MARCH NETWORKS WHITEPAPER:

IS THE CLOUD READY?

Five things to consider before moving your surveillance video to the cloud

MARCH networks®

An Infinova Company

5
CONSIDERATIONS

BANDWIDTH

STORAGE

COST

SECURITY

ACCESSIBILITY

Video surveillance systems have some unique requirements that set them apart from other types of enterprise applications. Determining where and how the cloud can support these systems depends on a set of five primary requirements: bandwidth, storage, cost, security and accessibility. This paper outlines some of the key considerations mid- and large-sized enterprises need to examine before deciding to move their video surveillance systems into the cloud — and looks at how they can leverage cloud capabilities for video in the meantime.

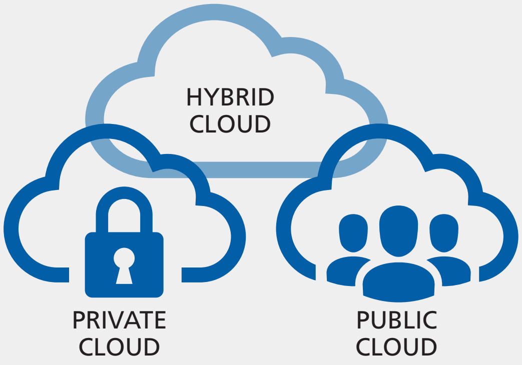
VIDEO SURVEILLANCE AND THE CLOUD

With companies across all sectors taking advantage of cloud technology to reduce IT costs, streamline application management, and make their infrastructure more flexible and scalable, it's no surprise many are now turning their attention to potential cloud applications for video surveillance.

Yet video surveillance systems have some unique requirements that set them apart from other types of enterprise cloud applications.

Video — especially high-definition video — demands much more bandwidth than the consumer-oriented cloud services you may use at home. Pushing video to the cloud reliably in real time requires a high-speed, highly available network. Security and privacy have to be considered, too: legislation, regulations and corporate policies may all impose restrictions on the transport and storage of video footage. In fact, some organizations explicitly prohibit video data from leaving the corporate network.

Keeping these and other factors in mind will help an organization make wise, forward-thinking decisions about how best to leverage the cloud for their business-critical video surveillance systems.



93%

"93 percent of organizations surveyed are running applications or experimenting with infrastructure-as-a-service"

Rightscale 2015 State of the Cloud Report

THE CLOUD IN CONTEXT

One of the challenges with any cloud conversation is that there are multiple types of 'clouds' and any number of cloud services available to enterprises. In every case, computing resources are shared among multiple locations or users, whether via the Internet (public cloud), within an enclosed corporate IT environment (private cloud) or through some combination of the two (hybrid cloud). The computing resources in question may be servers and data processors (Infrastructure as a Service), applications (Software as a Service), development tools (Platform as a Service) or others.

The two most relevant cloud applications for video surveillance are IaaS for video storage and SaaS for management and business analytics. These are increasingly talked about in combination as Video Surveillance as a Service (VSaaS) — though as we will see, there is some advantage to keeping the questions of storage and management separate.

WHAT CAN THE CLOUD BRING TO VIDEO SURVEILLANCE?

Until about a decade ago, most enterprises used their video surveillance systems primarily to review security incidents after the fact. Today, many are taking advantage of intelligent video solutions to reduce losses from theft and fraud; monitor and improve customer service; track commercial conversion rates and performance trends; and identify opportunities to strengthen their marketing, operations, compliance and sales strategies. To deliver this expanded set of functions, video surveillance systems require not only cameras, storage hardware, and dedicated management software but also integrated client-side applications including business analytics that allow for deeper insights and more in-depth investigations.

With all of this in mind, a key question companies should ask is: "What issues are we looking to solve by moving video surveillance to the cloud?"

