Protect Every Data Point

By Glenn Longley

The United States has more than 3,000 operational data centers, with more than 1,500 additional facilities in various stages of development, according to the Pew Research Center. Even more staggering is that this growth figure only reflects standalone, multi-client data centers. It doesn't even include data center expansion happening inside corporate offices and facilities.

Regardless of their size and physical location, data centers collectively help drive our economy with massive investments in construction and equipment that create thousands of jobs and provide the foundation for our online digital ecosystem. As a result, data centers have quickly become one of the fastest growing verticals for professional security services and systems.

The need for advanced cyber protections naturally comes to mind when discussing data center security. However, security experts agree that data center security is as reliant on physical security solutions, such as intrusion detection, as it is on cybersecurity solutions. The reason being that data thieves often find it faster and easier to physically break into a data center to steal servers or data using portable drives than spend weeks or months trying to exploit software vulnerabilities. In some cases, it can only take a few minutes to smash and grab servers. A physical breach must be considered a cyber incident.

This new cyber-physical security mindset is driving the demand for the latest advancements in physical security at data centers. High on the list is intrusion detection—not only for obvious entry/egress points like exterior doors and windows, but also for secondary points of entry and internal areas like server rooms, racks and cages, and environmental systems. Modern wireless-first intrusion detection systems can also extend beyond traditional security applications, providing autonomous means of monitoring environmental systems and staff activities.

EDGE POINTS, DEVICES AND DATA

One of the most effective and efficient ways to address multiple security system needs and applications is to layer solutions. There is a lengthy list of physical security technologies that can be layered to better secure data centers, but not all are right for every facility. The best practice is to combine the best workable solutions on a case-by-case basis into an integrated security solution that starts at an organization's perimeter and moves inward to critical interior areas that require more layers of security.

Modern wireless-first solutions are perhaps the fastest trending infrastructure preference for critical infrastructure facilities such as data centers. Commercial wireless security systems have continued to evolve over the years from simple door and window intrusion sensors to advanced access, video surveillance and sensor applications. Making the transition from legacy wired to new modern wireless security infrastructure provides a more economical and effective way to extend the capabilities, scale, reach, and effectiveness of security systems with little to no disruption of daily operations.

Cutting the need for long cable runs from equipment closets to endpoint devices found throughout a facility also saves time and money during installation and over the course of the system's lifetime. And as the scale and complexity of the system increases, so do the economies of scale, yielding greater return on investment (ROI) and a lower total cost of ownership (TCO).

Extended, reliable system communications is another significant advantage of new modern wireless-first solutions. For example, Inovonics' EchoStream 900 MHz wireless transmission solution is designed for deployment in commercial environments like data centers that are typically built with heavy, dense materials that can cause interference or block signal transmission altogether in some interior locations. Seamlessly integrated wireless-first solutions that include transmitters, receivers, gateways, and high-power repeaters also help ensure extended wireless coverage with minimal interference in facilities with complex construction.

BEYOND SECURITY AND INTRUSION DETECTION

When designing a wireless-first system for data centers, more sensors make more sense to accommodate a host of different applications. These can range from intrusion detection, occupancy monitoring, and motion detection to environmental monitoring, smoke and CO detection, and more.

In addition to performing their primary functions to detect specific types of activity, modern wireless sensors can also be integrated into access control and video management platforms to trigger specific system operations. This can include full-frame video recording, access system lockdowns, fire alarm activation, and numerous building automation events including HVAC activation, lighting management, and even people-mover system control.

Additionally, wireless-first infrastructure supports modern wearable pendants and panic duress buttons that allow onsite personnel to instantly call for help in emergency situations, with options for fixed, mobile, or location-tracking solutions.

New advancements in wireless-first system solutions allow data centers to easily scale to accommodate system expansion, upgrades, and physical layout alterations.

Modern wireless infrastructure solutions also provide the added convenience of mobile control, allowing data center admins and security personnel to manage, watch and respond to system activity from anywhere using an app on their smartphones. All these value propositions are not possible with legacy wired or wireless infrastructure.

Modern wireless-first systems deliver the reliability and resilience required for critical security applications in data centers. Inovonics pioneered the use of 900 MHz wireless spread-spectrum transmission technology in the physical security industry, which has proven to be highly secure and exceptionally dependable at thousands of mission-critical deployments.

As a result, 900 MHz wireless transmission technology is widely considered to be the industry standard for commercial security systems and critical infrastructure. Data centers that employ modern wireless-first system solutions will immediately receive help from superior performance, reliability, versatility and integrity.

Glenn Longley *is the chief products officer at Inovonics.*