

Use Case

Secure Internet Connectivity Without Added Complexity

Minimizing security noise while supporting flexible, high-performance connectivity

Organizations must balance network performance, flexibility, cost efficiency, and security without increasing operational overhead or complexity. As digital environments evolve, so does the attack surface, making visibility, control, and performance increasingly difficult to manage. For lean IT and security teams, success depends on delivering flexible, high-performance internet connectivity with built-in protection, so growth doesn't come at the cost of simplicity, security, or manageability.

Challenges

Organizations rely on internet connectivity to support cloud and internet-facing applications, but they face a dual challenge: maintaining reliable performance while managing constant internet-based threats. Lean IT and security teams struggle with fragmented vendors, reactive security tools, and attacks that lead to added operational complexity and greater risk.

- **Operational Complexity:** Managing connectivity and security through multiple, disconnected vendors adds unnecessary complexity for IT teams and can create blind spots that lead to attacks. Disparate solutions often come with their own tools, contracts, and management workflows, increasing operational overhead, while visibility gaps make it harder to see, control, and stop threats.
- **Balancing Growth with Performance and Cost:** As organizations adopt cloud and internet-based applications, connectivity must adapt to changing demand while delivering the right-sized level of performance and flexibility without overprovisioning or driving unnecessary cost. As applications become more internet-facing, teams must ensure protection keeps pace without adding complexity.
- **Consistent Availability and Performance:** As organizations rely more on internet connectivity to support cloud applications and digital operations, maintaining consistent performance and availability becomes critical. Without protection built into the network itself, IT teams are left reacting after performance is already impacted.
- **Security Noise and Resource Drain:** When security is layered on after connectivity, teams are left sorting through alerts, false positives, and noise after traffic has already entered the environment. Balancing agility with security often overburdens limited IT security resources, hindering innovation and growth.



42% of organizations struggle with real-time monitoring and threat detection, while 37% have difficulty hiring and retaining skilled cybersecurity professionals¹

Key usage examples

- Secure internet access for cloud and internet-facing applications
- Simplifying network and security management with one vendor
- Turning up and adjusting connections on demand without increasing security risk
- Reducing security noise to free up IT resources

¹IDC InfoBrief, sponsored by Lumen, [The New Cybersecurity Equation: Risk, Response, and Business Outcomes](#), doc #US53083025, February 2025

Solution

Lumen® Internet On-Demand provides a flexible foundation for on-demand connectivity. Lumen DefenderSM and DDoS Essentials extend that foundation with network-embedded security, enabling customers to flex internet access with simplified operations and protection already in place to help reduce threats without added complexity.

Lumen Internet On-Demand

Designed to support dynamic, internet-facing applications, Lumen® Internet On-Demand offers elastic, dedicated bandwidth options up to 100 Gbps so businesses can scale based on need to maintain continuity and respond quickly to demand while avoiding overprovisioning, long-term contracts*, or complex network redesigns.

Lumen Defender

Powered by Black Lotus Labs®, Lumen DefenderSM is an optional service to help fortify Lumen Internet On-Demand connections by blocking known malicious internet-based threats at the network edge. By stopping bots, scanning activity, proxy, malware, and command-and-control infrastructure upstream, Defender helps reduce noise and alert fatigue, to enhance security efficiency without added hardware.

Lumen DDoS Essentials

Lumen® DDoS Essentials provides pre-emptive, multi-layered, automated protection against common volumetric DDoS attacks from malicious actors for automated protection backed by Threat Intelligence from Black Lotus Labs. It is available as an add-on service to Internet On-Demand, making it easy and quick to implement.



*Lumen Network On-Demand Service requires access to a NaaS-enabled port subject to eligibility requirements and subject to separate minimum term agreement and associated early termination charges.

Results

By combining on-demand connectivity with network-embedded security, mid-market organizations can adapt internet access with confidence while simplifying operations. Lumen Internet On-Demand, Lumen Defender, and Lumen DDoS Essentials deliver the agility of cloud-like networking with built-in protection to help organizations reduce complexity, improve availability, and proactively stop threats before they impact the business.

Enable flexible connectivity

Internet services can be provisioned, adjusted, and scaled in real time through customer-controlled, API-driven connectivity. This allows organizations to respond quickly to changing application demands while maintaining consistent performance as internet exposure grows.

Integrated security from the start

Security can be embedded directly into connections and enabled during provisioning, so security is the default, not an afterthought. Known malicious traffic and volumetric attacks are addressed upstream to help reduce operational strain. This also helps organizations avoid adding tools, hardware, and management overhead as internet connectivity scales.

Proactively stop threats and minimize downstream costs

By proactively blocking malicious internet-based threats before they can infiltrate the customer's network, organizations preserve performance, minimize alert fatigue, and avoid the downstream strain and costs associated with reactive mitigation, helping lean teams protect internet-facing applications efficiently.

Unlock the power of Lumen Connectivity and Security Services to drive your digital transformation with secure, seamless, and scalable solutions.

Visit lumen.com today to learn more and take your connectivity strategy to the next level.

Why Lumen?

With a comprehensive portfolio, Lumen can help your business deliver high-quality connectivity, minimize costs and complexity, and enhance your security posture. Rely on the extensive and deeply peered Lumen global network, Black Lotus Labs' threat intelligence, and our team of experts to help deploy and manage the solution.

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