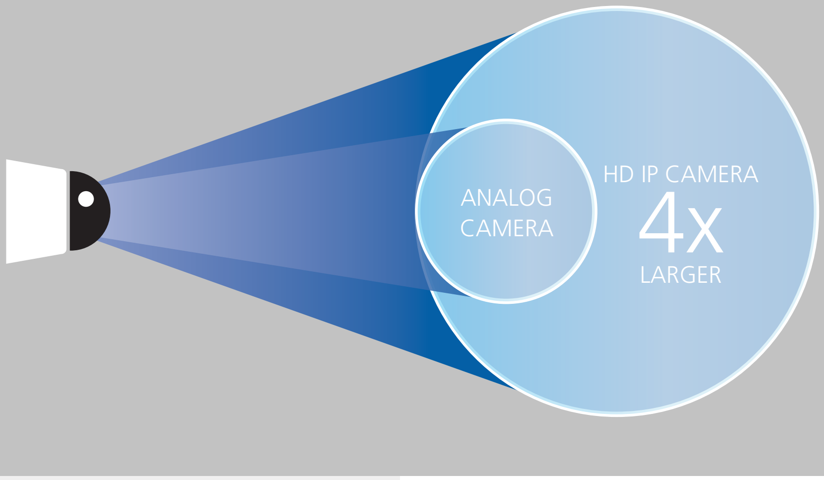
This is important because much of what the cloud has to offer is already provided by on-premises video surveillance solutions today. This includes centralized system control and management, the efficient distribution of software updates, and scalability and redundancy for business continuity.

In addition, other capabilities that enterprises have come to expect from their existing video management systems may not be fully supported by a cloud-based solution. Functions such as synchronized video playback from multiple cameras and seamless integrations with access control, point-of-sale or ATM/teller transaction systems are all critical aspects of many organizations' day-to-day video use. Sacrificing those capabilities during a transition to the cloud would actually be a step backward from what today's technologies can already support.

That said, the cloud does offer a number of unique strengths, including its ability to support valuable new business applications.

Business analytics represent a particularly compelling opportunity for leveraging the cloud today. Cloud-based analytics can be applied to locally stored video, with selected video ‘excerpts’ sent to the cloud for analysis. It takes a significant amount of computing resources to process analytics such as license plate or facial recognition, and because the cloud can make those resources easily available as a service, it can help companies reduce their internal infrastructure and management requirements.

DOING THE MATH ON HD VIDEO



An image captured by an HD IP camera is about four times the size of the best possible image captured by an analog camera — meaning it needs about four times the bandwidth to move through the network. Even with techniques like compression, scheduling and event-driven recording to help reduce file size, large-scale enterprises may find themselves challenged to send HD video to the cloud.

The cloud can also enable efficient and flexible mobile access to locally stored video data. While some mobile applications already provide access through the local network, they typically limit the video stream to a single device only. Cloud technology, on the other hand, can open up mobile access to live and recorded video to multiple devices simultaneously, meaning security professionals can keep an eye on their physical assets while colleagues in marketing, operations and other departments are using the same video for reporting and analysis.

Relying on the cloud for complete video storage should be approached with caution, however, because it requires technology that may not be available equally in all locations and could even have a detrimental effect on other network-based corporate applications.

Ultimately, determining where and how the cloud best supports the business depends on a set of five primary requirements: bandwidth, storage, cost, security and accessibility.

Most enterprises today simply do not have the bandwidth capacity required to upload video captured by multiple IP cameras from multiple locations to the cloud.

IT ALL BEGINS WITH BANDWIDTH

The total bandwidth required for a video stream varies depending on the number of frames or images being captured per second as well as the quality of the images being captured. Given that most enterprises are now replacing some (or even all) of their older analog cameras with new megapixel IP cameras, bandwidth becomes an even more important factor to consider as part of any video surveillance system upgrade or replacement.

Realistically, most enterprises today simply do not have the bandwidth capacity required to upload video captured by multiple IP cameras to the cloud. Even if they employ buffering, which can limit video streaming until a time when more bandwidth is available (such as after business hours), few organizations can access this kind of bandwidth consistently at all locations, especially those operating hundreds or thousands of sites. And while bandwidth speeds and accessibility will continue to improve, and therefore ease the barrier toward efficient video uploading to the cloud, the trend toward 4k and 7k IP cameras may counteract that advantage.

Even the organizations that do enjoy high-speed, high-capacity upload connections across all of their locations may not be in a position to dedicate all (or even a sizeable portion) of their network resources to their video surveillance systems. In fact, it's quite common for banks, retailers and other enterprises to restrict or 'throttle' the network capacity allotted to video to just 100–200 kb/s of their total bandwidth to ensure their corporate network has the capacity needed to transmit financial transactions or other business-critical data.

