Think Outside the DVR

Video Surveillance and External IP Storage Solutions

Technical Issues and Comparisons for IP SAN versus NAS Storage for Video Applications

White Paper

Executive Overview

With rising costs, new threats, and demands to do more with less, security practitioners are facing more challenges than ever in meeting video surveillance needs.

Traditional video surveillance requirements for physical security or gaming continue to grow. Many security practitioners find themselves also supporting new surveillance applications such as retail and bank branch surveillance, manufacturing and supply chain surveillance, education and campus security, transportation and traffic monitoring, infrastructure protection, hospitality, law enforcement, corrections, and homeland security surveillance needs. And all of these typically require for higher resolution and frame rate, higher reliability, and increased retention periods. At the same time, budgets are stagnant or declining, putting financial pressure to do more with less across the industry.

Few if any technologies offer more opportunity to meet the demands for reduced surveillance cost while also stepping up to these new requirements than does the introduction of external storage.

One third to one half of total surveillance cost is typically driven by the storage employed, yet is a typically low priority area in the minds of security practitioners. DVRs and many NVRs currently use direct attached storage (DAS), in a legacy model that is best described as fixed, captive storage.

This whitepaper will focus on a pair of dominant external storage technologies from the IT world, both now available in IP network format to be employed with DVRs, NVRs and IP cameras. The two solutions are *IP SAN* (or IP Storage Area Networks) and *NAS* (or Network Attached Storage). While the names may sound somewhat similar, they produce very different results.

This document examines why IP SAN is clearly the better choice for video surveillance deployments.

Actual lab tests are used with IP SAN and two different types of NAS storage, all engaged with typical surveillance cameras and video management software systems. These systems are examined in a controlled environment that eliminates the guess work associated with on-the-fly testing faced by most customers in live environments, and is thus able to clearly demonstrate why IP SAN is the superior solution for video surveillance applications.

Contents

Introduction

With most video surveillance practitioners now reaching the end of a multi-year trend of movement away from tape-based CCTV recording, DVRs (Digital Video Recorders) now represent about 70% of surveillance systems.

A DVR typically is a closed environment with its own motherboard, processor, analog-to-digital converter, and one or more disk drives.

Storage inside a DVR is fixed, and captive to that system. It cannot be shared with other DVRs, and is limited in reliability and expansion capacity. In IT, this is analogous to the use of Personal Computers (PCs) beginning in the early 80s. All storage was captive to an individual PC or computer platform, and could not be shared with other PCs. More on this in a moment.

While a DVR supports analog cameras, NVRs (Network Video Recorders) support digital, IP network cameras (there are some hybrid DVRs that also support both analog and IP cameras). NVRs can offer more throughput and additional cameras, along with more features than DVRs do, and thus are also growing in popularity for new installations.

Some NVRs are entirely software based, leveraging commodity server or workstation hardware as their platform, while others offer a complete hardware solution not unlike a DVR.

Regardless of format, both DVRs and NVRs can employ external storage for improved capacity and reliability.

Storage Types

There are many ways that video surveillance streams can be recorded to digital disk drive media, ranging from traditional DAS (Direct Attached Storage), NAS (Network Attached Storage) and SAN (Storage Area Network).

Each of these has its own advantages and disadvantages. DAS has been the most frequently implemented option for DVRs and is generally bundled with the recording system. As discussed earlier, Internal storage of this type is typically referred to as “fixed, captive storage” as it is limited to the single DVR/NVR that it is attached to in a very 1980s model of storage use.

For medium and large scale video surveillance applications, where performance, reliability and scalability of the storage system are important factors, the newer technologies of SAN and NAS are usually better options than fixed DAS storage.

Both SAN and NAS are external storage solutions, and are the focus of this paper. These networked storage technologies are where IT users moved to in the 1990s, away from the fixed, captive DAS storage found in most then common computer systems. The primary reasons for IT doing so were lower costs, higher performance, and increased reliability combined with a lower administrative burden, and all are benefits available to physical security today.

Network Storage

First, we will review *Storage Area Networks*.

SANs are powerful storage networks that record or write data to disk drives in native block format, just as IP network cameras do. The first SANs used Fibre Channel (FC) network infrastructure and delivered high performance, improved reliability and large storage capacity. FC SANs remain suitable for major databases, on line transaction processing, and other IT applications that require large amounts of data with rapid, dependable access.

The cost of the FC SAN infrastructure and the complexity and advanced storage skills necessary to deploy and administer these systems largely continues to restrict them to use in major organizational and corporate IT environments. FC SANs continue to dominate the IT storage requirements of these large data centers, and are offered primarily by a small number of major storage vendors.

Branch office and departmental IT requirements, as well as those of small and medium business (SMB) users, remain largely impractical for FC SANs. This is due to the cost of FC SAN technology, and the specialized storage skills needed to install and maintain it.

These limitations resulted in the spread of another IT network technology in the 1990s and early 2000s, *Network Attached Storage* (NAS).

NAS systems are often less expensive and lack the management complexity of FC SANs. They are therefore well suited for those same SMB, departmental or work group IT users. NAS systems record data in file format, so are good for many IT applications like word processing, email and presentations that work in that manner.

NAS systems leverage the NFS (Network File System) protocol, primarily used in Unix- or Linux-based operating systems, and CIFS (Common Internet File System), usually for Windows-based systems.

However, the desire for the scalability and reliability of SAN technology continues to grow even today, and resulted in the introduction and widespread acceptance of the newest network storage technology, IP SAN, in the mid 2000s. Intransa

was one of the first handful of IP SAN vendors, and continues to maintain a technological edge in scalability and performance.

IP SAN (for *Internet Protocol* SAN) is also known as iSCSI SAN (Internet Small Computer Storage Interface SAN) for the protocol it employs; the names are generally interchangeable for this discussion.

IP SANs offer the same high reliability and high capacity storage as FC SANs, but for a fraction of the price. IP SAN has another advantage in that it is much less complex than FC SAN to install and administer, and is comparable or even easier than many NAS solutions to deploy and use.

More recently, Green IT requirements have further driven IP SAN implementations, with high density, tight footprints resulting in less environmental impact and highly reliable, low energy SATA disk drives consuming a fraction of the power per terabyte (TB) than do similar FC SAN systems.

IP SAN technology has made huge inroads in IT as a result of these benefits, fulfilling many of the storage needs that departmental, workgroup and SMB IT users previously used NAS for since FC SAN was unattainable.

At the same time, IP SAN has grown to be a major competitor for many IT needs of even the largest corporate and government IT needs that formerly were exclusively deployed with FC SAN solutions, such as for large archival databases or for disk-to-disk backup solutions in place of tape storage.

Until recently in major IT installations however, FC SAN continued to have the edge over IP SAN due to better performance of the FC SAN infrastructure. That largely changed when several IP SAN vendors introduced 10GbE (10 Gigabit per second Ethernet) solutions (including Intransa), which are now competitive with FC SAN for performance, yet remain a fraction of the cost and without the complexity of FC SAN.

