SPECIAL TECHNICAL REPORT

Marc Packler

FULFILLING THE ZERO TRUST MANDATE

OPTIMIZING DEFENSE IN MODERN GOVERNMENT NETWORKS WITH TELLABS PON

JUNE 2026

FULFILLING THE ZERO TRUST MANDATE

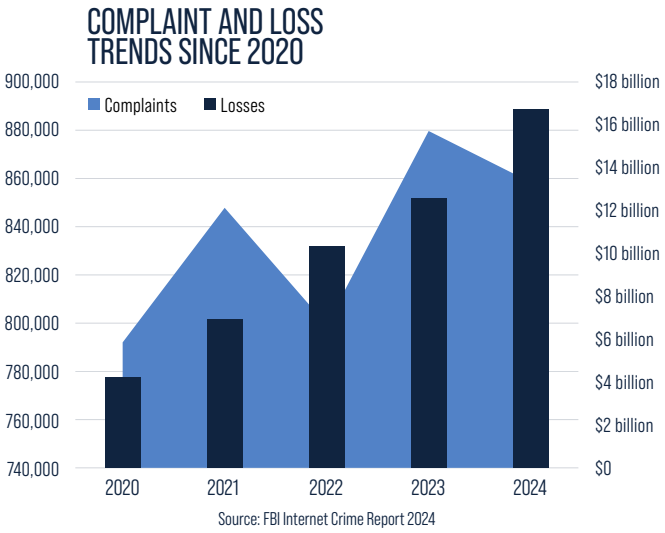
OPTIMIZING DEFENSE IN MODERN GOVERNMENT NETWORKS WITH TELLABS PON

The rapid digital transformation of government — aimed at streamlining operations and improving the quality and efficiency of services — has inadvertently created an exponentially larger, more complex cyber-attack surface amid an unprecedented threat surge. Cyber attacks have more than doubled from 2018 to 2024, resulting in reported financial losses of a staggering $16.6 billion last year alone[1]. This crisis is intensified by escalating state-sponsored adversaries that threaten critical infrastructure and the emergence of artificial intelligence (AI). While AI offers powerful defensive capabilities, it also enables more sophisticated, evasive attacks. An estimated 40% of all cyber attacks are now AI-driven, prompting urgent warnings from the FBI and the Cybersecurity and Infrastructure Security Agency (CISA).

Traditional perimeter cybersecurity is no longer adequate for modern government networks. With a range of cloud-based services, millions of connected IoT and mobile devices that span geographic borders, interfaces with external partners, and the rise of remote work and BYOD policies, these networks are increasingly complex and perimeter-less. At the same time, the complex mix of modern and legacy IT and OT systems, along with a shortage of IT talent, creates the potential for unmanaged and orphaned assets that are more vulnerable to attack.

To secure the landscape, Zero Trust architecture (ZTA) — a cybersecurity framework built on the foundational principle of "never trust, always verify" — is now the mandated standard. The U.S. government has committed to full Zero-Trust implementation across all branches by 2027, a considerable undertaking that spans every layer of unclassified and classified networks. Successfully moving toward ZTA cannot be achieved with a single tool or technology; instead, it requires building an integrated, cohesive ecosystem of Zero-Trust solutions, technologies, and processes that provide optimal security at each network layer while ensuring interoperability and scalability in multi-vendor environments.

Passive optical networking (PON) solutions provide a simple, security-first approach for the LAN, enabling centralized, policy-based control and seamless integration with advanced Zero-Trust systems and platforms, while facilitating scalability to support growing numbers of diverse users and devices and optimizing operational efficiency.



WHAT IS ZERO TRUST ARCHITECTURE (ZTA)?

Traditional cybersecurity methods assume trust once users or devices are inside the network, focusing on network-based perimeters to keep external threats out. In contrast, Zero Trust assumes that threats exist both inside and outside the network, shifting the focus to users, assets, and resources. It also assumes that a breach is inevitable and may have already occurred.

In ZTA, no user, device, or application is implicitly trusted, regardless of its location or connection method. Access to network resources is never guaranteed; it must be rigorously authenticated, authorized, and continuously validated in accordance with dynamic, risk-based policies. Implementing ZTA requires an integrated, multi-layered approach that includes several key components:

- **Identity and Access Management (IAM):** Strictly controls and monitors access for all assets (users, devices, and applications). It enforces the principle of least privilege by granting access only to what is needed, when it's needed, and requiring robust authentication, such as multi-factor authentication (MFA) and single sign-on (SSO).
- **Macrosegmentation:** Designates network assets into well-defined segments via VLANs and firewalls based on shared characteristics like asset type, function, or location. This protects north-south traffic (inbound and outbound).
- **Microsegmentation:** Divides network assets into more granular, isolated segments based on individual workloads. This protects east-west network traffic (lateral movement within the network) by isolating assets and preventing a single compromise from spreading.
- **Data and Device Security:** Protects data both

1. *Internet Crime Report 2024, Federal Bureau of Investigation*

in transit and at rest through encryption and continuously monitors and validates the health and security posture of all connected endpoints.

