By Fredrik Nilsson

Top 10 Myths of Hosted Video

Think it's unsafe or not for you? Think again

Back in the early 2000s, IP video was the new kid on the surveillance block. Even though the first network camera was invented in 1996, its performance wasn't immediately suitable for security applications (See December 2011 *SD&I* magazine, on the "Past, Present and Future of Network Video.") It wasn't until about 2003 that we saw large-scale IP surveillance implementations, the majority of which involved a heavy dose of encoders. The buzz around IP video was growing, but there was a lot of concern from analog users. This motivated me to write a whitepaper on the "Top 10 Myths About Network Video."

When I look back at some of those IP myths, they seem almost laughable—like the myth about image quality not being as good as analog, or the myth that IP "wasn't ready" for enterprise applications. Would you believe that I heard these very same myths at ASIS 2010? I did. Except this time, the difference centered around myths associated with hosted video.

It's eerie how similar today's skepticism about hosted video is to past concerns about network video. With millions and millions of network cameras and encoders installed in security systems around the globe, we seem to have debunked those original IP myths. In 2011, we can do the same with the top 10 myths of hosted video presented here.

MYTH #1: Software-as-a-Service technology is not mature enough for physical security

In simple terms, Software-as-a-Service (SaaS) is a distribution model where a service provider or vendor offers a product to its customers over a connected network, which in most cases is the Internet. How many services do you use in your professional and personal lives that fall into this category? Do you bank online? Do you use Gmail or Yahoo! mail? Do you use a third-party CRM system? How about your HR services? Do you stream movies to your TV at home? These are only a handful of cloud-based applications that consumers and companies use regularly today.

Today, the biggest IT companies in the world, such as Amazon, EMC, HP, Google and Microsoft, have firmly planted their flag in the cloud. Specifically, storage providers are forever searching for new opportunities with storage-intensive applications and there's no bigger storage opportunity than video.

Today there are numerous SaaS regulation and legislation guidelines that companies must follow to retain data integrity. The buzz around hosted services and the cloud in the physical security industry is similar to what the IT industry experienced five years ago. This IT buzz quickly translated into mass adoption thanks to cost savings and operational efficiencies offered by the cloud and soon the same will happen in physical security.

MYTH #2: Hosted video solutions are not secure enough for physical security

If you're using any of those services above, chances are that you're sending much more critical data over the cloud than you realize. If we trust our money and social security numbers in the cloud, why wouldn't we trust our video data? Since an IP-based security device is essentially

Hosted video technology allows video to be piped via the cloud to devices that include a laptop, the iPhone and tablet devices.

another node on the network, it should have all the same multi-level passwords, SSL encryption, VPNs and firewalls protecting it.

On top of the camera itself, hosted technology in physical security has also improved to protect your video. Safeguards are in place so that once you instruct a camera to connect to a specific hosting provider's cloud, it will only ever communicate with that server unless given a new authentication code and physically reset on the camera itself. Additionally, certain compliance regulations should be met by hosting providers to offer video-as-a-service, including SAS 70, RSA Encryption and ISO 27001-compliance. If the hosting provider does not have SAS 70 coverage or ISO 27001 certification – as there is a cost to maintain these certifications – then the end-user should ensure that the cloud operation is following all the best practices regarding logical security and inquire about the provider's internal auditing procedures.

Even the current Presidential administration has jumped in to outline cloud computing regulations in the Federal Risk and Authorization Management Program (FedRAMP).

If these initial data concerns are overcome, some could argue that storing your video data in the cloud is even more secure than on a DVR. With hosted video, there's no DVR to steal or video evidence onsite to destroy. If the user wants the peace of mind that redundant onsite storage offers, an inexpensive network attached storage (NAS) device can be added to the network, and the same rules apply if this device is damaged or stolen: Your video is still safe in the cloud.

MYTH #3: I have to abandon my existing analog system/infrastructure to migrate to hosted video

While IP cameras present many benefits not offered by analog cameras, we never recommend end-users throw out their working analog cameras if they are happy with the quality and the cameras are already installed. By using a hybrid solution with video encoders, the existing analog streams can be digitized and securely sent over the Internet to the hosting site. Remember, around 80 percent of the market is still analog-based—especially at smaller camera count installations—so a hybrid hosted video solution presents a significant opportunity for end-users interested in an IP migration strategy.

MYTH #4: Cloud solutions are too difficult to install and maintain as they require reconfiguration of local routers

With innovations in hosted video platforms coupled with growing partnerships behind the scenes, cloud partners have worked together to take the complexity out of the solution for the end-user and installer. Internet communication between the cameras and the hosting provider (also known as the storage provider) can be done without complex IP magic such as port forwarding or fixed IP addressing required in the past. Also, once there's a licensing agreement between the hosting provider and the camera manufacturer for each device, the camera can be auto-configured to communicate with and only with that hosting provider's network.

In fact, integrators can set up this communications link between the camera and the hosting

provider's cloud before they leave for the job site. In that case, all they will need to do onsite is install and power the camera in order to start the hosting service.