Service provider caps on broadband services represent another constraint to sending and storing video in the cloud. Again, even locations with sufficient upload and download speeds may have limits on how much data they can push through the network. Exceeding the limit can incur additional — and often prohibitively high — costs.

Digital Divide:
All bandwidth is not apportioned equally.

The availability and affordability of bandwidth is not consistent from city to city. While the average upload speed in Philadelphia, Pennsylvania is 15.8 Mb/s, it is only 5.4 Mb/s in Jackson, Wyoming. Country-to-country comparisons reveal similar differences with Sweden enjoying an average upload speed of 32.5 Mb/s compared to 12.5 Mb/s in the United States, 6.9 Mb/s in Mexico and 7.5 Mb/s in Australia (Ookla, July 2015). Moving video surveillance to the cloud can therefore have different implications for an organization depending on where its sites are located.

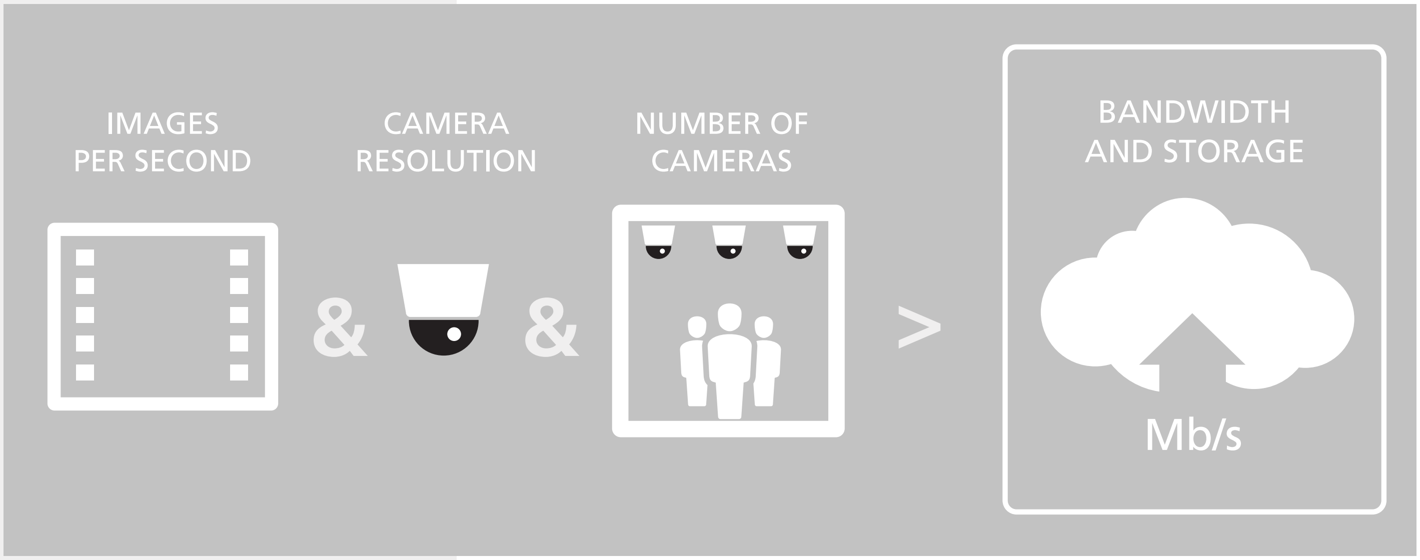
STORAGE AND COST

Before moving their video surveillance systems to the cloud, enterprises also need to consider that the majority of collected video is never used — at least by organizations that have not yet embraced the broader business analysis capabilities of today's video surveillance systems — because only specific events will trigger follow-up action. It is therefore important to determine when it makes sense to transmit video data for storage over potentially expensive network links.

If we take data transport out of the equation and imagine a company has been able to overcome the bandwidth barrier, the cloud could theoretically provide 'unlimited' storage — the cost of which will presumably continue to decrease as technology improves. (Consider how much more affordable hard drives are today compared to a few years ago.) Even so, companies should determine how long they need to retain their video for and how much redundancy they require, as both factors may add to the total cost of their cloud storage solution.

