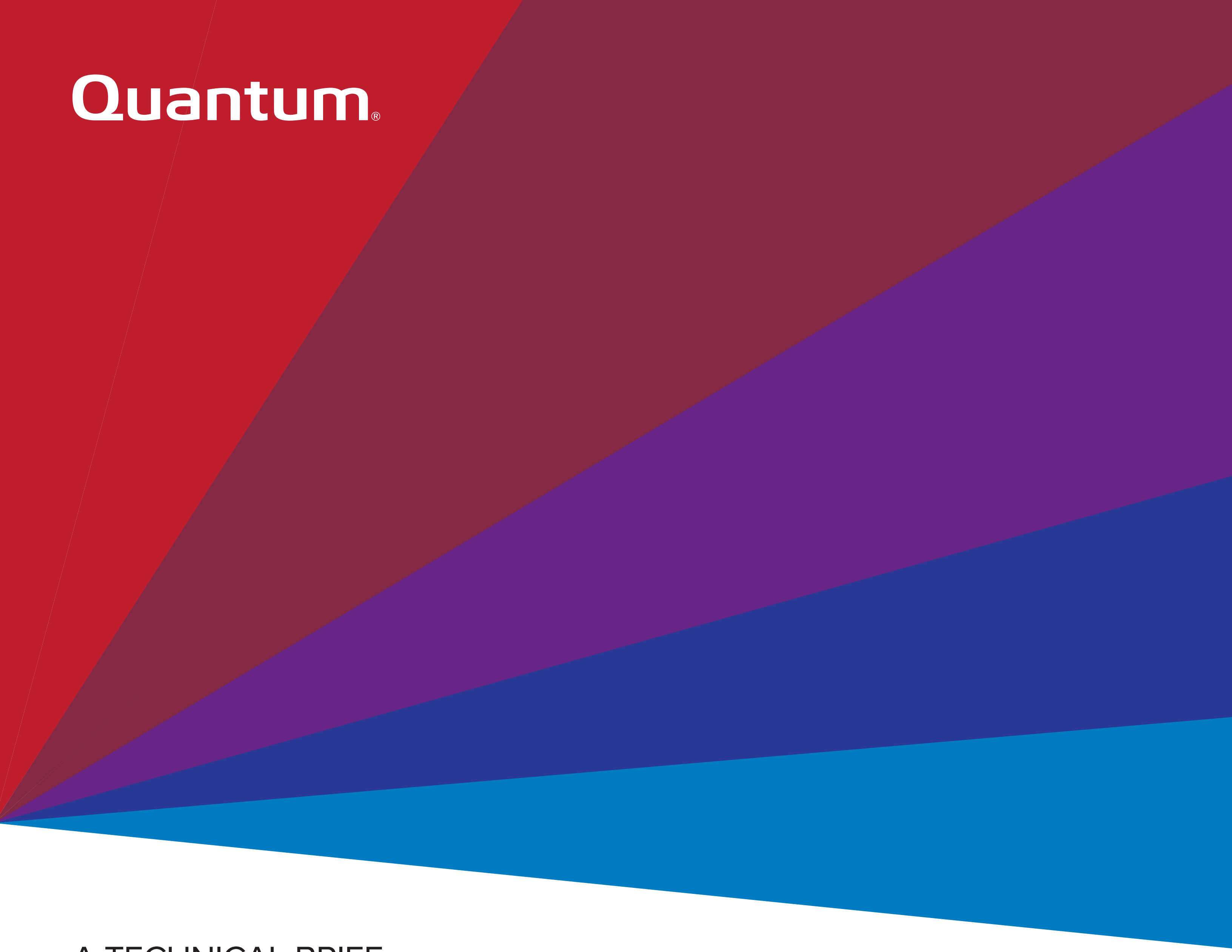

A TECHNICAL BRIEF

ENSURING UPTIME AND AVAILABILITY OF YOUR VIDEO DATA

Quantum's unified surveillance platform, a software-defined system specifically designed for ingesting, storing, and safeguarding video.

Introduction

Security professionals rely on surveillance footage to protect life and property. Municipalities use video to monitor traffic flow and document and report on incidents. Universities use it to help ensure student, faculty, and visitor safety. Retailers use it to analyze consumer behavior. Video cameras never blink, but if their output isn't captured, it's lost forever. Video storage systems must be capable of recording, replaying, and safeguarding camera output, no matter what.

Even in the newest and best system, there will be failures. Hard drives and network cards will die. Servers will crash. The real test of a video storage system is how it reacts under real-world conditions. When inevitable failures occur, can you still capture every frame? Can you still retrieve the footage you need? This tech brief highlights how the Quantum Unified Surveillance Platform ensures that your answer can be 'yes.'

