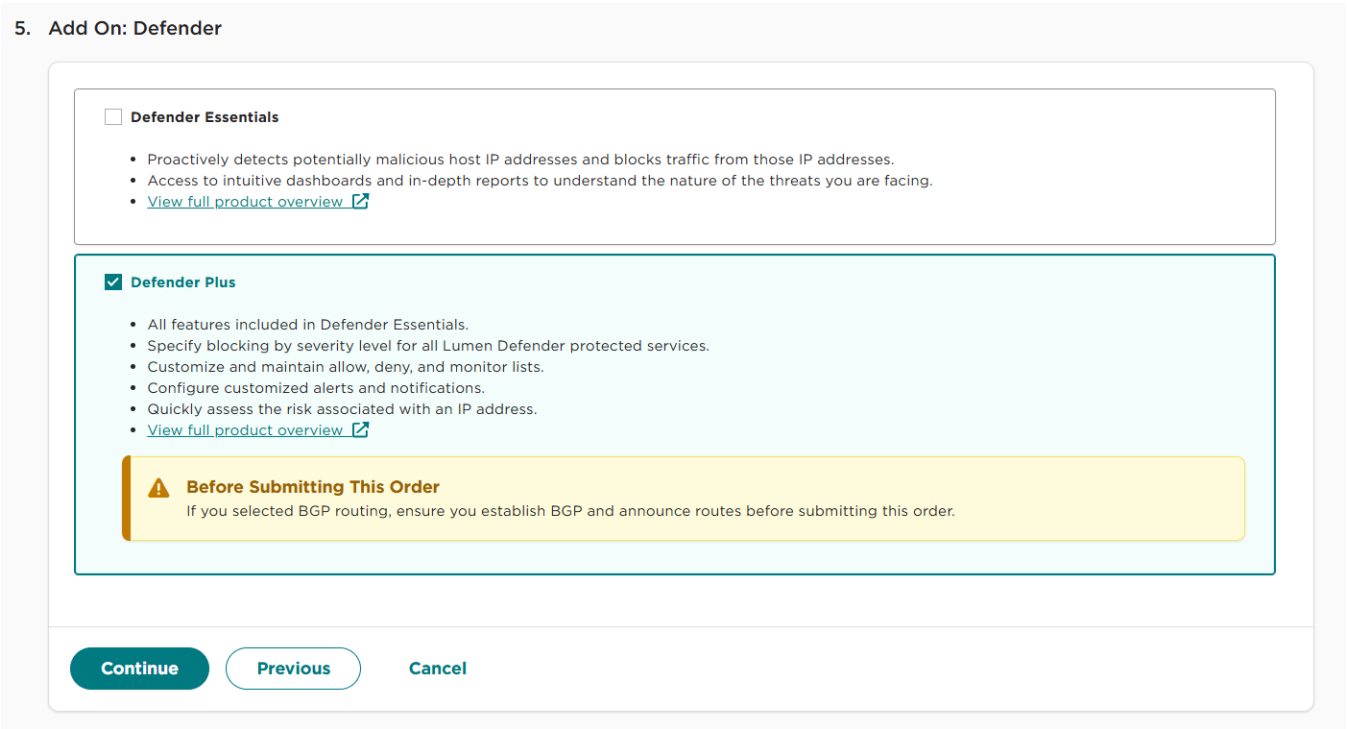
Adding Lumen Defender℠ Plus to a new Internet On-Demand Connection

1. Sign in to **Lumen Connect℠**
2. Navigate to **Add Services** and select **Add** under Internet On-Demand Connection to add a new Internet On-Demand connection



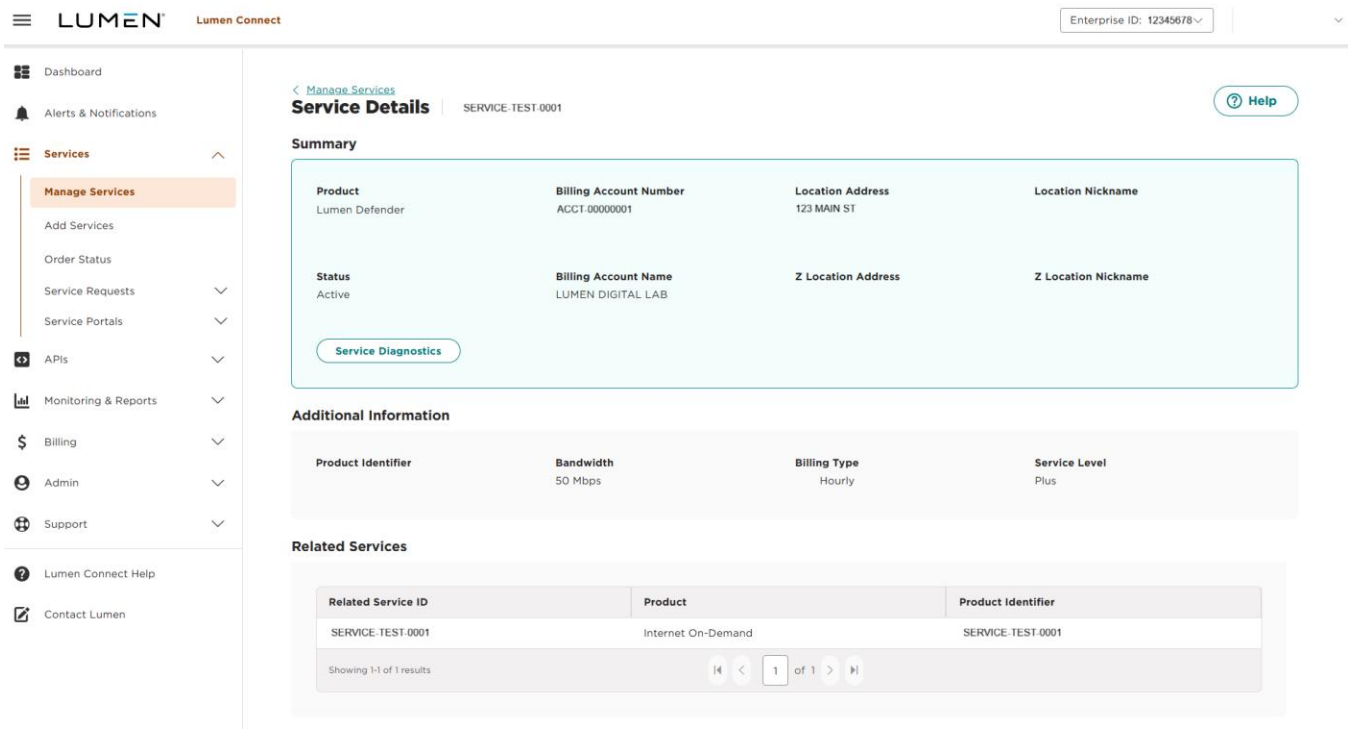
3. Select **Defender Plus** in **Step 5** of the Internet On-Demand ordering process to quickly add the service at the time of initial order.