Cloud Video by the Numbers

Calculating bandwidth and storage requirements is an essential step in the planning and design of any video surveillance system. Using metrics such as number of cameras, video resolution and images captured per second (ips), it is possible to determine approximately how much bandwidth and storage a given organization will need for cloud-based video surveillance.



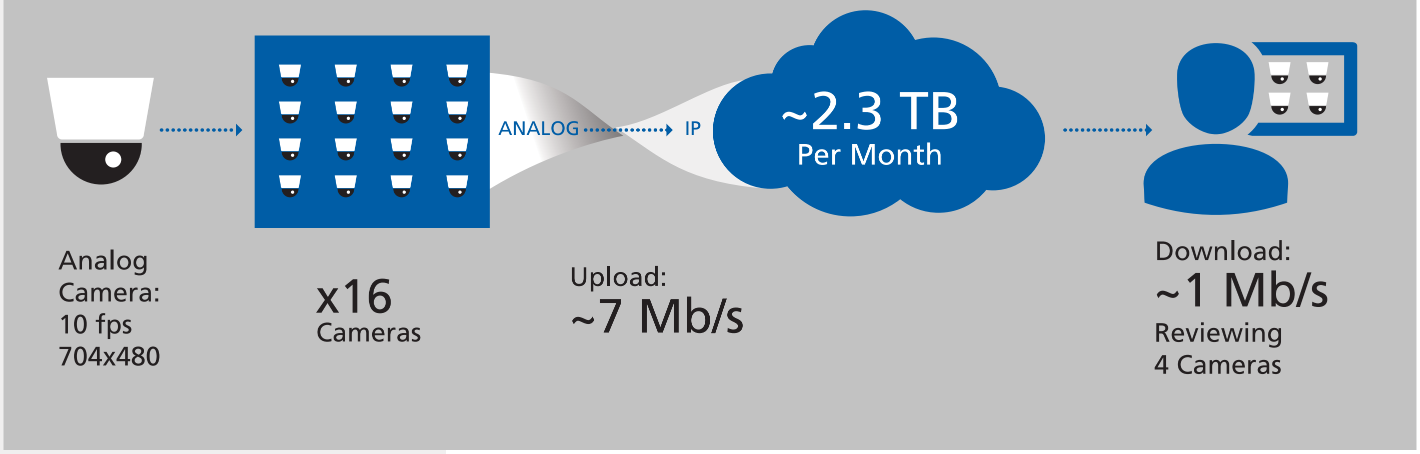
The following scenarios give examples of bandwidth and storage estimates for a typical enterprise, such as a retail organization or financial institution that usually captures significant volumes of video across multiple locations. Although most enterprises use a mix of analog and IP video surveillance cameras today, the trend is definitely heading toward full IP adoption, as analog cameras age and are replaced by IP cameras offering far better image quality.

An Analog Video User Case

Envision a single location of a large national enterprise capturing surveillance video with 16 analog cameras distributed strategically throughout its customer or public spaces, behind transaction terminals, at every entrance and exit, in the parking lot, and in employee-only areas such as stockrooms and break rooms. (For banks, this would also include cameras in secure areas such as the vault and safe-deposit rooms.)

All of these cameras are capturing video at an average rate of 10 frames per second (fps) at a 4CIF resolution (704x480), which means this particular location would need to first convert the analog video to a digital stream using an encoder or hybrid recorder. They would then need a total upload speed of approximately 7 Mb/s to push all that video to the cloud. In addition, if a staff member wanted to investigate an incident by simultaneously reviewing video captured by four of the location's cameras, this task would require an additional 1 Mb/s to download the archived video from the cloud. That's a significant amount of bandwidth for just one location — and even more to dedicate to video alone.