- **Policy-Based Enforcement:** Uses predefined, automated rules to implement and enforce dynamic, risk-based policies. This determines how data flows and which applications, users, and devices have access to it.
- **Real-time Visibility and Analytics:** Provides deep visibility into the network by continuously monitoring and analyzing traffic, user behavior, and event logs. This ensures real-time detection and response to vulnerabilities, anomalies, and potential threats.

These Zero-Trust components rely heavily on software-defined networking (SDN), which separates the network control plane (routing) from the data plane (traffic). SDN leverages standardized, open-source protocols to provide centralized network control and management, enabling dynamic, granular security policies across a multi-vendor network while providing real-time visibility.

SDN is a key feature of emerging secure access service edge (SASE) platforms that align with the U.S. government's Zero-Trust initiative. SASE is a cloud-based service that converges network orchestration and security functions into a single platform, including Zero Trust Network Access (ZTNA), Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), and firewall-as-a-service (FWaaS). SASE is beneficial for large, perimeter-less government networks because it routes all network assets, regardless of their location, through the cloud platform to gain secure access. This improves visibility, security, and control over traffic across all ports and protocols regardless of location, addressing the growing shift towards remote work, mobile access, and multi-cloud environments.

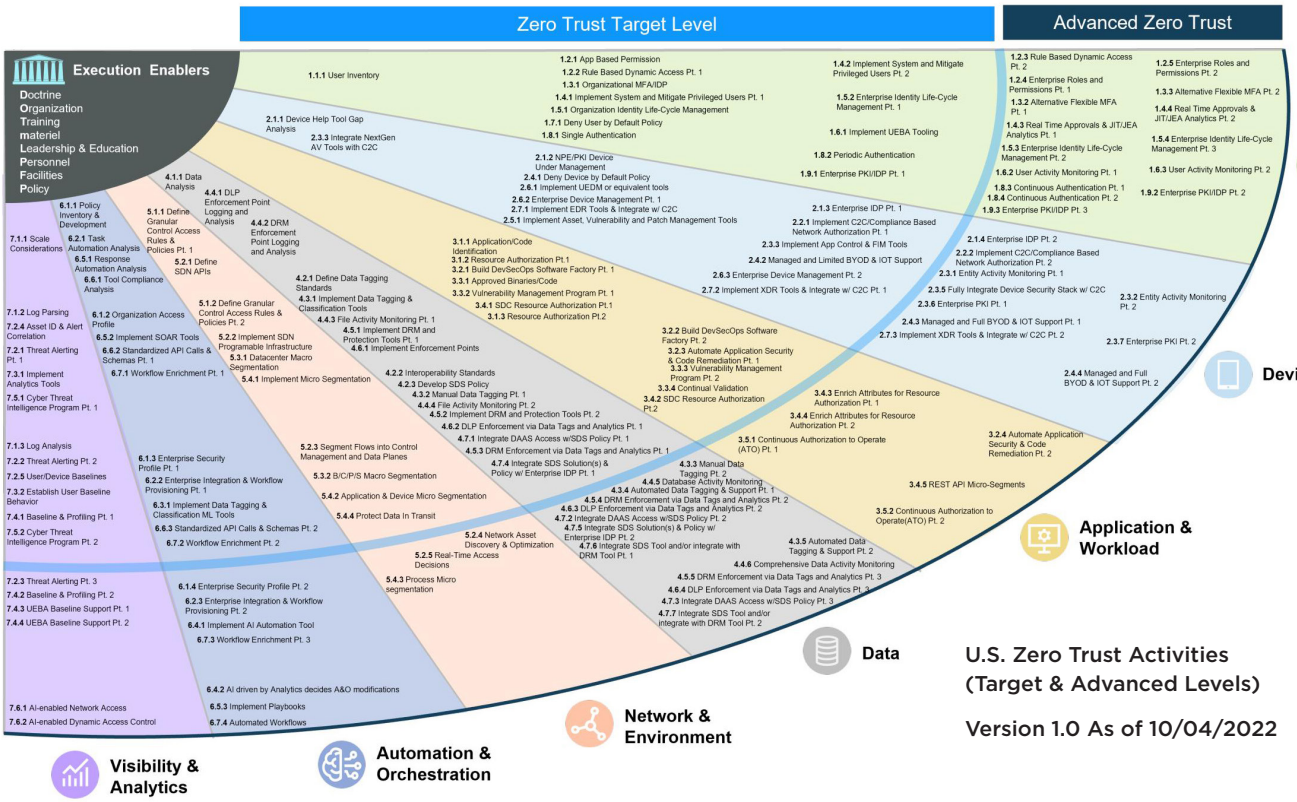
THE GOVERNMENT'S ZTA ROADMAP

The Pentagon established its Zero-Trust strategy in 2022, formalized by the White House Executive Order 14028. This order mandates that all federal agencies modernize their cybersecurity approach by accelerating the adoption of secure cloud services and fully implementing ZTA, recognizing that even the most advanced traditional perimeter defenses are now insufficient.