Conventional Approaches Don't Fit

As camera counts increase, it's tempting to just add more NVRs, but this approach creates more problems than it solves. Capacity increases, but so does the number of devices to manage, each with their own under-utilized storage, compute, and networking resources. Single points of failure multiply. When an NVR goes down, it stops recording, and existing footage is temporarily inaccessible. High-availability configurations require purchasing twice the hardware, and half of it sits idle. This approach to running business applications has been obsolete for over a decade, and it's time to abandon it for video surveillance as well.

Borrowing technology from the corporate IT world may seem like a better way, but these systems weren't designed for surveillance. IT shared storage doesn't perform well with streaming video and the techniques used to protect data such as snapshots and backups aren't practical for video. Generic server virtualization platforms are complex. Both are expensive and require special expertise to operate. They can be made to work but aren't the best tools for the job.

It's time for a modern architecture that uses the best practices from corporate IT but deploys them in a way that's specifically designed for video surveillance. A resilient architecture that can withstand multiple failures while still ingesting, protecting, and serving video. One that can grow without an increase in management effort, and one that delivers great value.

The Unified Surveillance Platform

Introduction

Quantum's answer to this challenge is the Unified Surveillance Platform (USP), a software-defined system specifically designed for ingesting, safeguarding, and processing video.

The USP architecture consists of Quantum USP software running on multiple industry standard servers to make them operate as a single entity – a cluster. The compute, storage, and networking resources of all the servers are pooled together, increasing in scale as additional servers are added. Instead of running on dedicated physical servers, NVRs, VMSs, and even access control and analytics applications run on virtual servers that share the pooled resources. In the IT world this is known as a “hyperconverged” system. This approach is popular because it makes things easier - simplifying management, increasing uptime, and reducing costs. Quantum USP is unique in that it is a hyperconverged system specifically optimized for the unique characteristics of video workloads.

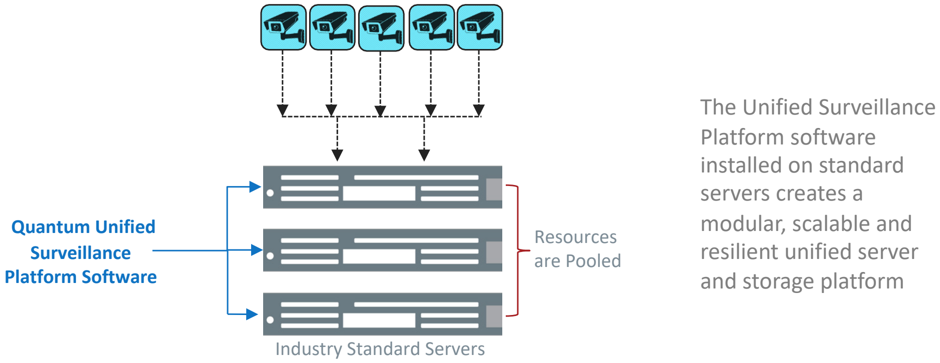
Quantum Unified
Surveillance
Platform Software
Resources
are Pooled
Industry Standard Servers
The Unified Surveillance Platform software installed on standard servers creates a modular, scalable and resilient unified server and storage platform

Figure 1 -Quantum USP Architecture

Ensuring Maximum Uptime and Availability

Several techniques are used by USP to maximize uptime and availability. In terms of hardware, all the servers in the cluster are equipped with redundant power supplies and network adapters, and a pair of network switches is used to provide redundant connectivity. But the real power of the system lies in the sharing of hardware resources through virtualization.

Built-in Application Failover

All modern servers support virtualization, which simply means that one physical server can run multiple copies of an operating system (Windows, for example) in isolated partitions that are unaware of each other. Each Operating System (OS) copy - known as a virtual machine or simply a ‘VM’ - believes it has dedicated compute, storage, and networking resources, but really, they are all sharing the resources of the physical server. Because VMs are not tied to specific hardware, they are portable and easily moved from one server to another, with any applications installed on them going along for the ride.

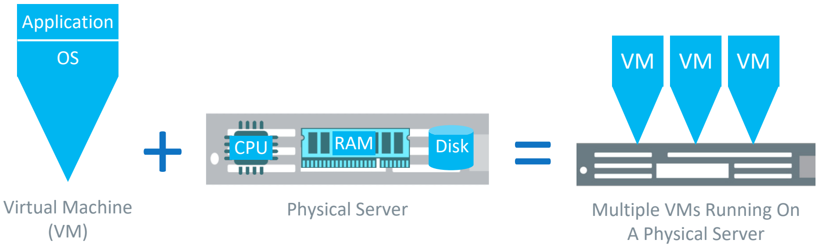

Figure 2- Server Virtualization

In USP, VMs are allocated across the physical servers in the cluster automatically, based on the resources available. If another server is needed – to run an additional recording server instance, for example - the administrator simply creates a new VM using the GUI and installs the application on it. USP takes care of all the details behind the scenes.