   Note: Lumen Defender is currently not available for IPv6 and Dual Stack.



Note: If you selected BGP routing, ensure you establish BGP and announce routes before submitting this order.

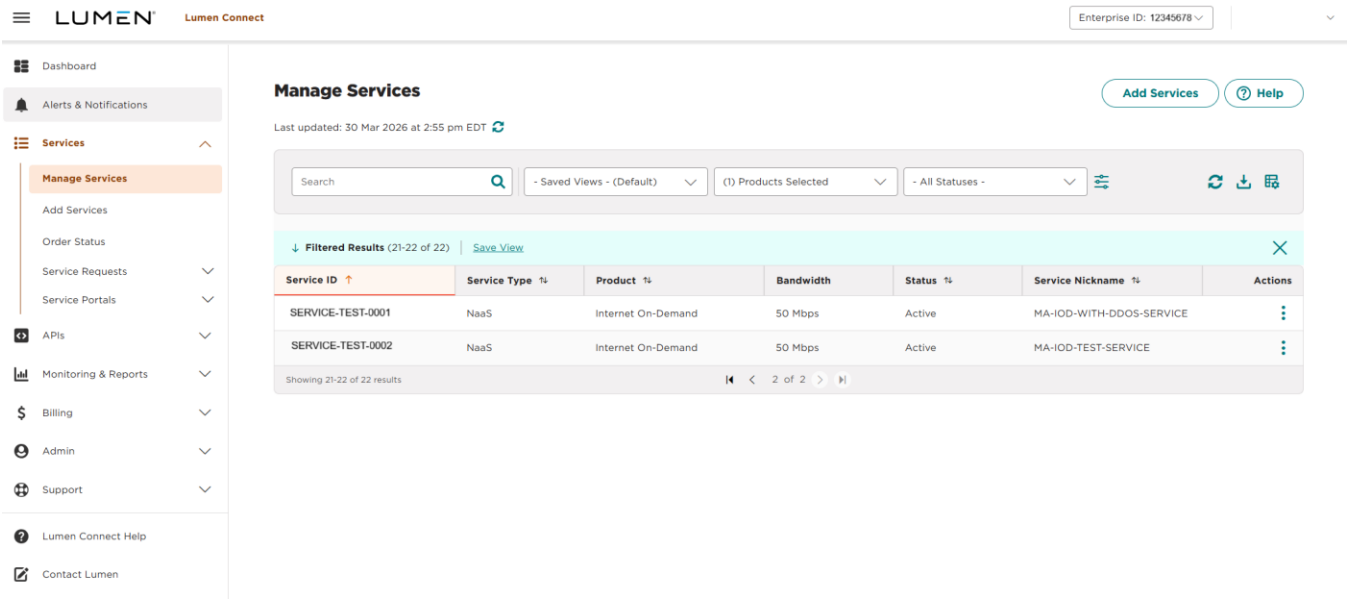
4. Review service details and pricing, **Lumen Defender Plus** will be in the **Security Add On** section.
5. Submit the Internet On-Demand order to create the service with Lumen Defender Plus enabled.
6. Once provisioning has been completed, navigate to **Manage Services**, and select the newly provisioned **Lumen Defender Plus Service** to see the details.



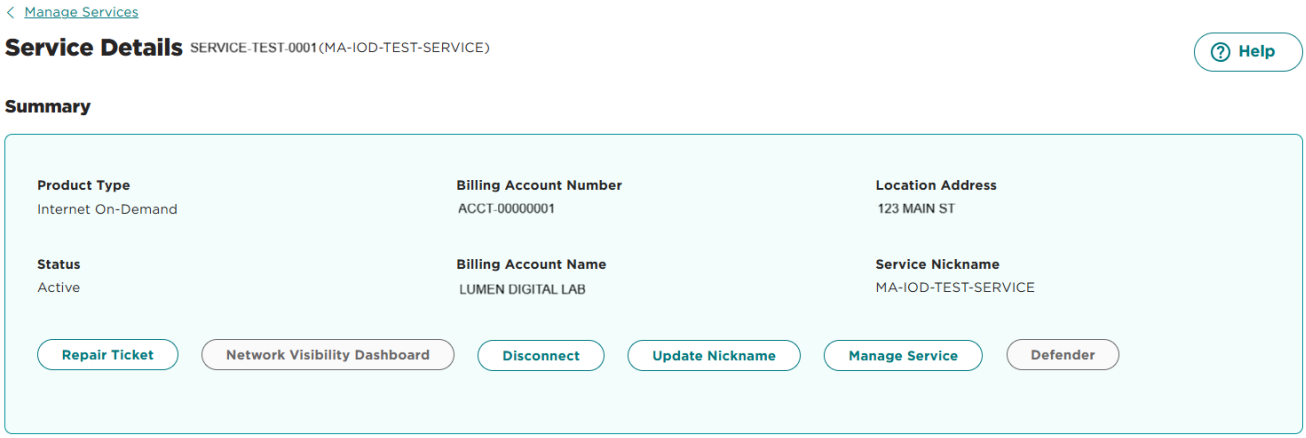
Adding Lumen Defender℠ Plus to an existing Internet On-Demand Connection

Lumen Defender Plus can be added to an **existing Internet On-Demand connection** or **upgraded from Lumen Defender Essentials** to intercept inbound traffic within the Lumen network, apply expanded threat blocking, and return clean traffic to the customer with enhanced visibility and control.

1. Sign in to **Lumen Connect℠**
2. Navigate to **Manage Services** and select the specific Internet On-Demand connection to add Lumen Defender Plus to.

