

FLIR Whitepaper

IP-Based Security Convergence Challenges and Solutions for Video Surveillance



The World's **Sixth Sense**[®]

Introduction

Physical and network security have traditionally been two very different disciplines. Intrusion detection, access control, video surveillance and similar physical security technologies operated primarily on analog infrastructure. Networks, servers, computers, tablet and smartphones operated independently, using IP-based infrastructure. When the two worlds intersected, if at all, it was primarily to ensure that physical access to servers or facilities was properly monitored and secured.

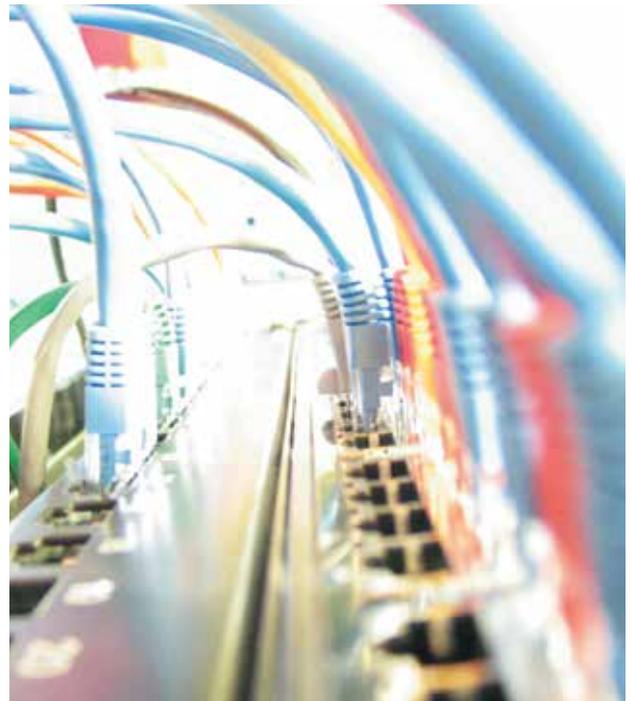
That separation is rapidly disappearing. The cost, flexibility and performance advantages that come from using IP-based infrastructure have revolutionized physical security. Almost every security camera or sensor technology sold today operates on an Ethernet-based wired or wireless network. As a result, physical security solutions such as video surveillance are vulnerable to the same forms of attack and misuse that have plagued data networks for decades.

The risks and rewards of IP-based convergence are particularly acute for video systems operating across enterprise networks. The high data capacity/low-latency performance of IP infrastructure, combined with the cost advantages of using the same network infrastructure employed elsewhere in the organization, underlie this evolution.

Given the essential role video surveillance plays in protecting everything from residential hallways to military bases to power generation facilities, protecting the physical security solution itself has become a major area of concern for vendors and customers alike. Older physical security implementations enjoyed a certain amount of protection simply by not being connected to other systems. An attacker needed direct, on-site access to equipment or infrastructure in order to take the system offline, monitor video footage without authorization, steal or destroy recordings, or modify content.

IP-based systems use the same network infrastructure as the rest of an organization. As a result, they are subject to the same risks as anything else that is, or has the potential to be, connected to the Internet. Complex multisite installations add another layer of risk, since edge devices must rely on LAN/WAN/Cloud connections to transmit video. Monitoring/management solutions in these scenarios typically use browser-based applications for remote access and configuration.

Mobile devices add yet another layer of complexity to the challenge. Laptops, tablets and smartphones integrated into a video surveillance framework use cellular connections for network communications.



These networks are outside the control of safety and security managers, leaving availability and performance dependent on third-party providers.

This whitepaper discusses the security challenges facing IP-based video surveillance. It then covers best-practices that organizations can apply to ensure that IP-based physical security solutions aren't themselves, ironically, the weakest link when it comes to securing networks and facilities.

The Consequences of Cyber Attack

Cyber-attackers are motivated by many reasons. Some act on political grounds or to gain personal notoriety. Others target specific types of organizations, or just ones that are popular. A cyber-attack focused on business data can result in major consequences, including financial loss, theft of data, intellectual property or classified information, and erosion of confidence with customers. An attack that cripples physical security systems, however, can lead to severe damage to a facility, along with significant injury and loss of life. These are liabilities that no organization should risk having to bear.

