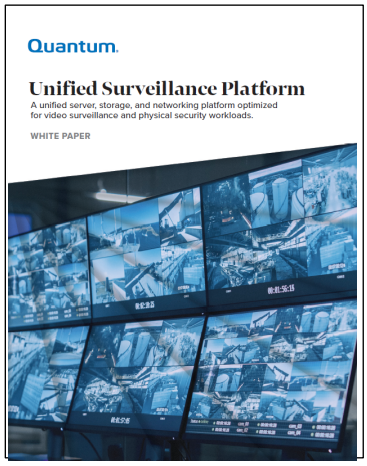
Quantum

carahsoft



Unified Surveillance Platform

A unified server, storage, and networking platform optimized for video surveillance and physical security workloads.

Thank you for downloading this Quantum whitepaper. Carahsoft is the public sector distributer for Quantum solutions available via the GSA Schedule 70, Quilt, and NJSBA contract vehicles.

To learn how to take the next step toward acquiring Quantum's solutions, please check out the following resources and information:

For additional resources:
carah.io/QuantumResources

For upcoming events:
carah.io/QuantumEvents

For additional Quantum solutions:
carah.io/QuantumSolutions

For additional Quantum Backup solutions:
carah.io/QuantumBackup

To set up a meeting:
Quantum@carahsoft.com
(571) 591-6220

To purchase, check out the contract vehicles available for procurement:
carah.io/QuantumContracts

For more information, contact Carahsoft or our reseller partners:
Quantum@carahsoft.com | (571) 591-6220

Quantum

Unified Surveillance Platform

A unified server, storage, and networking platform optimized for video surveillance and physical security workloads.

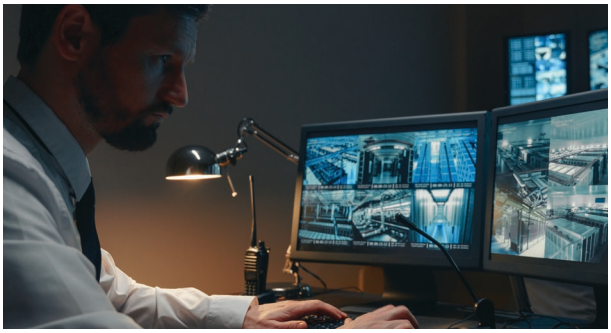
WHITE PAPER

Contents

Introduction

Security and video surveillance professionals face challenges created by upgrading cameras from analog to digital, higher camera resolutions, longer retention times, and video data being more mission-critical than ever driving the requirement for constant, reliable surveillance all day, every day.

Quantum introduced the Quantum Unified Surveillance Platform (USP) to help organizations address these challenges with an infrastructure to support video management systems (VMS) and other physical security applications, which provides the resilience, flexibility, security, performance, and economics needed to deliver on their physical security and business directives. The Unified Surveillance Platform brings together technologies proven in physical security and IT data centers and packages them in a unified server, storage, and networking platform optimized for video surveillance and physical security workloads.



This white paper describes the architecture and key features of the Quantum Unified Surveillance Platform software to help physical security and IT professionals understand how this solution might benefit their organization. Throughout this white paper the Quantum Unified Surveillance Platform will be referred to as the "Quantum USP" or "USP."

Video Surveillance Infrastructure Considerations

- *Effectively Capturing and Storing Your Video:* Can the infrastructure keep pace with the highest megapixel cameras, heaviest camera loads, and sophisticated VMS's and ensure video is captured with zero frame loss and image degradation? Is the storage or server solution truly optimized for the unique characteristics of video workloads?
- *Ensuring Video Will Always be There, Always Recording, Always Available for Playback or Analysis:* Can the system stay on-line even if disk drives fail, or an entire server fails? How resilient and highly available is the infrastructure?
- *Dealing with Change and Growth:* Will the infrastructure approach selected be flexible and easy to expand or change to accommodate adding compute, storage, or GPU resources to accommodate changes in camera technology, increasing camera counts, deploying additional security applications? Can the system be expanded or changed non-disruptively so that video recording and access can go on uninterrupted?
- *Longer Retention Times:* If you are asked to increase retention times for some reason, can you easily and cost-effectively add storage and migrate the video to a long-term retention tier?
- *Controlling Costs:* Instead of purchasing another server and/or storage system, can your infrastructure technology enable you to consolidate applications onto common infrastructure reducing server and storage acquisition, power, cooling, maintenance, update, and administration costs?

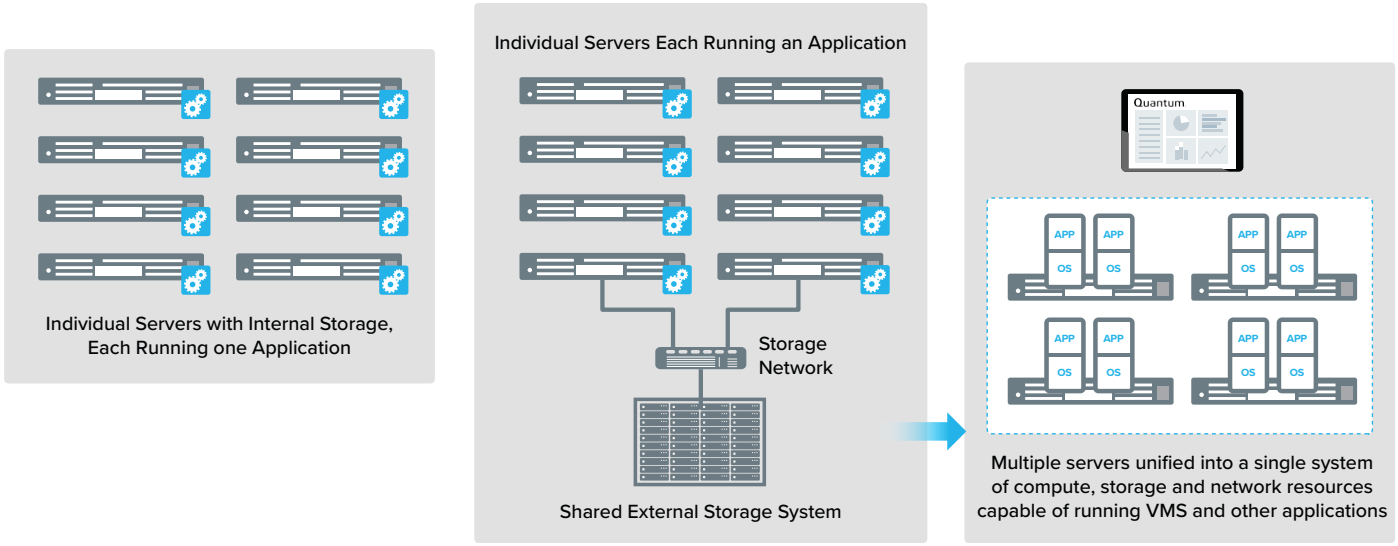
- *Protecting Your Video and Other Critical Data:* Does the infrastructure solution have built-in cyber and digital security capabilities to protect your video from unauthorized access? If accessed, is it in a format that it is useful?

What is the Quantum Unified Surveillance Platform (USP)?

