FIBER MOUNTAIN
A Green Lambda Company

Solution Brief
SB-183-00007 Rev 1

CyberSecurity

Driven by the increasing need for high security due to current world events, zero trust security is currently being implemented or mandated by government entities and most enterprises today. Should only Layers 2 through 7 be of concern, or should you include you cabling infrastructure as well to cover the complete netwrok stack?

Introduction

Corporations and government agencies have become increasingly committed to securing their internal networks against threats from external adversaries and compromised internal "trusted" personnel. These come by mandates from corporate CISOs, through compliance requirements and even from the US President through executive orders such as order 14028 put in place by President Biden on May 12, 2021.

The DoDIN directive goals are to improve the security posture of information systems and networks by ensuring that a baseline set of rules and procedures are provided to owners of these systems.

The growing threat of advanced cyber-attacks on critical infrastructure presents a unique challenge for the DoD (Department of Defense). SDN and other virtualization approaches have introduced unprecedented levels of security control to the management of servers and storage. Still, the physical layer of patch panels, cables, and connection points has been invisible to software.

Two key points on enhanced security that we will expand on are Zero Trust Security Framework and Configuration Management. orders. Built-in AC input power redundancy protects the Sensus management functionality from a failure of a power source.

Zero Trust Security is a framework that requires all users to be authenticated, authorized and continuously validated or monitored irrespective of whether they are outside or inside of the organization's network. **This means that the days of placing a firewall on the corporate network to keep "unwanted" users out is no longer sufficient.**

For more information, visit:
www.fibermountain.com

Zero Trust means trust no one, even internal users are explicitly denied to corporate resources unless specifically allowed and have had their identification validated at the time of the access request. Continuous monitoring is placed to catch those trying to circumvent the identification process.

Traditionally access authentication and authorization are done at the network (Layer 2) up through the applications (Layer 7). The physical connections of the miles of cables that are used to make all the devices communicate are just not monitored. There is no way to know that a port on a server goes down temporarily, or what actually happened unless you retrace the complete path of that cable from both endpoints.

This could go through multiple hops through server racks, data centers, wiring closets making it nearly impossible to figure out what happened. In most cases the IT professionals will chalk that event up as “no trouble found”. Could a connection have been disconnected in the middle and a recording/monitoring device have been inserted?

If intelligent panels from Fiber Mountain were utilized, the panels would detect that the event occurred and will explicitly tell you what panel and what port the disconnection happened and for how long.

This is done using sensor technology and identification of each and every cable. The identification is done through Fiber Mountain’s Intelligent Cable Identification (ICID®). Every cable is uniquely identified with a serial number. If a different cable is inserted back into the panel, the panel will report that information to the manager or a trap can be sent.

All connections are monitored, thus providing a zero trust by informing the management system that a cable event (pull, insert, change) occurred. If the event was expected, then no further action is required. If it was not, send a technician or security guard to interrogate the event.

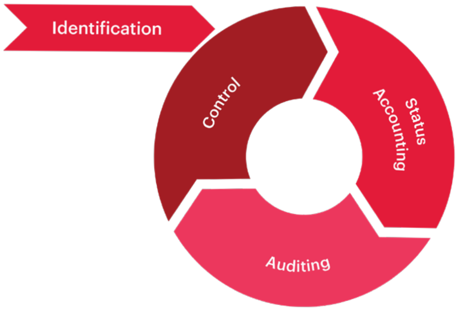
Configuration Management

Configuration Management has high operational value. Government Agencies and enterprises use Configuration Management systems to ensure the assets required to deliver services are configured consistently and adequately throughout the organization. It also audits assets to ensure that they meet the expected configuration state. It provides compliance features such as historical changes and current state.

From a security perspective, if you do not know how your network is configured (or is supposed to be configured), how can you effectively secure it? You can say the same thing about the cable infrastructure.

Sure, when the cable plant was initially put in, accurate records may have been produced, but it is a manual process to enter that information into a database for configuration management. The accuracy over time gets skewed because of the manual process. Either technicians forget to update the records, or they make a mistake in the manual update.

Fiber Mountain's intelligent panels address this by providing a database of all the changes and locations of cables in real-time, providing 100% accuracy of the current state. You can generate reports from Fiber Mountain's AllPath Director management systems, or use its RESTful Application Programmable Interface to update central configuration management systems.



Additional Features to Enchance Security

Alarms

Timely awareness of unplanned changes within the physical infrastructure allows network operators to detect and respond to physical security breaches and inadvertent cabling errors when they happen, rather than after they have already caused damage and downtime. Fiber Mountain's solution allows data centers to have the visibility and agility to respond to physical changes via software or by knowing exactly where and when to deploy technicians to make manual corrections.

Physical Network Topology and Documentation

Physical Network topologies are typically generated manually or not at all. However, a network using Fiber Mountain's solutions will enjoy the automated documentation of the actual network topology based on both ICID® and more general device detection. This topology makes it easy to see end-to-end connections, and APD also introduces the flexibility to group and arrange connections as needed.

Audit Trail

The Audit Trail functionality of APD protects the physical layer network by improving awareness of the current state and the timing and location of all changes that have occurred in the past. The audit is essential for reducing vulnerabilities and for improving regulatory conformance.

The Audit Trail provides another layer of visibility by preserving all events on the physical infrastructure in a record that cannot be altered or deleted by anyone. The Audit Trail starts when Fiber Mountain's solutions are enabled on the network, and the records can be exported for further analysis.

Conclusion

Why not include Layer 1 in your security architecture? Fiber Mountain's Sensus intelligent panels and AllPath Director with its sensor technology provides the ability of Zero Trust throughout all of the network assets including Layer 1. It provides unprecedented visibility and agility within the fiber-optic infrastructure. Real-time, accurate documentation becomes an automated process, improving day-to-day operations management, speeding up unplanned downtime resolution, and securing your entire network.