The goal of this Zero-Trust strategy is to ensure secure communication at all operational levels, enabling a more agile, mobile, and cloud-supported workforce to access network resources from anywhere via authorized, authenticated devices. The government's roadmap for achieving a ZTA is based on seven pillars, which guide the implementation of 152 activities across all agencies:

- **User:** Continually authenticate and monitor user activity patterns to secure and govern access to data, applications, assets, and services (DAAS), encompassing the use of identity capabilities such as MFA and Privileged Access Management (PAM).
- **Device:** Ensures continuous, real-time inspection, assessment, and patching information of every device. Every access request triggers examination of the device's health (compromise state, software versions, protection, and configuration) to determine authorization and limit access.
- **Network/Environment:** Focuses on logically and physically segmenting, isolating, and controlling network environments (on-premises and off-premises) with granular access and policy restrictions through macrosegmentation and microsegmentation that control privileges, secure internal and external data flows, and prevent lateral movement of threats.
- **Applications and Workload:** Secures and manages the complete application stack, from the application layer to the hypervisor, including on-premises and cloud-based workloads. Leverages development, security, and operations (DevSecOps) practices to secure applications and machines from inception.
- **Data:** Requires agencies to categorize their DAAS by mission criticality and develop a robust data management strategy. Protection is enforced through robust end-to-end encryption of data at rest and in transit, as well as solutions such as Digital Rights Management (DRM), data loss prevention (DLP), SDN, and data tagging.
- **Visibility and Analytics:** Captures and analyzes traffic and system telemetry to provide contextual details on events, activities, and behaviors. This improves anomaly detection and enables dynamic, real-time changes to security policy.
- **Automation and Orchestration:** Automates manual security processes to enable rapid, policy-based actions at scale. Security information and event management (SIEM) and AI-based Security Orchestration, Automation, and Response (SOAR) integrate disparate security systems to reduce response time and ensure consistent enforcement of security policies.

The Pentagon's roadmap sets a strict deadline. Agencies must achieve 91 "Target Level" Zero-Trust activities by September 30, 2027, with the remaining 61 "Advanced" Zero-Trust activities representing evolution towards next-generation security to address new and evolving threats.



KEY IMPLEMENTATION CONSIDERATIONS

Transitioning the vast U.S. government to ZTA poses significant challenges due to the sheer scale of its operations. Federal branches operate geographically dispersed, multi-vendor networks that are incredibly diverse and complex. These environments mix on-premises systems, private and public cloud environments, and legacy IT and OT systems, often featuring devices incompatible with modern protocols or encryption.

These networks also connect a myriad of devices and users, including millions of federal employees and contractors who often need to access resources outside traditional boundaries. ZTA requires that every user and device on every network be continuously identified, inventoried, authorized, and authenticated in accordance with dynamic security policies before accessing any data, application, asset, or service. Workforce challenges compound this massive technical undertaking — successfully embedding Zero-Trust training across a large, dispersed IT workforce is difficult, especially given the overall shortage of ZTA expertise in the market.

Since implementing ZTA is a time-consuming, costly, and disruptive undertaking, evaluating and procuring solutions must be highly strategic. Solutions should optimize security at every level of the network without adding complexity or hindering performance, maintenance, or scalability. It is essential to recognize that while no single solution can meet all ZTA requirements, all systems must work seamlessly together to form an integrated, cohesive security ecosystem.

The following key considerations can help streamline the implementation of ZTA:

1. Adopt a Best-In-Layer Approach

When designing ZTA, it's crucial to recognize that not all network levels are created equal. A strategic approach requires treating each level separately and selecting solutions that maximize security within that layer's confines without hindering its primary function.

Consider the physical layer (Layer 1), which includes components such as cables and connectors that carry data. While both copper and fiber connect devices, fiber is inherently more secure. It does not radiate emissions, making it impossible to "listen to" or eavesdrop on communications from a distance. Physically tapping fiber is also tremendously difficult, requiring specialized expertise and equipment. In contrast, copper cabling radiates emissions that can be intercepted without physical access.

The same approach applies to the data link layer (Layer 2) and the network layer (Layer 3), which are responsible for efficient data transport and routing. Here, information is evaluated based on basic network parameters (ports, MAC addresses, and IP addresses). Security at these levels — 802.1X port authentication,

bidirectional encryption, dynamic ARP inspection (DAI), access control lists (ACLs), network access control (NAC), and VLANs — must not introduce unnecessary complexity that impacts the objective of efficient data transport.

