IP-Based Surveillance

Storage becomes essential as IP video physical security needs dramatically expand.

Today's companies need to safeguard their offices and parking lots, survey stocks of raw materials and, more important, protect staffers and guests. Consequently, the need for advanced security and surveillance solutions is on the rise.

According to analysts, the presence of cameras can serve as a deterrent to people bent on committing burglary, assault or vandalism in the first place. And if a crime should occur, the stored video content can aid police in fingering the culprits.

To meet security and surveillance needs, more businesses are turning to IP-based video monitoring which leverages the existing network infrastructure already in place. These systems are replacing older analog-based cameras and recording devices.

With more digital video surveillance comes an increasing stream of information or data that must be captured and stored. And to support the data storage needs of these newer surveillance systems, many companies are using Network-Attached Storage (NAS) devices.

Digital Pays Dividends

IP surveillance provides video monitoring capability much like Closed-Circuit Television (CCTV). However, the video footage recorded by the cameras is distributed over an IP network.

The trend to IP-based security is driven by a number of factors. These include heightened security risks and increasing security responsibilities. Plus, the wider range of functions and cost effectiveness of IP-video plays to budget restraints which challenge security departments to do more with less.

The technology offers several key benefits over traditional analog CCTV systems. For one thing, the images are higher quality. IP-based systems provide more control and flexibility in camera functions and image resolution. And video content doesn't degrade over time, as with other systems.

Other benefits include improved search capability, greater ease of use and the ability to record and play content at the same time. In addition, the technology offers the ability to compress video content for more efficient storage.

Because IP surveillance systems run over a network, companies using the technology have the ability to remotely view images and control cameras. Any user that's on the network can potentially view or review video from any camera that's connected to the network.

Also, with IP surveillance systems, it's possible to store data in any location, creating more flexibility for companies. In addition, it's easier to distribute video information to users within the organization. Managers can collaborate more effectively when reviewing incidents or planning physical security strategies.

Finally, networked surveillance systems can be connected to e-mail and other online communications tools such as instant messaging. This allows security alerts to automatically be sent to specific managers.

Security System Components

IP-based video systems consist of several key components. These include the network infrastructure (routers, switches, cabling), IP cameras, video management software (to manage and record the video), a workstation or server to run the software, displays and data storage.

"Businesses will usually have some or most of these components already in house," such as the network infrastructure and a server, which helps reduce the overall cost, says Larry Chay, national distribution manager at AXIS Communications.

A number of things are boosting interest in security overall and IP security in particular. For one thing, the economic downturn has increased security risks and greater accountability within organizations when it comes to protecting people and assets.

For another, companies are looking to keep costs down. The cost-effective nature of IP video helps meet that goal.

Installing stand-alone analog cameras can require lots of extra wiring. This tends to drive up expenses. IP-based systems can connect to existing network cables.

The affordability of IP-based video systems makes them especially appealing to small businesses. Firms are using the technology to stop theft and other illegal activities and to monitor employee productivity.

Small businesses "want to be able to do remote monitoring, protect their assets from theft and vandalism, minimize liability and deter incidents," Chay says. "You can install one camera or 100 cameras, but the fundamentals will remain the same."

Companies often use IP surveillance to cover important entry and exit points at their facilities. This can include entrances, emergency exits and loading docks, says Larry Yablonicky, director, DMR channel sales, at Buffalo Technology.

"In addition, surveillance is used in areas that are large or obstructed from general view," Yablonicky says. "These include warehouses, back stairs and freight elevators.

"Many point-of-sale environments use IP surveillance to monitor cash registers and other areas for cash transactions," he adds. "These can include high-traffic areas that are primary targets for shoplifting."

IP-Surveillance and Storage

In order to provide optimum benefits, IP-based video security requires a reliable storage system to hold the video data. NAS devices are among the most effective alternatives, especially for small businesses looking for ease of use and cost effectiveness.

"Using NAS in an IP-surveillance system helps to make a very compact solution with abundant storage and redundant backup and recovery," says Joe Melfi, associate director, Business Solutions Marketing at D-Link Systems.

"In smaller systems, a PC running surveillance software is used to manage cameras, events, notifications, storage, retrieval and review of stored surveillance video," he explains. "But PC storage may be limited. Adding NAS provides significant expansion of storage."

NAS also supports various Redundant Array of Independent Disk (RAID) configurations. This architecture provides redundancy and high availability, allowing the system to keep running even if one disk goes down.

The disaster recovery component of RAID improves the integrity of recorded footage. "An additional layer of backup can be implemented to archive recordings to another NAS," Melfi adds. "Such as might be implemented to consolidate multiple remote locations into a central location."

With IP-surveillance systems, "there is need for extensive amounts of storage to store and archive a relevant history of events," Yablonicky says. "For example, many U.S. courts require the original unaltered video files to be available for review.

"If a particular video shows an event [such as a burglary] at a specific time, the courts may also require all preceding footage leading up to the event, and all later footage after the event, to understand the cause of events," he adds.

This means companies have to keep extensive event history on file. NAS is ideal for this type as it provides large amounts of capacity.