ANALOG VIDEO USER CASE



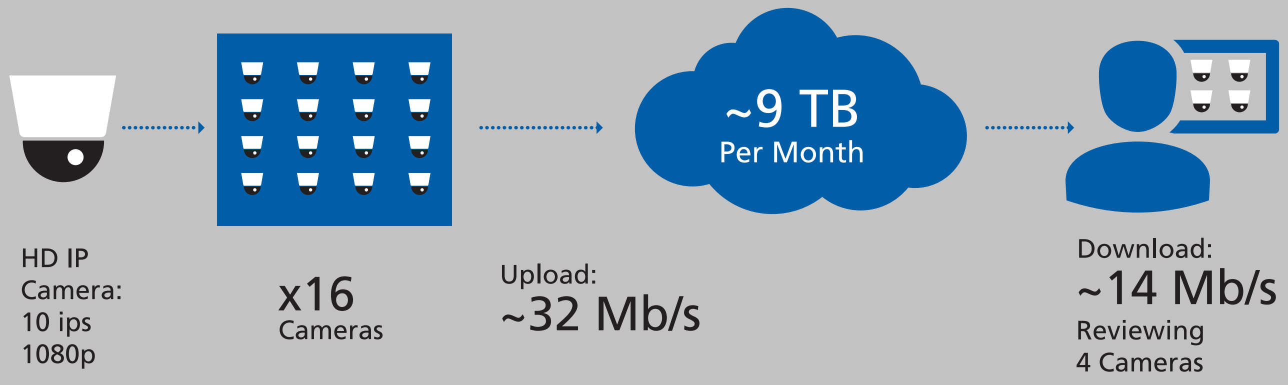
An IP Video User Case

Now imagine that this same location has replaced its analog cameras with 16 HD IP cameras. Those cameras, capturing 1080p video at a rate of 10 ips, would now require an astounding 32 Mb/s to upload all of the captured video to the cloud — and roughly 14 Mb/s to download and review video from just four cameras.

With respect to storage, although retention rates vary widely from organization to organization, if we assume this particular enterprise keeps its video archived for at least 30 days, it would need approximately 9 TB of cloud storage each month to accommodate its 16 IP cameras. (This is comparable to the amount of space needed to store about 1,800 HD feature-length movies!)

While storage has become much more affordable in recent years, this can quickly add up when multiple locations are added to the mix. In addition, for enterprises dealing with more sensitive personal or financial information, video retention rates could be 90 days or longer — meaning even more cloud storage will be needed to ensure nothing is lost or overwritten.

IP VIDEO USER CASE



HD IP Camera: 10 ips 1080p

x16 Cameras

Upload: ~32 Mb/s

~9 TB Per Month

Download: ~14 Mb/s Reviewing 4 Cameras

So what does this all mean?

In short, streaming video and storing it in the cloud might be a reasonable option for a smaller organization with just a few cameras, but would likely be too expensive for most mid- to large-sized enterprises with more than a handful of IP cameras and multiple locations. And while some, such as a large bank, might have the financial resources to pursue a cloud-based solution, very few enterprises would be eager to pay the high bandwidth and storage costs just for the sake of putting their video in the cloud.

SECURITY AND ACCESSIBILITY

With video surveillance systems increasingly connected to the Internet, it is critical that they receive the same level of attention to cybersecurity risk and vulnerabilities as traditional IT systems such as servers and workstations. Given the legal, financial and reputational risks associated with data breaches and leaked video, enterprises are intensely concerned about ensuring the integrity and security of their video networks.

Given the legal, financial and reputational risks associated with data breaches and leaked video, enterprises are intensely concerned about ensuring the integrity and security of their video networks.

Port forwarding, firewalls, network topology and video encryption can all have a significant impact on the security and protection of a cloud-based video surveillance system, requiring a greater degree of expertise and effort in these areas on the part of an organization’s in-house IT support team.

At the same time, some companies have internal policies that strictly prohibit video data from leaving the corporate network or having it stored on a third-party server (even one run by a trusted and reputable provider); others prefer not to take the risk whether or not their formal policies preclude using the public cloud.

Relying on a third-party network to upload or download video means any outage could cut the organization off from its video assets. Uploads may fail, data may be lost and information may be unavailable until the service comes back online.

Consider how frustrating it would be to sit in a security control room knowing all your cameras are recording, but not being able to view what they’re capturing because the external network is down. In the very worst case, a network outage could cause data loss — packets that can’t leave the location might be overwritten or discarded, leaving no video record at all. This would be especially unfortunate if a robbery or violent incident was not recorded as a result. When video is stored on premises, there’s always the comfort of having local access and control. Most enterprise-class servers and NVRs, for example, include battery backups to ensure video recording continues in the event of a temporary network outage.

Even if video data is stored on a local server rather than in the cloud, security and privacy remain important concerns, with data protection and user authentication being two key considerations.