While FC SAN is not commonly found in video storage environments due to these cost and complexity limitations, a limited number of NAS solutions have been available for some time to the physical security user. Thus this document reviews the merits of IP SAN and NAS, and ignores the relatively few implementations of FC SAN in the surveillance space.

Overall, IP SAN is newer to physical security, but is growing very rapidly in market presence, displacing both fixed, captive DAS storage commonly found in DVRs, and the NAS storage previously marketed for use with NVRs.

Live Video Recording Workload Profiles

The typical components of a video surveillance system are familiar to physical security practitioners. These are usually one or more analog or IP network cameras, a network, one or more DVRs or NVRs, and a storage subsystem.

Figure 1 details at a high level how video frames are recorded onto digital media. This example shows storage as an external component, instead of fixed, captive DAS storage in the DVR or NVR. In the case of the NVR, it features a video surveillance management system (VSMS), also referred to as a video management system (VMS). I/O or IO is a storage term, for input/output functions, which is a component of the system workload and throughput.

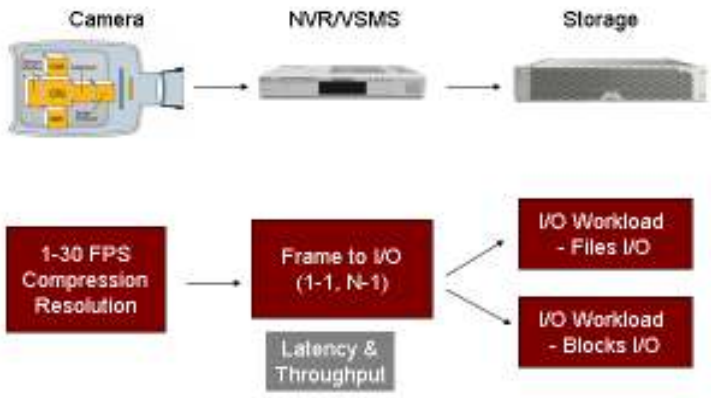


Figure 1: Video recording I/O diagram

Overall system performance is characterized by how many cameras or video streams the surveillance system can deliver without dropping frames or otherwise losing video.

Camera Terminology

Camera, DVR and NVR vendors typically think of system performance as a combination of the number of channels supported, image resolution, frames per second, and compression method.

A channel typically represents one camera that can be viewed by one or more subscribers independently. Image resolution is typically thought of as CIF, 4CIF, megapixel, or 10 megapixel, etc. Frames per second or FPS indicate the number of images recorded per second; the higher the FPS, the better the video quality. The compression method is typically expressed as MJPEG, MPEG-2, MPEG-4, H.264, etc.

Networking Terminology

In the networking world, performance is measured in bandwidth. Bandwidth is a measure of the throughput capacity available to move data, as well as how fast the switch/router moves the data in packetized digital format. This is often referred to as “latency” or “network latency”.

Typical network bandwidth ranges from 10Mbps (10 Megabits per second) to 100Mbps (fast Ethernet), 1000Mbps (1Gbps or 1GbE for IP Ethernet) and more recently 10Gbps (or 10GbE).

For a router or network switch, performance is related to how many packets per second it can “switch” or direct, and what the latency (delay) is for each packet to transverse the switching device.

The focus in the networking environment is on how much data can be moved in a single second, and the technology is indifferent to the type of data being transmitted. In this world, the volume of data being captured or stored is only important for its impact on how much data can flow and how quickly.

DVRs, NVRs and Storage Terminology

The third major component of a surveillance system is the DVR or NVR, which acts as the engine of the entire solution. These devices manage one or more cameras and the storage subsystem. The storage component may be internal, fixed, captive DAS storage or may employ some type of external storage.

The DVR/NVR receives video frames from connected cameras, converts the frames into digital IO (input/output), and then writes the IOs to the storage subsystem.

There are two ways that DVRs and NVRs can write to a storage system, known as either “direct” or “indirect”. This brings us back to the differences between SAN and NAS storage systems.

A *direct write* is an IO recorded to a storage block device such as a disk drive on an IP SAN. *Indirect writes* interject another interface layer into the process, using a specialty storage device such as a NAS server, which then in turns writes to the disk drive.

Video frames from cameras are passed from the DVR or NVR to the storage system.

Video recording is generally a non-stop operation, and is typically a write-dominant workload. This means that recording (writes to disk) continue without halting while the system is in record mode, and represents the majority of the

activity under this workload. Playback (reads from disk) is much less common and as such is not as demanding in typical video surveillance applications. It occurs more infrequently, such as when an incident occurs and playback is required for analysis or review.

In a NAS system, with many streams continuously writing to the DVR or NVR in a very short amount of time, the storage continually re-allocates space on the disk drives in the file-based storage system. This will result in a severely fragmented drive over time, where files are recorded in disjointed segments across the disk.

With video, this fragmentation is much worse than what normally occurs in an office or personal desktop or IT application such as word processing, email or spreadsheet files reads and writes. The performance impact that results is a major concern.

IP-SAN and NAS Differences

NAS

As previously mentioned, NAS systems employ and "serve up" files to a DVR or NVR using two IT protocols: CIFS (Common Internet File System) for Windows platforms, and NFS (Network File System) for Linux or Unix.

CIFS is a network protocol whose most common use is for sharing files on a Local Area Network (LAN). The protocol allows a client (such as a DVR, PC or workstation) to manipulate files over the data network as easily as if they were on the local desktop computer.

The CIFS protocol works by sending packets from the client to the server. Each packet is typically a request for action of some kind, such as "open file", "close file", or "read file". The server then receives the packet, checks to see if the request is legal, verifies the client has the appropriate file permissions, and finally executes the request and returns a response packet to the client. The client then parses the response packet and can determine whether or not the initial request was successful.

NFS (Network File System) is another common network file system protocol allowing a user on a client computer to access files over a network. NFS is the standard file sharing protocol for all Unix- and Linux-based NAS systems.

Because they are based on Linux or Microsoft Windows operating systems, most DVRs and NVRs are able to support NFS, CIFS and/or iSCSI/IP.

IP SAN and iSCSI

By taking advantage of the wide use of Ethernet-based IP networks, IP technology has moved from being primarily an IT-only solution to increasingly being deployed for physical security needs like access control, life safety, and surveillance systems.

IP SANs use the iSCSI (IP) protocol to transport data from a client system (such as a PC or DVR/NVR) to a target system (such as the external storage) over an IP network.

A software client called an iSCSI initiator is used to initiate connectivity between the target and client systems over the IP network. Each iSCSI initiator is identified by a unique name, and many DVRs and NVRs have the initiator software pre-installed. Others allow it to be added quickly when upgrading to external storage.