Quantum Unified Surveillance Platform (USP) is a modern innovative approach to bring the best compute, storage, and networking infrastructure under a single umbrella for the physical security world. Each word in the naming for USP has been carefully selected and represents what Quantum set out to bring to systems integrators and customers.

Let's begin with the term **"Surveillance",** which represents the "S" in USP. While modern day IT has been rapidly evolving and the data center has seen new and better solutions every year, the same cannot be said for the video surveillance industry. This is because ideas like virtualization and software-defined everything, while offering benefits, such as higher application availability, reduction in physical hardware, and flexible scalability, have not been as widely accepted in the physical security arena due to unfamiliarity, being viewed as more complex, and requiring specialized skills. As such, to date only certain medium and large enterprises have had the commitment to implement these in their physical security environment. Quantum USP is changing that with orchestration software that automates and simplifies complex operations, so that security professionals can now enjoy the very same benefits that their IT counterparts get in the data center via a simple, consumer application-like dashboard. The technologies implemented (as discussed in later sections) are focused on the needs of video surveillance, so not to clutter the user with unnecessary features.

Next, the **"Unified"** in USP is used to refer to how the entire infrastructure backbone for running video surveillance is now under a single umbrella solution. The figure below illustrates what USP helps achieve.



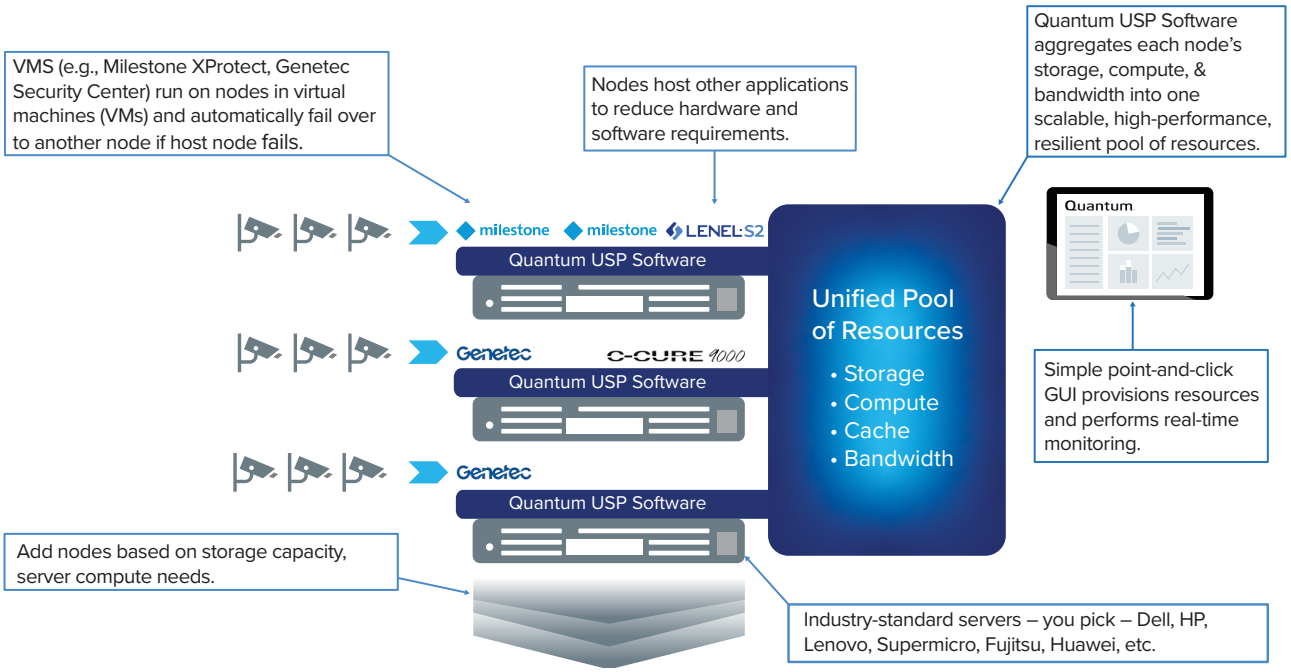
The Unified Surveillance Platform enables you to reduce the number of physical servers required in your physical security environment.

There are three main infrastructure components necessary in any design: Server, Storage & Network. And to complement these from an operational point of view are two necessities – redundancy and management. After all, the one simple requirement of video surveillance is that the recorder needs to keep on running and video needs to always be accessible.

As you move from left to right in the figure above, you can see how technology has evolved. You started off with having individual servers running a single application with no built-in redundancy and failover. This led to requiring an excess number of servers and individual management for each server. We then moved to a slightly better form where you still had the same number of servers, but now there was a single shared storage platform, like a SAN or NAS. This was an upgrade from the individual server systems, but still required separate storage management as well as numbers of servers to deploy and manage.

The final technology of hyperconverged infrastructure (HCI) is what is accepted as a minimum level of efficiency in today's IT infrastructure world. It is a software defined approach, which uses a combination of regular servers to create the entire infrastructure backbone. You have a fewer number of total servers and no separate storage system. The individual disks in each server are pooled to create a single software-defined storage pool which can then be allocated to each application per their needs. The best thing about it is that failover is automatic, redundancy, and system-level resilience is at a much higher level and of course, the entire infrastructure can be managed from a single dashboard with pro-active health monitoring and alerts.

While virtualization is at the core of delivering this design, Quantum USP ensures that this layer is invisible to the security professional and does not require any specialized skills, active intervention, or maintenance from them. With HCI, software defined networking can also be used by the surveillance industry to better ensure that network bottlenecks and loopholes are a thing of the past.



The last letter in USP represents **"Platform"** as that is what the solution delivers. No matter what your physical security application needs are, everything can run on a USP-based infrastructure. Whether it is the VMS management server or multiple recording servers or security applications like facial recognition, access management, license plate recognition or other analytics, everything can co-exist harmoniously within the Quantum USP group of servers.

For multiple sets of applications to co-exist in the same environment, it is important that resources can be carved out from a pool that meet the requirements of each application. While one of them may be compute intensive, the other may be throughput intensive, and another may be IOPs hungry. While databases prefer to run on flash drives, recorders dump their endless recording streams on a much more affordable storage media, hard disk drives (HDDs). Quantum USP can run a mix and match environment where different tiers of storage and different classes of compute can be created from one pool of software defined resources. Each type of application can then be mapped to its necessary quality of service parameters (e.g., the type of storage required, the compute criticality compared to others etc.). This mapping happens behind the scenes and all the security professional needs to do is denote the type of application that he wishes to launch within the platform. The USP software takes care of the rest.

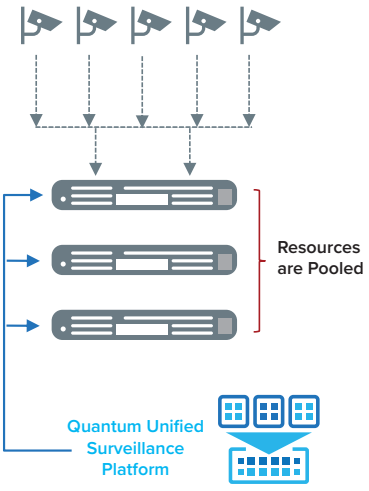
So, in essence, Quantum USP is the most complete platform that a surveillance user will ever need as an infrastructure backbone. You can host any application you want with an assurance that the software is intelligent enough to ensure that both high performance and resilience is taken care of behind the scenes.