Advances in video compression and faster, more affordable bandwidth services will help make cloud-based storage solutions a more viable option for many larger, multi-site enterprises.

WHAT'S AHEAD FOR CLOUD-BASED VIDEO STORAGE

Cloud-based video surveillance storage and management is an emerging approach with considerable potential. However, until the substantial bandwidth challenge can be overcome, it does not offer a cost-effective alternative to today's video surveillance solutions for most mid- and large-sized enterprises with multiple locations and more demanding video requirements.

As with most network technologies, the point of feasibility will be reached over time as new solutions emerge and build on previous technical capabilities. In the longer term, advances in video compression and faster, more affordable bandwidth services will help make cloud-based storage solutions a more viable option for many larger, multi-site enterprises.

One promising intermediate application may be using the cloud for business continuity and disaster recovery (in the form of cloud-based backups that provide an additional layer of redundancy). Much like full-fledged cloud video storage, this will depend on greater bandwidth being available to individual locations; however, it also comes with potentially less pressure to transport data in real time. In addition, not all video needs to be uploaded and stored in this way; some organizations might choose to only send their significant event or alarm-based recordings to the cloud to help reduce their in-house infrastructure costs.

Business intelligence applications that integrate select video, data and analytics also lend themselves to cloud-based solutions. As noted in the introduction, some organizations are already using these cloud services to reduce the computing and management resources required to process complex analytics such as facial recognition without opting for full-scale cloud storage.

Similarly, some organizations are taking advantage of cloud services to gain enterprise-scale access to their live and locally-archived video via their mobile devices. Such services can support unlimited concurrent connections to any compatible server or recorder, allowing multiple users to view the same video without increasing bandwidth usage.

CONCLUSION

Given the challenges associated with bandwidth and security, it is clear that the wholesale storage of surveillance video in the cloud is not quite ready for large-scale implementation, especially by retail chains, financial institutions and other enterprises with multiple sites that use dozens, hundreds or even thousands of IP cameras.

Still, the advantages remain enticing — and that's why many video surveillance providers are actively pitching cloud-based solutions to their customers. Enterprises are always looking for ways to reduce their spending on in-house technology infrastructure and provide their teams with improved access to archived video.

When exploring the opportunities associated with the cloud, it is important that all enterprises move beyond the hype and take the time to carefully consider the implications a VSaaS model might have on their business. This should include preparing an appropriate set of questions to ask of any potential cloud service provider so they can accurately assess the advantages and disadvantages of the solution over their existing video management system, especially with respect to bandwidth, storage, cost, security and accessibility.

Without the right questions in hand, it is possible that an enterprise could end up with a solution that does not include all of the functionality it needs on a day-to-day basis and one that may actually be more expensive in the long-term compared to what's currently in place — significantly hindering the organization's ability to access effective video surveillance and related business intelligence.

A CHECKLIST FOR VIDEO STORAGE IN THE CLOUD

Before deciding to move your video surveillance system into the cloud, ask yourself and/or your prospective service provider the following:

- ❑ What issues are we looking to solve by moving video surveillance to the cloud?
- ❑ Does the solution offer the same level of functionality as our existing video surveillance system?
- ❑ Are there any limits on the amount of data that our organization can upload/download each month? If so, what are the penalties for going over the limit?
- ❑ Do we currently set internal limits on how much bandwidth we allot to video transmission over our corporate network? If so, how will those limits be affected by a cloud-based solution?
- ❑ How much storage is available per month? How much does it cost?
- ❑ How long can our video be stored in the cloud?
- ❑ Where is the video actually stored? If it’s in another country, do our policies allow that?
- ❑ Are any backup mechanisms in place to safeguard the video stored in the cloud?
- ❑ What network security standards are in place to protect our data?
- ❑ What happens to our video recordings if Internet access goes down? How can we access our archived video if Internet access goes down?
- ❑ Does the cloud solution provide mobile/remote access to our recordings?
- ❑ Are business analytics or other applications included in the solution?

North America	1 800 563 5564
Latin America	+5255 5259 9511
Europe	+39 0362 17935
Asia	+65 6818 0963
Australia and New Zealand	+61 1300 089 419
Middle East and Africa	+971 4 399 5525

marchnetworks.com

MARCH® networks
An Infinova Company