A network used by an IP SAN is often physically separated from other IP network infrastructure, such as the IT network in an organization. Or it can be logically separate, able to access a segment or portion of the overall network so as not to impact performance on the larger corporate or organizational network system.

DVRs, NVRs and storage devices are connected to the IP network via standard network interface cards (NICs), typically either supporting 1GbE (1 Gigabit per second over Ethernet) or the less common but newer and faster 10GbE infrastructures.

A small percentage of DVRs employ proprietary, non-standard operating systems that are unable to support the iSCSI initiator and therefore are unable to leverage the benefits of external IP storage (IP SAN or NAS).

IP SAN and NAS Comparisons

Both IP SAN and NAS systems may use IP networks to access external storage. However, there are major differences in how SAN and NAS leverage the network and access the storage, which result in very difference performance and long term reliability.

Going back to the earlier discussion, NAS accesses storage through a file level protocol (NFS or CIFS) over the IP network.

IP SAN uses the iSCSI protocol to access storage directly at the block level over the IP network. This difference is shown in Figure 2.

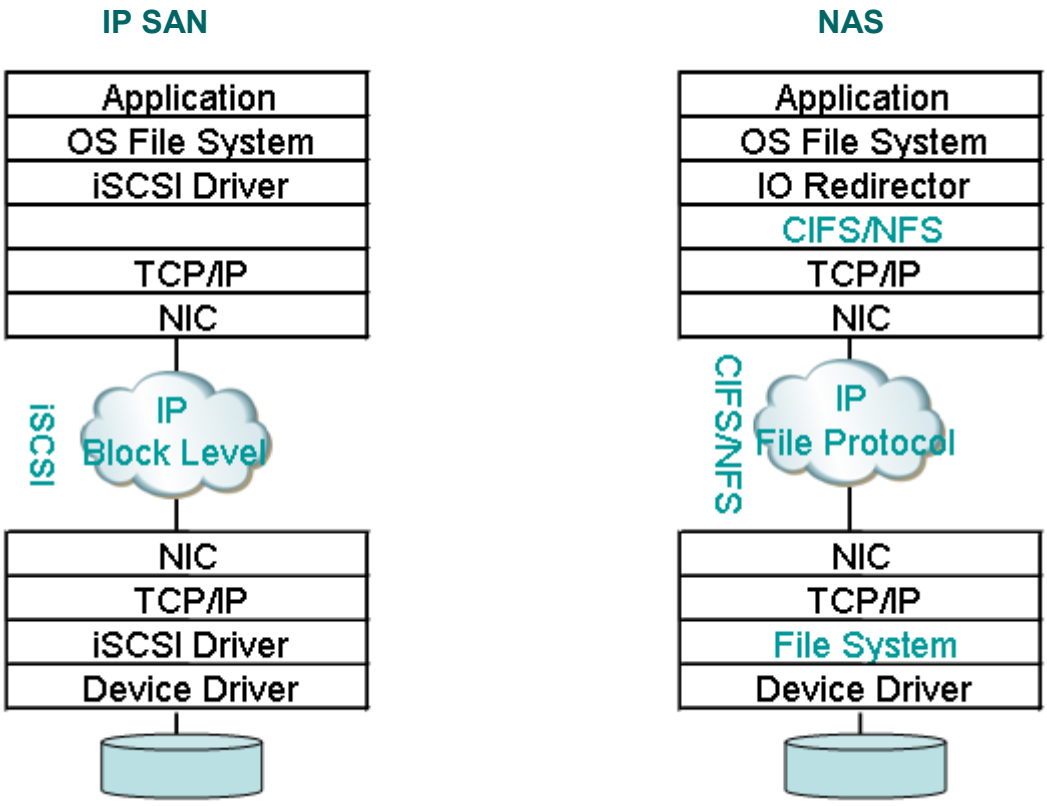


Figure 2: NAS and IP SAN protocol diagram

The left side of the diagram shows how IP SAN enables the DVR or NVR (the application) to write directly to the storage.

On the right side of the diagram, a NAS system is shown. NAS requires that writes to the storage access an additional layer, implemented by the network file system. This extra file layer typically creates increased network traffic, resulting in unintended video recording performance degradation and file fragmentation.

Because video recording applications are very different from traditional IT needs, with a much heavier, constant write (record) profile, the disk drive quality, system design and application customization for video are also very important factors to consider.

Figure 3 shows an example network topology. In this example, over 50 IP cameras were managed through a VSMS (Video Surveillance Management System) or VMS (Video Management System) in a lab environment under controlled conditions to ensure optimum problem identification and elimination.

The storage systems tested were an IP SAN (shown on the left) and a NAS solution (on the right). Both example systems were deployed using 1GbE interfaces over an identical IP network.

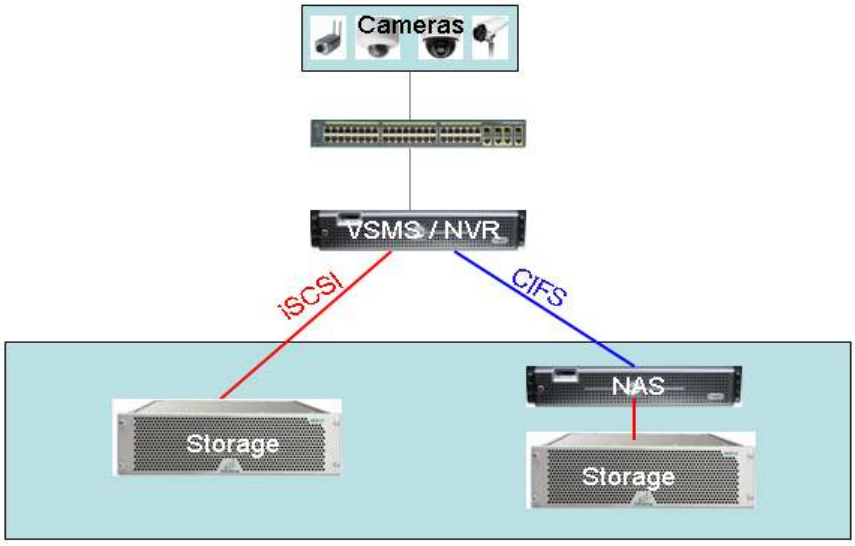


Figure 3: Network topology used for performance measurement

Performance as measured in FPS

For video surveillance applications, the most representative performance testing is based on measuring actual video throughput. Using the test system, it was possible to measure the number of video frames recorded as cameras are added to the system. Also measured was the rate of performance, video loss or other failures.

For the purposes of this paper, two individual CIFS-based NAS servers were used for the measurement, and each compared with a single IP SAN. One NAS server ran Microsoft Windows File Server (a common Windows-based NAS) and the other was a Linux-based file system using Samba (creating a Samba NAS). An Intransa IP storage system was used as the IP SAN example. Figure 4 shows the measured results of the testing.