The Four Architectural Pillars Of USP Driving Benefits For Video Surveillance

To keep USP focused on the video surveillance world, the engineering and product teams at Quantum focused their development efforts into 4 key areas:

Resilience
- Always have access to video
- Withstand server and multiple disk failures
- Automatic application failover

Flexibility
- No hardware lock-in
- Use your server of choice, new or existing
- Start small, scale granularly, no dependence on existing servers



Video Integrity
- Optimized for write-intensive video workloads
- Video captured without frame loss
- Combines different disk types to create the optimum tiers of storage for video

Security
- Data center best practices applied to video surveillance environment
- Control access based on personnel roles
- Multiple levels of cyber-attack protection

A modular, scalable unified storage and server platform.

While a detailed analysis and walkthrough of the prime features is carried out in the next section, here we will focus on how they are related to physical security environments.

Flexibility and Convenience – For video surveillance environments, the fundamental need is to capture a constant stream of video on the field of observation. For this the number, quality, and positioning of cameras are critical. Everything else from VMS to servers to storage to network is just to help with this end objective. As such, it is important to not be locked into a particular vendor in any of these areas and give yourself full flexibility in making the best infrastructure choice now and be able to accommodate future growth and change.

This is what USP delivers. Complete flexibility in terms of the infrastructure needed to record and keep video. It starts off by enabling an unrestricted choice of hardware. The system integrator or end-user can purchase new server hardware or use existing server hardware. These can be any regular physical servers, which meet the minimum specifications to run the USP software. There are no restrictions in make, model, or configuration. In fact, each server that goes into a physical cluster can be from a different vendor and configuration than the one beside it. For storing the video, no specialized external storage boxes are required. The hard disks that go into these regular physical servers are combined to form a highly available clustered storage pool.

Once the cluster is up, any applications can be installed on it. As mentioned in the previous section, this can be the VMS as well as any other applications. The entire platform is managed through a single pane of glass which is a web-based dashboard that resembles modern day web applications.

The flexibility doesn't just stop there. If at a later point in time, new resources must be added, they can be done so without any restrictions. New additions can be in the form of only compute resources or adding more storage via disks/nodes or can be a mixture of both compute and storage. And all of these can be added non-disruptively with no downtime for ongoing operations.

Resilience – There should be no disruptions to recording, period. The cameras never stop sending in the frames and it is essential that the infrastructure is always available to record this never-ending stream of video data. So, it's a good thing that the USP has always been designed with this in mind.

This resilience is delivered via three key properties:

- Ensuring that individual physical servers can withstand multiple failures and video recording is not disrupted and video integrity is not compromised.
- Ensuring that a complete server in a cluster can fail and recorded video is still accessible.
- Ensuring that once a server fails, the VMS or other applications are automatically moved to another available server and recording quickly resumes.

Quantum Erasure Coding (EC) in USP ensures these highest levels of resiliency and enables a design that protects against failure at all levels and ensures that once a failure occurs, there is an automated mechanism to restore applications to their operating state.

Characteristic	RAID	Erasure Coding
Protection against multiple disk failures	LOW	HIGH
Protects against full service failure	NO	YES
Failure recovery time	DAYS	HOURS
Performance impact during recovery	HIGH	LOW
Storage overhead	HIGH	LOW

Table 1 - The Unified Surveillance Platform's erasure coding technology is more effective than RAID in protecting video data.

What is also important is that if a disk fails, adequate measures are in place to rebuild the data and spread it to newer locations. This prompt action helps restore the level of resiliency in the system even after a failure. Such pro-active actions continuously happen in the background and do not need any intervention from the customer's team.

One another key area of upkeep is to be able to ensure that critical events and warnings are brought to the right notice without delay. The robust call home notification and alerting system does just that. This reduces the need to constantly monitor the platform as event-driven alerts are sent across to both the local administrator's device as well as to the Quantum support team if enabled, leading to prompt resolutions.

Video Integrity – Frame drops are every surveillance solution designer's and operator's nightmare. Not being able to deliver adequate performance that keeps up with the incoming video streams is often the weak point in a surveillance setup. This is where USP excels.

There are two contradictory requirements in this video recording – the system storage should be fast enough to be able to keep up with the incoming speed of frames, but at the same time the primary storage layer should be affordable enough to store hundreds of terabytes to petabytes of data. USP delivers just this with its **write online – distribute offline algorithm.**

A finely tuned cached layer built on a fast flash tier optimized for video writing is presented for all initial writes so that no frames are dropped when they arrive. And then, the video is written on a storage backend, which is built on an erasure coded pool of affordable hard disks. The key here is to be able to maximize performance from the flash tier so that it can operate with a minimum size. A value that has been perfected with tens of thousands of hours of testing in Quantum labs.

Additional optimizations, no less important, are also carried out in the BIOS layer, the operating system image as well as the VMS application. All contributing to maximize the performance from any selection of server hardware.

Advanced Security – Cyber protection is the need of the hour and surveillance systems cannot operate in a vacuum. While anti-virus and operating system patches are a means of isolating malware once they have attacked the system, security and protection should begin at an earlier stage than that. Things are also compounded often with unauthorized access as surveillance data is sensitive and prone to misguided access.

The USP platform takes the best of IT data center security practices and brings them to the surveillance infrastructure. This defense is built on a four-layer approach – **perimeter protection, access control, attack segregation and core encryption.**

> "Cybersecurity due diligence and best practices, which are more ingrained IT professional workflows from working with other IT solutions, are increasingly part of video surveillance."
>
> Novaira Insights, Worldwide Market for Video Surveillance Hardware and Software 2021 Edition

Detailed Description Of Unified Surveillance Platform Features

This section is a detailed technical description of the features covered as an overview in the previous section. The features are categorized under the same categories as above.

FLEXIBILITY & CONVENIENCE

Host Multiple Applications Within the Same Server

USP gives users the flexibility of hosting multiple applications within the same server or cluster. This is delivered by an integrated virtualization layer that enables hosting multiple virtual machines within the same physical node. USP uses a KVM-based hypervisor that is natively integrated within the USP software platform.

The user does not need to interact with the hypervisor due to the invisible virtualization that USP delivers. They can simply specify their hosting requirements per application and USP takes care of both the provisioning and balancing of resources in the backend. Each VM has its own operation system (e.g., MS Windows or Linux) as required by the application and its range of virtual resources that are exactly as would have been provisioned in a physical single server.

