Cabinet-level Agency

Zero Trust Architecture

Lumen Authors/Contributors:
Jeff Knisely, Solution Architect
Raleigh Rhodes, Solutions Architect Manager
Chris Sieber, Principal Architect
David Voegele, Technology Architect

LUMEN® TECHNOLOGIES

1. Overview: Zero Trust Architecture (ZTA)

The recently issued Executive Order (EO) 14028, Improving the Nation's Cybersecurity, represents an opportunity for your agency to transform, further secure their critical infrastructure and meet the requirements of this EO. Lumen offers your agency the following technology roadmap to leverage best practices and solutions, and the opportunity to work together on a timeline to achieve your agency objectives.

Based on the growing threat to your agency information assets and ability to conduct its mission, Lumen recommends your agency adopt a three-prong approach to achieve transformation while enhancing security and mitigating known risks. As your agency's mission partner we can jointly leverage security best practices in a tactical as well as strategic manner. With a focus on accelerating secure Cloud adoption and Zero Trust Architecture (ZTA) enablement, Lumen's vision for your agency Enterprise Services Network (ESN) network architecture includes immediate deployment of Software-Defined Wide Area Network (SD-WAN) implementation, Trusted Internet Connection (TIC) 3.0 integration and ultimately full adoption of a Lumen® Secure Access Service Edge (SASE) solution to achieve a Zero Trust Architecture. These three pillars will provide your agency a roadmap to modernize its security posture in compliance with EO and emerging requirements such as the Federal Risk and Authorization Management Program (FedRAMP) while maintaining existing security protections and compliance with National Institute of Standards and Technology (NIST) and Department of Homeland Security (DHS) Guidelines.

2. Executive Order (EO) and actions across bureaus

Based on the requirements defined in the EO, Lumen recommends the following course of action to address these new requirements to enhance your agency cybersecurity practices.

Table 2-1. Lumen recommendations to help agency achieve compliance with EO.

Executive Order	Lumen recommended approach to compliance
Incident reporting requirements for IT contractor	Leverage Lumen Best Practices and Bureau Best practices to define and develop Guidelines for Incident Reporting to the Joint Incident Response Team (JIRT).
Security requirements for software contractors	Integrate DHS Guidelines-Integration with your agency and Lumen security requirements.
Encryption, Multi-Factor Authentication (MFA), Endpoint Detection and Response (EDR) requirements for agencies	Enable MFA across your agency infrastructure for SD-WAN, Network Operations Center/Security Operations Center (NOC/SOC) Tools and access to EDR, Indicators of Compromise (IOC's), Incident Response (IR) and risk mitigations.
Cyber incident review board	Establish a cabinet-level agency-Lumen JIRT to develop Guidelines for adoption by each Bureau SOC and Lumen SOC.
Pushes toward ZTA	Align your agency initiatives toward a zero-trust network security model. Implement network segmentation using Software-Defined Wide Area Networks (SD-WANs) with the addition of identity and access management for full Layer 7 visibility.
FedRAMP cloud security modernization	Adopt applicable Modernization guidelines and implement automation as needed to support evolving Cloud accreditation practices.
New fed cloud strategy	DHS Guidelines-Adopt as applicable and integrate into your agency cloud adoption strategy and ZTA.
Internet of Things (IoT) security labeling pilot program	Identify pilot bureau and groups to trial IOT Tagging. Identify available solutions, develop your agency specific groups and policies document Lessons Learned for Methods and Procedures documentation.
Encourages Software Bill of Materials (SBOM)	Define requirements for when a SBOM is required, and level of detail needed for each application.
CISA incident response "playbooks" for agencies	Lumen Managed Security Service (MSS) provides timely reaction and is equipped to be adept for future responses to new threats; policies continually refined and implemented; automated adoption of new countermeasures
Government-wide log retention/analysis policy	Lumens ZTA facilitates the secure capture, retention, and transmission of logs to the Cloud Log Aggregation Warehouse (CLAW) for analysis.