The resulting differences between the IP SAN and the NAS solutions were rapidly discernable. The IP SAN successfully recorded nearly all video frames from 1 to 30 cameras. However, the NAS system began dropping frames once the system exceeded just 10 cameras, losing video.

The testing was actually performed when conditions were best for a NAS system, specifically when the file system was mostly almost empty of recorded video or data. As the storage fills up with recorded video, NAS systems experience file fragmentation that will further reduce performance and potential video loss.

Security practitioners and integrators who opt to benchmark external storage solutions should therefore expect that initial performance of NAS systems will decline with extended use.

It is important to understand that this discrepancy in performance is specific to video workloads. When measuring only storage IO performance such as by copying standard files to and from the storage, or using benchmark tools such as IOmeter, both IP SAN and NAS test systems demonstrated similar performance results, each delivering over 70MBps throughput.

For surveillance, this can be very misleading, since these test methods do not reveal the fragmentation issue caused by the video workload. Clearly, IP SAN and NAS solutions are both suitable for IT use. But the unusual, write-heavy video surveillance workload makes NAS a poor storage solution choice for this market.

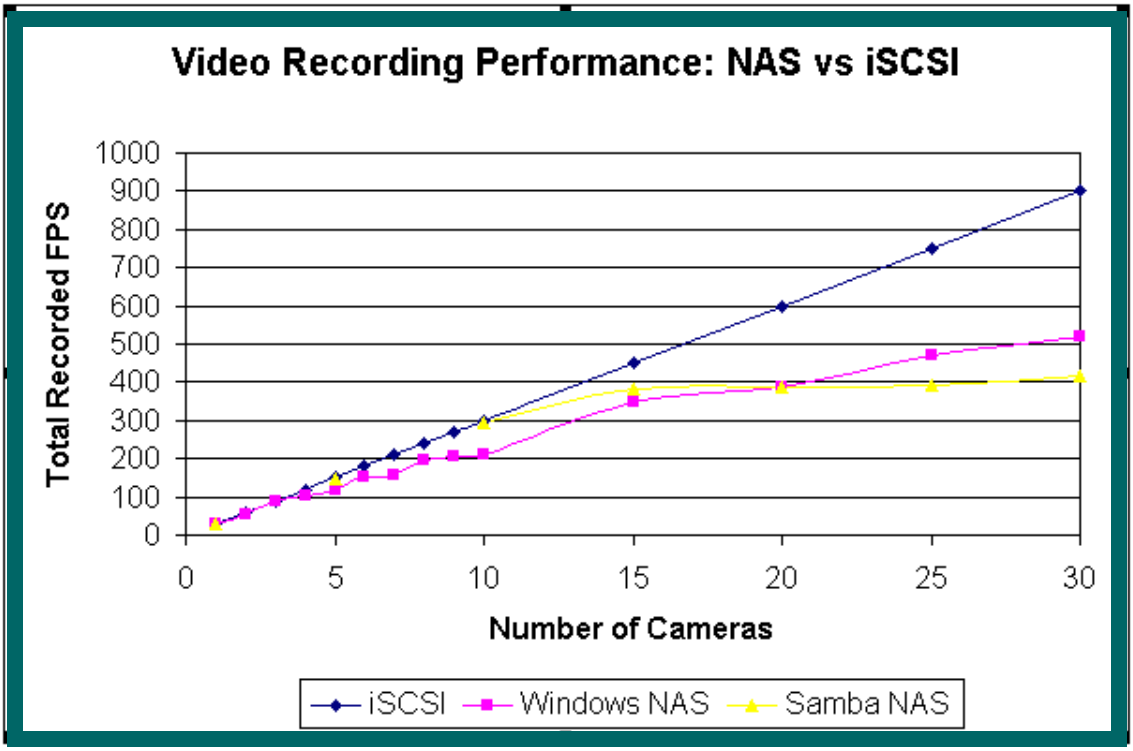


Figure 4: Video Recording Performance Comparisons: NAS vs. IP SAN (iSCSI)

File Fragmentation in NAS Systems

In a typical surveillance environment, when cameras record video to a disk device, video files are created, recorded, deleted, and then created again as disk capacity is used and reused. A single video file may end up spread across multiple locations on the disk in segments. This segmentation results in significant file fragmentation in NAS systems and many captive, fixed DAS storage systems alike.

NAS file fragmentation and its impact on video performance does not show up until the file system is “aged”. Aging occurs when all disk capacity has been allocated for file use, and then de-allocated at least a few times for new file recording. This can take days or weeks to show up, depending on the video application environment and the file system capacity, but the results are always the same. Fragmentation of disk storage systems will result in declining read (playback) and write (record) performance for the surveillance system.

In addressing this issue, many NAS vendors recommend that you de-fragment the file system regularly by running a provided maintenance application. This is a common solution for IT environments, since there is often downtime or off-peak hours for workgroup or departmental NAS systems and it is not generally considered a hardship to perform system maintenance in IT.

However, the need for this frequent defragmentation to maintain optimum or even acceptable performance is a major challenge for video surveillance systems.

De-fragmentation is a system-intensive activity, consuming both computing and storage resources. Unfortunately it can often take hours to defragment one or more large disk drives. Due to the performance impact, surveillance systems may need to be shutdown during de-fragmentation. This makes NAS unacceptable for any non-stop recording environment, which is a significant portion of video surveillance system needs.

Some NAS systems do allow continued operation while defragmenting. However, they will often suffer major performance issues due to the simultaneous video and de-fragmentation workload, resulting in them still being unsuitable for many surveillance environments. This can also result in reduced numbers of cameras and frame rates or resolution that truly can be supported while de-fragmentation is underway.

Figure 5 shows a NAS file system that was measured using standard Microsoft Windows utilities.

When the initial video file was created by the NAS system in the lab test, all of the storage blocks on the disk drive were allocated sequentially. This is shown in the first, left side image. The entire file system is blue, with no gaps between segments of the video file stored.

The second time that the disk is examined, in the middle image, there are already gaps appearing between files as the NAS system starts to overwrite the initial files recorded with new images. These gaps are denoted in red.

By the time the third file is written, red is dominant, showing that the files are badly fragmented and written all over the disk. This results in greatly reduced write and playback performance by the NAS system.

.