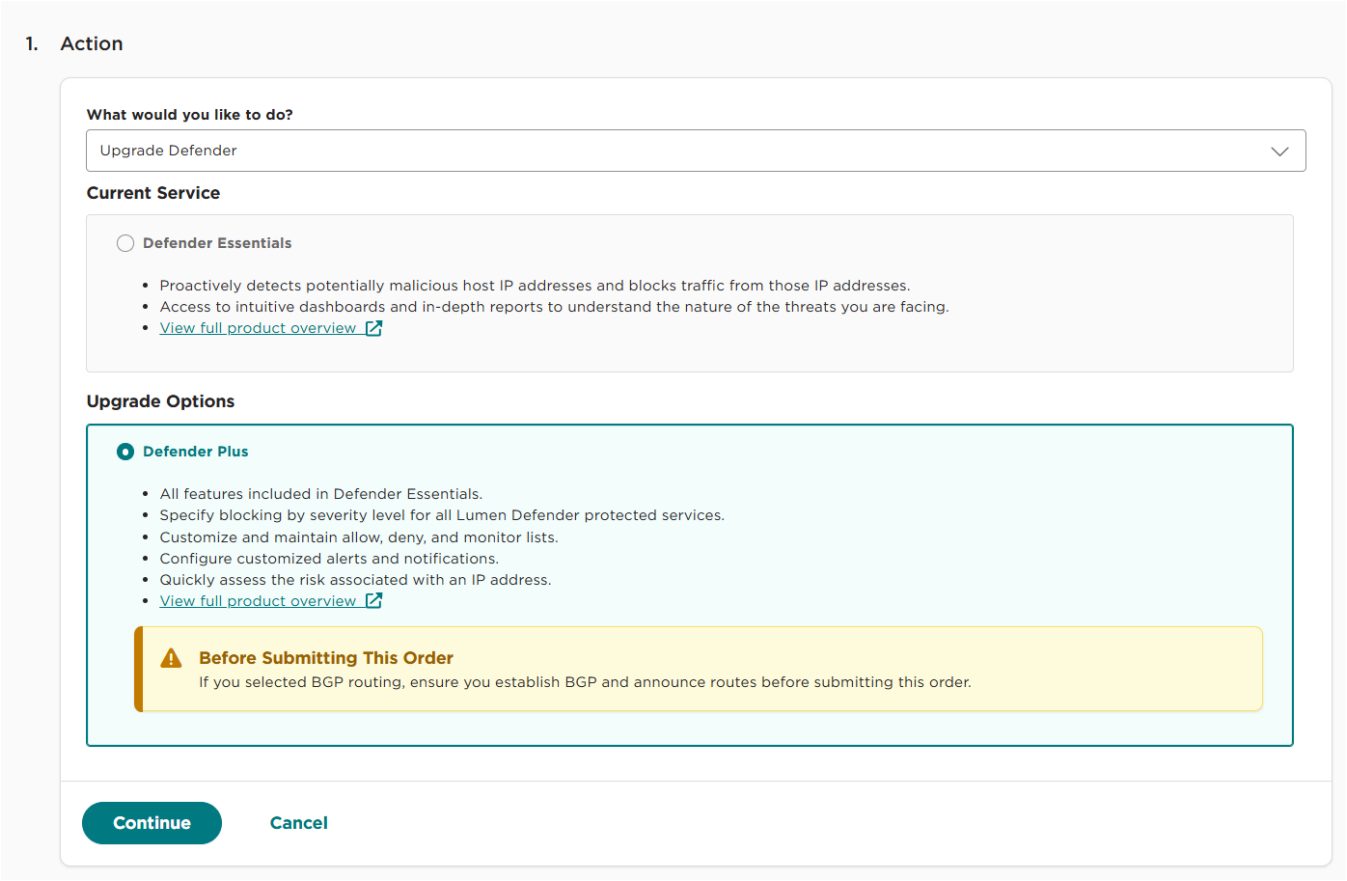


3. Click **Manage Service**.

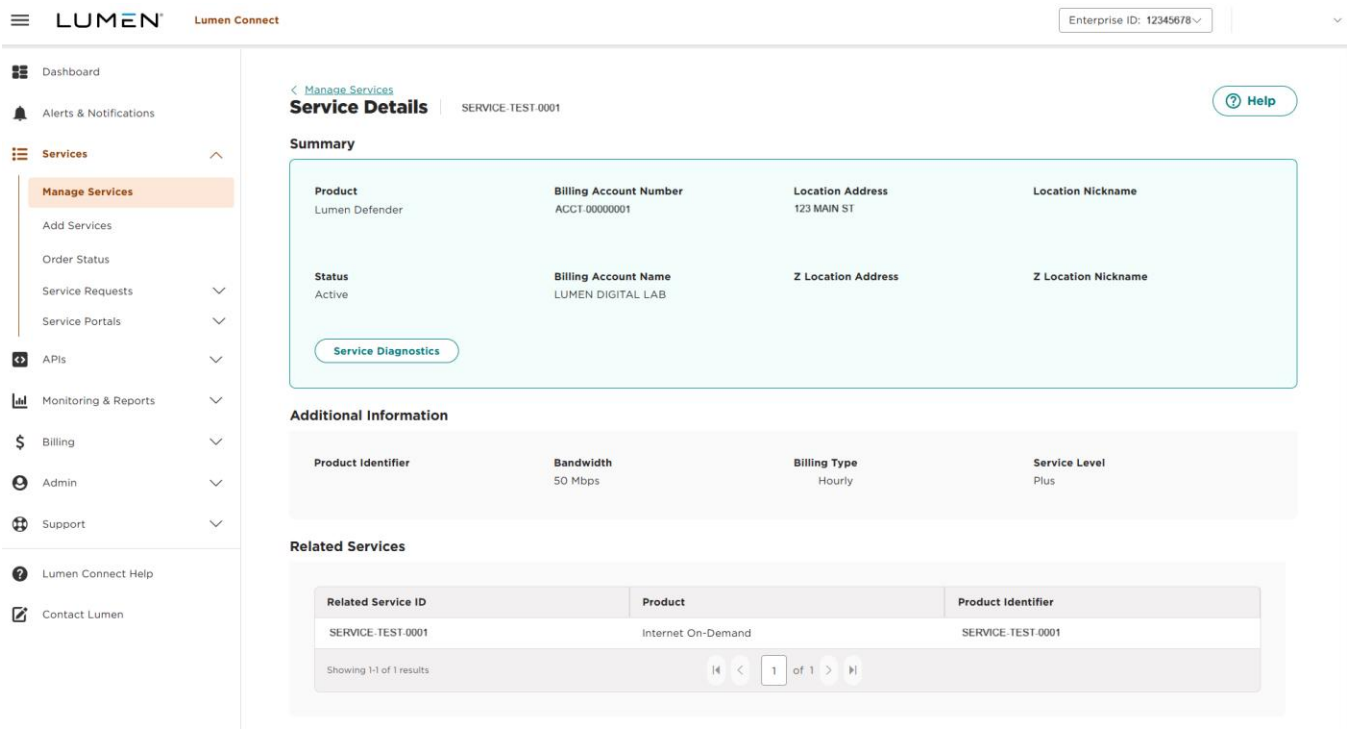


4. In the Action section, select **Add Defender** (or if upgrading from Lumen Defender Essentials to Plus, select **Upgrade Defender**).
5. Review the notes and cost, then select **Continue**.

