

# cloud

## Managed Services Moving Mountains

With network connectivity and cloud-based services becoming readily available, device manufacturers and service providers have found new ways to protect end users' properties and serve their evolving security and operational needs. A&S surveys current market conditions for managed video as a service and examines real-life usability issues, technical limitations and business development opportunities.

BY HAYDEN HSU

The prevalence of broadband along with 3-G and 4-G connections is making video accessibility easier than ever. While current uptake of managed video as a service (MVaaS) is limited to certain markets and business venues, momentum is picking up with increasing functionality and reliability. According to John Honovich, founder of website *ipvideomarket.info*, 2010 global subscription revenue was estimated to be US\$50 million to \$100 million, with a total of 200,000 to 300,000 cameras hosted, of which 75,000 to 125,000 were new. IMS Research pegged the world market for video surveillance as a service and remote video monitoring in 2010 at approximately \$692.4 million.

A highlighted benefit of MVaaS is plug-and-play, meaning that edge devices such as cameras and D/NVRs automatically connect to the video service without configuration by the customer. "However, not all managed and hosted video providers offer plug-and-play setup yet," said Matt Steinfort, President and CEO

of Envysion. "Some providers, especially those hardware companies who have developed managed or hosted video solutions, do restrict users' camera choice. Others, like ourselves, are camera-agnostic and can deploy their video solutions with any mix of analog or network cameras."

Another important aspect of plug-and-play that remains inconsistent among MVaaS providers is the ability to run managed or hosted video independent of a computer's operating system, security configuration or other system configuration. "Web-based applications, like Envysion's, bypass these issues because no software is downloaded to the computer. Still, not all managed and hosted providers offer a cloud-based solution, meaning users must install software on their computers using the system and any time an upgrade is released," Steinfort said.

Many cloud offerings allow edge devices such as cameras and readers to autonegotiate their connections

with the hosted application. "This is very valuable for both dealers and end users as it removes the necessity to configure the port forwarding and static IP addresses on the network, making it plug-and-play," said Brian Lohse, Director of Business Development for Secure-i. "Unfortunately, this requires the edge device to have proprietary connection information built into it from the manufacturer, and is thus not very open. For an MVaaS provider to add another camera model to its compatibility list, it can be time-consuming and expensive."

Indeed, many MVaaS offerings claim that they will work with multiple brands. "However, some of the vendors make their own encoders and cameras, making it difficult to use another line of product such as access and intrusion detection," said Jim Shepherd, National Account Manager for Retail, Protection One. "In addition, the newer entry-level technologies in the market may not have reached out to all the major video-monitoring service companies and provided their SDKs to work with the software and equipment."

As a result, options may be limited. "For example, older components that include analog technologies such as DVRs may have limited network functionality," said Jumbi Edulbehram, VP of Business Development, Next Level Security Systems. "If analog cameras and encoders are used, they typically have less functionality and flexibility when compared to network cameras." Newer MVaaS offerings rely on the full power of the network infrastructure to provide users with the ability to access, configure and monitor all features of their security system from anywhere and at any time through Web browsers or mobile devices. "When coupled with platforms that integrate multiple subsystems, security data is correlated across sites on a consolidated interface, offering users a comprehensive view of security operations."

"Our key strategy is to function as part of the cloud-computing network," said Stanley Mill, Technical

Director of Virtual Eye. "Since many network cameras comply with M-JPEG and H.264 compression standards, video streaming is not an issue any more." For DVRs, fully integrated solutions are limited to a handful of brands; for intrusion detection, solution providers can usually work with alarm control panels that are compliant with Honeywell's Ademco or Bosch's contact ID protocols, offering automatic video recordings and text/email notifications when alarms are triggered.

In the case of iControl Networks, numerous camera OEMs were sourced to put its software into their cameras to work on the software platform. "This does not limit features," said Gregory Roberts, VP of Marketing. "Rather, it significantly increases the use cases for end users as they, as subscribers of home management/security offerings from our deployment partners such as ADT Pulse, can not only see live video of their premises remotely, but can set their system to capture video clips and pictures when events occur, such as doors being opened or rooms being entered."

## FAILSAFE?

Be it landline or mobile, no network connections are perfect 100 percent of the time, which could be a reason to the seemingly slow uptake of MVaaS offerings in most parts of the world. "There are no assurances, which is a huge issue," Shepherd said. "Other issues include a lack of sufficient bandwidth to port video over networks, not having the video stored on mission-critical servers, and losing video when there is any power interruption." Protection One has seen large national accounts, especially in retail, with very little bandwidth at their locations. "The Internet connections are often sized solely for the purpose of uploading PoS data at night, not for transporting video on demand. Increasing bandwidth at thousands of locations is a huge expense," cautioned Douglas Paul, VP of Operations and Corporate Services.

On the other hand, many others feel the fear of service disruptions on IP networks is greatly exaggerated. "For example, how many times do you find that Google or your bank's website is down? The Internet was designed specifically to be 'self-healing' or able to withstand disruptions," Edulbehram explained. "That means when one part of the network is affected, other parts make up for



▲ **Matt Steinfert**, President and CEO of Envysion



▲ **Brian Lohse**, Director of Business Development for Secure-i



▲ **Jim Shepherd**, National Account Manager for Retail, Protection One

the disruption. Traditional security integrators need to be knowledgeable about the inherent best practices of robust network design.” Mill agreed, adding that SAS 70-compliant data centers today guarantee portal uptime by using redundant power sources, multiple network carriers providing reliability and performance, on-site staff to monitor and provide assistance, managed firewall and data backup services, flood-proofed raised floors, advanced canopy cold-row cooling, smoke detection systems, 24/7 security and digital video surveillance.