2. Deploy High-Level ZTA at the Application Layer

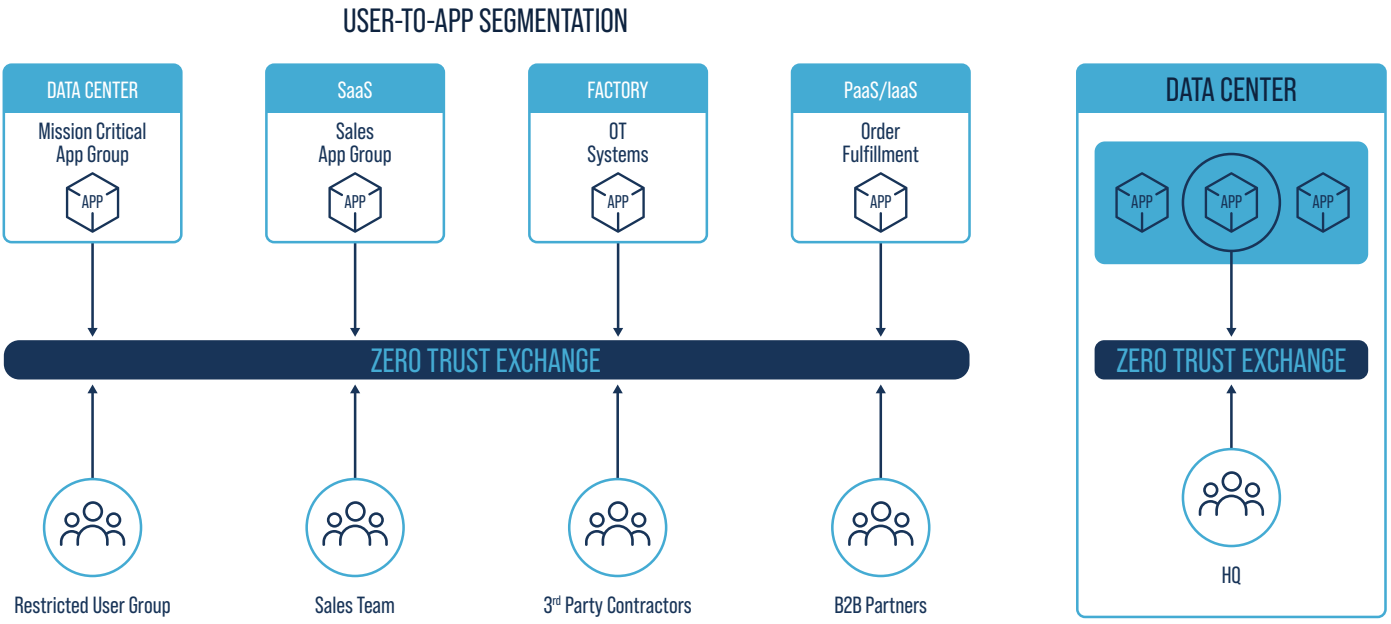
The application layer (Layer 7) serves as the interface through which users interact. Information here is evaluated based on the actual application being used and the specific user accessing it. This makes the application layer the best option for implementing higher-level, more complex ZTA components, such as IAM policies and microsegmentation. Deploying microsegmentation at the application layer defines access based on workload and identity rather than location, granting users access only to what they need, when they need it – regardless of location. This user-to-application segmentation offers the best risk reduction because users are the weakest link. It also avoids impacting network performance, allowing Layer 2 and Layer 3 to remain simple and focused on their core function of efficiently transporting data.

While solutions exist for deploying microsegmentation at the network layer, managing and scaling these solutions can be complicated, disruptive, and resource-intensive — especially in large networks. Proprietary microsegmentation at the network level, such as inline tagging, can also lead to costly vendor lock-in. These solutions require specific switches and routers from a single vendor, limiting integration in multi-vendor environments and lacking support for existing legacy IT and OT systems. This increases licensing and maintenance costs while raising the risk of misconfigurations that can create security gaps, access issues, and network instability.

3. Ensure Support for Multi-Vendor Environments

The government's highly diverse and complex networks require Zero-Trust solutions that ensure seamless support for multi-vendor environments across various systems and locations. The use of Application Programming Interfaces (APIs) is essential for integrating multiple network systems, applications, and hardware within the ZTA. Given the rise of cloud computing, it's also crucial for Zero-Trust solutions to integrate with public and private cloud platforms, as well as on-premises systems.

Zero-Trust platforms that integrate seamlessly with all systems maximize security and simplify implementation. This allows agencies to select solutions based on their specific best-in-class capabilities rather than deploying inadequate solutions that attempt to cover too much ground. Integrating



platforms that optimize various Zero-Trust capabilities — microsegmentation, threat detection and response, policy enforcement, and integrity monitoring — allows for a cohesive end-to-end Zero Trust ecosystem that delivers a highly robust, interoperable, multi-vendor network.