   Note: If you selected BGP routing, ensure you establish BGP and announce routes before submitting this order.

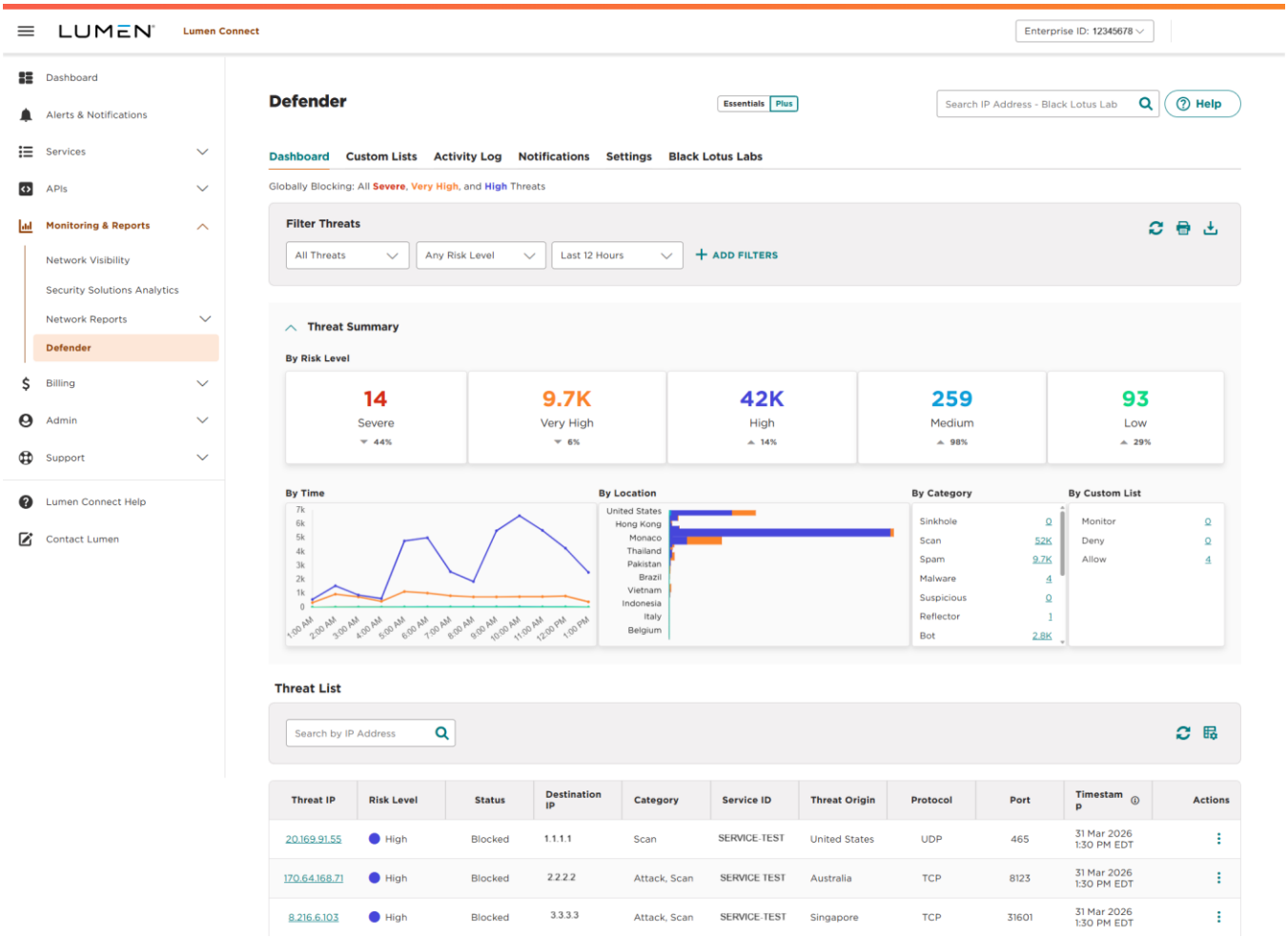


6. Select **Submit Order**.
7. The **Service Details** page for the Internet On-Demand connection will be displayed with activation progress and updated automatically once the new Lumen Defender Plus service is activated.
8. Once provisioning has been completed, navigate to **Manage Services**, and select the newly provisioned **Lumen Defender Plus Service** to see the details.



Lumen Defender℠ Monitoring and Reporting

Lumen Defender monitoring and reporting capabilities are delivered through **Lumen Connect℠**, providing customers with visibility into internet-based threats detected and mitigated at the Lumen network edge using **Black Lotus Labs®** threat intelligence. Reporting capabilities vary by service tier (Lumen Defender Essentials and Plus) and are designed to give customers actionable insight without requiring on-premises appliances or inline configuration.



General Monitoring & Reporting

Both Lumen Defender Essentials and Lumen Defender Plus surface threat information via the Lumen Defender dashboard within **Monitoring & Reports** for Defender in Lumen Connect. The core dashboard experience includes:

- **Threat Summary** cards showing active and blocked threats by risk level
- **Threat List** tables listing individual threat IPs with additional drill-down data:
  - Risk level
  - Threat category
  - Protocol
  - Source and Destination IP and port
- **Graphical Time-based views** of threats by:
  - Time
  - Risk level
  - Category
  - Protocol