While network attacks sometimes come from individuals or groups interested in testing vulnerabilities wherever they may be found, international terrorists and nations who employ professional agents to destroy or sabotage critical infrastructure are more likely to target physical security systems. These agents seek to compromise national security, damage morale, achieve political gain, cause casualties, gather intelligence and extract revenge. Similar threats might arise from domestic terrorists, organized criminals seeking financial gain, or unethical businesses employing industrial espionage.

Internal threats represent another attack vector, one that is notoriously difficult to defend. In these situations, employees or contractors, intentionally or accidentally, expose the organization to risk. These threats can be as simple as a dropped spyware-infected USB drive on the company's parking lot or weak passwords, or as planned as an intentional effort to assist outside agents.

In short, the landscape of cyber-threats is complicated, and it changes on a daily, even hourly, basis. And yet, organizations of all sizes and markets now operate in a world of global connectivity. With on-demand access to data from anywhere, by any device now established as the norm, detailed, defense-in-depth security is an essential response.

The Unique Vulnerabilities of Video Surveillance

Video Surveillance Systems can operate side-by-side with other IT systems, or they can run partially or entirely

A cyber-attack focused on business data can result in major consequences, including financial loss, theft of data, intellectual property or classified information, and erosion of confidence with customers.

within the corporate network. As a result, potential attackers can exploit the vulnerabilities in a video surveillance deployment in order to attack the video system itself, or to use that network to launch attacks against other systems in the organization. In short, IP-based video surveillance is like any other IT system. It runs over the same network infrastructure, often using the same equipment. It is probably connected to the Internet. Therefore, this physical security solution itself must be secured against IP-based cyber attacks.

A typical deployment connects servers and management consoles to IP-enabled cameras and digital video recorders (DVRs). These systems also interact with broader security measures, such as access control systems, alarms and security incident management software. Every one of these connections represents the potential for unauthorized access. In this sense, IP-based physical security is no different from business-based network security.

In many aspects, however, physical security and video surveillance are different, with unique vulnerabilities that must be addressed. Common breach points include:

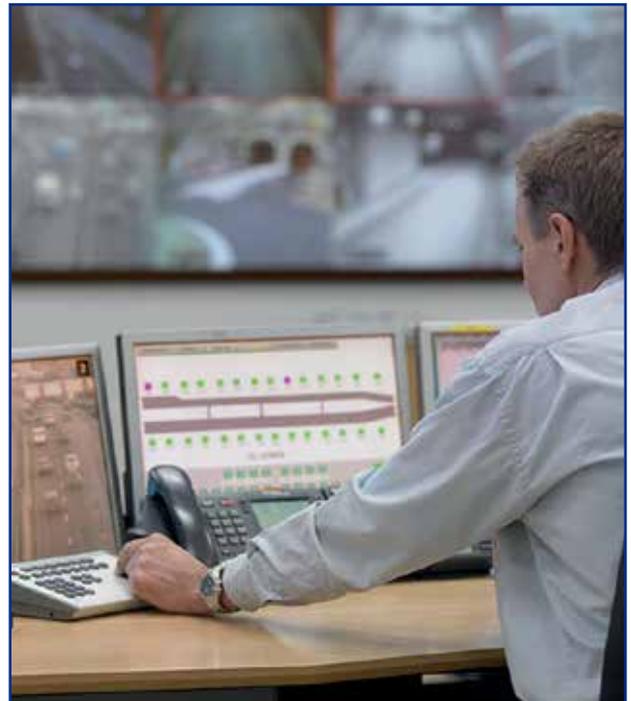
Specialized IP Devices

Almost every IT system is built out of different IP endpoints: servers, workstations, switches, routers and mobile devices. For all aspects, including cyber defense, this is the challenge for every IT professional. Security Management Systems introduce additional IP devices such as IP cameras, Encoders, Access-Control devices, etc. In many cases, these devices are not treated as other end-points in the network. From the attacker's point-of-view, there is no difference between a CRM or ERP server and an IP camera, they are both connected to the network and they both run an Operating System.

Physically Exposed Network Cables and Cameras

IP cameras are installed wherever they are required, whether indoors within an organization's facilities, on the perimeter of unmanned infrastructure, or in a public location such as a park. Ethernet cables connect these cameras to network switches located in communication cabinets, which often are located outside of a secure perimeter. Physically securing this infrastructure is not always feasible or affordable.