Given the significant risks posed by legacy IT and OT systems, it's also essential to choose solutions that provide secure access to legacy applications. Cloud-based Zero-Trust solutions can provide this capability by routing users through their platform, establishing a secure, one-to-one user-to-application connection without relying on traditional, vulnerable technologies.

4. Deliver Scalability and Operational Efficiency

When implementing ZTA, it's vital to choose solutions that can quickly and easily scale to keep pace with the ever-growing number of systems, applications, users, and devices deployed for digital transformation. Scalable solutions should achieve this without requiring manual processes and complex reconfiguration of network architectures that can disrupt operations. Automated solutions can significantly reduce the time and resources needed to authenticate new devices by automatically applying policies that ensure consistency across expanding network environments. Keeping higher-level, more complex ZTA capabilities at the application layer also means less time spent configuring and troubleshooting network appliances. This reduces errors and allows IT staff to focus on higher-value security solutions and initiatives.

To optimize operational efficiency and reduce costs, solutions should also be easy to use without requiring additional resources, intensive training, or ongoing certifications. Furthermore, solutions should simplify ongoing maintenance by enabling fast, automated firmware updates across all machines, eliminating the need for individual configuration and costly licensing fees. Finally, considering solutions with less power, cooling, and space requirements can help reduce energy consumption and the overall carbon footprint.

TELLABS PON: OPTIMIZING ZERO TRUST FOR THE NETWORK

Tellabs PON solutions play a vital role in the government's ZTA implementation, providing superior, best-in-layer network security for the LAN compared to traditional copper-switched networks — all while seamlessly integrating with advanced cybersecurity systems and platforms across multi-vendor environments, providing superior scalability, and improving overall operational efficiency.

99% Reduced Attack Surface

A network's attack surface is the sum of various ingress points where bad actors can initiate attacks. Tellabs PON reduces the attack surface by 99% compared to traditional networks.

In a traditional network, numerous, dispersed, full-functioning managed switches provide connectivity for users and devices, each requiring a public key infrastructure (PKI) for security and an IP address that represents a potential entry point. These switches are often web-based or accessed via command-line interfaces, and if not properly secured, can be exploited by attackers to manipulate network configurations,

redirect traffic, or intercept sensitive data. They also pose a security risk because they often store secure information, such as device configurations, user credentials, and network topology. Furthermore, Layer 2 switches must be located within 100 meters of their connected endpoints, requiring several physically secured IT spaces (e.g., IDF rooms) throughout facilities, which may not have uniform security policies.

In a Tellabs PON, unmanaged optical network terminals (ONTs) provide connectivity for users and devices on the LAN. Unlike traditional full-function Layer 2 switches, ONTs are extremely simple — they have no IP address for management, no physical management interface, and store no configuration or user information, thereby preventing attackers from exploiting them. ONTs are controlled exclusively by an Optical Line Terminal (OLT), the only component in the LAN that requires an IP address, PKI, and a physically secured location.

A single OLT can be sized to support up to 8,192 Ethernet ports and about 250,000 endpoints, providing superior scalability. The same number of ports in a traditional switched network would ultimately require 171 switches (48-port), each of which must be adequately secured (both logically and physically).

Best-in-Layer Security

While high-level ZTA capabilities such as microsegmentation are better handled at the application layer via focused Zero-Trust platforms, Tellabs PON solutions provide superior Zero-Trust security for the LAN while optimizing the primary function of efficient data transport.