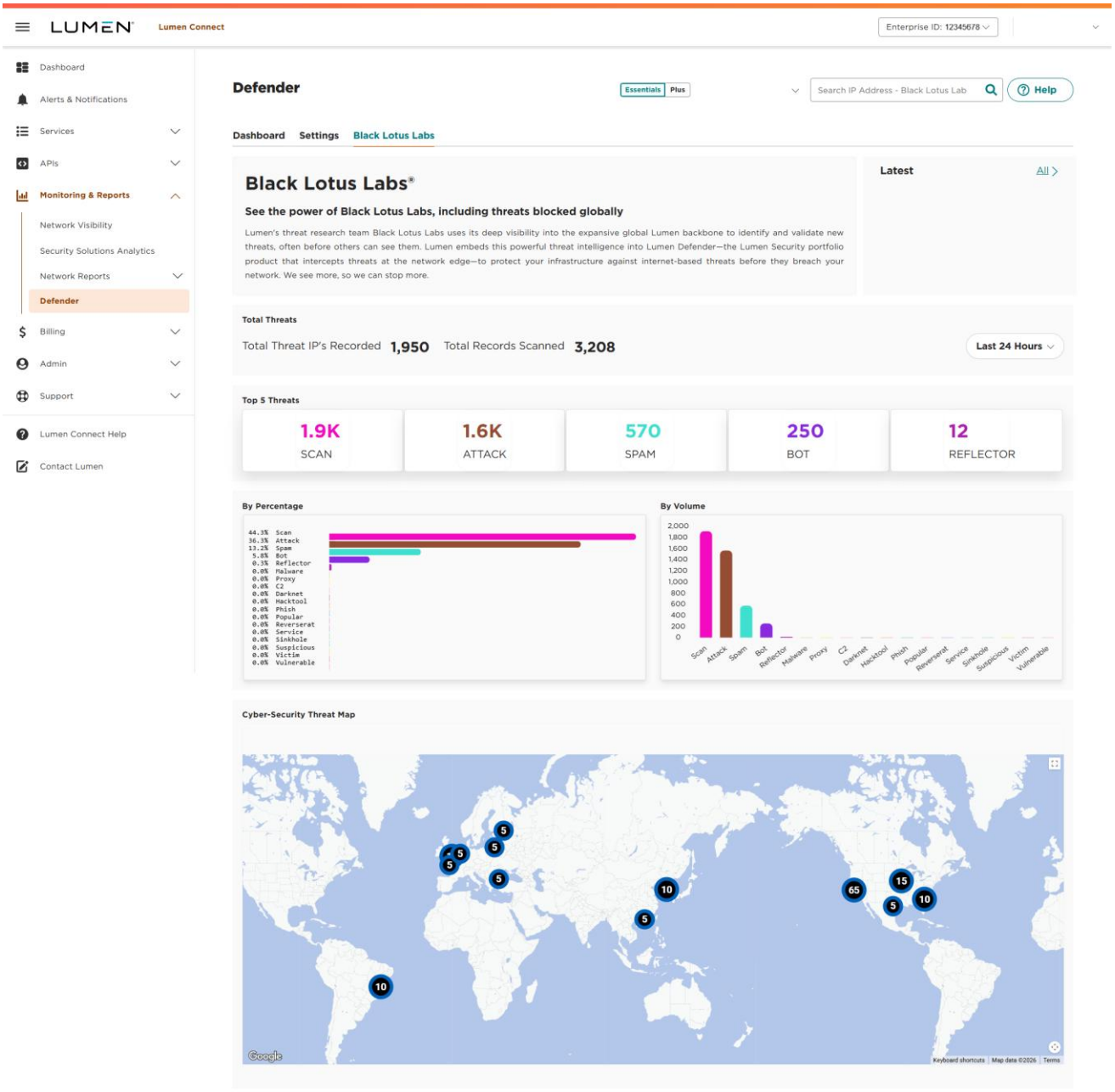
Global Threat Visibility: Black Lotus Labs® Intelligence Dashboard

The Lumen Defender℠ Threat Intelligence Dashboard, powered by **Black Lotus Labs®**, provides customers with a near real-time, global view of malicious activity observed across the Lumen network. By aggregating internet-scale telemetry and applying advanced threat intelligence, the dashboard illustrates the depth and breadth of threats Lumen is detecting and mitigating worldwide, not just what is targeting an individual service. This perspective gives customers valuable context, helping them understand the scale, diversity, and geographic distribution of modern internet threats, and reinforces the advantage of network-embedded security intelligence operating at global scale.

What This Dashboard Shows:

- **Total threat activity observed globally** over a selectable time window
- **Threats categorized by type**, such as scanning, attacks, bots, spam, and reflection-based activity
- **Threat distribution and relative volume** by category, highlighting dominant threat behaviors

- **Geographic visualization of threat sources**, showing where malicious activity originates around the world
- **Trend context over time**, helping customers see how threat activity fluctuates and evolves



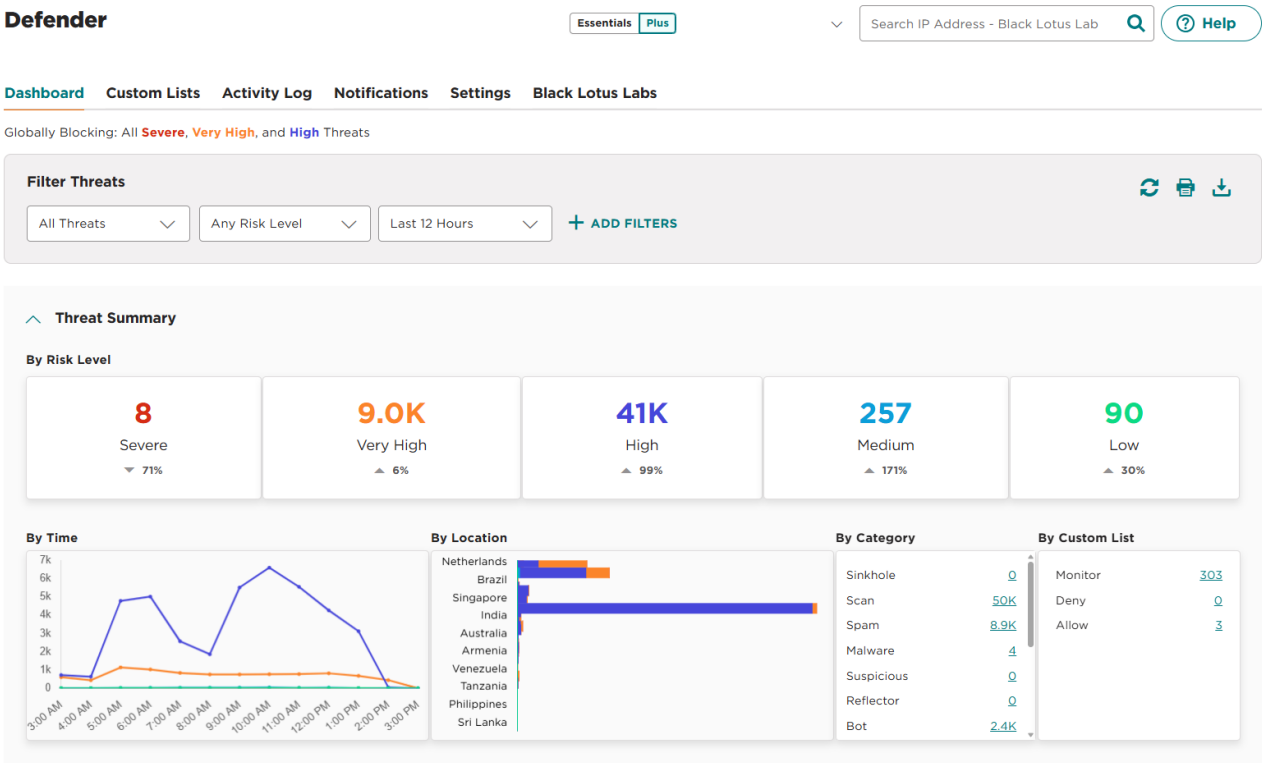
Lumen Defender℠ Plus Monitoring & Reporting