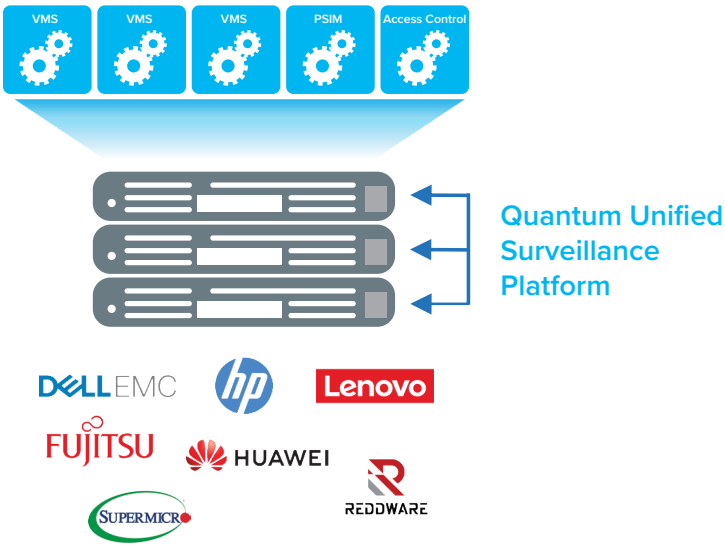
A single physical server can host multiple virtual machines (no hard restrictions on the number) and each virtual machine can have a different or same OS as well as configuration. This enables a mix and match of applications as necessary – multiple VMS recorders/archivers as well as security applications like access control, LPR, etc.

The biggest single benefit of this architecture is the reduction in the number of servers to purchase and maintain as well as a drastic reduction in the overall hardware requirements.

Use New or Existing Industry Standard Servers

USP does not merely provide the flexibility of hosting multiple apps in the same group of physical servers, but also enables that to be done on the preferred choice of server. There is no restriction on the make, model and configuration of the physical server that goes into a cluster if it has the necessary physical resources to run the applications within the virtual machines.

What this practically means for the system integrator and end-user is that they can continue to use their existing servers and deploy USP on top of them. Or purchase few or all new servers for creating the cluster. A single cluster can be built out of different servers from different vendors like Dell, Lenovo, HP, Supermicro etc. If they are x86, they are fit for this purpose. And of course, they also need to have the actual physical resources necessary for running the desired applications and the storage necessary for storing the video data.



The Unified Surveillance Platform supports any industry-standard server.

Please refer the system requirements section for the precise minimum server configurations.

Choice of a Compute-Only, Storage-Only or a Mixed Node – Add Just What is Needed

The objective behind the development of USP is to provide both a hardware agnostic approach, as well as an efficient approach that eliminates unnecessary costs and enables granular scaling of compute and storage resources.

You can design a USP system cluster with different types of physical servers that meet the precise requirements. For example, the physical servers that act as individual nodes can be compute only (hosts only applications, but not the video data), storage only (hosts only video data) or a mixed node (hosts both applications as well as video data).

When the initial system cluster is designed, the nodes likely will be mixed nodes, as this provides the right balance of resources to effectively run the applications and provide the associated storage. Where this flexibility is most useful is when the system needs to grow because of:

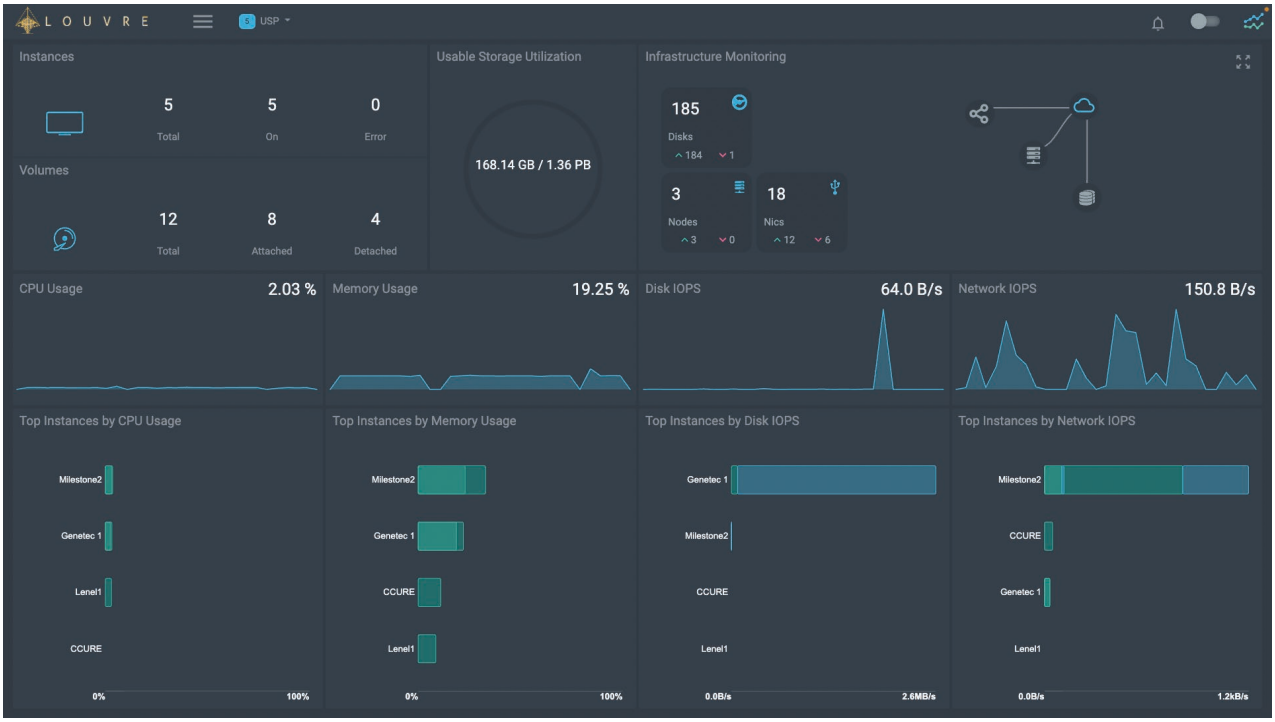
- Retention times change leading to a need for just storage space, delivered by a storage-only node.
- New cameras are added needing both compute and storage, delivered by a mixed node.
- New applications need to be run, delivered by a compute-only node.

In essence, the focus is on growing exactly as per the need and keeping it flexible so that this growth is on demand.

Single-Pane Management of the Entire Infrastructure

USP introduces a new, more flexible, efficient software defined world. However, the experience of managing this needs no new skillsets because of the single, intuitive-management dashboard that enables control and visibility of all resources in the system cluster – physical as well as virtual.

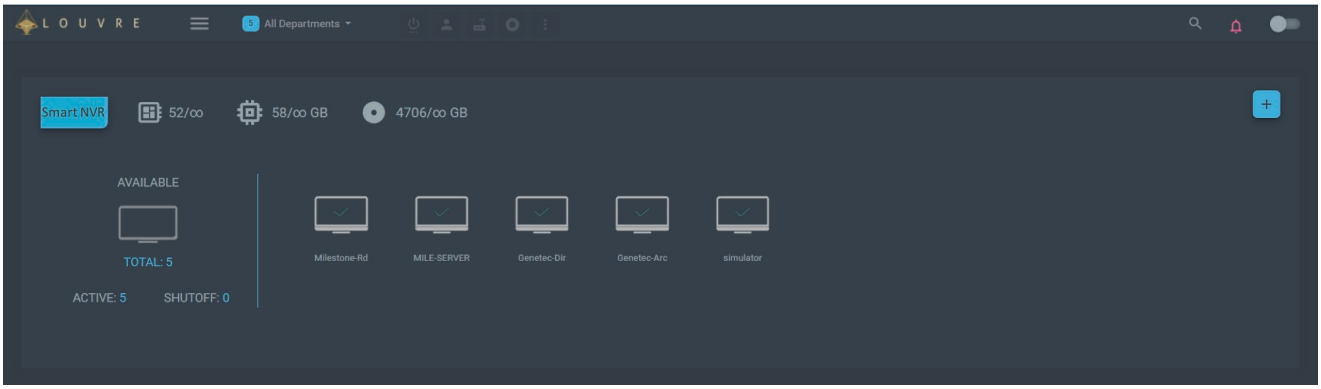
The entire system is available through a browser-based dashboard. No local installation is required, and a simple https URL entered into a browser of the user's choice opens the management platform.



