TELEDYNE FLIR

APPLICATION NOTE
Security Solutions

DATA CENTER SECURITY: PROTECTING THE PERIMETER AND CRITICAL ASSETS

In 2013, United States President Barack Obama announced his Presidential Policy Directive 21: Critical Infrastructure Security and Resilience, which states that the Federal government has a responsibility to strengthen the security and resilience of its own critical infrastructure against both physical and cyber threats. Though this particular directive was designed to secure critical infrastructure in the U.S., this responsibility extends to nations around the globe.

In an age where any threat to the global economy's most vital assets, systems, and networks has the potential to incapacitate the security, economy, public health, or safety of any number of nations, securing the globe's critical infrastructure is an intuitive priority. As far as comprehensive solutions are concerned, critical infrastructure is the security industry's front lines.

CENTERING DATA AS CRITICAL INFRASTRUCTURE

When the White House published Obama's initiative in February of 2013, the sum of the world's data—i.e., the datasphere—was approximately 4.3 zettabytes. For reference, one zettabyte equals one sextillion (1,000,000,000,000,000,000,000) bytes. Based on the size and importance of protecting U.S. information networks from the threat of cyberattacks or disruptions, President Obama asked Congress that same year for $769 million to fund information data security initiatives via the Department of Homeland Security.

The President's budget request described supporting the defense of the nation's data infrastructure as "critical to national security," doubling down on the same emphasis in his Policy Directive 21.

Five years later, the datasphere had grown from 4.3 to 33 zettabytes, by a compound average growth rate (CAGR) of 40 percent. By 2025, IDC predicts that the global datasphere will increase to 175 zettabytes, meaning there will be 40 times more data generated globally than when data was first categorized as critical infrastructure.

The more the globe transitions toward digital interfaces to meet all its needs, the more vital data as a resource will become. For the security managers responsible for data center security, this only means one thing: perimeter security and asset management are more important today than ever.

High resolution radar can provide the first layer of defense.

Within the fence-line, a short-range commercial radar offers a second layer of defense.

TOP CHALLENGES TO DATA CENTER PHYSICAL SECURITY

Data centers simply cannot afford to ignore physical and perimeter security. Data center clusters can contain more than 2.5 million IU servers and house some of the most important resources to enterprises and governments world-wide, so their perimeters must be protected at all times. Securing these facilities, however, is no simple task. Data center clusters are often contained within massive, remote facilities with expansive perimeters, making the threat of bad actors attempting to break in to physically access a network and sabotage data ever present.

In the event of a perimeter breach at a data center, the loss of data has the potential to be monumental, affecting business operations and customer information extensively. Beyond data loss, however, unplanned data center outages can cost anywhere from $9,000 to $17,000 per minute, according to a Ponemon Institute study. These sometimes occur as a result of sabotage, but they can also occur when a server overheats or goes offline due to a power outage.

For this reason, today's security, asset protection, and preventative maintenance for data centers must account for everything from beyond the perimeter to each individual server cabinet.

THE SHORTCOMINGS OF TRADITIONAL PIDS

For years, data centers have implemented traditional perimeter protection. But it is all too common for these facilities to underinvest in perimeter intrusion detection systems (PIDS), resulting in significant limitations.

Exactly half of the respondents to the 2020 State of the Data Center Report said the biggest security concerns for their facilities are "outside human threats." Another 46 percent noted advanced persistent threats, "such as theft of IT and corporate data," as well as schemes to inflict damage on equipment that could sabotage data center operations.

While conventional PIDS might be able to secure smaller, lower-priority facilities using basic visible surveillance cameras or access control technologies—data centers house resources too vital and too vulnerable for a solution this minimal.

WHY PARTNER WITH TELEDYNE FLIR

For this reason, security directors and operations managers are turning to Teledyne FLIR's advanced suite of perimeter protection and asset management technologies to meet their data center needs.

Since 1978, Teledyne FLIR has been a pioneer in the development of high-performance infrared imaging systems, which have been successfully deployed by defense departments. In the decades since, the company has innovated and expanded their product offerings to include industry-leading air and ground-based radar, powerful video management software (VMS), video analytics, and condition monitoring technologies, as well as a suite of multispectral devices purpose-built to deliver reliable and cybersecure intrusion detection, no matter the environmental conditions. All in all, Teledyne FLIR provides field-proven technologies that both protect data centers from outside threats as well as improve the safety and efficiency of operations and systems inside data centers.

At the Perimeter

With a Teledyne FLIR PIDS, data center perimeters will benefit from field proven intrusion detection technologies that are built to deliver peace of mind.

Far beyond the fence line, the FLIR Ranger R2 provides the first layer of intrusion detection. A mid-range, high-resolution radar that accurately detects personnel and vehicles at a range of up to 1,400 meters, the Ranger R2 works in virtually any climate, weather, or lighting condition. The FLIR Ranger R1, on the other hand, accurately detects foreign objects at a range of up to 700 meters and covers up to 1.5 square kilometers; and the FLIR Ranger R3, a high-resolution, long-range radar system, delivers a detection range of up to 2,800 meters and covers more than 24 square kilometers. Designed to network with other devices, the FLIR Ranger series can be networked in an overlapping array to protect larger areas. As an alternative option for shorter range applications, customers can also deploy a FLIR R-Series Radar.