A malicious attacker might disconnect one of these IP cameras and use its connection to link a laptop to the network. If communications aren't authorized and secured, the intruder is now part of the system. He/she can steal video, disable cameras, acquire or alter user credentials, and download other sensitive information. The attacker can also use this access to penetrate other networks.



Wireless Networks

Five years ago, video surveillance systems rarely operated across WiFi, cellular or satellite networks. Today, these connections are commonplace, extending across:

- Wireless cameras, either fixed or designed for quick deployment
- Wearable cameras
- Remote sites connected via satellite
- Remote access and configuration
- Mesh networks operating in large facilities and across "Safe City" deployments

Wireless networks are accessible by anyone in the correct geographical area using appropriate equipment. Many of these networks are weakly encrypted, or not encrypted at all. When operated by third parties, such as cellular providers, an important part of the security equation is outside the organization's direct control. Unless carefully configured, deployed and monitored, the convenience of wireless access can introduce a great deal of underappreciated risk.



Open and Forwarded Firewall Ports

Firewalls are a foundational technology for protecting enterprise networks from unauthorized access. However, every firewall must allow network traffic through specific ports in order to connect with the outside world. As in other IT systems, video surveillance networks are also expected to allow remote access, whether it's from different networks within the organization or from outside the organization.

For example, a business application such as an ERP system will maintain Port 80 or Port 443 for other offices and remote employees to connect to the central server. These ports are also widely used for encrypted and unencrypted Web browsing.

Therefore, and by definition, no firewall provides perfect protection. An organization might choose to use unauthorized or unexpected ports to connect cameras, encoders and DVRs to the enterprise network in order to relieve congestion for "normal" business operations. In some situations, remote access is enabled across improperly secured and forwarded port addresses. As above, the inability of physical security staff to understand network security, and network security staff's lack of familiarity with IP-based video surveillance create accidental opportunities for attack and misuse.

The Challenge of Global Connectivity and BYOD

The explosion of cellular, WiFi and satellite communications has led to the expectation that anyone or anything can be connected to the Internet, at any time, regardless of where any given device might be located. Video surveillance is no different. Wireless connectivity

enables cameras to be located in geographically challenging locations that were impossible to service only a few years ago. Operators can configure equipment remotely, as well as access video feeds and management consoles, from laptops, tablets and smartphones. Physical connection is no longer an obstacle to effective operations.

These methods of access introduce new security challenges, many of which have already been discussed above. However, remote access also introduces another type of threat – bring your own device (BYOD). Many organizations encourage staff to use personal devices to access corporate resources such as video surveillance systems. These devices rarely meet corporate standards for antimalware, network access control, passwords, and other basic security measures.

Consider what happens when a system issues an alert. Personnel are likely to need to login from home or while on the road, with the only device available being a personal smartphone. The pressure to allow direct internal access to these personal devices is intense, and network security almost always has to allow some degree of acquiescence. These connections represent lightly protected avenues of access that are easily available for attack or misuse. Even worse, stolen devices that have no password protection or weak passcodes will give an attacker direct access security system.

Transition from On-Premise to the Cloud

The low cost and universal accessibility of Cloud-based storage and computing also affects video surveillance. As the concept of discrete physical and network perimeters becomes more fluid over time, the location of where video recordings are stored, and where command, control and analytics take place, becomes increasingly divorced from actual location.

At the same time, Cloud environments are yet another element of the security landscape that sit outside the control of the customer. Security staff have to trust that the Cloud service provider has implemented a comprehensive security and continuity program, and that the sensors and analytics engines connected to the Cloud are properly hardened against attack.

Ironically, Cloud-based video surveillance and physical security incident management can be just as secure, if not more so, than on-premises solutions. Cloud vendors have a vested interest in reliability, security and uptime. Localized solutions can be poorly implemented, with a lack of attention to security threats.

Regardless of whether an IP-based video surveillance

Security staff have to trust that the Cloud service provider has implemented a comprehensive security and continuity program, and that the sensors and analytics engines connected to the Cloud are properly hardened against attack.

solution is hosted entirely in-house, in the Cloud, or a hybrid of the two, data and services will be exposed if a robust, auditable security program is not in place. Multitenancy and data transmission over public networks can complicate the situation, but the fundamental issues apply to either model.

Best-Practices for Securing IP-Based Video Surveillance

While the risks of an IP-based video surveillance are real, the advantages of this technology clearly justify the transition from older, analog-based systems. Fortunately, video surveillance specialists can apply a well-understood range of best-practices to ensure that physical security solutions are hardened against attack or misuse.