Example of Unified Surveillance Platform management dashboard

The dashboard, as seen above, opens with a live view of the entire cluster. It shows the total resources and consumed resources as well as critical infrastructure with live rankings. This view enables the user to be well informed about the state of the system cluster at any point in time.

The actual virtual machine and associated application management is delivered through a set of simple icons and a point and click approach. The idea is to mimic the familiarity of a modern consumer grade web application where everything is like a widget and button and can be easily navigated for actions.



Multiple VMS applications running in virtual machines (VMs)

The dashboard provides basic capabilities, like single click, create, and modify for actions on storage and networking, as well as more detailed menus in case this infrastructure is managed by a dedicated IT team, who appreciates more detailed controls. The basic functions are designed for running day-to-day operations for any security professional.

Automated, Customizable Phone Home

The objective of a video surveillance deployment is: install it and let it run—where the focus is not on active day-to-day management, but only taking actions when needed. As such, USP delivers a range of alerts and information to the user/operator that can be provided via a variety of communication mechanisms commonly referred to as "call or phone home."

There are three key areas for these alerts:

1. **Physical infrastructure –** These pertain to any kind of system failures. For example, if a disk or node fails, the alert can be sent to the right individual for prompt action.

2. **Application servers –** These are alerts based on the state of the virtual machines and the applications running within them.

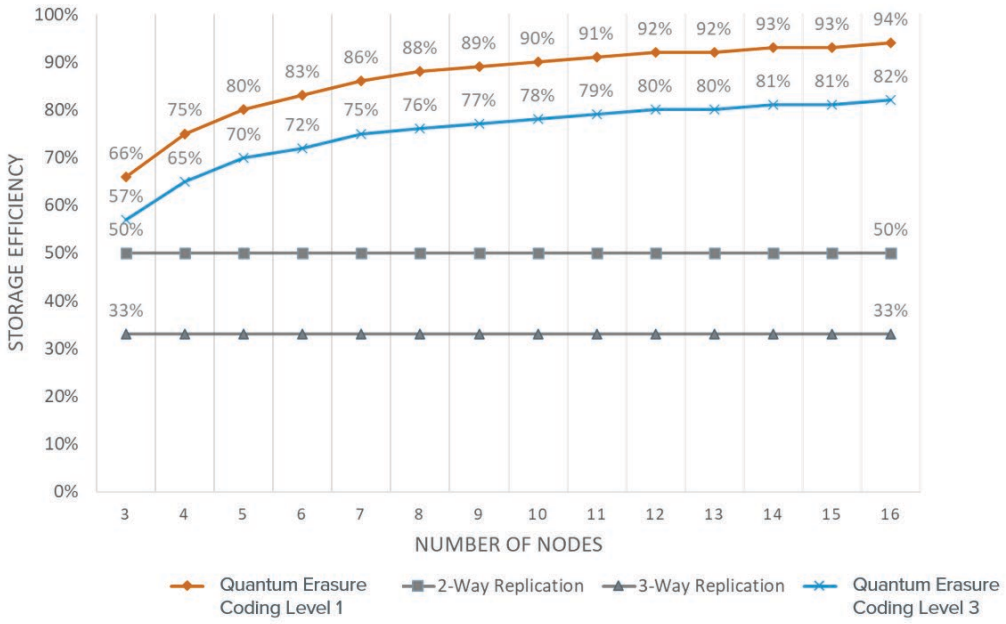
3. **Resource shortage –** A periodic update on the system resources can be monitored and sent as a report to the person in charge. A more critical use of this mechanism is to send proactive alerts when there is a shortage of resources in the cluster whether it is CPU, RAM, or disk space.

These alerts can be triggered via email as well as any messaging system. There are APIs available for mapping these into specific monitoring systems if desired. Or simply use the built-in USP alerting capabilities and input the desired email addresses or phone numbers for sending these alerts.

RESILIENCE – ALWAYS ON AND AVAILABLE

Configurable Erasure Coding for Highest Levels of System Resilience

The most resilient systems are built using erasure coding (EC), a more efficient and resilient way of storing data across a group of physical servers and disk drives than traditional RAID. USP takes the concept of erasure coding and improves on it by optimizing it for video workloads and enabling a configurable fault tolerance aspect. This configurable setting enables the user to map their precise resiliency requirements into the cluster. Each incoming data block is divided into multiple data chunks and each chunk is stored on a different disk of a different node. The algorithm at the back end decides on this data placement depending on the specific erasure coding profile.



The Unified Surveillance Platform delivers the highest levels of storage utilization and efficiency.

In simple terms, what this means for the system integrator or user is a choice of how many disks, as well as a node, can fail at the same time without loss of recording or access to video. Configurable erasure coding not only allows for a design where multiple disks can fail at the same time, but also allows for these failed disks to be present across multiple nodes at the same time without disruption to running cameras, as well as protection against loss of data.

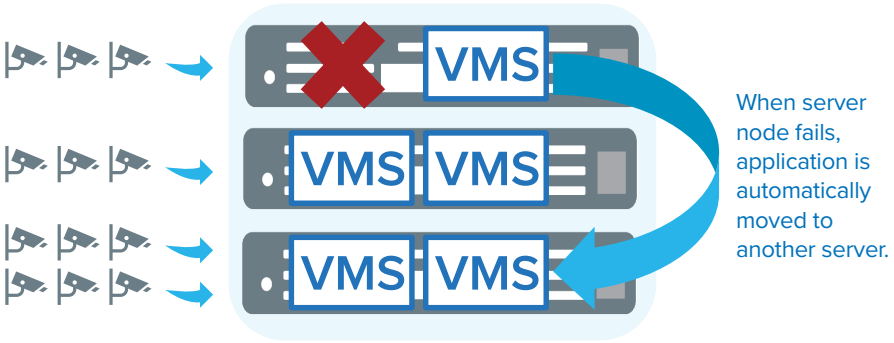
This provides the highest amount of resiliency seen across any video surveillance system. A point to be noted here is that this resiliency is not just from a physical storage perspective (like other external storage designs), but also extends to the physical servers running the applications.

Usable storage in the cluster will keep on growing with the number of nodes within the cluster and can grow to beyond 90% of usable space in the higher node configurations.

High Availability With Auto Failover

Failure protection is not merely needed for storage, but for the applications running on the system as well. This is where USP's invisible virtualization platform delivers additional capabilities.

Each VMS (or any other) application runs within a virtual machine that runs on a single server, but the information and configuration of this application server is available throughout the cluster. So, in the scenario of the physical server failing and becoming unavailable, the USP software automatically recognizes this failure and triggers a failover process for the application server.



The virtual machine automatically looks for an available space in the remaining servers and initiates a process to bring up the virtual machine on the new physical host. There is minimal time required for the application to come up on the new server. There is no active intervention required from the user for this failover. This happens automatically and is delivered by the high availability module within the USP platform.

