USE CASE

Layer-1 Infrastructure Security

The First Layer of Defense in Data Center Cyber Security; the Oft-Forgotten Layer of Data Center Infrastructure Management

Executive Summary

In a world of increasing data demand, where companies like Amazon, Facebook and Google all indicate that traffic in their mega-datacenters increased more than 100% in 2016 and is likely to do the same in 2017*, the network infrastructure carrying this traffic (also known as Layer-1: cables, interconnect points, etc.) has increasingly become a critical point of IT operational dependency. The fact is that network infrastructure is an under-publicized point of vulnerability as it can be easily targeted for attacks aimed at fiber optic tapping and denial of service. A solution to protect and manage network infrastructure as part of a total Data Center Infrastructure Management (DCIM) system should be considered.

Leveraging the **VANGUARD™ CS** Network Infrastructure Cyber Security Solution adds physical protection and situational awareness to critical Layer-1 infrastructure. This ensures harmful events are identified before they are carried out, preventing data theft or damage that could degrade network performance or availability; helping to ensure data continuity to avoid potential losses of revenue and customer dissatisfaction.

Challenges

Data Center and Web Service Providers spend heavily on "traditional" cyber security measures, but rarely do they focus on Layer-1 network infrastructure – the cables that carry their vast amounts of data – which could be considered one of their largest assets. A single fiber carries massive amounts of information, making fiber optic cables, some containing up to hundreds and even thousands of fibers, attractive targets for attackers intent on intercepting proprietary company and customer information or disrupting service, either of which would be disastrous to the organization.

Some providers are beginning to understand this gap in their security plan and are deploying our VANGUARD CS solution. However, most companies have yet to consider Layer-1 infrastructure a part of their Data Center Infrastructure Management (DCIM) profile and therefore have little insight or situational awareness into when or where an intruder is looming, damage is occurring, or an outage is impending. As such, when a problem does ensue, tools are not available to quickly determine the location of the event (in the Inside Plant or Outside Plant) without the costly and time-consuming process of dispatching teams to various locations to begin investigations. Depending on the severity and the time it takes to find the problem, the outage may span hours or even days, and the costs of lost revenues, customer trust and corporate reputation, could be immeasurable.

Traditionally, electrical metallic tubing (EMT) or ridged metallic conduit has been the sole method for physically securing network infrastructure in data centers. However, the installation of metallic conduit systems is costly and cumbersome and only deters damage and intrusion; it cannot prevent it or detect it. In addition, relying upon such systems as the sole security measure does not provide the situational awareness that enables security forces to know where a potential issue is occurring or about to occur.

Co-located data centers make network infrastructure security even more important as employees and vendors can enter areas where infrastructure passes within easy access, giving no control over the security or management of those areas of the data center.

"If the VANGUARD CS had not been installed on our network, we would have had no way of knowing that critical patch cords were inadvertently unplugged. By the time we would have found the source of the problem, there is no telling how much revenue would have been lost."

-An Existing Cloud Services Customer

The VANGUARD CS Network Infrastructure Cyber Security Solution Provides:

- ✓ A centrally managed solution that provides real-time insight into the security and integrity of network infrastructure.
- ✓ A streamlined response to *real* threats, including appropriate first responder notification for increased personnel safety and fast network recovery times.
- ✓ Rapid and easy deployment without costly changes to existing network infrastructure and the ability to eliminate EMT.

The Solution

The VANGUARD™ CS Network Infrastructure Cyber Security Solution is the only Layer-1 cyber security solution that utilizes proven defense grade technologies developed for and used extensively by the US Government and Military to defend and protect networks from physical attack. The system performs continuous analysis of cables and/or pathways to detect minute events which could indicate unauthorized access to cables, intrusions into the pathways or network infrastructure, tampering with the cable system to apply a tap, or accidental and intentional damage that could degrade network performance or availability, all while having zero impact on network bandwidth.

VANGUARD CS incorporates an enterprise alarm management software system which enables remote monitoring and management of alarm devices from anywhere in the world and provides further intelligence and situational awareness, identifying whether the issue is occurring in the ISP or OSP environment. VANGUARD CS allows organizations to define the severity of an event, and Fiber Forensics™ technology reveals insight into the type of event (i.e. accidental touch or fiber tap), eliminating nuisance alarms. The software also automates site-specific Standard Operating Procedures (SOPs) – which include an alarm notification contact list, zone media (digital images & CAD drawings), and the ability to integrate with physical security systems such as CCTV, Access Control Systems, and PSIM systems. Additionally, VANGUARD CS software can automatically shut-off or reroute data, further protecting Data Center and Web Services Providers and their customers. VANGUARD CS can be easily added to a data center's current DCIM profile.

With Plug-and-Protect™ capability, VANGUARD can rapidly be added to existing network infrastructure. As an added advantage, monitoring standard armored fiber optic cable with VANGUARD CS could eliminate the need for costly EMT, greatly reducing the overall CAPEX and OPEX for an organization, providing instantaneous ROI, and enabling cost-effective scalability across various sites around the globe.

The Results

By leveraging the VANGUARD CS solution as part of a DCIM profile, Data Center and Web Services Providers can obtain a complete cyber security solution by protecting their Layer-1 infrastructure, one of their most valuable assets. Benefits include: constant situational awareness and real-time detection of intruders and destruction and a targeted, streamlined response so the threat can be immediately and effectively addressed.

VANGUARD CS closes an open door to cyber security vulnerabilities and prevents critical downtime and devastating costs to the company.

Network Integrity SYSTEMS

www.networkintegritysystems.com

*Source: LightCounting