Lumen Defender Plus expands on the baseline visibility provided by Lumen Defender Essentials by adding **operational reporting, historical insight, and proactive alerting**. While Lumen Defender Essentials focuses on high-level awareness of severe threats, Lumen Defender Plus enables customers to **investigate, track, export, and act on threat intelligence** over time, turning network-embedded security visibility into a practical operational capability.

All Lumen Defender Plus reporting and monitoring features are delivered through **Lumen Connect℠** and are powered by **Black Lotus Labs®** threat intelligence, providing consistent context across dashboards, reports, and alerts.

Dashboard Threat Summary

The **Threat Summary** within the main Lumen Defender dashboard provides a consolidated view of threat activity across protected services, combining summary metrics, graphical insights, and detailed threat listings in a single interface. Filters can be applied to show all threats, active, or blocked, across risk levels and time.



The filters within the Threat Summary allow customers to quickly pivot between **wide visibility and focused investigation**, narrowing threat data by status, risk level, and time window. This makes it easy to move from broad situational awareness to targeted analysis without leaving the main dashboard.

Using the **Threat Summary filters**, customers can:

- **Understand the full threat landscape** by viewing all detected and mitigated threats across services, categories, and risk levels
- **Isolate active threats** to focus on ongoing malicious activity that may require closer attention
- **Review blocked threats** to validate that attacks are being mitigated at the network edge
- **Analyze trends over time** by adjusting time ranges to identify changes in threat volume or behavior
- **Drill down efficiently** from summary views into detailed threat records for investigation, reporting, or action

Dashboard Threat List

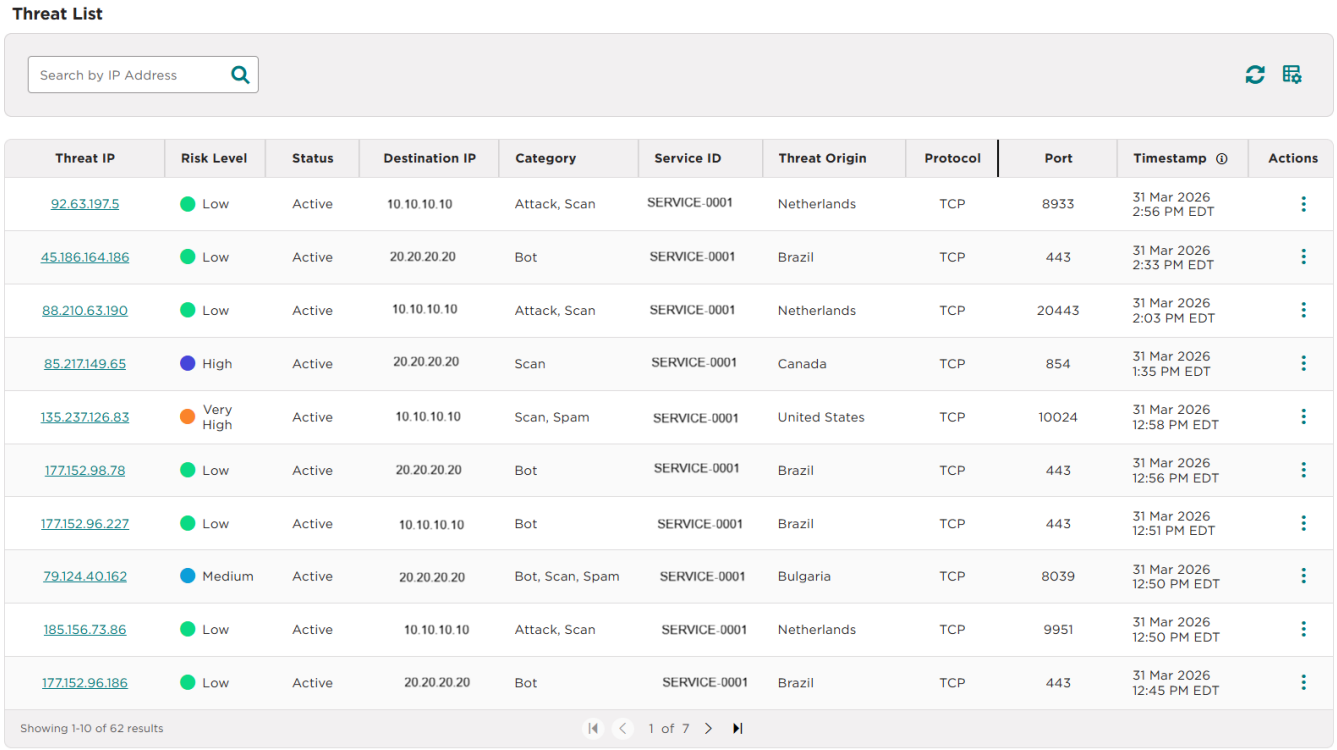
The **Threat List** within the Lumen Defender Plus dashboard provides customers with a detailed, service-level view of individual threats detected across protected connections. While summary views highlight overall threat conditions, the Threat List is where customers **inspect specific threat events, understand their context, and take informed action**, all from a single, centralized interface.