MYTH #5: Hosted video solutions require too much bandwidth, so you will never get high enough frame rates and can't use HDTV or megapixel

Since the video will be sent out over the Internet, bandwidth usage will always be a concern. However, with the rise of more efficient compression methods like H.264 users are able to send unmatched video quality over mere DSL and cable modem connections. Even with in-house analog solutions, most security departments record video at only five to eight frames per second at CIF or 4CIF resolution to save on internal storage. Point being, the quality of hosted video today is still better than analog. Since bandwidth capabilities and compression standards will continue to improve, the amount of data that's capable of being sent over the network will grow as well.

For those who require HDTV or megapixel performance, an inexpensive Network Attached Storage (NAS) device can be added to the system. Users can today purchase multi-Terabytes worth of storage for less than $300. By using a NAS box, integrators can set up event-based or scheduled recordings to store high-definition quality video onsite, while a redundant stream is sent to the cloud.

MYTH #6: If my video is sent to the cloud it is out of my control

Think of hosted video as a normal surveillance system, only delivered through different pipes. Those who might be used to having an onsite recording device will still have access to live and recorded video anytime, anywhere by partnering with their service provider/integrator. Options for frame rate, resolution, recording length, etc. will be negotiated with the service provider and offered at a monthly rate (in most cases). All archived recordings will be available by logging in to the user's viewing portal just as they would on a proprietary VMS.

MYTH #7: If the network goes down, video will be lost

For those with unreliable networks or who live in areas of the world with unpredictable weather, this can be a major concern. But keep in mind that the beauty of the hosted video/NAS device relationship discussed in Myth #2 goes both ways. Just as having the video being stored in the cloud protects you against a thief stealing your onsite recording device, a NAS device acting as redundant storage protects against losing video if your network goes down.

I've spoken with some of our largest integrator partners about this myth and they are quick to remind me that an analog-based system will also be "down" when the DVR is being serviced. They'll go on to tell servicing horror stories of it taking days or even weeks to repair or replace a DVR and during that entire time, no video is being recorded.

One final thing to keep in mind: Without power, NO video surveillance system will operate. But if the end-user deploys an uninterruptible power supply (UPS) in an IT-based system, they will have an easy back-up power solution for critical applications, which includes powering the cameras via PoE.

MYTH #8: Hosted video works well for residential applications, but not for professional customers

While TV commercials for home surveillance service are being shown more and more, this is by no means the target market for hosted video (although it might be an interesting market in the future). Network video has seen tremendous success in major camera installations, historically when the camera count exceeds 32. But there's a significant commercial market—gas stations, convenient stores, restaurants and boutiques—who have only four to 10 cameras per site and are currently using analog technology.

Not only is hosted video a perfect solution for this professional customer, it's an even better solution for the customer who owns multiple sites and needs to monitor all of his or her properties at once. Also, aside from pure security purposes, hosted video can be an asset for major franchises who want to ensure operational and marketing efficiencies, such as confirming remotely that end-cap displays are properly installed, seasonal decorations are taken down, or that deliveries are being made on time. Hosted video can also be used in tandem with in-house surveillance systems. More on this in MYTH #10.

MYTH #9: Hosted video using IP technology will be too costly for small sites since network cameras are so expensive

IP cameras are certainly more expensive than their analog counterparts as they come with greater video

quality and functionality. But using network-based technology means that other system component costs will be lower; i.e. NAS vs. DVR, Cloud Storage vs. DVR, PoE vs. Coax plus DC power, installation by the integrator only vs. hiring a qualified electrician, and so on. In other words, while the network camera is more expensive, the other costs that come along with analog in the total solution can offset the difference in camera prices.

Most service providers will roll the cost of the camera and any other hardware into the monthly fee with hosted video. This provides the end-user with newer technology, better quality, increased functionality and a more scalable system for a fixed rate that can be reported as an operational expense and not tie up scarce capital like a DVR-based solution.

Taking these factors into consideration, an IP-based hosted video solution in some cases can turn out to be a lower capital expenditure than installing an analog solution for small camera count systems. As storage, compression and bandwidth technologies continue to improve following Moore's Law, this cost discrepancy will only continue to move in favor of IP.

MYTH #10: There is no need to consider hosted video on a large, proprietary system because the technology is only a fit for small camera count systems

While a lower camera count customer is the sweet spot for hosted video, some end-users are using hosted video in tandem with their in-house surveillance system in two ways. First, some have identified "critical cameras" in their systems that cannot lose recording under any circumstances and therefore must have redundant storage in the cloud. These cameras might be deemed critical due to internal policies or compliance issues. By leveraging hosted video and storing the data in the cloud, the video evidence will be safe off-site or in the user's Private Cloud if their internal systems go down or if the DVR/NAS is stolen or damaged.

Second, organizations with large in-house systems can use hosted video to watch the watchers. Security staff or other employees who have access to the control center or recording equipment will not be able to manipulate, delete or accidentally lose video if it's protected by your hosting provider. But remember, if you decide to leverage hosted video as part of a larger proprietary system, there should only be a few cameras onsite running in the cloud to get the most out of the technology.

Myths busted!

As partners and solution providers, we all have a role to educate the market so that end-users get the most bang for their surveillance bucks. In 2011 and forward, that will come in the form of hosted video for smaller systems.

Fredrik Nilsson is the general manager of Axis Communications Inc. in North America. He can be reached at Fredrik.Nilsson@axis.com.