Before we talk about guidelines and methods to secure the Video Surveillance System, there are several things to keep in mind:

- *There is no silver bullet*
There isn't a single solution that will provide full protection from all threats. There are many threats and different methods of attacks. A single attack can consist of several different methods.
- *A chain is as weak as its weakest link*
A determined attacker will eventually find the weakest link in order to fulfil his malicious intent. The best firewall or the most sophisticated encryption algorithm are useless if the password is simply '1234'.
- *Everyone is responsible*
From the vendors, to the integrators and VARs and the end-users. Vendors are obviously responsible for developing and manufacturing secured products, undergoing audit processes, running penetration tests, using S/W code analysis and planning proper training for integrators and VARs. The integrators and VARs are responsible for planning a secured infrastructure, revealing all potential breaches and threats to the customer, utilizing tools and best practices provided by the vendors, ensuring end-user awareness and performing end-user training. The end-users are probably the most important link in the chain and it's crucial to make sure they are not the weakest link. They must be made aware of the threats and the implications of their actions – hence training.

Coordination

Security for video surveillance begins with close coordination between IT and physical security staff. Each group has expertise that the other needs for overall safety and security to be effective. Personnel with expertise in video surveillance, including how cameras, encoders, recorders and analytics engines connect to corporate networks, must share that knowledge with network security, so that vulnerability assessment and intrusion prevention efforts include the physical security implementation.



Likewise, network security needs to understand the infrastructure, access, and bandwidth requirements of data-intensive operations such as video surveillance, and build these needs into broader corporate protection programs. Service prioritization, network reliability, secure remote access, and a variety of other elements can all impact IT network and security operations. These issues need to be fully understood, coordinated and controlled as physical security integrates with overall network operations.

Vendor Openness

Organizations moving to IP-based video surveillance must have access to known vulnerabilities in the firmware and operating systems employed in cameras, encoders, recorders, management systems and analytics engines. This model is well-established for IP-based network devices and software applications. Responsible video surveillance vendors should regularly test their offerings and accept input from independent investigators. This information creates the foundation for trust that products are properly protected against attack, and that patches and workarounds will be provided in a timely manner to protect customer deployments.

Secured Communications

An obvious foundational step to protect IP-based video surveillance systems is to secure the communications between sensors/devices and the network itself. At the least, all communications should be based on encrypted traffic. SSL/TLS should be the minimum standard for connections that take place across the Internet using a Web browser.

Virtual Private Networks (VPNs) provide an extra layer of protection. VPNs typically carry a modest performance penalty, but ensure that only properly authorized and encrypted connections are in use, whether between camera and network, remote user and DVR, or any other linkage in the system.

Robust Password Policies

Passwords tend to be one of weakest links in any security chain. Strictly enforced, robust password policies greatly enhance the level of security for the overall system. Such policies should address:

- Password strength
- Time to expiration
- Account lockout to prevent password guessing

In addition, staff seeking remote access to the system should have to use two-factor authentication (TFA). TFA requires a secondary random password generator or use-once code for each communications session. The goal is to establish that any individual seeking access is authorized for that access, and that stolen equipment or credentials cannot compromise the system. Enterprise-

An obvious foundational step to protect IP-based video surveillance systems is to secure the communications between sensors/devices and the network itself.

grade TFA validates these requests by employing techniques that are extremely difficult to fake, and codes that cannot be replicated by someone lacking specialized internal knowledge.

Network Access Control

Network Access Control (NAC) is a security method that permits network access according to certain policies. One of the most common forms of NAC is the 802.1X standard which uses an authentication server to authenticate and authorize every end-point that tries to connect to the network before access is granted. Endpoints that are not authenticated and authorized are blocked from network access.

Firewalls

Firewalls remain a foundational element for protecting enterprise networks. While most commonly used to protect an organization from external threats, firewalls are also used to separate trusted internal networks from non-trusted or external networks. IP-based video surveillance networks are often isolated from other operational networks using a firewall, so that the risks that are required for successful operations in one part of the organization do not affect the surveillance system, nor do the necessary risks inherent in IP-based video surveillance affect the rest of the network infrastructure.