"NAS devices are also more cost efficient than full-scale servers," Yablonicky says. Those servers offer feature sets not necessary for the recording and archiving of surveillance video. With NAS devices, you pay for exactly what you need."

Companies are using NAS storage with IP surveillance for their primary and secondary storage. "IP surveillance can generate large amounts of data," Yablonicky adds. "The PCs running the surveillance software often do not have enough storage capacity for the surveillance feeds."

What's more, PCs often are far more prone to viruses and hardware failure. This makes them a less-than-ideal location to store surveillance data. A NAS storage system, on the other hand, provides redundancy, replication capabilities and generally better security for the stored data.

Several leading vendors offer NAS devices. These include Buffalo Technology, D-Link, Iomega, NetGear, Seagate, SonicWALL and Western Digital.

Simple Installation

A NAS appliance can be attached to the network and configured in minutes. The device is simple to install and administer, while providing a low-cost storage solution for IP surveillance applications.

One way to look at it is that it's a file serving computer without a monitor, keyboard or general purpose Operating System (OS) like Windows. The form factor can be a box, which you put on or under a desk, or it can be in rack-mount format, which fits in a standard rack.

When selecting NAS, one of the most important buying criteria is capacity. Unlike a SAN, which allows you to cluster units and manage them as a single storage network, most NAS appliances are self contained.

When you run out of space, you may have to ditch your device and buy a larger one. Of course, you can add additional NAS devices to the network.

However, you will have to manage each one separately. (Sometimes you can use one browser screen to manage all network-attached storage from the same vendor.)

Recently Seagate released NAS devices which do provide some scalability. For example, its BlackArmor NAS 420 comes with two preinstalled drives, but has slots to add two additional drives.

Some of Seagate's NAS devices also allow you to exchange drives with ones that are up to double the capacity of the preinstalled media. Within the next quarter, Seagate will release firmware to manage migration of data from smaller to larger drives and from one RAID configuration to another.

"Our goal is to allow businesses to buy the NAS capacity they need now and not worry that they'll lose their investment when their storage requirement grows, says Rob Giardinelli, Seagate's senior product line manager for network-attached storage.

IP-Video Backup

NAS devices can play a role in IP surveillance backup. "Using RAID, the NAS itself can become the backup," Melfi explains. "In some situations, a separate NAS is used exclusively as backup from the primary storage, which may be a PC or another NAS."

Many NAS devices "can act as both the storage target and backup system, integrated into a single device," says Marc Tanguay, global product manager, network storage solutions at Iomega Corp.

Additional NAS devices can be added inexpensively, he notes. And in some cases they can seamlessly be replicated to one another for additional backup protection.

The storage devices are often used to back up the primary storage sources that contain IP surveillance data. While the primary storage sources are often NAS devices as well, backup is often necessary to move content offsite and for long-term archival storage.

"Certain industries and regulations require that content be available for many months or even years," Yablonicky says. "Keeping surveillance storage onsite can pose a security risk if it can be removed from the premises.

"An ideal solution, which covers backup and security, is to replicate the content from the primary NAS device to an offsite device," he adds. "This will provide a real-time backup, and it keeps the content in a location that is inaccessible to intruders."

As for deciding which NAS device is best for IP-surveillance needs, "You should go with a NAS from a well-known company with multiple NAS products with various storage amounts," Chay says. "You should also check to be sure the NAS is optimized for video storage applications."

There are a number of key factors to consider when selecting a system. For one thing, the performance must be adequate to process video feeds from a number of sources. Therefore, the processor in the NAS should be up to the task of managing the volume of information.

Another consideration is whether the NAS device offers RAID redundancy for hard drives containing video content. This assures that years of data are not lost in the event of a drive failure.

Remote accessibility to content is often another requirement, Yablonicky says. Companies might wish to access data from the NAS unit remotely in case of emergency, or if the location under surveillance is in another geographic location.

Jeff Chen, product marketing manager at Western Digital, says other features to consider include network protocol compatibility and security capabilities. This includes such things as password protection or encryption.

Before selecting a NAS system, small businesses need to thoroughly evaluate their video storage requirements and determine which features they need. Once a selection is made, they can truly optimize the value of their IP-based video surveillance system.

How Much Storage Is Enough?

When companies decide to invest in IP video surveillance systems, one major consideration is how much storage is needed to store video data.

"There really is no standard because each business's configuration is different," says Larry Chay, national distribution manager at AXIS Communications. "In most cases, it's less than the business thinks."

Chay says storage is dependent upon six different variables: retention period for information; frame rate; resolution; compression; whether continuous or motion detection is being used; and if motion detection is in place — an estimation of how often it will be triggered.

"You can adjust all or some of these variables to decrease your storage requirements," Chay explains. He says AXIS provides a "storage calculator" that enables companies to see how adjusting these factors affects storage requirements.

Marc Tanguay, global product manager, network storage solutions at Iomega Corp., agrees that storage needs vary widely. "This is based on the physical size and layout of the building being surveyed, and with company policies and concepts on how long footage files should be retained."

Tanguay says minimums are generally five-to-seven IP video cameras, with 640x480 resolution and retained at 30 days. For this minimum specification, Iomega recommends a minimum of 2 terabytes of raw storage capacity.

091111