Built to complement this functionality, FLIR FH-Series ID cameras—integrated at the fence line—can provide a second layer of intrusion detection. These ruggedized, multispectral fixed cameras integrate industry-leading thermal imaging, 4K visible imaging, and FLIR Virtual Barrier convolutional neural network analytics for accurate intruder detection and classification. Inside the fence line, a suite of FLIR devices—including compact, short-range ground radar such as the FLIR Elara R-290, proprietary LiDAR (light detection and ranging) technology, or visible pan-tilt (PT) cameras—deliver detailed situational awareness in any condition.

The third layer of perimeter defense is advanced video analytics, designed to detect, classify, and notify security personnel of unauthorized vehicles and humans. Whether a security manager utilizes the TRK 101P analytics encoder (which automatically sends alarm notifications when people, vehicles, and objects cross perimeter lines, enter pre-defined regions, or are left behind or removed from a scene) or deploys a camera with built-in FLIR Virtual Barrier analytics—a PIDS outfitted with FLIR video analytics technology enables users to track targets and disseminate instant alerts for greater for continuous threat assessment and real-time prevention.

The fourth layer, supported by FLIR Cameleon V5, or any third-party VMS platform, features enhanced cyber security and a user-friendly interface to equip security operators with versatile and powerful edge device integration, target tracking hand-off, forensic-quality image processing, and global administration.

Using military-grade radar, multispectral cameras, best-in-class video analytics, and powerful VMS from end-to-end, each of these devices ensure data center perimeters are covered from all angles.

Inside the Facility

The fence line, however; is not the only area in need of surveillance. For points of entry, indoor environments, server rooms, and more, evidentiary-class indoor cameras such as the FLIR Quasar series of 5MP HD and 4K UHD visible and IR-illumination cameras deliver superior image quality.

Moving further into the interior of data center facilities, operations managers use FLIR handheld and fixed thermal cameras for traditional condition monitoring at the asset level and heat mapping. Infrared thermography enables operations managers to discover, diagnose, and

report problems, including short-cycling of the air conditioning system, loose electrical connections, and worn-out bearings. Once technicians complete their repairs, the thermal devices are then used to re-inspect equipment to ensure it is properly functioning.

In summary, both FLIR handheld and fixed thermal cameras empower operational personnel to:

- Identify and correct hidden problems, before they become unplanned outages
- Reduce the risk of undetected component degradation over time, due to overloaded circuits or loose connections
- Collect a detailed history of equipment to improve the resiliency of critical facility infrastructure
- Enable cost savings by preventing equipment failure and downtime

Within the Server Cabinet

Teledyne FLIR equips data center personnel to monitor and secure the most critical assets: actual data servers. Inside servers themselves, technicians can use thermal cameras to regularly check electrical switchgear, uninterruptible power supply (UPS), automatic transfer switches (ATS), server systems, and cooling systems for wiring, fuse, and air leak issues that are undetectable by the naked eye. Using FLIR thermal technology for predictive maintenance ensures the resiliency of a data center's infrastructure and saves enterprises time and money, all at once.

When using handheld thermal devices for predictive maintenance, the FLIR IR Window—a broadband crystal lens that transmits short, mid, and longwave IR while allowing illumination to shine through—adds a barrier between personnel and energized equipment. This protects personnel from arc flash accidents and promotes effortless, safe thermal inspections while still allowing them to spot potential failures before they occur. Overheating servers and system downtime are the top concerns to consider when it comes to condition monitoring. For this reason, portable critical condition monitoring devices are not always the best options. With infrastructure this important, fixed continuous monitoring systems are a data center's best bet for ensuring their equipment is running at its best. They are at the crux of proactive, predictive, and preventative maintenance programs that detect faulty components prior to failure, burnout, fires, and costly insurance claims.

KEY TAKEAWAYS

With Teledyne FLIR solutions, security and safety personnel can not only rely on continuous, end-to-end perimeter and asset monitoring, they will also enjoy a much lower total cost of ownership. Because Teledyne FLIR technology provides exceptional sensor sensitivity, detection accuracy, instantaneous alerts, and actionable insights, data centers avoid costly false alarms, equipment downtime, and intruder threats.

Combining powerful devices like air and ground-based radar, multispectral fence line cameras, video analytics, and VMS software, data centers can layer intrusion detection capabilities so that Teledyne FLIR PIDS can detect intruders at long range, verify those threats using thermal and visible cameras and then distribute critical alerts well before an event unfolds. Using handheld and fixed condition monitoring thermal cameras, operations managers are able to quickly detect overheating equipment or asset irregularities for immediate intervention prior to systems failing that result in unplanned, costly outages.

For more information about FLIR Security thermal cameras, please visit:
www.flir.com/applications/security

With a handheld thermal imaging camera, operations managers can find and diagnose problems, then verify the repairs.

A FLIR IR Window creates a safe barrier between the inspector and energized equipment.

TELEDYNE FLIR

www.teledyneflir.com

Teledyne FLIR, LLC
27700 SW Parkway Avenue
Wilsonville, OR 97070
USA
PH: +1 866.477.3687