IP/MAC Filtering

Many IP devices (routers, switches, cameras, etc.) limit access to specific IP and/or MAC addresses. For example, surveillance cameras can be programmed to allow access only from a specific server – or the server can be programmed to communicate only with devices with pre-defined IP or MAC addresses. Access is denied for any device not on this whitelist. In this scenario, an attacker who hijacks the network connection of a camera in the field will not gain access to the network, since his/her computer will not have the correct device identifier.

Physical Access

It may sound odd, but physical security for a physical security technology such as video surveillance is essential. Direct access to devices and network infrastructure introduces opportunities for attack and abuse. Everything from cameras to server cabinets should be hardened against unauthorized physical access, no differently from any other valuable corporate asset. Likewise, in-person access to any part of the video surveillance system should be limited strictly to authorized personnel only.

Intrusion Detection and Prevention

The suggestions above focus primarily on prevention. Other tools and processes, primarily from the network security world, supplement these recommendations



with the ability to test infrastructure for vulnerabilities, to detect improper or unauthorized network access or activity, and to recognize and terminate active attacks. These technologies can be complicated to tune to the operational requirements of video surveillance across large-scale deployments, but are extremely effective in defending high-risk installations.

Conclusion

Effective security happens at every level inside an organization, and outside across vendors, integrators, VARs, and remote end-users. However, not all forms of security are the same. IP-based physical security and network security, while using similar tools and infrastructure, may have to apply different policies and procedures in order to create a fully effective protection program. As a result, it is critical that physical security professionals, such as video surveillance staff and network security personnel, work cooperatively and understand the unique nature of each other's mission.

Vendors, integrators, and VARs also have an important role in this conversation. These third parties represent a broad range of security products, infrastructure and deployments. They see a greater range of vulnerabilities and potential breaches than end user organizations, with deep experience helping customers determine the tools and processes most likely to secure the enterprise, generate end user awareness, and perform training for staff. This latter element is also critical for success, since end user activity is frequently the weakest link in enterprise security, and the most difficult to address.

IP-based video surveillance vendors such as FLIR also have the responsibility of protecting the surveillance system itself. To that end, FLIR's IP-immune platform, launched as ASIS 2015, prescribes a set of offerings that operate within a security-specific framework. Some of these elements are sold as separate products and services. Others are included as part of every FLIR IP-based product, such as encryption and server hardening within FLIR's Video Management System (VMS) applications. FLIR also works in concert with certification and regulation entities such as NIST, to ensure that FLIR products meet current and future standards for secure operation.

IP-based video surveillance is a powerful, cost-effective platform that increases the reach, flexibility, utility and affordability of this critical physical security solution. The challenge comes from protecting this infrastructure itself against network-based attack and misuse. Fortunately, the tools, techniques, training and operational processes exist to make it happen. A carefully planned and implemented program will enable enterprise

IP-based video surveillance is a powerful, cost-effective platform that increases the reach, flexibility, utility and affordability of this critical physical security solution.

organizations to proceed from analog to digital video surveillance with confidence, knowing that any potential vulnerabilities are understood, monitored and contained.

For more information on IP-based video surveillance, network security for IP-based physical security solution and FLIR products and services, contact on of our offices below or email flir@flir.com.

About FLIR Systems

FLIR Systems, Inc. is a world leader in the design, manufacture, and marketing of sensor systems that enhance perception and awareness. FLIR's advanced thermal imaging and threat detection systems are used for a wide variety of imaging, thermography, and security applications, including airborne and ground-based surveillance, condition monitoring, research and development, manufacturing process control, search and rescue, drug interdiction, navigation, transportation safety, border and maritime patrol, environmental monitoring, and chemical, biological, radiological, nuclear, and explosives (CBRNE) detection. For more information, go to FLIR's web site at www.FLIR.com.

Images for illustrative purposes only. ©2016 – FLIR Systems Inc., All rights reserved (created 02/16)

SANTA BARBARA

FLIR Systems, Inc.
70 Castilian Drive
Goleta, CA 93117
USA
PH: +1 866.344.4674

PORTLAND

Corporate Headquarters
FLIR Systems, Inc.
27700 SW Parkway Ave.
Wilsonville, OR 97070
USA
PH: +1 866.344.4674

EUROPE

FLIR Systems
Luxemburgstraat 2
2321 Meer
Belgium
PH: +32 (0) 3665 5100

CANADA

FLIR Systems - Canada
250 Royal Crest Court
Markham, Ontario,
Canada L3R 3S1
PH: +1 866.344.4674

www.flir.com
NASDAQ: FLIR

