Lumen Releases an Updated Connected Security Strategy

Martha Vazquez   Christopher Rodriguez

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: The Lumen Platform and Enhanced DDoS Mitigation Services

In September 2020, CenturyLink was restructured and rebranded as Lumen Technologies, representing the company's overall and enterprise business. In October, the new company announced enhancements to its DDoS mitigation capabilities and a new offering, DDoS Hyper, built on the Lumen platform. The announcements are the fruition of months of planning and development from its CenturyLink days. Overall, the enhanced DDoS mitigation updates show the company's focus on security as a key component of its enterprise platform.

Key Takeaways

- Lumen's enhanced DDoS mitigation capabilities include a three-tier scrubbing center architecture to minimize latency and mitigate massive attacks.

- Lumen updated its DDoS mitigation service to leverage its Rapid Threat Defense automated detection and response capabilities. Rapid Threat Defense is automatically updated with Black Lotus Labs intelligence to provide instant protection against the latest threats.

- DDoS Hyper is a self-service offering currently for midsize to low-end large enterprises in North America (with expansion planned) that provides automated quote, order, and activation in minutes for simple and quick on-demand protection.

- For Layer 7 DDoS attacks, the Lumen Secure CDN Cloud Edge platform delivers application performance and protection including DDoS mitigation, antibot services, and web app firewall.

- Lumen Connected Security includes botnet takedowns, which have been used to stop proliferation of DDoS attacks and ransomware. While the tactic helps Lumen better defend customers' networks, the takedown service offers a communal benefit by slowing and deterring attackers.

Source: IDC, 2020

IN THIS MARKET NOTE

Following Lumen Technologies' rebranding and restructuring from CenturyLink to Lumen Technologies, the company released a series of new offerings based on the Lumen platform. Among them were enhancements to the company's DDoS mitigation capabilities: automated threat detection and response based on integration of high-fidelity threat intelligence from the company's Black Lotus Labs research, a new tiered architecture, and a new offering – DDoS Hyper – that permits customers to self-serve through the company's new digital buying experience. Lumen's platform places security at the forefront in providing a seamless application experience for the customer. With security becoming virtualized, the buyer experience will become much easier for customers to consume Lumen's services. The company has integrated automation to provide a digital self-service and real-time buying experience. This IDC Market Note provides insight into the enhanced Lumen DDoS mitigation services and the new DDoS Hyper offering.

The Lumen platform is the heart of the company's new brand vision. It helps enterprises orchestrate and automate on-premises, multicloud, and edge infrastructure to accelerate the next generation of business applications and data. The tagline for the platform, "The platform for amazing things," highlights the platform's potential for enabling innovation, business agility and, ultimately, user experiences. One of the platforms that will support this application experience is the Lumen Cloud Edge. Lumen has already repurposed over a 100 legacy datacenters into microcloud datacenters to ensure a better application experience for the customers by allowing them to be closer to where they are being consumed.

DDoS Hyper is a first step in Lumen's launch of the company's new buying experience, which also included the introduction of Hyper WAN and Layer 3 Dynamic Connections. DDoS Hyper is an enhanced automated, on-demand, and self-service DDoS mitigation offering that allows customers to deploy DDoS mitigation services through an online portal in minutes. Lumen's DDoS Hyper can be activated on demand and helps customers protect their third-party internet assets and/or applications.

The following Lumen enhancements apply to both DDoS Mitigation Service – which is targeted to the broad global DDoS market – and DDoS Hyper – which is currently targeted to midsize to low-end large enterprises in North America, with expansion to come:

- **Rapid Threat Defense.** It is a network-based detection service that uses the IP backbone and DNS as a threat sensor. It leverages Lumen's threat research and response team, Black Lotus Labs, for its threat intelligence to see and stop attacks before entering the customer's network. Black Lotus Labs will refresh every 15 minutes for any new security policy updates. By using SOC-defined security policies, it can automatically block attack traffic before the threats impact the customer.

- **A new proprietary Three-Tier Scrubbing Architecture:** The new scrubbing architecture is built on next-generation technologies that enable intelligent scaling for mitigation against massive DDoS attacks. The three-tiered approach is built on super, regional, and local scrubbing centers. The platform can detect when a customer's application is being attacked or not, depending on what is occurring at that time. Lumen can serve the application at a microscrubbing center closer to where the application is being hosted at. But in the case of an attack, the network can intelligently route the application traffic to either a regional or a super

scrubbing center, depending on which will provide the most optimal protection and application performance.

