Designing server, storage and client workstation solutions for mission-critical IP-based physical security applications.
INTRODUCTION

Network video is the leading driver of growth in the video surveillance security market. It’s not only altering the fundamental infrastructure of security systems, but it is also spurring innovation in tangential areas, such as marketing, behavioural analytics and traffic management. Servers, storage and workstation technologies are therefore key components of an IP-based physical security solution. However, many organizations seek to leverage existing assets or idle capacity to meet their video surveillance needs instead of creating a tailored solution to meet the organization’s needs. Even though analog video solutions put together over the years in a disparate way might pass for minimally sufficient, the data-intensive nature of network video technologies make this approach problematic. With the prediction that more than 70 percent of all network cameras will have megapixel resolution by 2015, an integrated and holistic approach to building an IP-based video surveillance solution is needed today.

Evidence indicates that the use of manufacturers’ minimum specifications as a one-size-fits-all solution is creating systems that struggle to address customers’ application requirements for video surveillance and other business functions. Given the forecast that nearly half of all video security systems will run off network cameras by 2014, nonstandard systems will begin to under perform as systems scale.

This white paper pays special attention to the future of network video and the servers, storage and client workstations needed to ensure mission-critical video surveillance remains available and high performing.

DIGITAL DRIVERS AND VERTICAL VISIONS

The migration toward IP-based physical security is being driven by the convergence of Internet technologies and the need for a faster, more reliable and cost-effective network video solutions. The shift from VGA resolution to megapixel and high-definition resolutions has placed a burden on network bandwidth and has created several system management challenges. Compared to standard resolution cameras, bandwidth needs from high-resolution cameras can increase tenfold. Consequently, the input/output (I/O) capabilities of IP video servers need to be significantly greater, and in many cases, standard data servers, even powerful enterprise servers, are not built to withstand the rigours and nuances of IP video feeds.

While the advances in video technology continue to fuel the move toward IP-based physical security, the concurrent need to ensure that technologies work together seamlessly is critical to success. Industry standards organizations, such as ONVIF continue to make great strides in promoting standardization, interoperability and a true open architecture for network video products.

Standardization becomes increasingly important as vertical markets drive overall growth in the IP-based physical security industry. Segments such as retail, education, public safety, government, and healthcare are finding more value in expanding, upgrading or migrating to IP-based video surveillance solutions. However, growth is not limited to security. Video is now being offered as a business service, and improving technologies such as video content analytics (VCA), people counting or traffic pattern analysis are fueling network video adoption. IMS Research predicts that by 2015 the VCA market will grow by $600 million.

TRENDING TOWARD INTEGRATION AND OPEN ARCHITECTURE

The shift toward integration and open-architecture platforms for IP-based physical security is placing greater importance on facilities, security and IT professionals to collaborate in making key hardware decisions. Research shows that an increasing part of the physical security system will run on the IT network:

- 26.4 percent of cameras were IP-based in 2010. (IMS Research)
- Conservative projections put that figure at 48.9 percent in 2014, which means that nearly half of video security systems will run off of network cameras. (IMS Research)
- More than 70 percent of all network camera shipments will be megapixel resolution by 2015. (IMS Research)

Discounting all the other significant advancements in video technology, the move toward network cameras and high-resolution alone will drive IP-based physical security planners to seek out integrated server, storage and workstation solutions that can handle the immense increase in bandwidth and processing needs. New technologies such as edge storage are inherently integrative, which allows users to fill in the gaps for out-of-network mobile applications or network failures. In some instances, companies are leveraging third-party data centres to host cloud-based video, this is still an emerging technology, but can be a cost-effective solution for smaller applications today. From the shift to open and redundant architecture hardware, to the emphasis on total cost of ownership and return on investment, market trends all point to a more integrated IP-based physical security vision.

THE BENEFITS OF INTEGRATION

An integrated network video solution is more robust, scalable and cost effective than an analog system. With improved reliability, redundancy and flexibility of an open-architecture solution, which can exceed any appliance or commercial off-the-shelf (COTS) solution, a truly integrated IP-based physical security solution can also take advantage of today’s best technology, such as higher camera counts, resolutions, access control integration, more intuitive and powerful user interfaces, and multiple analytics.

A purpose-built IP-based physical security solution can also result in both short- and long-term cost savings. By removing the necessity to maintain separate networks, organizations can experience a reduction in capital, maintenance, manpower and equipment costs. When properly planned and executed, an integrated IP-based physical security solution will result in less downtime, which lowers the total cost of ownership.

MARKET CHALLENGES

Of course, as with any complex technology, there are always significant challenges. Complexity can also be a hindrance to a clear migration path, with maintaining legacy infrastructure, long-term organization strategy and cost which is always top-of-mind. Interoperability limitations also present obstacles, with end users concerned about being too dependent on any single manufacturer, managing the multiple communication protocols and dependence on support, especially for highly sophisticated IP-based physical security solutions.
For those looking for a defined migration strategy to network video, the path is muddled as well. Today there are countless manufacturers that purport to have a clear migration path toward an open architecture platform. However, there is simply no one clear migration path to network video that applies to all applications. Even though organizations such as ONVIF are working toward industry standards, the lack of interoperability in many video system products is a serious concern for planners and integrators, which is especially true when it comes to mission-critical functions. Supporting high-resolution cameras from multiple manufacturers requires significant storage and server capabilities to handle the increased bandwidth.

