Campbell Palmer
Vice President, Solutions Architecture
Lumen Technologies

It Starts With The Network

Lumen is a global telecommunications company that empowers organizations to ignite growth by connecting people, data and apps—quickly, securely and effortlessly.

Lumen brings together the talent, experience, infrastructure and capabilities of leading technology companies to address the dynamic data needs of next-generation applications.

During our history, Lumen has served multiple government agencies providing Multiprotocol Label Switching (MPLS)* networks, really focusing on that castle-and-moat topology and the legacy services of security outside of your network itself.

That said, we recognize the landscape is shifting due to the NIST 800-27 ZTA framework and we have pivoted as a result. And being a network backbone service provider, we recognize that Lumen brings a lot of value to Zero Trust architecture (ZTA) overall.

Lumen operates one of the most peered global IP networks. Our internet service network is integrated with our Black Lotus Labs platform that actually allows us to capture zero day security vulnerabilities so that our security operations teams can communicate any type of incident that takes place inside of a particular agency.

ZTA opportunities like this need an advanced application delivery architecture — designed specifically to handle the complex, data-intensive workloads of next-gen technology and businesses.

Use EIS For ZTA

Lumen also offers a framework for an acquisition strategy to obtain ZTA frameworks using the EIS contract leveraging Black Lotus Labs, our security operations team and our partners to help build out those policy enforcement points. This is then fully integrated with our security operations team where we have a SIEM and SOAR function that allows some level of automation for those endpoint devices.

It's key, though, as part of Zero Trust, to have strong authentication and identity management. So Lumen is going to be partnering with others in the marketplace to ensure that we have that capability to bring that all encompassing offer. And again, our goal is to make sure that we have that acquisition approach that we can provide a fully managed service offering.

Ultimately, agency CISOs have the responsibility of delivering that authority to operate to their agency. Part of the Lumen portfolio is offering managed services support that would aid the agency's CISOs in development of the system security plan and documentation to allow for that ZTA framework to be adopted into that agency's portfolio.

ZTA Secure Pathway

CISOs and CIOs are constantly balancing that management of risk with network transformation, and figuring out a path to accomplish both.

Lumen's Secure Access Service Edge (SASE) and SD-WAN are being integrated into agencies' topology as they move away from legacy networks such as MPLS and move forward into internet bound environments. They help you manage and maintain that risk framework and the integration of TIC (Trusted Internet Connection) infrastructure.

As agencies move from one contract to another, we're seeing they're taking that adoption opportunity to bring in new TIC capabilities and new technologies. They are leveraging the benefits of partners such as Palo Alto and integrating into a network service provider such as Lumen. Doing this enables them to get the benefits and the economies of scale to really build out that Zero Trust framework.

I think it's fair to say that malware attacks are here to stay, and they're going to be constant. We're all likely to undergo some type of exploitative event inside of the agency or your organization. The bad actors are prevalent and they're ever evolving. It's the only way that we can really focus on recognizing that we're going to have bad events. So, build up a framework and a policy that includes that DR and COOP capability to mitigate those zero day events.

Work with your vendors and your partners to allow your policy adoption to incorporate security event monitoring and the automation of application integration.

This is necessary to manage the downtime and minimize event impact. Further, recognize that you're constantly going to be under attack. In short, work with and partner with your vendors and your customers in order to ensure that you're building out the right architecture.

Moving ZTA Forward

Many of the agencies we work with are moving forward to that Zero Trust architecture. That includes moving into that world of identity management where you have human and non-human entities interacting. Human-to-machine and machine-to-machine interaction will be ongoing and require all the appropriate ZTA identity management infrastructure.

That entails building out the APIs and the enforcement

points, and being able to incorporate those into the security domain while recognizing that there's constant attack coming in from the outside. Managing those attacks, recognizing the overall risk posture and developing that policy optimization through governance and compliance will be a huge benefit to how agencies are able to be successful.

Our focus in this upcoming year is on building out infrastructure and embedding the foundational elements, such as securing our backbone using Black Lotus Labs (the security team that has the capability to monitor billions of network events that are taking place across our network every day).

We're able to extend those capabilities out to individual agencies and institutions. And we want to be able to incorporate that capability alongside other security offerings — e.g., distributed denial service mitigation — as well as taking that up to the application layer and extending that overall security framework out to our customers and agencies as we deliver those services to those endpoint users.

Our real focus is on securing those endpoints. Agencies are going to have their own device platforms and systems. We are able to incorporate the best possible user experience into a Zero Trust model that'll allow the agency to meet that full compliance, while we're continuing to focus on security and performance.

But in the end, it's about the end user experience. Our goal is to make sure that we have the best possible end user experience that we can envision.

Constant Growth

In the upcoming years the one thing that's constant is internet connectivity and traffic increasing exponentially every year. We're going to continually invest in that network backbone and build up the capacity to support the ever-growing application usage that's constantly taking place within agencies and the private sector.

So the complexity is going to be: How are you able to secure all of that network traffic as it's coming across your network? Our answer is to integrate our security services through Black Lotus Labs, DDoS mitigation, AI and machine learning. All are going to be absolutely critical to ensure that we're bringing and delivering that cleanest possible traffic to our end user agencies.

If you think about that from a Zero Trust standpoint, it always starts with the network. Our focus is really going to be on building out that network capacity and then augmenting the network with our security services and capabilities to deliver the best possible experience to our end users. ■

**Multiprotocol Label Switching, or MPLS, is a networking technology that routes traffic using the shortest path based on "labels," rather than network addresses, to handle forwarding over private wide area networks*

AUTHOR INFORMATION

Campbell Palmer is Vice President of Solutions Architecture for Lumen Technologies' Public Sector organization. He leads a team of solutions engineers, architects and associates supporting Lumen's federal, state and local government and education market. He is responsible for the technical development and delivery of complex services purchased on the open market as well as by government agencies via the General Services Administration's EIS, Schedule 70, and legacy Networx and WITS contract vehicles.

Campbell has held various leadership and individual contributor roles with Lumen's Public Sector organization spanning back to 2008. His primary focus as a leader has been to continually bolster the engineering organization's technical skillset and proficiency, while incorporating best-in-breed industry technologies into the Lumen product portfolio. Campbell and his team are responsible for delivering the technical solutions for all task orders awarded to Lumen under the EIS contract, including work supporting the U.S. Department of Veterans Affairs, Social Security Administration, Department of Interior, Department of Homeland Security, Department of Agriculture and multiple Department of Defense contracts.