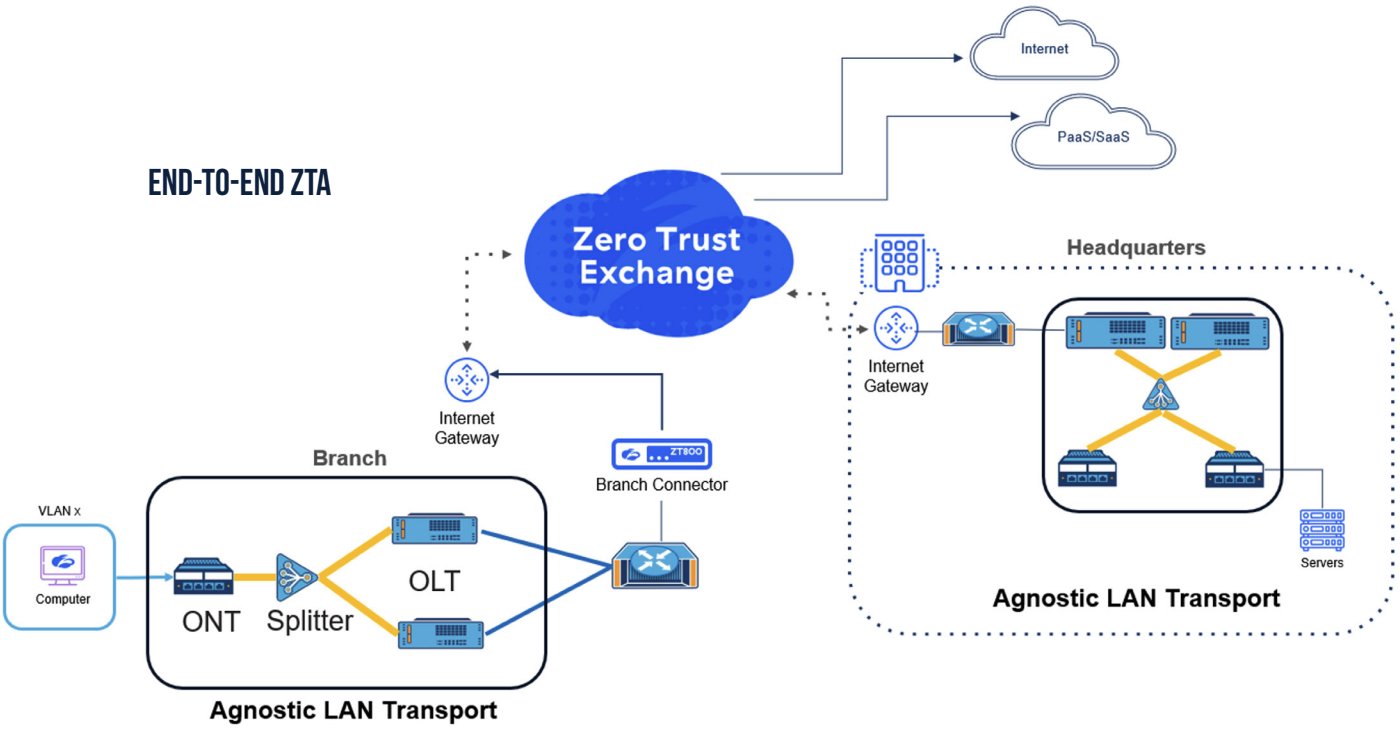
- **Optical Fiber Infrastructure:** PON uses fiber optic cabling, which is more secure than copper since it's not susceptible to interference, does not radiate emissions, and is virtually impossible to tap. PON also works with alarmed fiber cabling solutions that establish government-certified (NSTISSI 7003) protective distribution systems (PDS) for secure pathways.
- **Data Protection:** Tellabs OLTs use 128-bit bidirectional encryption (AES) with dynamic changing keys for all downstream and upstream transmissions, while all management interfaces are encrypted per Federal Information Processing Standards (FIPS) 140-2 standards.
- **Authentication:** Tellabs OLTs assign 802.1X port authentication to individual ONT ports and will deny access to all ports until the device has authenticated. Unused ONT ports are unconfigured by default and cannot pass traffic. OLTs also support MAC Authentication Bypass (MAB) to authenticate devices that do not support 802.1x using MAC addresses. This includes legacy hardware and peripherals, which are typically not supported by complex inline data tagging.