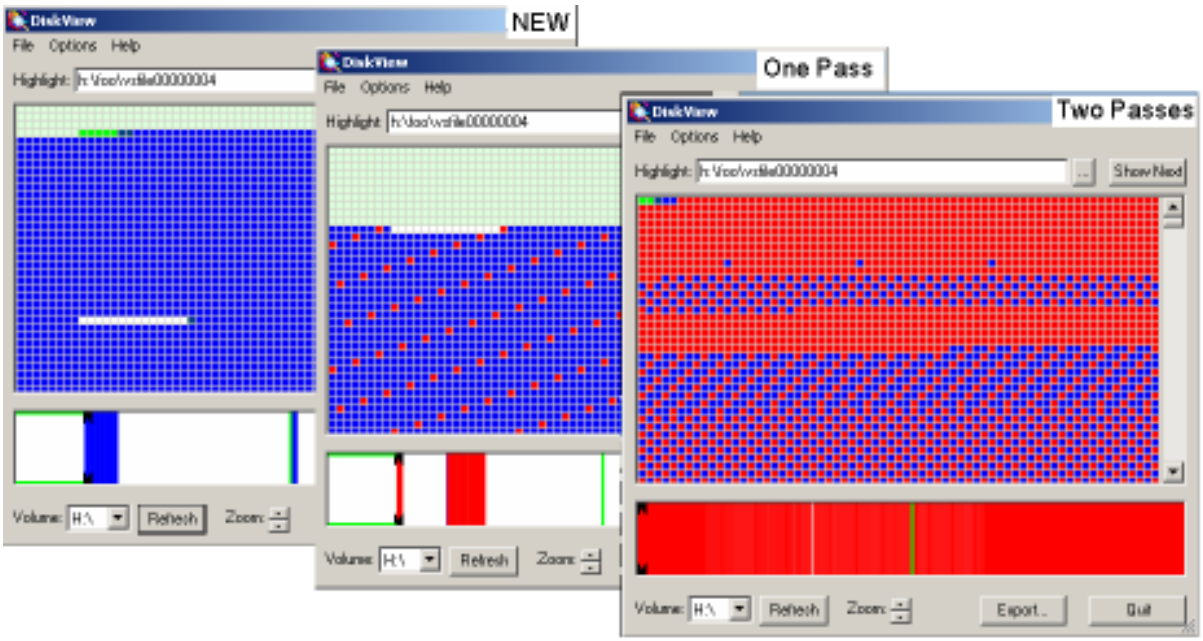


Figure 5: File fragmentation view on NAS

The impact of fragmentation eliminates NAS as a suitable external storage solution for many surveillance environments.

Video Loss and 3rd Party Certifications

Dropped video frames are also an issue for NAS systems. This accelerates as more cameras are added to the system or as video quality requirements increase, putting more demand on the NAS.

Still another reason to avoid NAS for surveillance is data integrity when used in a video storage environment. As the controlled labs tests showed earlier, when the NVR system was supporting 30 cameras for stress testing with NAS, many video frames failed to be immediately recorded, and then many delayed writes failed to be recorded as well. Only by reducing cameras could this issue be eliminated.

Both conditions represent dropped video frames, losing perhaps critical video images in a very unpredictable manner. Part of this testing is shown in Figure 6. Similar poor results did not occur with SAN in the same environment.

Video management system vendors are often aware of some of these NAS system challenges, if not the specific cause. For reasons such as these, Milestone Systems, JDS Digital Video and other experienced video VMS vendors typically recommend the use of SAN systems for live video recording and not NAS. Detailed technical whitepapers with Milestone, JDS, OnSSI, Genetec and other VMS vendors are available for download on the Intransa website.

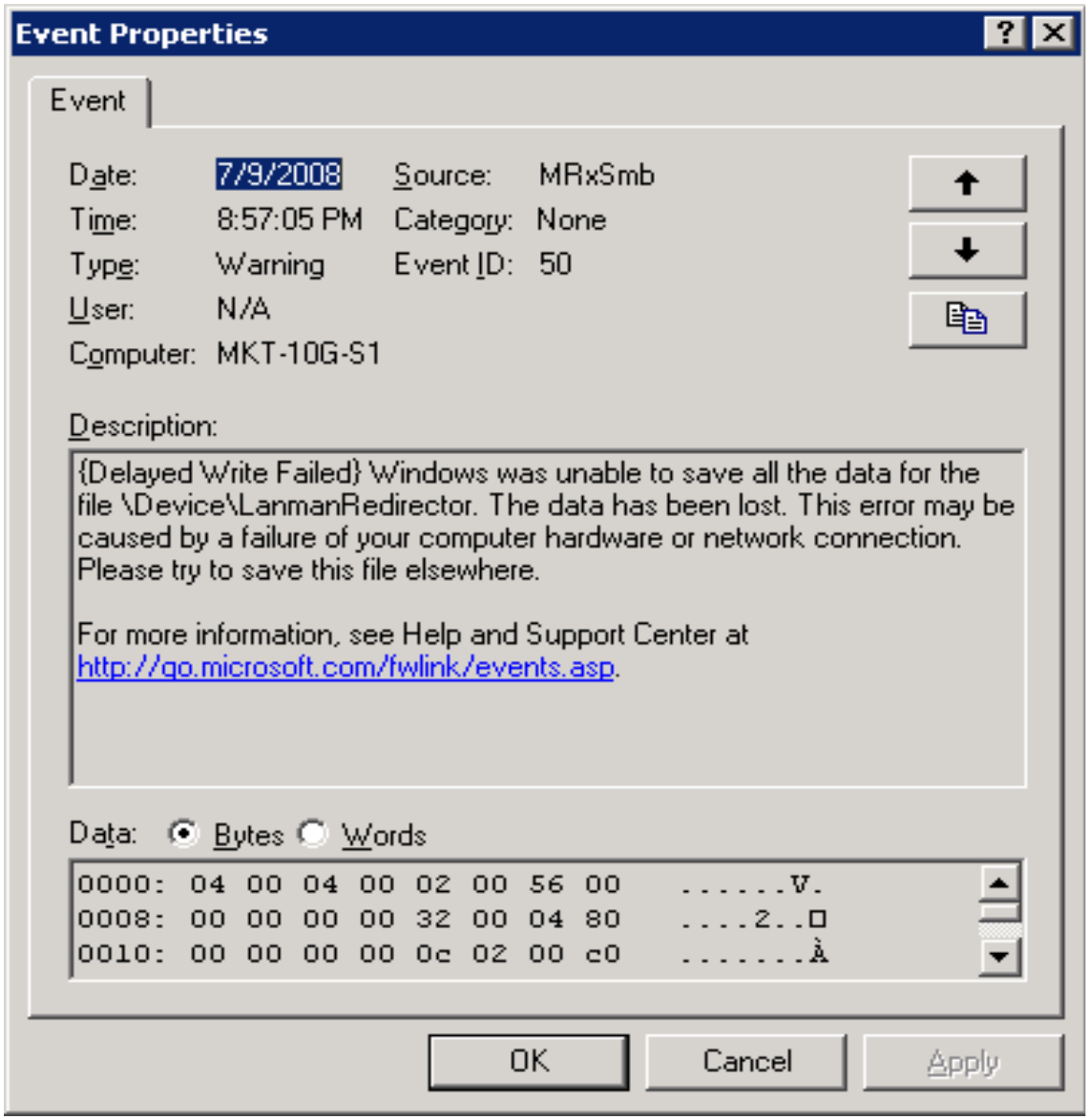


Figure 6: Frame recording issues with NAS on Windows

Network Utilization and Protocol Overhead

When comparing NAS and IP SAN systems, another factor to consider is bandwidth utilization. This is particularly important since the bandwidth between the DVRs/NVRs and the storage system often proves to be a performance bottleneck.