**BEST PRACTICES: PURPOSE-BUILT, VIDEO-OPTIMIZED SERVERS**

When designing or migrating toward a new IP-based physical security solution, the best servers are purpose-built and optimized for video applications. Servers need mission-critical drives with high I/O capabilities and near unconstrained workload capacity. Server configuration is vital and should include memory, storage and processor specifications that ensure optimum scalability for video. Servers should have the capacity to accommodate future growth, including the ability to record higher frame rates without dropping frames, higher resolutions, and cost-effectively store video data for longer periods.

**6G SAS DRIVE TECHNOLOGY**

6G SAS drive technology offers significant advantages over SATA, such as dual port, full duplex, concurrent active channels, robust command queuing and superior error detection and correction. Dual port provides two redundant paths to every hard drive for increased availability and reliability in case of a single-path failure.

Two active (concurrent) SAS channels allow data to be transmitted to and from the disk drive on two separate channels. The drive can execute two write commands, two read commands or a write and read command at the same time.

According to Seagate, a leading hard drive manufacturer of both SAS and SATA drives, the combination of dual ports and concurrent channels on SAS hard drives yields an average performance increase of 135 percent over SATA. SAS is available in three RPM speed: 7,200, 10,000 and 15,000. SATA is only available at 7,200 RPM and 10,000 RPM. As 6G SATA drives have now hit the computer marketplace, the advantages of 6G SAS still has a definite effect on video server storage.

The importance of using 6G SAS drive technology in IP-based physical security solutions cannot be understated. The high I/O workload of network cameras can constantly inundate servers, with client workstations on the other end simultaneously trying to pull video for review. Slower RPM and SATA drives can be a significant issue because of the buffering that is required with single channel data transfer. This lag can result in dropped frames, artifacting and a host of user experience issues. Mission-critical applications require much greater protection than typical data servers, regardless of size and scope.

Besides these advantages, SAS drives also provide double the bandwidth and four times the mean time between failure (MTBF) of SATA drives. Error detection and correction is also superior. Full error correction and detection occurs for both read and writes. SATA drives do not provide error correction on reads, which may result in taking drives offline unnecessarily.

**STORAGE TECHNOLOGIES**

Another vital consideration is external storage, typically needed for greater than 30 TB requirements. The storage needs in a typical network video solution can be immense, with potentially hundreds or more high-resolution cameras capturing as many as thirty frames per second, operating 24x7.

The most common mistake made is to look at streaming video as just another form of data. The case for purpose-built video storage over traditional data solutions focuses on five key areas:

- Massive database size needs
- I/O-intensive operations
- Intolerances of system latencies
- Constant bit-rate streaming
- Demanding operating environments, such as temperature, vibration, bit-error rate and more

Because of the intrinsic nature of streaming video, each of these five areas requires a purpose-built approach that takes into account unique needs, capabilities and system demands. There are many external storage options available, including direct attached storage (DAS), network attached storage (NAS), iSCSI, Fibre Channel and storage area networks (SAN).

An emerging trend is edge or on-board storage, which stores audio and video recordings within cameras, typically using an SD card. Edge storage is particularly beneficial for mobile security or applications that experience network connection interruptions. Edge storage is an excellent complimentary enhancement to central storage to facilitate comprehensive and seamless video coverage building additional redundancy in the solution.
Because video surveillance is a mission-critical application, an IP-based physical security system needs to perform even as individual components may fail. Because hard drives fail, RAID technologies can effectively protect data. RAID is a configuration of multiple physical drives operating as one logical array. There are a variety of RAID levels that are designed to increase I/O performance and data reliability. Selecting the right RAID level configuration for mission-critical video surveillance applications is vital.

**RAID 0** — This level offers the highest performance and low cost using block-level striping without parity or mirroring, so no redundancy is provided in the event of a drive failure. Any drive failure destroys the entire array, as drive capacity increases the likelihood of failure also increases. RAID 0 alone is not recommended for mission-critical security applications.

**RAID 1** — This two-drive function mirrors all of the data written to the first drive, without parity or striping, to the second drive. In the event of a complete system crash, all information would be saved on the second drive. This is crucial for supporting drives that house the operating system (OS) and video software.

**RAID 5** — This level provides redundancy in the event of a single-drive failure that reduces the loss of video data using block-level striping and distributed parity. However, performance of the entire array will suffer as the array runs in a degraded state until the failed drive is replaced and rebuilt. RAID 5 has been commonly used in video surveillance applications over the past several years.

**RAID 6** — Similar to RAID 5, RAID 6 provides redundancy for up to two failed drives using block-level striping and double-distributed parity, which allows the array to continue to function in a degraded state in the event of two drive failures. This configuration gives additional time to replace and rebuild a failed drive, which is an important advantage as disk capacities continue to increase requiring more time for drives to rebuild, making arrays such as RAID 5 more vulnerable. RAID 6 has become popular in video surveillance applications due to its increased fault-tolerance for mission critical security applications.