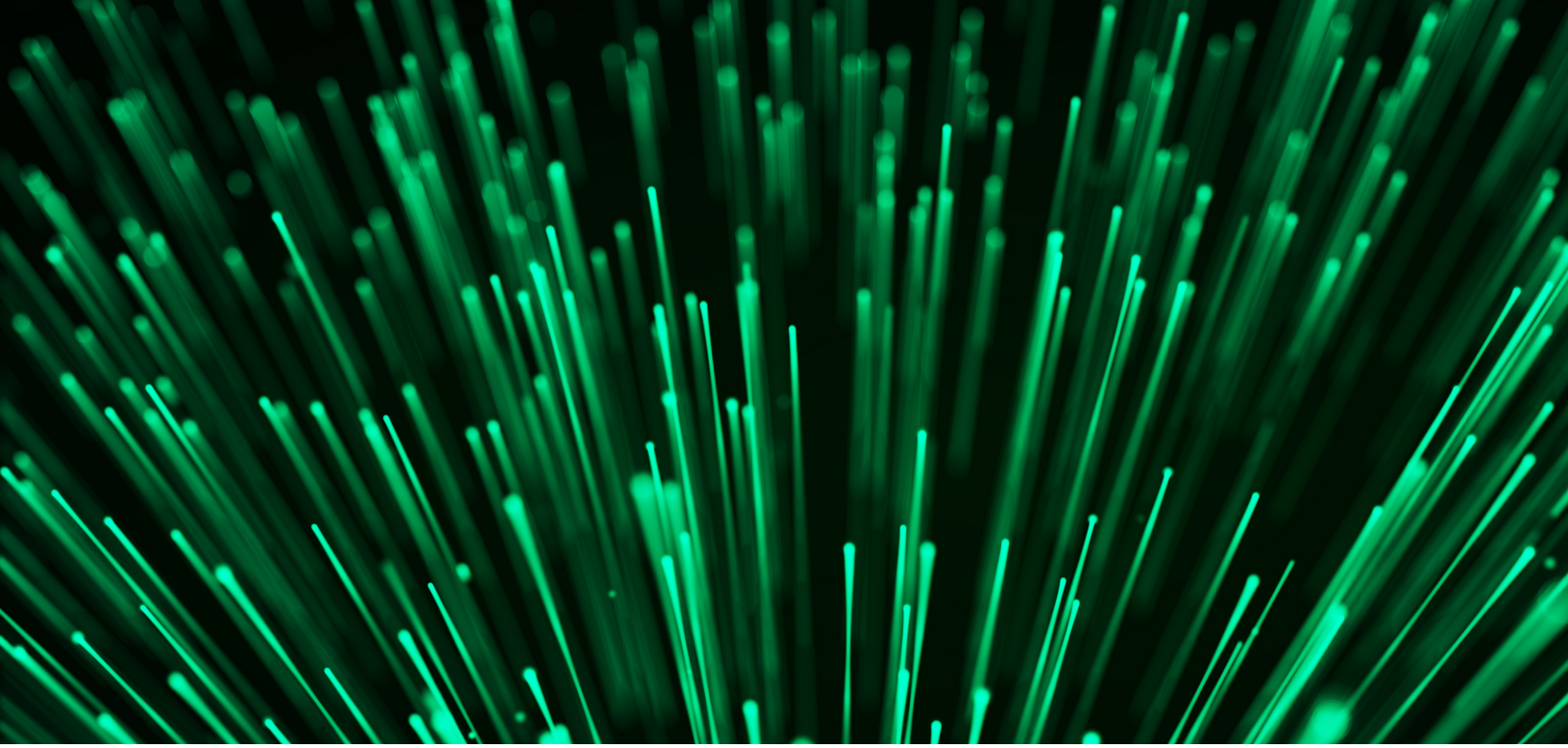
- **Segmentation:** Tellabs PON excels at macrosegmentation with OLTs supporting up to 4,000 VLANs on all ports, applied upon authentication. OLTs also provide native VLAN support and VLAN trunking via 802.1Q that prevents leakage between VLANs. Bridging between ports on the same VLAN can be disabled, forcing all traffic to flow upstream for microsegmentation. Ideal for smaller networks, OLTs also support microsegmentation via both static and dynamic ACLs to permit or deny data flows to and from users and devices.
- **Dynamic ARP Inspection:** Tellabs PON uses DAI to protect against Address Resolution Protocol (ARP) spoofing and man-in-the-middle attacks that attempt to bind a MAC address to an IP address they want to spoof to intercept or modify traffic. DAI uses DHCP snooping to maintain a database of legitimate MAC-to-IP bindings and validate all ARP packets, dropping those that do not match. DAI can also use ACLs to handle static IP addresses and maintain them in the database. Tellabs pairs this with trusted host validation and features like sticky MAC on specified ports when DHCP is not used, which saves dynamically learned MAC addresses to memory and allows access only to devices with those addresses.
- **Advanced Management Security:** Tellabs PON supports Local Certificates, single sign-on control via Microsoft Active Directory, and MFA to secure access to management platforms and OLTs. It also supports a "Trusted Host" feature that limits access to only trusted IP addresses while appearing dark to all other addresses.
- **Wavelength Separation:** Because PON uses optical fiber that transmits data over multiple wavelengths, it is possible to run multiple networks over the same fiber.
- **Event Logging:** Tellabs OLTs record events into Syslog messages for analysis and reporting, including any access to the OLT, user/device logins and logouts, the addition of a new ONT on the network, and any device connect or disconnect. Tellabs also logs security events, configuration change events, and alarm history.

In addition to security attributes, Tellabs OLTs use Link Layer Discovery Protocol (LLDP) and LLDP-Media Endpoint Discovery (LLDP-MED) to discover, manage, and inventory all connected devices. OLTs also distribute bandwidth, PoE, and Quality of Service (QoS) configuration information to individual ONT ports. This process is automated using templates and profiles in the OLT, dynamically allocating resources on a per-service, per-port, per-end-device, and per-user basis according to real-time needs and SLA attributes.

Seamless Zero-Trust Integration

In addition to reducing the attack surface and providing best-in-layer security for the LAN, Tellabs PON technology is inherently software-defined due to its centralized architecture – it does not utilize SDN as an overlay on top of an existing network. This enables centralized management and control while enabling





seamless vendor-agnostic integration with multi-vendor networks, third-party Zero-Trust platforms, and cloud-based management systems through standard protocols and APIs.