NAS-based file sharing protocols such as CIFS or NFS are commonly referred to as being “chatty”. This is caused by the need of NAS systems to generate more round trips between the storage and the DVR or NVR than a “non-chatty” system like an IP SAN. Thus NAS systems put more traffic onto the system, reducing the amount of bandwidth available for video transmission.

Further, to protect against data loss when an application or user is using any kind of file, many applications will also do periodic automatic saves. This will result in more bandwidth being consumed by the NAS, further negatively impacting performance. CIFS systems do this by sending updates of the files back to the DVR or NVR. These round trips increase network utilization, and negatively affect both network availability and overall system performance.

Figure 7 compares the network utilization of a NVR in the lab test using NAS (shown on left), versus using IP SAN (on right). In both examples, the network is 1GbE Ethernet, and measured using 1 camera at 4CIF, MJPEG and at 30FPS.

The green line represents total network utilization. The red denotes sending data, and yellow receiving data.

Examination of the chart shows that for IP SAN, the link utilization was around 0.81%, with mostly write activity. In comparison, NAS link utilization nearly doubles to about 2%. This is due to extra read activity, even when using only a single camera with a NAS system.

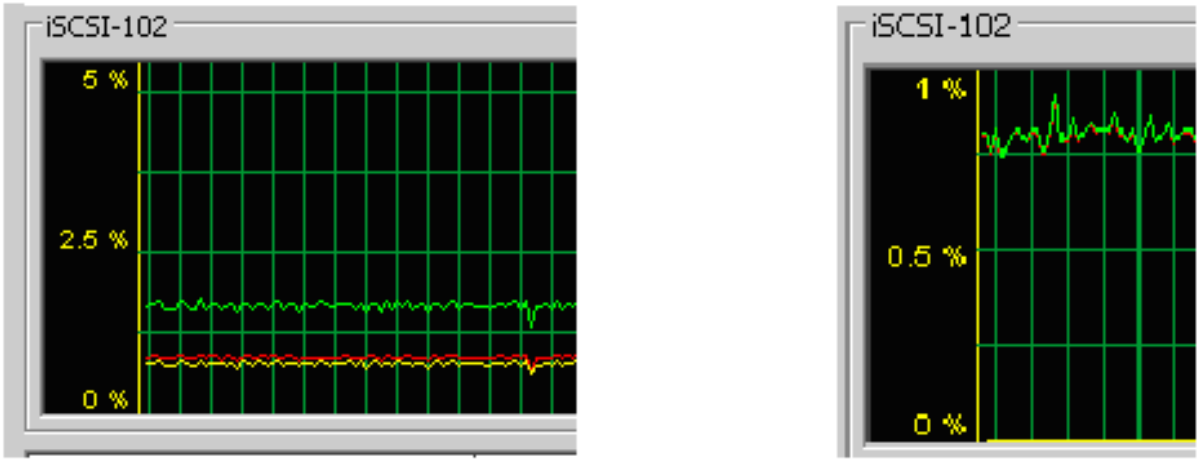


Figure 7: Network Link Utilization for NAS (left) and iSCSI (right) for 1 camera

Figure 8 shows a typical network trace between an NVR and a NAS device.

Without analyzing all of the individual actions and requests it details, even a casual review shows the NAS protocol is indeed very chatty and quite heavy in read operations, impacting performance available for video storing (writes to disk).

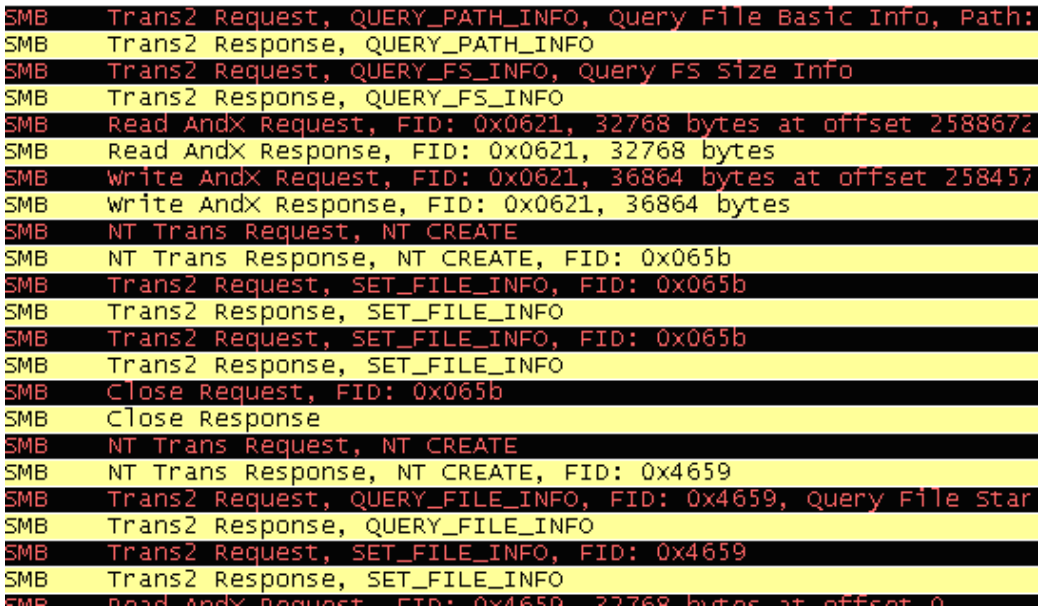


Figure 8: Network Trace collected between an NVR & NAS storage

Disk Drives: PC Grade vs. Enterprise Grade

NAS systems (and to a lesser degree some SAN system) used in the IT world cover a broad spectrum of classes and types. Many of these lower end storage solutions use PC or commercial grade disk drives rather than higher cost enterprise or OEM grade versions. This enables the vendor to offer a lower system price.

Unfortunately, PC-grade drives fail at least twice as often as do their enterprise-grade counterparts. For video, with a non-stop 24x7 workload, these lower quality drives can lead to lost video, system downtime and unnecessary performance challenges.

While some storage systems offer RAID protection and hot-swap disk drives that can alleviate some of the impact of constantly failing PC-grade drives, they do not remove all of the risk of poorly designed and non-reliable hardware.

Security practitioners need to consider the quality of the components deployed due to the intensive nature of video, something that is often overlooked and

results in unexpected results. A surveillance system that loses video or is unavailable for recording when needed is not worth the investment.

What You Can Do to Protect Your Investment

Some organizations have unused NAS system capacity on an existing IT storage system, or have made a recent investment in a NAS solution for an IT requirement. Care should be taken before seriously contemplating using that IT-focused storage for video. As detailed in this document, NAS is not typically an ideal video surveillance storage platform.