Non-Disruptive Scaling

Any kind of expansion that needs to be enabled within the physical servers, as well as replacement of components within them can also take place without any downtime and disruptions.

Node additions to the system cluster can be granular in nature per the specific compute or storage required. When a new node (server) must be added, it is loaded with the USP software and joined to the existing cluster. The running cluster does not need to be stopped or paused in any manner. Once the node addition is complete, the new resources are automatically added to the overall pool of cluster resources. The user can then proceed to add more applications to the existing virtual machines or create new virtual machines to host more applications and associated data.

Scale just the resources needed and non-disruptively by simply adding more nodes.

The USP software also enables individual physical server level changes without downtime for the running applications. The live migration feature within USP allows for the virtual machine running within the specific physical server to be moved from that host to a different running server without any downtime. This frees up the physical server and any modifications in terms of part replacement or addition as necessary can be performed.

The overall focus is on being able to continuously adapt to present and future requirements without needing to stop video recording and access to recorded video.

PERFORMANCE FOR VIDEO INTEGRITY

Distributed Storage Pools Combined With Intelligent Caching & Tiering

The most critical performance parameter in a surveillance environment is the ability to cope with the constant stream of video data that is being written 24 hours a day, 7 days a week, 365 days a year. The cameras never stop and so shouldn't the recording.

As such, it is the disks that make up the backbone of the surveillance platform. USP gets the most effective utilization out of all the storage disk technologies. The same system cluster and even the same server can support all kinds of disk media – starting from top-of-the -line NVMe SSDs to SSD flash drives to SAS as well as SATA hard disk drives. All these disks in both small form factors, as well as large form factors, can co-exist within the same physical server and system cluster.

USP identifies and assimilates all the disk capacity that is distributed across the entire cluster. It categorizes the different types of disks into their individual pools. For example, the user can have a SAS SSD or NVMe SSD only pool for their top-of-the-line storage requirements, whereas an HDD based pool for their video data retention tiers. To make things more performant, the slower HDD media pool is front ended with a much faster and appropriately sized flash tier that enables the right combination of performance and cost. This is discussed in more detail in the next section.

As a user and consumer of this storage pool, all one needs to do is specify the space required for their applications and data. Simply specify the size and type of storage (high, medium, low performance) desired for the C: or D: drive is enough as an input. The USP software at the backend automatically creates these storage volumes and assigns them as drives for the virtual machine and its application. Another key point to note is that even though the disks are distributed across the whole cluster, they are available as a single storage pool. So, the total aggregated storage capacity can be given to just one application or distributed across multiple applications as per the user requires.

Write Online, Distribute Offline Algorithm for Best Performance

It is important to ensure performance for ingesting video data without causing a lag or latency in writing the frames to disk. Any sort of delay in this writing process first causes the memory buffer to become full and subsequently drops frames till the congestion is reduced.

The USP software has its own optimized algorithm to tackle this and make it into a non-issue. Video data is non-stop in terms of generation and thus must be written to a storage media that can keep up with. And the best fit for that purpose is a flash tier of either SAS SSDs or NVMe SSDs.

USP first takes these frames and writes them initially on a super-fast flash tier. This is done "online," meaning at the same speed as the incoming data stream; thereby, ensuring that no frames are dropped, and the speed of writing can match up with the speed of incoming data.

The second part of the writing operation is done "offline," meaning it is done as a background activity and does not interfere with the primary write operations. To write to the erasure coded HDD pool, the data blocks first must be broken up into different chunks and newer chunks generated and each chunk stored in a distributed manner which can allow for maximum failure resiliency. As this is a multi-stage operation, it is carried out in the backend without a need to keep pace with the primary online writes.

Knowing how to size, build and optimize these operations is one of the unique, differentiating capabilities of the USP and helps deliver optimum performance with an affordable design.

The Unified Surveillance Platform software has multiple techniques for making the most effective use of storage media types, ingesting video with no frame loss or image degradation and ensuring VMS applications have the resources they need for optimal performance.

Quality-of-Service (QoS) for VMS Optimization

VMS applications are the backbone of a video surveillance infrastructure, so it is critical they get the performance needed. One of the reasons HCI solutions designed for data center applications have not been the best fit for hosting VMS applications alongside other applications is because the real-time operational priority for a VMS recorder may be much higher than some of the other applications that run within the cluster. On some occasions, the reverse may be true with some other critical application needing higher priority to resources such as compute or storage.

Traditional HCI is at a loss in hosting such diverse requirements within the same cluster. This is where the Quality-of-Service (QoS) controls of USP come in very handy. Each application that is hosted within the same system cluster or server's virtual machines come with a set of tunable selections, which allows for easy prioritization by the user. Each application can be prioritized on several parameters of resource contention. These relate to CPU, disk, and network throughput.

By default, if a user has no need to differentiate between their different applications, they don't need to take any active step and can let the platform run its default settings. If there is a more critical application that is more compute intensive, they can just select the priority of the virtual machine that hosts the application as 2x or 4x higher than normal. This is a simple checkbox in the management dashboard, but what it will now empower the software to do is assign more compute priority to this application whenever there is a resource contention.

Similarly, less critical applications can be kept contained by keeping a threshold level for their disk or network activity. Mentioning limits to which they can write or read into the disk or send/receive traffic on the network enables for efficient distribution of resources between all the application workloads.

It is empowering to know that as a user you have the option of prioritizing resources to select applications whenever the need arises.

Monitoring Tools for Optimizing Performance

At the end of the day, the efforts to deliver performance are at one end of the spectrum, while the efforts to maintain them are at the other end. Hence, it's important that the server and storage platform running your physical security applications are not only configured with the best possible default settings, but also provide tools and visibility to track and adjust those settings for optimum performance.

USP comes with a host of monitoring tools – which are sometimes described as "360-degree monitoring" since they provide visibility into the system from every angle ranging from:

- The overall physical infrastructure consisting of a cluster of multiple servers (nodes)
- The individual servers (nodes)
- Cluster level resource monitoring
- Individual virtual machine utilization tracking
- In-virtual machine process monitoring