**RAID 1+0 (10)** — RAID 10 provides high performance and redundancy. Data are simultaneously mirrored and striped. Under certain circumstances, RAID 10 can support multiple drive failures.

**RAID 5+0 (50)** — RAID 50 is a combination of RAID 5 and RAID 0. RAID 50 includes both parity and striping across multiple drives. RAID 50 is best implemented across two RAID 5 arrays with data striped across both disk arrays. RAID 50 breaks the data into smaller blocks, and then stripes the blocks to each RAID 5 array. RAID 50 improves the performance of RAID 5 during writes and provides better overall fault-tolerance.

**RAID 6+0 (60)** — RAID 60 is a combination of RAID 6 and RAID 0. RAID 60 includes both parity and disk striping across multiple drives. RAID 60 is best implemented across two RAID 6 arrays with data striped across both disk arrays. RAID 60 breaks the data into smaller blocks, and then stripes the blocks to each RAID 6 array. RAID 60 improves the performance capabilities of RAID 6 alone and provided better overall fault-tolerance.

The trend in the IP-based physical security market is for more network cameras per server and more storage per server. With network video servers that exceed 24 TB, RAID 50 or RAID 60 may be the best RAID level to use for archive video. These array configurations allow for the best storage capacity utilization. Instead of having multiple RAID 5 or 6 arrays per server and having to point different groups of network cameras to each array, RAID 50 and 60 will combine the RAID arrays together into one RAID 50 or 60 array, which will allow all network cameras to be pointed directly to the array.

### ADDITIONAL CONSIDERATIONS

**RAID Controller and Cache** — Using dual RAID controllers in storage arrays will provide extra protection against failures. Battery-backed write cache or Flash-backed write cache also provide additional redundancy within the RAID adapter, saving critical yet-to-be archived video streams should the system power fail prior to archival recording.

**Redundant Power** — Servers and storage should have primary and secondary power supplies. Should one power supply fail, the system will continue to function without incident. An alternative option is to split the power feed between two uninterruptible power supply (UPS) units to increase fault-tolerance.

### THE MISSING LINK: VIDEO-OPTIMIZED WORKSTATIONS

One often overlooked piece is the client viewing station. Many times an existing workstation or standard PC specification meant for employees is used as the client viewing station, which vary in configuration based on their originally intended purpose. However, the highly demanding needs of video requires a workstation built for continuous 24/7 performance, 365 days a year. Purpose-built workstations for video feature higher level cooling systems, 450 watt and greater power supplies, dual Ethernet adapters (for management), server-grade processors and expanded display capabilities. Today’s high-resolution graphics adapters draw from the power source, increasing impact when installing multiple adapters. The primary demands on client viewing stations are compression and process-intensive decoding in order to properly render video. And, as compression algorithms continue to evolve, the demand on workstation performance will only grow exponentially. Keeping that in mind, video processing workstations should be as future-proof as possible, with the ability to expand and scale up to support future compression algorithms.

At the end of the day the client viewing station represents the user experience and should not be cut short only to reduce the quality and effectiveness of the entire network video solution.

### CONCLUSION

With rapid advancements in network video technology, consultants, integrators and end-users are challenged with migrating away from disparate legacy systems to a more integrated, holistic approach. Migrating to a network video solution requires servers, storage and workstations that can scale and support future technologies, meet specific application challenges and allow for the development of a long-term technology continuum. By going beyond single-manufacturer systems and embracing open-architecture solutions, organizations can better meet their application requirements and provide flexibility throughout the network. Given the forecast the nearly half of all video security systems will run off network cameras by 2014, nonstandard systems will begin to under perform as systems scale. Choosing servers, storage and workstations that perform seamlessly with the network will ensure mission-critical video surveillance systems remain available and high performing.
Anixter Inc. World Headquarters • 2301 Patriot Boulevard, Glenview, IL 60026-8020 • 1.800.ANIXTER • 224.521.8000 • anixter.com

Anixter is a leading global supplier of communications and security products, electrical and electronic wire and cable, fasteners and other small components. We help our customers specify solutions and make informed purchasing decisions around technology, applications and relevant standards. Throughout the world, we provide innovative supply chain management solutions to reduce our customers’ total cost of production and implementation. A NYSE listed company, Anixter, with its subsidiaries, serves companies in more than 50 countries around the world. Anixter’s total revenue approximated $6.1 billion in 2011.

Anixter does not manufacture the items described in this publication. Any applicable product warranties are provided by the manufacturers. To the fullest extent permitted by law, Anixter disclaims all warranties, either express or implied. The information provided and any images shown are for descriptive purposes only. Anixter makes no warranty or representation, express or implied, about the accuracy or completeness of any information provided. Data and suggestions made in the publication are not to be construed as recommendations to purchase or as authorizations to use any products in violation of any law or regulation. All products are sold subject to Anixter’s General Conditions of Sale.