If a network card or switch fails, traffic to and from affected VMs is re-routed over alternate paths. If a physical server completely fails, all VMs that were running on it are immediately restarted on one of the remaining servers in the cluster. These recovery processes are automatic, requiring no security operator intervention.

Erasure Coding Video Data Protection and System-level Resilience

Traditional data storage and servers (NVRs) use RAID (redundant array of independent disks) to protect against data loss. Each array of disk drives in a RAID system can survive the failure of a few disks, typically two, without losing any data. The problem with RAID is recovering from failures. A busy system can easily take a week or more to recover from a single disk failure, and during that time performance is reduced. Additional disk failures reduce performance further and increase the probability of catastrophic data loss.

Characteristic	RAID	ERASURE CODING
Protection against multiple disk failures	LOW	HIGH
Protects against full server failure	NO	YES
Failure recovery time	DAYS	HOURS
Performance impact during recovery	HIGH	LOW
Storage Overhead	HIGH	LOW

Table 1 -RAID vs. Erasure Coding

In video capture and storage environments low performing storage can lead to dropped frames, and it goes without saying that data loss is unacceptable. To avoid the downsides of RAID, USP uses a different method for storing video known as erasure coding.

Erasure coding (EC) uses a more sophisticated and flexible algorithm than RAID. As a result, it can protect against more, and more severe failures while minimizing recovery time and performance impact. Remember that with USP the disks attached to each server are combined into a single logical pool of storage. The erasure coding algorithm spreads data and extra information – known as parity – across all the disks in this pool.

When an NVR suffers a catastrophic problem, such as a disk controller or motherboard failure, video recording stops and access to all the video stored on that NVR is lost. VMS failover configurations switch affected camera feeds to a backup NVR, but existing video on the failed NVR remains stranded. In contrast, because it writes video across all servers in the cluster with erasure coding, USP can overcome even complete server failures, preserving the ability to continue recording and access all stored video. This provides true system level resilience through all types of hardware failures.

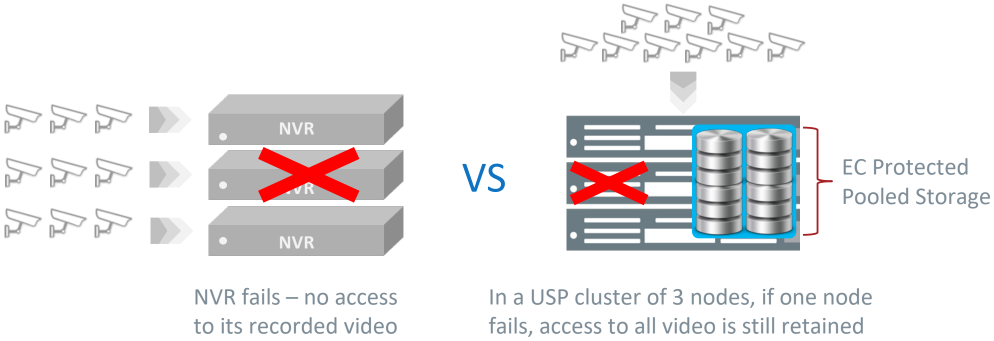
NVR
NVR
NVR
VS
EC Protected
Pooled Storage
NVR fails – no access
to its recorded video
In a USP cluster of 3 nodes, if one node
fails, access to all video is still retained

Figure 3- VMS vs. USP Recorded Video Availability

When disk or server failures occur, missing data is automatically reconstructed by the erasure coding algorithm from the data and parity information on the surviving disks. Because recovery activity is spread across many more disks than with RAID, it completes much more quickly with less impact on performance.

VM-related data like operating system and application files are also protected with erasure coding, enabling VMs to survive server and storage failures along with saved video.

Conclusion

To ensure maximum protection for valuable mission-critical video surveillance footage and preserve the ability to capture and access it even when hardware and software failures occur, a new approach is required. Simply stacking NVRs creates management headaches and doesn't provide the required availability. Force-fitting technology from the corporate IT world is problematic because it's not designed for video, it's too complex, and it costs too much.

Quantum's Unified Surveillance Platform successfully marries the special needs of video capture and playback with modern data center technology. USP's combination of virtualization technology with erasure coding produces a system that's resilient, flexible, secure, and cost effective.

To learn more about Quantum USP, visit www.quantum.com.

Quantum technology, software, and services provide the solutions that today's organizations need to make video and other unstructured data smarter – so their data works for them and not the other way around. With over 40 years of innovation, Quantum's end-to-end platform is uniquely equipped to orchestrate, protect, and enrich data across its lifecycle, providing enhanced intelligence and actionable insights. Leading organizations in cloud services, entertainment, government, research, education, transportation, and enterprise IT trust Quantum to bring their data to life, because data makes life better, safer, and smarter. Quantum is listed on Nasdaq (QMCO) and the Russell 2000® Index. For more information visit www.quantum.com.

www.quantum.com | 800-677-6268