3. FY2021–2022 Tactical Approach

3.1 Implement Software-defined Wide Area Network (SD-WAN)

Lumen recommends immediate implementation of SD-WAN and parallel adoption of Lumen's TIC 3.0 solution. Jointly implementing SD-WAN and TIC 3.0 accelerates your agency's enablement of ZTA by using distributed security at the edge for all inbound/outbound traffic. With SD-WAN and TIC 3.0 now in place, we assess the device posture and combine that with the Multi-Factor Authentication (MFA) to authenticate the user identity before the user can connect. ZTA allows only access based on policies tied to users' identities; therefore, the user's Active Directory (AD) identity and role is tied into agency-specific user security policies. The Lumen solution supports several of the ZTA pillars:

- Authenticate before connecting Multi-Factor Authentication
- Segmented access-Security Group Tagging/VPN Segmentation
- Identity Based Access AD integration with your agency identity and role-based access policy

Lumen's recommended timeline for your agency's 2023 approach to implementing ZTA is to transition your agency to a network foundation that enables the adoption of both TIC 3.0 Architecture and ZTA in the next 24 months. Leveraging Lumen's SD-WAN solution we will first transition and transform the existing agency network. Secondly, and in parallel, we will transition from five TIC gateways to a distributed TIC 3.0 Architecture.

SD-WAN is built on the idea of Zero Trust, which starts by verifying the identity of each Edge device that attempts to join the network using trusted certificates. Subsequently, encrypted tunnels are established between Edge devices. This ensures that no untrusted elements are used to build the network and all data traversing the network is protected, regardless of the underlying transport. Lumen's SD-WAN solution offers VPN segmentation and topology control. This allows data to flow only where it is required, eliminating exposure to sites, endpoints, or users who should never have access. This topology control allows traffic to be sent through a centralized security infrastructure if necessary.

In addition to these elements, SD-WAN has multiple ways of enforcing security at the Edge locations where users and endpoints join the network, also driving towards a Secure Access Service Edge (SASE) architecture. Locations with user and endpoint authentication can take advantage of micro segmentation. Users are assigned least privilege access and can subsequently be assigned a specific security group label allowing further segmentation within a VPN or micro-segmentation. SD-WAN carries and enforces these labels across the overlay to provide a uniform security policy and segmentation across the entire network. Additionally, SD-WAN offers a full stack of security features at the Edge including on-box Firewall, intrusion detection system (IDS), Malware, URL Filtering, and Domain Name Service (DNS) protection. This can be applied to traffic before it enters the rest of the network, or as it comes in from external connections or services.

In addition to the embedded security features, Lumen's SD-WAN offers the ability to tunnel traffic to a Cloud Security stack for Security as a Service (SaaS). This allows traffic to or from a location to utilize a full suite of features such as a Cloud Firewall, DNS protection, and Secure Web Gateway, including Malware protection.

SD-WAN establishes trust of its own devices, provides mechanisms for "least trust" access to the network, and offers multiple layers of security at the premises and in the cloud securing traffic from all entry points to the network. All these features and capabilities are key components to a Zero Trust Network Architecture.

3.2 Develop Internal Cloud Access Point Security Standards and Guidelines

Lumen will assist in the development of your Agency Internal Cloud Access Point (ICAP) guidelines documenting your agency best practices for increased use of cloud service models, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and SaaS. This agency internal effort can provide your agency's or bureau's standards-based cloud security access and provide a foundation for ongoing cloud security collaboration. Centralization, encryption, and access to threat data to the agency infrastructure can be facilitated through adoption of secure cloud compute services. Access to encrypted data at rest by cabinet-level agency authorized personnel using a standards-based risk model will enable threat discovery and automated risk mitigations to be implemented based on your agency standardized metrics. Further, risk metrics unique to each Bureau can be developed while continuing to protect the existing agency network infrastructure during transformation.

Lumen best practices can be leveraged by your agency to establish their internal security controls for securing access to IaaS, PaaS, and SaaS cloud service models. Working with your agency, Lumen® Cloud Security Experts can assist your agency in documenting industry best practices as well as agency-unique requirements that will support and facilitate the overall ZTA and infrastructure. We recommend a joint Cloud Security Team be established to define the agency-specific controls and policy to meet current and ongoing cloud security requirements to maintain a secure agency infrastructure.