Each entry in the Threat List represents an individual threat IP observed by Lumen Defender, enriched with **Black Lotus Labs®** intelligence and surfaced with key attributes such as risk level, threat category, origin, protocol, destination IP, and timestamp. This level of detail allows customers to move quickly from awareness to investigation.

From the Threat List, customers can **Inspect and Investigate Specific Threats**:

- **Review individual threat entries** with full contextual details, including risk level, category, source geography, and affected service
- **Search or filter by threat IP**, risk level, status, or time to focus on what matters most
- **Drill down into a specific threat IP** to view comprehensive threat details and history

This enables efficient investigation without requiring external tools or log correlation.



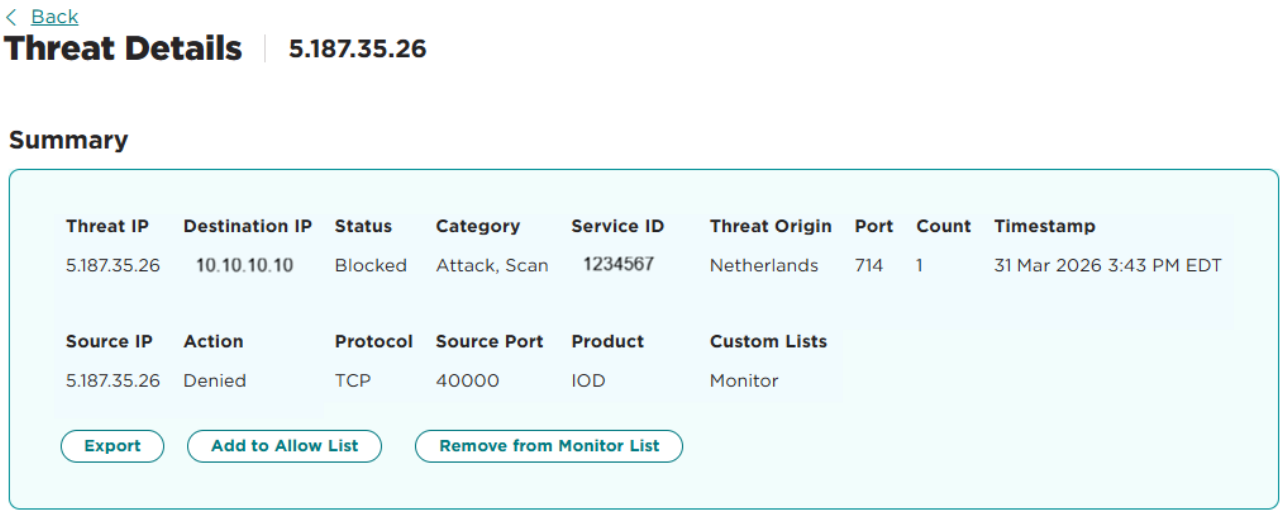
Threat Drill-Down with In-Context Control

When customers drill into a specific threat IP from the Threat List, the **Threat Details** view provides deeper insight and immediate control options.

From this view, Lumen Defender Plus customers can:

- **Add a threat IP to a Monitor List** to continue observing activity without immediate blocking
- **Remove a threat IP from an Allow List** if it no longer represents trusted traffic
- **Add a threat IP to a Deny List** to enforce blocking at the network edge
- Export threat details for reporting or offline analysis

Because these actions are taken directly from the threat investigation screen, customers can make decisions with full context, reducing operational guesswork and minimizing false positives.

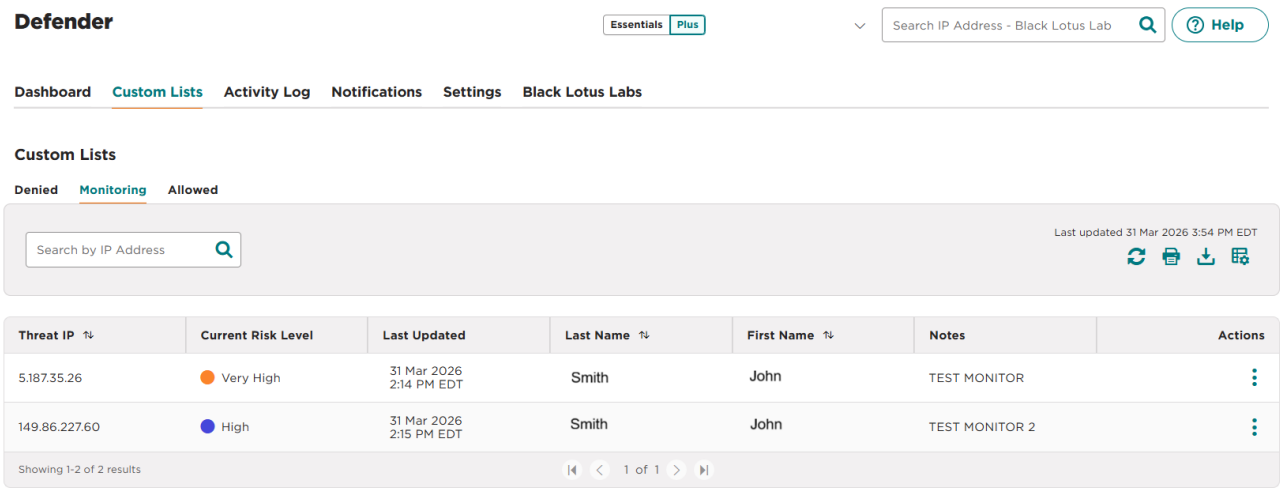


Custom Lists and Operational Transparency

All threat-level actions taken from the Threat List feed directly into **Custom Lists**, where customers can centrally manage:

