CHAPTER 8

PHYSICAL-LAYER DATA SECURITY REDUCES THREAT OF UNAUTHORIZED ACCESS

> In today's hyper-connected smart buildings, every network connection is a path into a corporate or mission-critical network. At the same time, the size of the attack surface when it comes to insider threats varies directly with the number of people who have access to the data being protected.

PHYSICAL-LAYER SECURITY

The cost of a data breach in the enterprise network goes beyond financial damage; it can take years for a business to regain trust and rebuild its reputation. It is estimated that 60% of data security breaches were carried out by insiders with either malicious or inadvertent intent. The physical layer infrastructure is clearly a critical a part of any data security plan against internal and external threats.

In industries such as healthcare and finance, the issue of network security has spawned regulations and compliance requirements regarding data storage. Network infrastructure security concerns generally fall into two categories:

- Unauthorized access by an unauthorized person can be reduced or prevented through the deployment of IP-connected cameras, occupancy sensors, access controls and other connected elements of physical security. Physical cabling security such as keyed connectors, secure patch cords and port blockers can be deployed to reduce the threat of unauthorized access. Similarly, AIM solutions can record and report activity on the physical layer.

- Unauthorized access by an authorized person can be more difficult to detect and repel. Given the depth and complexity of the enterprise network, an AIM system enables network managers to monitor and manage network connections from the inside. Using intelligent cabling, connectors and patch panels, it automatically detects and maps all physical layer activity at the port and device level, in real time. If an authorized user connects or disconnects a device, an AIM solution like CommScope's imVision automatically alerts IT personnel.

SECURITY MONITORING AND POWERED FIBER/ POE CABLING

Networks of IP security cameras and occupancy sensors commonly installed in intelligent buildings are helping to spot unauthorized intruders. With the right cabling infrastructure, these PoE internal security monitors can be distributed throughout the building or campus.

While an AIM system can locate a would-be hacker, cameras provide corroborating visual proof. Low-voltage powered-fiber or PoE network supports these connected sensors, cameras and controllers. If the main power fails, the AIM system and all connected security devices continue to function because they draw their power from the switches, which are typically backed up by UPS batteries and generators. This power structure is inherently more resilient and secure.

GLOBAL SUCCESS STORIES

CONSTANT MONITORING AND ALERTS MAKE A TRULY SECURE NETWORK

Establishing a secure network infrastructure and reliable connectivity performance is a key priority across all industry sectors. Examples include resilient connectivity for a stock exchange's critical infrastructure systems, and secure and reliable networks for research efficiency at major research establishments.

Intelligent infrastructure management is needed to provide systems managers a real-time view of the network physical layer, speed up troubleshooting, and improve security while reducing network downtime and making maintenance more cost effective.

SOLUTION

CommScope, a leading supplier of structured cabling, has helped IT organizations to meet these requirements with its SYSTIMAX iPatch system, consisting of the System Manager software, iPatch Manager, and iPatch intelligent copper and fiber panels.

For physical security and video surveillance, the infrastructure connects CCTV and access control systems while SYSTIMAX cabling connects servers with a storage area network within the data center.

Additionally, the SYSTIMAX 360 solutions-based network infrastructure connects data systems and supports extra-low-voltage systems, including building management, security, voice-over-IP and lighting control. These critical applications depend on copper and fiber cabling with high performance and reliability. CommScope's installations are backed by a global support network and industry-leading 20-year guarantees.

BENEFITS

These solutions provide IT administrators with real-time visibility and control of the physical layer. Copper and fiber connections

GLOBAL SUCCESS STORIES

in the installations are managed using iPatch panels that allow monitoring of network connections and attached devices.

The iPatch software also alerts administrators immediately of any changes by detecting and locating unauthorized APs while the System Manager software helps to document and monitor the infrastructure through a standard web browser.

IMVISION AIM PLATFORM

Beyond the iPatch System, CommScope's imVision AIM solution drives actionable insights as well as real-time intelligence and visibility into events that impact the network's physical layer and the devices connected to it.

An AIM solution uses intelligent cabling, connectors and patch panels to monitor the connected environment in real time. Should it detect an unauthorized or authorized device attempting to access unauthorized information, the system issues an immediate alert.

The System Manager tracks all devices, even those operating wirelessly, as they move about a network. The software also integrates with PoE devices, verifying that power is available to a connection. Further, the iPatch intelligent panels initiate real-time alerts whenever they detect unexpected changes to the network.

Deploying PoE and powered-fiber technology using Category 6A cabling also increases the resilience in security systems such as IP security cameras and AIM-based intelligence.