To protect your surveillance system, it is strongly recommend your NAS vendor first provide documentation outlining video surveillance-specific testing for performance and frame loss as a first step to ensure you receive the reliability and performance required and expected.

You should also require a list of typical physical security applications that have been tested and certified in some comprehensive manner with the NAS system. If intending the video storage to record from DVRs, multiple applications such as video management systems, physical security information management systems, and video analytics at a minimum should be certified to give some assurance that the system really is suitable for video surveillance usage.

If you plan to use the NAS system to record from not just DVRs but instead from NVRs and/or directly from IP cameras, not only is the above list critical, but you also need to verify that they have tested and certified with NVR software and with IP network cameras. The number of cameras that can realistically be supported and for how much video retention will be very important to review.

Unfortunately, you will likely discover that the NAS system you are considering is a general purpose IT storage system, exactly like the systems sold to that market. While it may be a suitable solution for traditional IT workloads, if the vendor hasn't done performance and capacity testing, and partnered with 3rd party physical security vendors, they likely have no idea of the magnitude of problems that may be encountered.

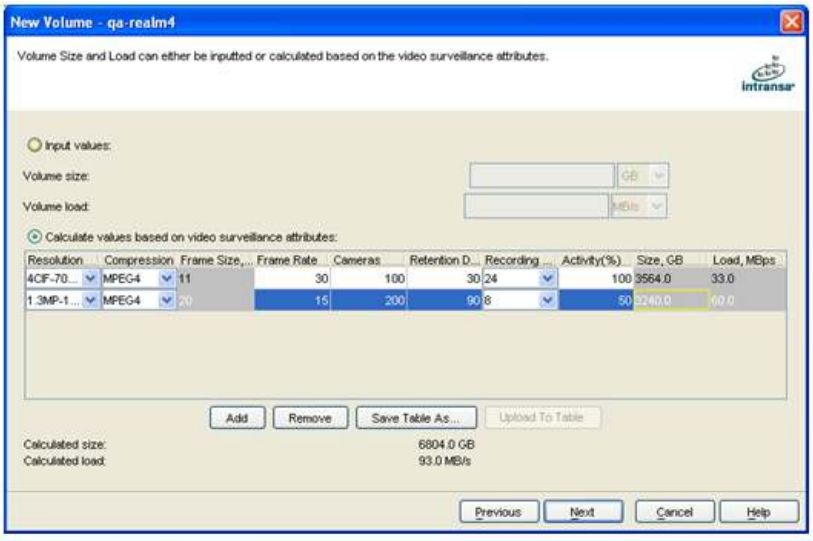
A final recommendation is that you do not accept a general-purpose storage system that has not been optimized for video surveillance needs. Instead of requiring detailed IT network and storage expertise to set up and administer a basic NAS – or SAN – system, the solution that you select should be clearly *physical security friendly*. The best SAN systems for video surveillance have a physical security-optimized user and administration interface that uses security friendly terms like number of cameras, frame rate, resolution, compression and days of retention and not specialized IT terms for setup and day-to-day administration.

About Intransa

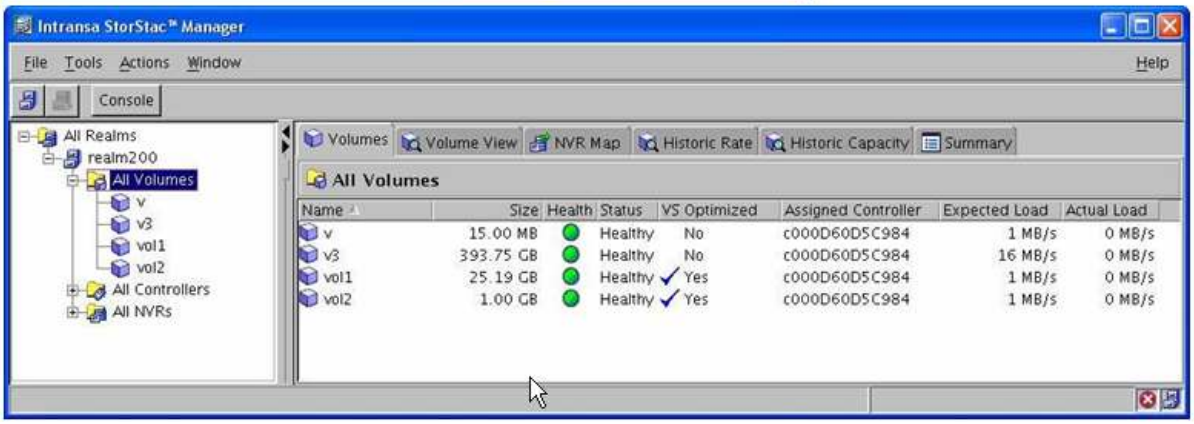
Intransa provides affordable, scalable and dependable external IP storage optimized for video. Intransa solutions are designed specifically for use as shared, external video retention capacity for DVRs, Hybrid DVRs, and NVRs, or as all-IP video surveillance storage system platforms and for direct from IP camera recording. Intransa IP storage is cost effective for a surveillance system using a single DVR, with benefits and savings growing as more DVRs, NVRs, surveillance cameras and other devices are added, or as retention and video quality requirements increase to meet new challenges.

Intransa external video storage is based on our proven IP SAN storage system, shipping since 2003. It is ideal for use as an edge recording platform or as the primary video storage for surveillance deployments. Intransa IP storage has been certified through our *Security-Grade IP Video Storage* program with nearly 100 physical security, imaging and IT products for risk-free integration and use.

The integrated Video Storage Administrator (VSA) functionality of Intransa StorStac shared, external IP storage allows non-storage experts to get the most out of their



