

The Opportunity of Hyperconvergence

Holding the key to simplifying surveillance and building systems

By Eric Bassier | Sep 01, 2019

As security and loss prevention become more critical – and more difficult – airports, public transit, stadiums, universities, hospitals, hotels, casinos, retail stores, restaurants and even entire cities increasingly rely on surveillance footage for new purposes. Now a new IT trend—“hyperconvergence”—may hold the key to simplifying this task while also enabling significantly more sophisticated ways to tap the value of data many organizations are already collecting.

Major Market Trends

As a technology provider that has sold storage for surveillance recording for many years, here are some of the trends we’ve observed: Camera counts and resolutions increasing. As camera prices continue to drop, the number of cameras being deployed has multiplied, and the resolution of the cameras has increased. HD-capable 1080p 25/30 fps cameras are the new baseline for what is expected from any new cameras. This enables better and more granular surveillance – and significantly increases the volume of data to be stored and managed.

Adoption of analytics. Security departments are analyzing the surveillance data they collect using object recognition, license plate recognition (LPR) and other “AI” techniques. These analytical capabilities enable more sophisticated approaches to security management, provided the security department has the means to quickly and easily access the data they have at their disposal. For example, some retailers are now analyzing surveillance footage to study shopper behavior – did they pause at any particular kiosk? What was their facial expression or reaction when looking at a sign?

Airports are analyzing footage to study security lines throughout the day as stadiums look at attendee traffic patterns to determine the best locations to place food carts. This doesn’t even cover using analytics for security reasons. In a specific frame of video, is that person holding a gun? What is the license plate on that car that sped away?

Buildings, facilities and cities are becoming smarter and more connected. Although the

biggest server workload within most security departments is driven by video recording, now applications as diverse as access control, lighting and HVAC have all become digital. Access control, lighting and other systems are based on Internet-connected devices—sometimes referred to as the “Internet of Things (IoT)”—and require oversight and management from the security and facilities department. Some examples include being able to adjust lighting for each office in a way to create a better working environment, or adjusting the angle of window shades throughout the day to maximize sunlight.

These major trends have combined to drive the need for hyperconvergence in surveillance and building systems.

What is Hyperconvergence?

Hyperconvergence is a term that originated with large cloud providers and large enterprise IT departments. It refers to “converging together” separate compute/servers, networking and storage into a single hyperconverged infrastructure.

To understand hyperconvergence, let’s start with what most security department infrastructures look like today. A typical security infrastructure utilizes a traditional “three-tier” architecture, which simply means they have:

- Servers that run applications such as VMS software or an access control application, etc.
- Networking switches that connect the servers to the storage.
- Storage systems where surveillance footage is retained.

New software technologies have emerged in recent years that enable companies to hyperconverge these functions onto a single server platform. This server platform contains embedded storage, and smart software handles the communication and networking functions.

An architecture based on this hyperconverged design is referred to in enterprise IT departments as a hyperconverged infrastructure, or HCI. This architecture has been widely deployed for enterprise applications in the datacenter but it has not yet been widely adopted for surveillance and security.

In comparing the traditional infrastructure with the hyperconverged infrastructure, it is helpful to break down how the data transfer occurs in either scenario by looking at a VMS recording server.

In the traditional model, the VMS recording server is connected to a camera over the network. The camera sends data over the network to the recording server, and the recording server then sends that data to the network switch, which then sends the data over the network (again) to the storage device. Each step adds some network latency.

In the hyperconverged model, the VMS management server, as well as the recording servers, runs directly on the same server that is controlling the storage. Surveillance footage is sent over the network, but the VMS application then communicates directly with local storage, bypassing the need for an intermediate network switch. This approach reduces latency and is more efficient.

Hyperconvergence: Why It Matters for Security and Surveillance

I know what you're thinking; hyperconvergence is a "buzzy" technology term—used widely in the cloud and in enterprise IT. Why does it matter for surveillance and security?

First, it dramatically simplifies the architecture and makes it easier to manage. Rather than manage multiple servers, switches and storage devices, security and facilities professionals can interact with a single platform and with fewer components requiring maintenance and management. This makes their lives easier, but also improves security and reduces business risk by reducing technical complexity.

Second, one of the attributes of a hyperconverged infrastructure is that the "compute," or server resources, sit right next to the storage. This becomes critically important when running analytics against frames of video. Analytics will run faster on a hyperconverged platform, and this can lead to discovering potential security threats and vulnerabilities more quickly. It could also translate into discovering new ways to optimize a business, such as managing staffing and more.

Hyperconverged architecture is built for the smart buildings and smart cities of today and tomorrow. Rather than managing these applications on different dedicated servers—which is expensive, inefficient and complex—these applications can now be hosted and run on the same hyperconverged server that is capturing video.

An Inflection Point for AI and Machine Learning

We are at an inflection point in this market where surveillance is transitioning from its historical role—which was strictly security and loss prevention—to also providing data that can be used to gain new insights and business opportunities. At their core, many of these applications are using compute-intensive analytics to, for example, analyze a large number of frames of video to search for objects and trends. These compute-intensive operations can be run on a central processing unit (CPU) and now a graphics processing unit (GPU).

A major advantage to hyperconvergence is that it "enables" these types of analytics because the compute resources are close to the storage. These architectures can be more flexible about deploying CPU and/or GPU resources to suit the needs of the application.

However, one of the downsides of a hyperconverged infrastructure is that the traditional model allows compute and storage resources to be scaled independently. This can prove important if, say, a security department wants to increase surveillance retention times. That change may not require any additional compute resources, but it does require additional storage.

Conversely, if a security department is adding more cameras and already has sufficient storage in place, new compute resources can be added independent of storage. A hyperconverged infrastructure has fewer “building blocks” and is simpler in that respect, but one implication is that compute and storage resources are always added as the system scales. Many HCI vendors minimize this disadvantage by offering different hardware configurations that can be adjusted to meet the specific needs of the user.

Considerations For HCI Solutions

There are many server and storage vendors that sell hyperconverged solutions into the surveillance and security space. Many of these hyperconverged infrastructure products were designed to run enterprise IT workloads and applications but were not necessarily designed for the unique workloads video surveillance can produce.

The main workload within a security infrastructure is still video recording. Recording video of tens, hundreds or thousands of cameras without dropping a frame requires specialized software architecture and design. The workloads driven by other applications—such as access control and badging systems and smart lighting systems—are relatively small compared to the workload driven by video recording.

Understanding hyperconverged solutions is becoming increasingly important for integrators, security officers and CSOs who are looking to minimize IT management requirements while also maximizing system effectiveness. Therefore, whatever your role for security within your organization, do your due diligence. It's your role to assess the vendor's capabilities and performance based on your requirements before making a final decision.

About the Author

Eric Bassier is the senior director, products, at Quantum Corp.

Copyright 2017 1105 Media, Inc. See our Privacy Policy.

Reproduction in whole or in part in any form or medium without express permission of 1105 Media Inc. is prohibited.