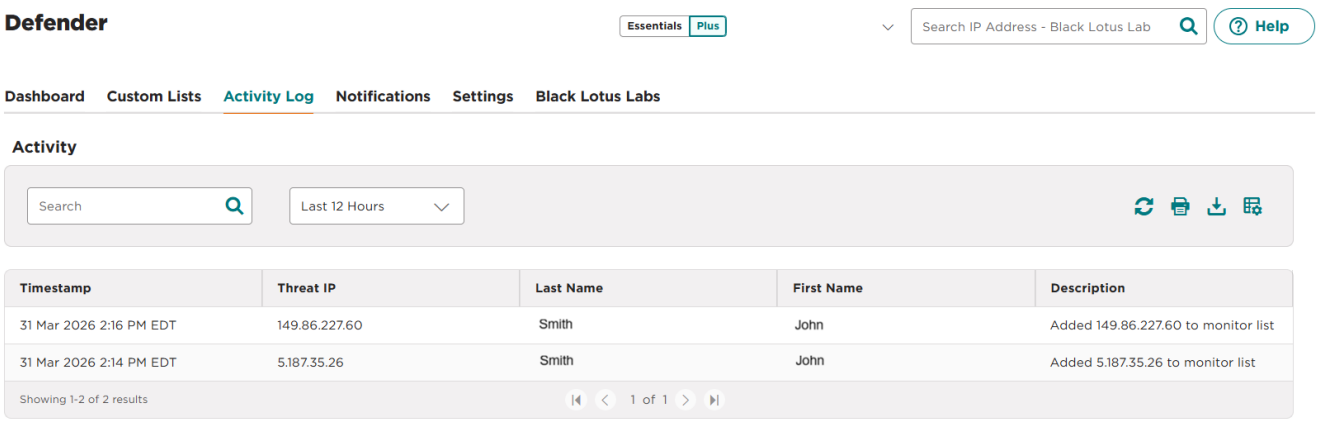
- IPs they are **monitoring**
- IPs they have **explicitly allowed**
- IPs they have **explicitly denied**

This provides a clear, organized view of how specific threats are being handled across services.



To ensure full visibility and accountability, every change made, such as adding or removing an IP from a custom list, is automatically captured in the **Activity Log**, allowing customers to:

- Track **what changes were made and when**
- Support audit, review, and operational assurance use cases
- Maintain confidence in security configuration decisions over time



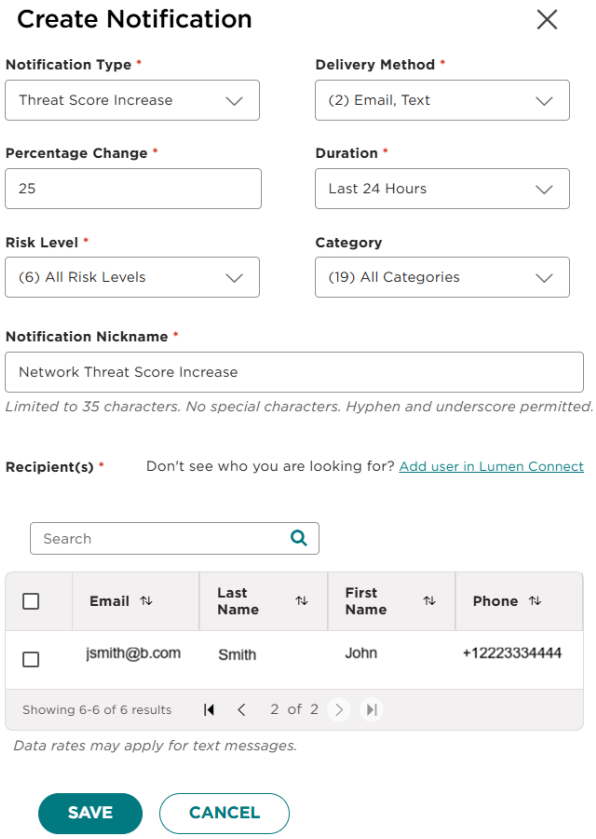
Threat Notifications: Proactive Awareness Without Constant Monitoring

The **Notifications** tab in Lumen Defender Plus reporting allows customers to proactively track changes in threat conditions without needing to continuously monitor the dashboard. By configuring targeted notifications, teams can stay informed when threat activity meets specific criteria that matter to their environment.

Using threat notifications, customers can:

- Create alerts based on **threat type, risk level, and category**
- Choose **delivery method**, such as email or text message
- Assign notifications to specific recipients within Lumen Connect
- Use clear nicknames to manage multiple notifications easily

This capability helps security and network teams remain **aware of emerging or changing threats in real time**, enabling faster awareness and response while reducing the operational burden of manual monitoring.



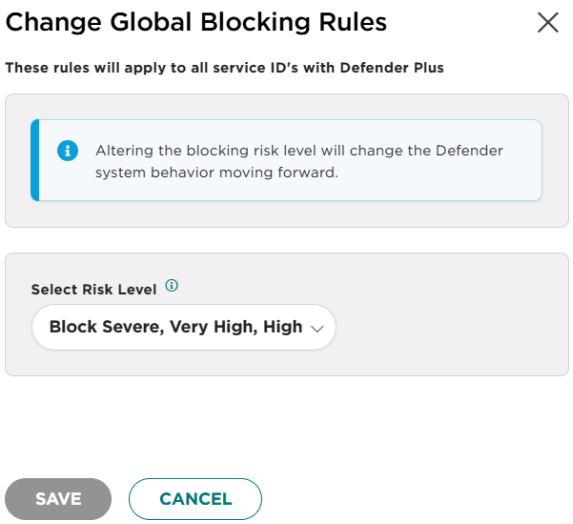
Global Blocking Rules: Consistent Policy Across Protected Services

The **Settings** tab in Lumen Defender Plus reporting gives customers centralized control over how threats are handled at the network edge through **Global Blocking Rules**. These rules define which threat risk levels are automatically blocked and are applied **consistently across all services protected by Defender Plus**.

From this view customers can:

- Select which **risk levels** (such as Severe, Very High, and High) are automatically blocked
- Update Defender behavior **moving forward** with a single configuration change
- Apply policy consistently without per-service configuration

Clear guidance within the interface reinforces that changes to global blocking rules affect **future system behavior**, helping customers make informed decisions.



Lumen Defender Plus brings together visibility, control, and consistency to help customers manage internet-based threats with confidence. It extends global, network-embedded threat intelligence into actionable insight, giving teams clear visibility into threat activity, direct control over how specific threats are handled, and centralized policies that apply consistently across protected services. With integrated investigation, custom lists, notifications, activity logging, and global blocking rules all managed through a single interface, Lumen Defender Plus enables customers to move efficiently from awareness to action while maintaining transparency and operational simplicity at scale.

For More Information

- Lumen Security Solutions: https://www.lumen.com/en-us/solutions/connected-security.html
- Lumen Internet On-Demand: https://www.lumen.com/en-us/services/internet-on-demand.html
- Black Lotus Labs: https://www.lumen.com/en-us/security/black-lotus-labs.html
- Sign in to Lumen Connect℠: https://connect.lumen.com/
- Learn more about Lumen: https://www.lumen.com/