- **Zero-Touch Provisioning (ZTP):** Through Dynamic Host Configuration Protocol (DHCP), Tellabs OLTs learn their IP address, PKI certification, host name, and the location of the ZTP server. OLTs retrieve their ZTP configuration, including any required authentication credentials and security certificates, to establish secure communication with all network components via profiles, services, and rules. During setup, the OLT will also compare its software version with the ZTP configuration and download and apply the correct versions if necessary.
- **RADIUS/Network Access Control (NAC):** Tellabs PON supports NAC via RADIUS protocols, sending credentials to RADIUS authentication servers for verification before granting network access.
- **Cloud-Based Orchestration and Security Integration:** In addition to Syslog, Tellabs PON supports SMNPv2/SMNPv3 interfaces for real-time monitoring and network telemetry via management information bases (MIBs). It also effectively integrates with cloud-based and third-party orchestration and SASE platforms via open APIs, including YANG-based protocols such as NETCONF, RESTCONF, gNMI, and Command Line Interface (CLI). Tellabs PON supports the use of playbooks based on common programming languages for automation workflows, security hardening policies, QoS settings, and routing configurations.
- **Network Access Control (NAC):** Tellabs OLTs support advanced NAC appliance integration to enforce authentication policies for users and devices. The OLT supports leading NAC policy managers, including Aruba Clearpass, Cisco ISE, Juniper Unified Access Control, ForeScout CounterACT, and Windows Policy Server.
- **Dual Stacking:** Tellabs OLTs support both IPv4 and IPv6, accepting management connections over either protocol and processing and forwarding both types of packets. This makes a Tellabs PON interoperable with both modern and legacy systems, facilitating converged networks and enabling management of a wide range of IP-based devices, from VoIP phones and Wi-Fi access points to surveillance cameras.

Additional Benefits

Not only does a Tellabs PON reduce attack surface by 99% compared to traditional switched networks, but it also significantly reduces equipment installation costs by eliminating hundreds or even thousands of traditional switches. This also considerably reduces IT space, power, and cooling requirements, resulting in superior energy savings and a reduced carbon footprint. It's worth noting that optical fiber cables are composed of more sustainable materials, weigh nearly one-tenth as much as copper cables, and have a smaller overall diameter, which significantly reduces the amount of pathway material and space while improving connectivity density.

Operational costs are further minimized by reducing downtime, inventory, and licensing fees with fewer active components. Fewer active devices also reduce

the time spent on network troubleshooting, moves, adds, and changes, thereby reducing IT staff and training needs and shifting the operational focus to more mission-critical tasks.

THE RIGHT CHOICE FOR SECURE GOVERNMENT NETWORKS

Tellabs PON solutions are deployed in highly secure U.S. government and military networks, including Intelligence, Civilian, and State/Local government environments. PON is recognized in DoD Digital Modernization Strategy Plan FY19-23. Tellabs PON hardware and software successfully completed rigorous interoperability and security testing through the Joint Interoperability Test Command (JITC) under the former DISA Unified Capabilities Approved Products List (UC APL) program and was previously listed on the DISA UC APL. In addition to JITC interoperability testing, Tellabs PON successfully completed the U.S. Army I3MP/I3C2 Performance Evaluation Test and meets Unified Capabilities Requirements (UCR), applicable Security Technical Implementation Guide (STIG), and FIPS 140-3 requirements. Tellabs also maintains Certified TEMPEST Technical Authority (CTTA) expertise in support of secure government deployments.

Unlike solutions that attempt to deploy microsegmentation at the network level via inline tagging, Tellabs PON keeps the network simple and focused on its core function of efficiently routing data. Attempting microsegmentation at the network via inline tagging is highly complex and challenging to maintain, especially as the network grows and more users and devices are added. Instead, Tellabs PON seamlessly integrates with advanced cloud-based Zero-Trust platforms that excel at integrity monitoring and microsegmentation by defining application-level access based on workload and identity.

In summary, Tellabs PON offers the following benefits over traditional switched networks in ZTA:

- **Reduces the attack surface by up to 99%**
- **Delivers best-in-layer security for the network without complexity**
- **Enables phased deployment onto existing network infrastructure with minimal training requirements and no rip-and-replace redesign**
- **Maximizes the use of more secure government-preferred fiber**
- **Supports standards-based integration for end-to-end Zero Trust**
- **Reduces the burden of vulnerability management and day-to-day operations**
- **Lowers total cost of ownership and reduces equipment refresh cycles**

ABOUT THE AUTHOR

Pioneering, innovative, and deeply mission-driven, **Marc Packler** serves as the **President and Chief Strategy Officer (CSO) of SIMPACK LLC**, guiding the company's long-range vision, strategic positioning, and growth across the Department of Defense and federal acquisition ecosystem. With more than 25 years of leadership experience in the U.S. Air Force, Marc brings expertise in digital modernization, risk management, AI/ML integration, and cybersecurity transformation.

At SIMPACK, Marc leads enterprise strategy, solution architecture, and customer engagement across the company's cyber, cloud, and AI portfolios. He is the principal interface with senior military and government stakeholders, shaping mission-aligned strategies and translating operational requirements into innovative, executable solutions.

Marc's forward-thinking approach and extensive command experience make him a trusted advisor to defense and industry leaders navigating today's complex digital landscape.