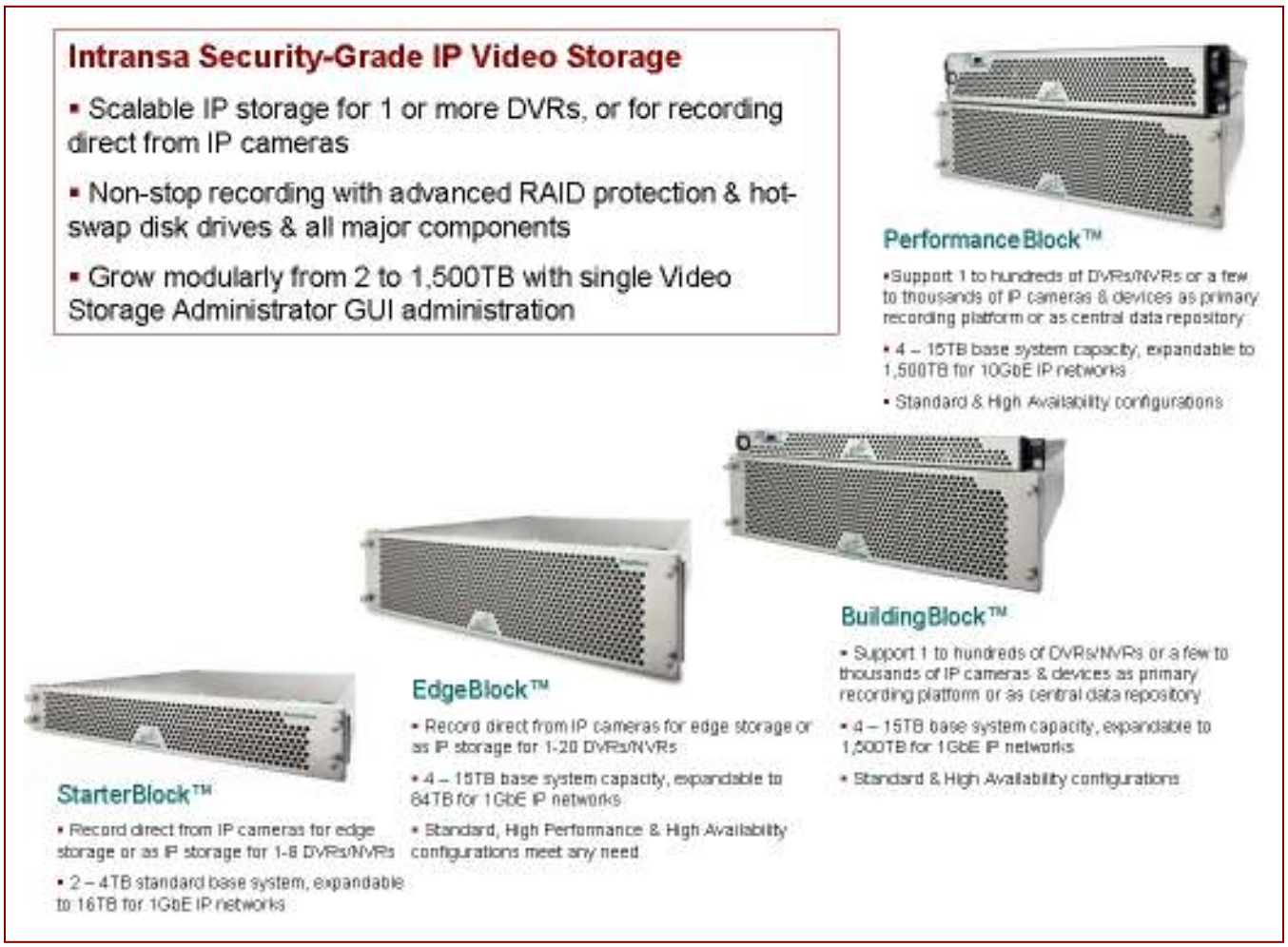
The Intransa Video Storage Administrator (VSA) provides the ability to set up and administer storage in physical security terms such as resolution, compression, frame rate, number of cameras and desired retention, not complicated IT terminology.



Intransa IP storage, and dramatically reduces the learning curve to get maximum benefit from our IP storage solutions without mandating extensive IT knowledge and effort.

Unlike captive, fixed DAS storage commonly found in DVRs, or standard IT workload SAN and NAS storage sometimes found with NVR systems, Intransa shared, external IP storage is optimized for video workloads. This video optimization also eliminates performance problems related to disk fragmentation found in general purpose IT storage and allows higher total storage utilization, which can dramatically lessen the total amount of storage required.

Intransa scalable IP storage solutions scale modularly from 2TB of IP storage, suitable for edge recording for a few IP cameras or a few DVRs for perhaps a month of typical retention. Intransa StorStac Systems scale modularly to more than 1,500TB to affordably support thousands of cameras and hundreds of DVRs or NVRs. That is enough affordable capacity to delivering months or years of video retention at maximum resolution and frame rate for optimum video quality.



Performance can be similarly scaled, allowing faster recording and support for many more cameras and IP devices than similar systems.

Other physical security applications such as access control, biometrics, life safety, compression modules, and utilities can simultaneously leverage the power of Intransa storage used for video surveillance.

Some users choose to leverage Intransa's IT-proven features as well, including DynaStac Thin Provisioning, StorAR Asynchronous Replication, RAID 0, 1, 5, 6, and 10 support, StorCluster N+1 Clustering and Failover, StorStac Snapshot, Global Sparing, Dynamic Load Balancing, Non-disruptive Upgrades, call home support, and the powerful StorManager graphical user interface (GUI) and integrated command line interface (CLI).

All Intransa systems feature advanced RAID protection, field replaceable components, and hot-swap disk drives for non-stop recording with enterprise-grade components.

Intransa believes in the power of partnership and alliances, and has funded the StorAlliance Technology Lab to ensure that the promise of IP is delivered in real world solutions. The lab certifies IT products through the *Intransa 10GbE IP SAN Certified* program and the *Security-Grade IP Video Storage Certified* program for physical security.

Through the StorAlliance program and other real-world test environments such as the GSO 2010 (www.gsoevents.com) conference series, security practitioner participants get to perform hands-on testing simultaneously with multiple IP systems from a dozen or more vendors all using Intransa IP storage, shared, external IP storage simultaneously. Intransa storage and upgrades are tested in real world conditions before reaching customers.

Physical security applications like life safety, access control, physical security information systems and IP devices ranging from surveillance cameras through to card readers, slot machines and retail systems can all benefit from using the Intransa shared, external IP storage solution.

IT vendors certified include those offering operating systems, email, relational databases, ILM, CDP, HSM, VTL, backup and recovery, data warehousing, data mining, clustered file systems, network attached storage, and server and storage consolidation. Participants include Microsoft, with the first IP storage to be certified with 10GbE interfaces supporting Microsoft Exchange 2007, and VMware ESX virtualization.

Only vendor products that have been tested in a similar manner can be considered as low risk for physical security applications, in addition to demonstrating real-world customer deployments.

The Intransa Sharable Security Platform (ISSP) also offers NVR, analytics, and other physical security products the ability to leverage the power of an Intransa storage system, running the application directly integrated with the Intransa storage without application server hardware. This can dramatically reduce customer cost, since the need for server platforms is completely eliminated.

Intransa believes in standards for the good of the industry and our customers. As such we also are members and supporters of key industry associations, including the Security Industry Association (SIA), the Storage Networking Industry Association (SNIA) and its Green Storage Initiative, and the Green Grid for green IT. Intransa employees are also members and participants in important professional associations, including ASIS International and its Physical Security Council and the American Corrections Association (ACA).

Intransa Security-Grade IP Video Storage is available from Intransa StorPartner integrators and dealers worldwide. To learn more, contact Intransa or an Intransa StorPartner. Think outside the DVR!

Intransa, Inc.

Corporate Headquarters
2870 Zanker Road, Suite 200, San Jose, CA 95134-2114

866 446 7726 or 408 678 8600 / www.intransa.com / sales@intransa.com