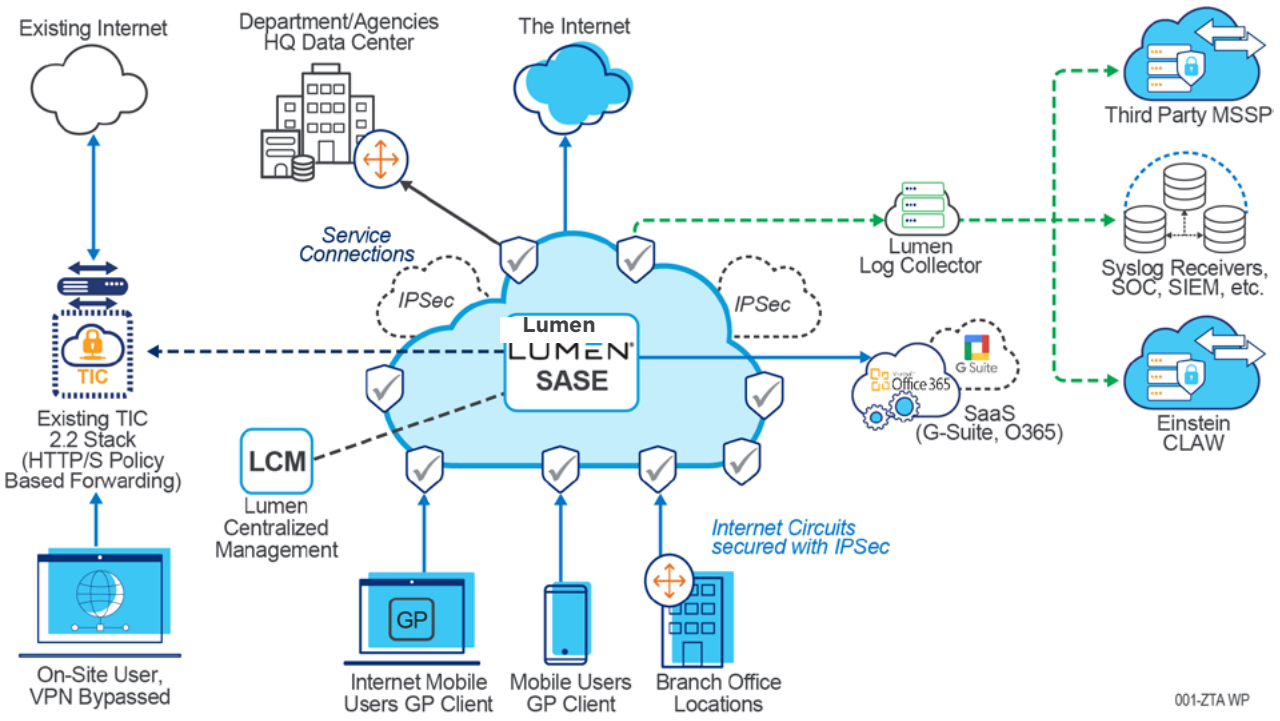

Figure 3.2-1 Typical Configuration of Lumen's proposed ZTS solution

4. FY2022-2023 strategic approach

As your agency completes transition from the SD-WAN implementation and TIC 3.0 adoption enabling a foundation for ZTA, we will pivot to the next phase of the strategic plan in Q1/2023. Lumen and your agency will further leverage Lumen's ZTA capabilities with the next phase focused on SASE. Working with our industry partners and building on our TIC 3.0 Architecture we plan to incorporate a Lumen centralized access solution that addresses Federal agency TIC 3.0 initiatives and the Executive Order 14028, Improving the Nation's Cybersecurity EO 14028, including the adoption of a Zero Trust security architectural model.

As a pioneer in TIC and Zero Trust solutions, Lumen enables the most comprehensive set of capabilities that align with the NIST SP 800-207 and TIC 3.0 concepts of Policy Enforcement Points to enable a true, end-to-end ZTA with common policy enforcement, including full Layer 7 visibility over all ports and protocols.

Figure 3.2-1, above, depicts a typical configuration of a high-level architecture of Lumen's proposed ZTA solution for your agency. Lumen's ZTA solution shields private applications from public exposure to the internet by directing users through the cloud-based SASE where they are authenticated. User access is then provisioned according to the policies the organization sets for the given user, role, or type of device, regardless of location. Lumen's ZTA solution monitors all authenticated user traffic to and from the application for malware signatures, intrusion behaviors, and indicators of data loss with single-pass architecture.

As a unified and consistent set of policies and enforcement across physical, virtual next-generation firewalls, the Lumen SASE infrastructure facilitates the improved Incident Response objectives of EO 14028. Lumen is working closely with the Cybersecurity and Infrastructure Security Agency (CISA) to enable DHS situational awareness of the federal government's security posture by integrating with the CLAW. Lumen's approach to TIC 3.0 and SASE is a wholistic security strategy that can provide your agency with an integrated security solution in providing Zero Trust capabilities and compliance with applicable standards and requirements of EO 14028.

Lumen looks forward to continuing work with your agency to plan and execute a near-term solution that will transform and secure the agency infrastructure and meet the requirements of EO 14028, while maintaining existing agency security protections and accreditations.

Connect with a Federal Security Solutions Expert

LUMEN® TECHNOLOGIES