

Mission-partner relationship for

innovative data security solutions



Challenge:

- **Replace an end-of-life solution** for capturing NetFlow and identify additional potential capability gaps
- **Extend visibility outside of customer's defensive perimeter**, including on blocked traffic

Solution:

- **Scalable Lumen-hosted solution** enabled rapid adaptation to meet evolving needs
- **As-a-service model** came at a flat rate to simplify budgeting

Results:

- **Successfully implemented global NetFlow solution at scale**, capturing line rates at 10 Gbps.
- **Fifty percent cost reduction** over previous solution

The U.S. government is one of the nation's largest employers, overseeing millions of employees worldwide. Various agencies work in concert to support the internet defense of the nation, including maintaining robust cyber defense capabilities. To provide the IT services required for mission success, these agencies leverage the expertise of network service providers and managed security service providers, like Lumen, to deliver adaptable, best-in-class solutions while complying with federal regulations and procurement requirements. The ability to obtain solutions that enable agility, while maintaining the highest level of security and performance, is imperative. In keeping with the mission-led government and industry partnership developed over a years-long relationship, Lumen solutions are helping the government innovate against the most serious of threats.

Global NetFlow solution

In 2014, a federal agency sought provider support to replace an end-of-life NetFlow solution, as well as identifying additional complementary and synergistic capabilities that could be provided commercially outside of the agency's defensive perimeter. The agency articulated the need for a service-oriented and managed solution that would eliminate the up-front capital investment and long-term life cycle support normally associated with government-owned and operated solutions.

Lumen designed and proposed a NetFlow as-a-service solution that exceeded the capabilities of the customer's end-of-life solution in several important ways:

- **Financial:** The Lumen solution eliminated the need for the customer to invest capital up front for system procurement. Additionally, the as-a-service model came at a flat rate to simplify budgeting. Finally, Lumen's solution delivered a more robust capability at a significantly lower cost than the current end-of-life system.
- **Flexibility and agility:** Because the customer could not wait years to work through federal procurement processes to acquire a new solution, Lumen proposed a commercial solution hosted in our ISP space which enables us to rapidly adapt the solution to meet the customer's evolving needs. Lumen also added meta data fields, modified how the NetFlow data was labeled and delivered, and created summary records for some NetFlow data types to reduce data storage requirements while still meeting analyst's mission needs.
- **Robust solution:** Lumen's solution provided new and additional information to the agency's analysts, such as NetFlow on all traffic, including traffic that was later blocked at the agency's boundary, as well as new metadata fields not provided by the current end-of-life solution.

Traffic blocking solution

Based on the success of the NetFlow solution, Lumen was asked to develop and implement a geo-based blocking capability in under a month. While the initial requirement was limited to blocking traffic based on geography, the Lumen team designed the solution on a highly flexible architecture to help ensure the end solution would support a myriad of full firewall capabilities. Within 30 days, Lumen delivered an operational geo-based blocking capability to limit IP traffic based on specific geographic parameters. Because flexibility and agility were designed in from the start, the customer has been able to quickly add certain firewall rule sets and additional types of blocking capabilities.

Building to the future

One of the key benefits Lumen provides these federal agencies is the company's ability and willingness to pivot resources on demand for agile troubleshooting and addressing issues as they arise. Thanks to Lumen's

Combined customer outcomes

- Lumen's innovative approach to solving the varied network and security solution needs of these federal agencies resulted in the following essential outcomes:
- Shared mission focus: Lumen was able to offer more than a solution that just delivered data securely, but the greater ability to put that data to use through developing countermeasures and maintaining joint TTPs.
- Fifty percent cost reduction for global NetFlow solution for one of the agencies
- Expanded and improved meta data quality by adding 15 new meta data fields, allowing analysts to provide more refined analysis than previously possible
- Created summary records for certain types of traffic to reduce the agency's data storage needs
- Successfully implemented global NetFlow solution at scale, capturing line rates at 10 Gbps.
- Fully integrated DDoS solution leveraging Lumen's network to prevent attacks from impacting customer network infrastructure.
- Quality of Service capability implemented on Lumen routers to help ensure certain internet traffic bound for one agency will be delivered even in the event of global internet disruption.
- Analytics and data science at scale with security expertise and tools to thoroughly evaluate emerging problem sets and provide meaningful analysis at scale to detect and deflect threats such as nation-state actors.
- Responsive, on-call engineering support by Lumen security experts.

deep missionpartner relationship, one of the agencies implemented a new contract designed to be highly adaptable for rapid addition of new capabilities. Additionally, the deep mission-partner relationship with this customer will soon include personnel exchanges between the organizations to share tactics, techniques and procedures and further educate each other's workforces. This agency also indicated a growing interest to extend its view of the global threat landscape through Lumen's commercial products such as Adaptive Threat intelligence.