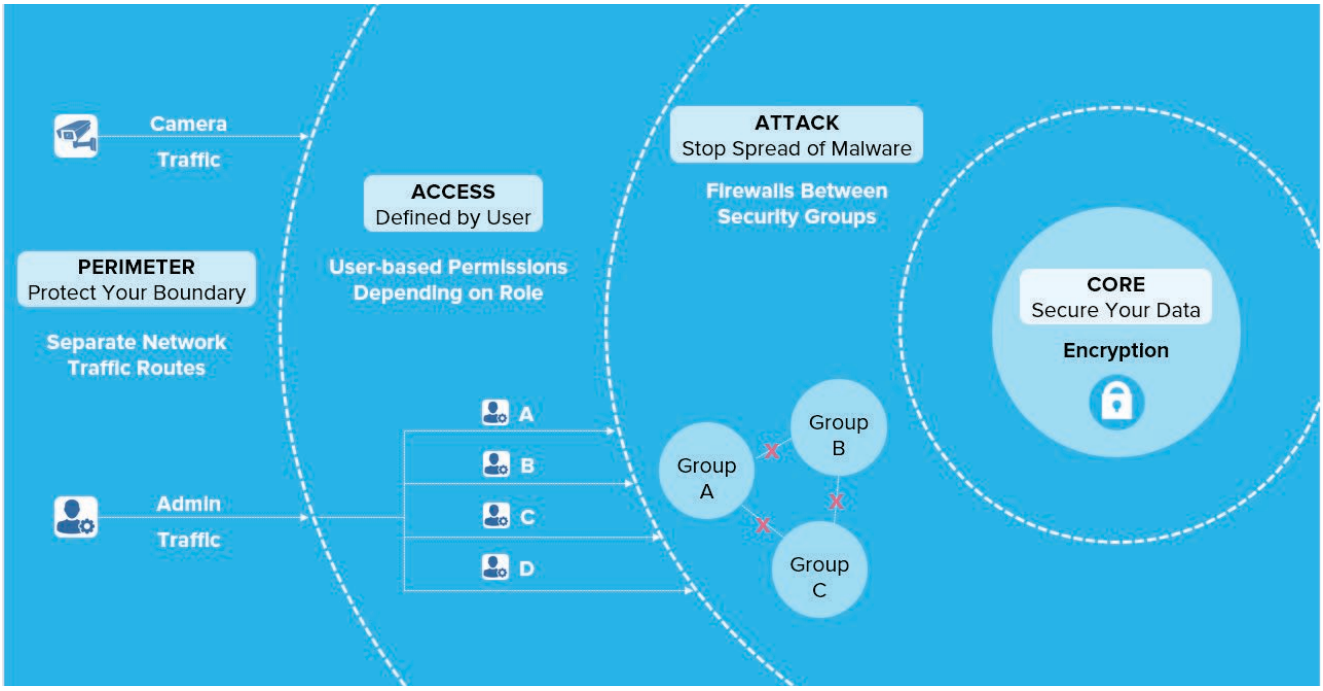
All these metrics are tracked and reported both live and historically. As a special feature, there is a real time ranking of the application servers on different resource parameters, which allows an administrator to see and track servers which are about to run out of resources. So, problems can be pre-empted and solved pro-actively even before they occur.

The user has tools that give complete visibility into the system including real-time ranking of the applications usage of specific resources, so there is never a surprise in running out of resources.

At an overall level, this information is particularly useful for right sizing the total infrastructure, as well as the individual application servers. The charts and graphs provide a very visual and easy to understand view of where resources have been over-provisioned and where there is a resource shortage; thereby, providing the ability to size all applications with practical feedback from the actual running environment rather than just theoretical assumptions.

ADVANCED SECURITY

USP brings the best of data center security practices to the video surveillance and physical security environment with a very focused set of features. A four-layer defense mechanism enables the right set of controls and protections from unauthorized and malicious access. The diagram below shows these visually and the points below delve deeper into each of these defense designs.



The Unified Surveillance Platform has four layers of digital security capabilities built in.

Perimeter Protection

The first level of protection should always be at the perimeter – in this case, the network architecture. There are two primary network segregations that should be followed at a minimum in a VMS based recording platform. The first is where the management and configuration of all the physical servers as well as the applications take place. This network is the one which holds the higher set of permissions as key administrator roles are necessary for the overall configuration of the whole setup. For easier understanding, this can be classified as the Management Traffic.

The second minimum segregation is for the cameras sending the video data to the individual VMS recording servers that they are connected to. A range of IPs are needed for this communication in a modern IP based camera system. Here, the cameras can be quite distributed in multiple locations and may need to send data from both supervised as well as unsupervised locations. This can be classified as the Camera Traffic.

In terms of support, USP supports both a flat and VLAN architecture where the management traffic and the camera traffic can be in a VLAN or no VLAN mode. However, as a best practice, it is recommended to use the USP's VLAN mapping feature to separate out these two types of traffic into two separate and independent VLANs. The configuration from the USP software is quite simple and merely a selection from a drop down, but the peace of mind that comes from knowing that one network cannot be the hack into getting entry into the other can be truly enormous.

Access Protection

The second critical security feature that comes with USP is the ability to keep a select set of recording servers and in turn a select set of cameras separated from one another.

Suppose there are cameras which have monitoring more sensitive areas than others and in an ideal world, the administration of the recording servers to which these cameras are connected need to be separated from the rest of the group. USP supports this level of segregation via a grouping mechanism that allows for separation of administrators.

As seen in the diagram, different groups can be created, for example A, B & C. Group A has recording servers that have highest criticality, followed by group B and then finally group C. Now, each group can have their own administrators. For example, if an administrator in the organization has the highest level of access, they can add a group admins for all the groups. While someone with lower clearance can only be assigned permissions for accessing Group C recording servers.

While this should not be confused with the live camera feed monitoring that a VMS provides, it is still a highly useful and good security posture. It is the access and configuration for the cameras via the recording servers that is at the end of the day the control to store and keep video data in the different storage media.

Attack Segregation

This feature builds on the grouping mechanism mentioned in the previous features. Different recording servers have network paths that need to communicate to the cameras in different locations. As such, these can be gateways to malicious access into the overall network and the proliferation of dangerous malware.

While connection to end camera sites cannot be forgone, what can be implemented is the right kind of grouping that keeps the more critical and sensitive data that comes in within a defined group of recording servers segregated. The previous section dealt with how access from an administration perspective is confined to people with higher clearances, but here it is important to strengthen those boundaries between the groups so that a compromised group, very often one with less critical video data, does not spread the malware into the other groups.

Once again, this can be done at the network layer. USP provides the functionality of network micro-segmentation, which does not need intervention from the physical switching layer but rather achieves that from a software defined networking perspective. What this micro-segmentation does is to create each group as an independent network silo. Permissions can then be set as to whether the groups can communicate between themselves or not.

This creates a software-defined boundary between the groups and ensures that even if one group is compromised, the other can stay intact provided it has been segmented appropriately.

Core Encryption

Data encryption has become quite prevalent in the IT world, but not in the video surveillance world. This is because of two primary reasons:

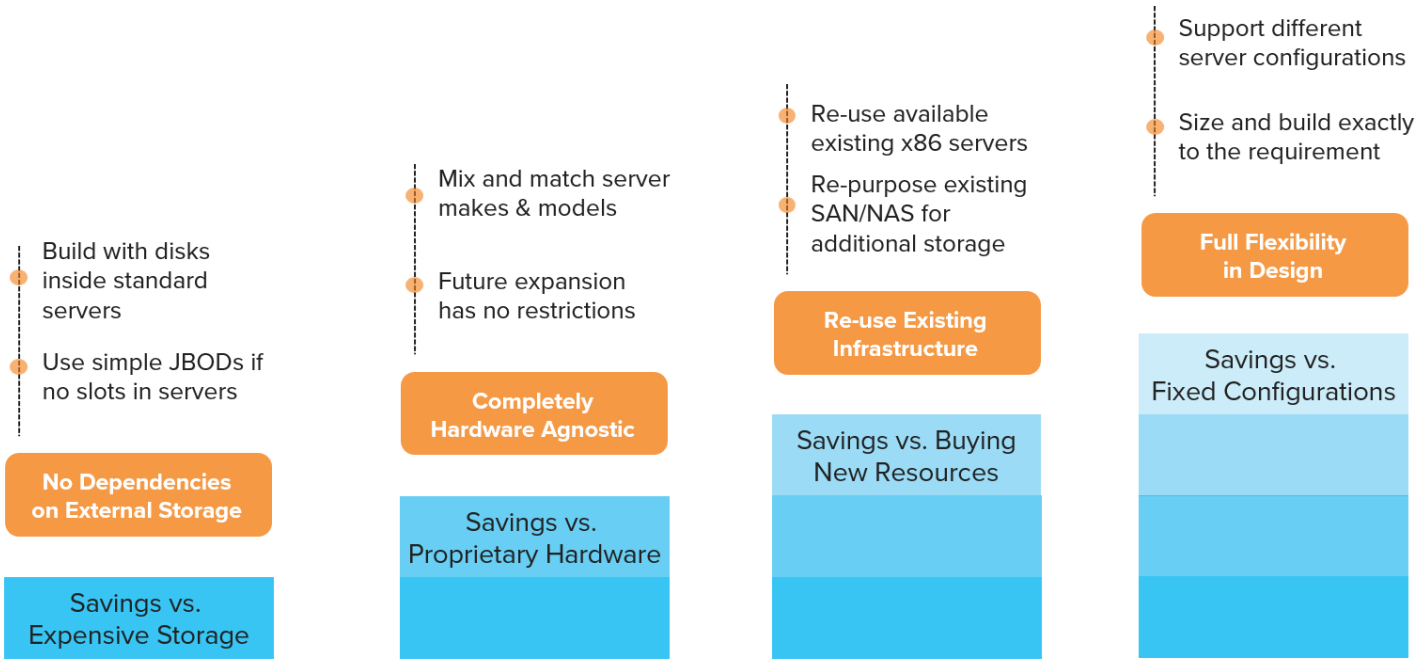
- The need for expensive self-encrypting drives or very expensive software
- The performance reduction in adding a step of encryption to recording

The USP software removes at least one of these roadblocks. The user no longer needs to purchase self-encrypting drives or expensive software for this purpose. USP comes with its own volume encryption module that ensures that each drive of the application servers is secured with 256-bit encryption and the keys are also securely managed.

From a performance perspective, this additional step of encryption reduces the overall throughput of the storage media. As such, it is important to use this enhanced level of security for the more sensitive kind of video data and compensate the reduction in performance by an increase in the overall sizing of storage and other resources.

Economics

USP delivers the highest value for any investment in a server and storage infrastructure solution for video surveillance. It is a modern simplistic architecture designed to deliver the best performance at a lower cost. This is practically possible because the financial benefits of adopting USP come from multiple sources.



NO DEPENDENCIES ON EXPENSIVE EXTERNAL STORAGE

The first key differentiator is the ability to eliminate the need for expensive external storage requirements, like a SAN or NAS. All that needs to be done is to populate the compute servers, which are required for the VMS and other applications with the right number and size of hard disks based on the total video data that will be stored.

No other boxes or special servers will be required. This group of disks spreads across the different compute servers are combined by the USP software into one single pool and can provide all the performance and redundancy that the customer could possibly need.

This enables considerable savings as the additional hardware cost is just the cost of bare disks rather than complete storage platforms.

NO LOCK-IN OF VENDOR-SPECIFIC OR PROPRIETARY HARDWARE

USP was designed to provide true flexibility for the system integrator and end-user organization and that can only be delivered if they have full control and choice of what hardware and servers they prefer to purchase.

The USP software is completely hardware agnostic. The platform can be built with any combination of physical servers. Compatibility exists with Dell, Lenovo, HP, Supermicro, Hitachi, Fujitsu and almost every other x86 vendor. And this flexibility is not just in the choice of setting up the cluster with one server brand, but the capability of building a cluster with multiple server brands and multiple make and models within the same cluster.

And even later, when one wants to expand or replace a server, the choice is open and not restricted to what went into the original setup. There is no dependency on previous hardware when the time comes for expansion. So, all in all, the system integrator and end user can always pick their preferred and most affordable choice of hardware.

WORKS WITH EXISTING AVAILABLE INFRASTRUCTURE

The true test of hardware agnostic is if the solution works with existing hardware and does not always mandate the need for new servers to build the platform. And USP is built exactly on this premise. If there are existing servers which are in a good enough state, they can practically be repurposed for deploying USP on and creating a unified server and storage infrastructure for video surveillance. New servers are not a mandatory requirement.

The design and sizing process will differ slightly when it is a new vs. an existing group of servers. In case of all new servers, the Quantum team will assist by specifying the exact size and configuration of servers that need to be procured for running the specific customer workloads.

Whereas in case of existing servers, the Quantum technical team will first look at the configurations and help you understand the total size of the applications that can potentially run in them. If that is enough to run all the applications and associated storage required, then the USP software will be deployed on them. If the size of the existing servers is not adequate, you have the choice of procuring one or more new servers to make up for the difference.

WORKS WITH ANY CUSTOM CONFIGURATION

As mentioned in the two prior sections, you have the flexibility of mixing and matching multiple server brands, as well as new or old servers within the same system cluster. This is possible because the USP software supports different configurations of servers within the same cluster.

There is no mandatory requirement of all servers being the same size with respect to the different hardware resources. Here is a quick look at the different resources required:

CPU: As long as the servers are either all Intel or all AMD they can co-exist in the same cluster, i.e., either as an Intel cluster or as an AMD cluster. Different generations of processors can be mixed and matched as long as they are from the same server vendor.

RAM: Different servers can have different RAM. The total quantity of RAM within a server along with the CPU size will determine how many virtual machines/applications can run in each of them. So, in effect, the running workloads will be distributed between the physical servers as per their size.

Storage: The total disks within the cluster are generally aggregated within a single pool. However, as a best practice, servers with larger amounts of total disk space are used to store as much data as can be stored in the server with the lowest amount of disk space.

This is generally done so that if the server with the largest amount of disk space fails, there is enough space in the cluster to take over that data. An easy solution for this would be to redistribute the disks before the deployment.

It is this flexible configuration feature of USP that enables a system integrator or end user to repurpose their existing hardware and combine it with new hardware for the total requirement, enabling true savings.

WORKS WITH ANY VMS, SUPPORTS MULTIPLE APPLICATIONS SIMULTANEOUSLY

This last feature is the most critical piece of the story in making USP the most affordable infrastructure platform for physical security. The ability to run multiple applications that can co-exist happily in the same physical server or cluster of servers without comprising performance is the fundamental benefit of the entire USP platform. This is delivered without the complexity of traditional virtualization.

Sample of applications including VMS, Access Control, Incident Management, Intrusion Detection, Security Management, and more that run on the Unified Surveillance Platform.

The financial savings are significant. A list of the savings includes a reduction in the:

- Number of physical servers that need to be purchased
- Amount of time and effort needed for installation and setup
- Manpower and skillset needed to manage and secure the server, storage, and networking infrastructure
- Rack space, power, and cooling required

Conclusion

From reducing security risks and complexity to lowering CapEx and OpEx, it is indeed a win-win for the system integrator and end-user organization who choose to deploy the Quantum Unified Surveillance Platform (USP) to support their video surveillance and physical security environment.

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

WP00272A-v02 Oct 2022