DDoS Hyper includes:

- **The digital buying experience:** Customers can rapidly utilize a self-service portal ordering, configuring, and deploying DDoS mitigation services to protect Lumen or third-party internet.
- **Professional security services option:** Lumen will also offer additional professional services if needed, with a security specialist to guide the customer during the installation process and after the service is implemented. The customer can get assistance around the attacks that are occurring and get recommendations and guidance to make the service more efficient.

IDC'S POINT OF VIEW

Lumen has made positive changes in its security offerings throughout 2020, culminating in a series of announcements throughout October. As technology evolves toward the edge, customers have become concerned about their applications' security, availability, and performance. Lumen addresses these areas by structuring its services to help customers by protecting Layers 3, 4, and 7. For Layers 3 and 4, the service protects against volumetric DDoS attacks as a carrier-agnostic first line of defense. At Layer 7, Lumen provides application performance and security at the edge, with capabilities such as web application firewall, bot management, and API protections.

Lumen Technologies has been on the journey to elevating its security position and has recently made significant strides in its DDoS mitigation offerings. First, it offers DDoS Hyper, allowing customers to go through a seamless quote to purchase and then configuration through an automated means. The company has also simplified its pricing model to offer up to 10 clean traffic return paths and 10 flow-based monitoring instances. Second, its DDoS mitigation offerings are built on a proprietary multitiered intelligent scrubbing architecture through its 15 global scrubbing centers, which will help customers with large volumetric attacks. The service can also offer customers DDoS mitigation in a carrier-agnostic manner and allow the customer to be on Lumen or a third-party internet.

With Lumen's updated DDoS mitigation offering, going through a tiered scrubbing approach will help the customers (especially the "always-on customer") by having their network traffic analyzed closer to them, which will reduce latency and provide better application performance.

Another key differentiator in the updated DDoS Mitigation Service is the integration of Black Lotus Labs that leverages Lumen's global backbone traffic as a threat sensor to see threats on the network. Black Lotus Labs ingests 190 billion NetFlow sessions and takes in 771 million DNS queries daily to help build a baseline of expected and abnormal traffic behavior. The threat validation model used by Black Lotus Labs drives network-based intelligence and can validate command and control (C2) servers on an ongoing basis, taking down an average of 63 C2s each month. Having this breadth of visibility and capabilities embedded into its security offerings enables Lumen to identify and stop threats before they cause massive damage to a customer.

DDoS risk escalated again in 2020, with a resurgence of massive record-breaking attacks, in terms of both bandwidth and packets per second attacks. With the recent spike in DDoS attacks, service providers are at a point where they need to speed up response times to stop these advanced attacks from occurring immediately. Having an automated response that can prevent bad traffic from ever reaching the customer is critical. Also, having the ability to instantly spin up a security service rapidly — such as with DDoS Hyper — is beneficial for those already under attack or believe one is imminent.

IDC has continued to see the emergence of platforms in the security services market. The market has been undergoing these new architectures that bring in various components of computing functions. From a security standpoint, adopting a unified platform helps integrate specific functions, optimizes operational efficiencies by delivering better automated and response mechanisms against cyberattacks, and streamlines ticket workflows.

The rebranding effort has been in development for a long while, but Lumen believes that it lays the foundation for its future growth. Positively, Lumen made investments in its security services and platform that the company announced during the first half of 2020. The platform-centric approach for its security and other offerings, such as DDoS mitigation, demonstrates Lumen's commitment to prepare for the fourth industrial revolution, which also adds in IoT/OT. Lumen has raised the bar for the type of future advancements that enterprise buyers might expect from a security perspective.

LEARN MORE

- *Market Analysis Perspective: Worldwide Security Services, 2020 – The New Normal in Security Services* (IDC #US46870720, October 2020)
- *IDC FutureScape: Worldwide Future of Trust 2021 Predictions* (IDC #US46912920, October 2020)
- *CenturyLink Rebrands, Restructures as Lumen Technologies* (IDC #lcUS46861420, September 2020)
- *Pervasive Application Edge Defense: An Application-Based Framework for Trust* (IDC #US46810219, September 2020)
- *IDC Market Glance: Software-Defined Secure Access, 2Q20* (IDC #US46291520, May 2020)
- *Worldwide DDoS Prevention Products and Services Forecast, 2020-2024* (IDC #US46015019, February 2020)

Synopsis

This IDC Market Note provides insight into the enhanced Lumen DDoS mitigation services and the new DDoS Hyper offering.

Following Lumen Technologies' rebranding and restructuring from CenturyLink to Lumen Technologies, the company released a series of new offerings based on the Lumen platform. Among them were enhancements to the company's DDoS mitigation capabilities: automated threat detection and response based on integration of high-fidelity threat intelligence from the company's Black Lotus Labs research, a new tiered architecture, and a new offering – DDoS Hyper – that permits customers to self-serve through the company's new digital buying experience.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com