

Mission-partner relationship

For innovative data security solutions

Overview

Enhance cybersecurity defense while maintaining compliance with federal regulations and reduce cost

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 threats.

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.

Solution

Global NetFlow and traffic blocking

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:



Challenges

- 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

Solutions

- 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

Solution (cont.)

- **Financial:** The Lumen solution eliminated the need for the agency 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.

Results

Lumen's deep mission-partner relationship with federal agencies helps enable agile troubleshooting and rapid adaptation to emerging issues. This strong partnership has led to the implementation of a highly adaptable contract, allowing for the swift addition of new capabilities.

The collaboration includes personnel exchanges to share tactics, techniques, and procedures, further educating each other's workforces. Additionally, there is a growing interest in extending the agency's view of the global threat landscape through Lumen's commercial products, such as Adaptive Threat Intelligence

Results and the future

Innovative solutions that enhance cyber defense capabilities helping ensure secure, efficient, and scalable operations

Lumen's innovative approach to addressing the varied network and security needs of these federal agencies has resulted in several essential outcomes:

- **Shared mission focus:** Beyond secure data delivery, Lumen enhanced the ability to put the data to use through developing countermeasures and maintaining joint TTPs.
- **Cost efficiency:** Achieved a 50% cost reduction for a global NetFlow solution for one agency.
- **Enhanced data quality:** Added 15 new metadata fields, enabling more refined analysis.
- **Data storage optimization:** Created summary records for certain traffic types, reducing data storage needs.
- **Scalable solutions:** Successfully implemented a global NetFlow solution at scale, capturing line rates at 10 Gbps.
- **Integrated DDoS protection:** Leveraged Lumen's network to prevent attacks from impacting customer infrastructure.
- **Quality of Service:** Helped ensure delivery of critical internet traffic even during global disruptions.
- **Advanced analytics:** Provided analytics and data science at scale to detect and deflect threats, including those from nation-state actors.
- **Responsive support:** Offered on-call engineering support by Lumen security experts.

Through these efforts, Lumen continues to empower federal agencies with agile, secure IT solutions, enhancing their cyber defense capabilities.