Most commercial-grade MVaaS solutions today use a hybrid of local and hosted storage, Lohse added. “They incorporate SD cards or local NAS drives to supplement the cloud infrastructure, which allows them to mitigate bandwidth concerns and provide redundancy in the event of a network failure. Furthermore, many MVaaS applications are constantly monitoring for connectivity and send out an alert to users if an outage is detected, so it can be addressed immediately.”

Security communication to central monitoring stations can include cellular backup; thus, when the power and broadband service are out, emergency backup battery and cellular services initiate, keeping a constant level of communication to central stations, Roberts said. “This is critical to ensure the peace-of-mind value proposition that home security delivers, and features that solution providers like us offer.”

For Envysion, much like the Internet a decade ago and software-as-a-service applications (SaaS, such as *salesforce.com*) a few years ago, questions of MVaaS uptime and redundancy are largely a thing of the past. “Internet connectivity and reliability continue to improve, and many enterprises have redundant or backup IP. In addition, MVaaS solutions can be designed and deployed to work ‘locally’ if the Internet does go down,” Steinfort said. Customers’ video can actually reside both on the on-site DVR and in the cloud. The video remains on the DVR until the hard drive is full (typically 30 to 60 days depending on camera configurations and the drive size). The Web-based application, through which users backup footage, review video and export reports, resides in the cloud. When customers log into the portal to view live or recorded video, the application streams the video content on demand from the DVR at the site.



▲ **Jumbi Edulbehram**, VP of Business Development, Next Level Security Systems



▲ **Stanley Mill**, Technical Director of Virtual Eye



▲ **Gregory Roberts**, VP of Marketing at iControl Networks

An added advantage of managed video over traditional security is that many providers have system health monitoring in place and can immediately alert customers if a camera or DVR goes down, whereas traditional cameras could be down months before anyone knew.

## ONLY FOR COMMERCIAL USE?

The driving force behind MVaaS in the US commercial space has been a lack of internal resources to manage the video and to have the administrator expertise to use it wisely. “Much of the MVaaS supply chain is outsourced to cheaper labor, which allows users to pay low recurring fees over time as opposed to large capital expenditure that may not show an ROI. Also, various MVaaS models exist, allowing customers to pay by the service, specific device channel or their specific uses,” Shepherd said.

In the past few years, businesses have begun to see that surveillance footage holds hidden business intelligence that can be used as a strategic management tool to drive bottom line improvements. “Businesses understand that by integrating video to key business data systems, users gain access to actionable insight,” Steinfort said. “This insight gives operators a clearer understanding of what’s happening in the day-to-day operations of their business and enables users to make positive changes within the organization to improve productivity and financial performance.” During the same time period, MVaaS providers began developing easy-to-use, rapidly scalable solutions that require minimal IT support on the customer’s end. “Perhaps the largest deviation from traditional solutions is that these MVaaS solutions are designed to be used by hundreds or thousands of users in the organization, which provide the network effect,” Steinfort observed.

Other driving forces noted by Lohse include more mature and refined options to choose from, increased dealer and end-user awareness and understanding of

cloud technology, and more affordable solutions as they incur economies of scale in bandwidth and storage.

That is not to say it is all smoothing sailing, though. "Porting video to third parties, sending them overseas for review, and opening up closed networks to possible threats and hackers have become common concerns as of late. Additional concern with liability and risk is added if a video is somehow publicized without the customer's permission," Shepherd said.

However, Edulbehram expects that the private/residential sector will use nothing but MVaaS in a few years. "Today's concerns are largely based on a lack of information or not following basic security practices. Most users are comfortable with conducting sensitive financial transactions over the network, and I expect to see similar comfort levels with remote security services."

Lohse echoed in agreement. "I do believe that the private/residential sector will eventually pick up. The limiting forces right now are just cost and need."

For iControl, residential applications in the U.S. are significantly increasing due to recent mass-market

launches such as ADT Pulse interactive services and other interactive home management and security offerings by major broadband service providers, Roberts said. "While consumer concern regarding privacy is prevalent, many software solutions address this via encryption techniques. Our solution actually creates a Wi-Fi subnet in the home, enabling encryption of the data using the latest technologies."

3DES and SSL security encryption protocols, along with ISO certifications, should ensure the peace of mind most customers require, Mill added.

## **BUSINESS POTENTIAL**

In physical security, many solutions have "tried" and failed or gone quiet (in the case of video analytics). What is to say MVaaS will not suffer the same fate?

"Telco efforts have been half-hearted and underfunded," Lohse analyzed. "Telcos don't understand the security industry, how to market and sell solutions effectively. Customers know the likes of ADT, Protection One and Stanley as security companies and that their

respective success is based on core competency in security, whereas it seems telcos are doing this 'on the side,' which isn't as comforting to customers."

Roberts agreed. "Consumer research directed us to integrate home management services with home security, enabling broadband service providers to offer a new, next-generation interactive home security solution and helping existing security companies upgrade their existing offerings. There is tremendous potential for add-ons like energy management solutions as well." To accommodate different wireless technologies such as Wi-Fi, ZigBee, Z-Wave and cellular, solution providers also need to have the ability to adapt to the needs of their deployment partners.

By contrast, telco offerings are normally video-centric, and other systems, such as access control, are very difficult, if not impossible, to integrate, Edulbehram said. "Another difference is that telcos sell directly to end customers, bypassing the traditional security channel. Security integrators have the market knowledge and expertise to deliver proven solutions to customers; today's integrators provide a high level of service and support that telcos can't match."

Clearly, alarm-monitoring companies play an important role in managed video services, "because we are in the data and analytics business to observe behavior that requires actions," said Jamie Rosand Haenggi, CMO for Protection One. "We see more applications of video being used for 'guard replacement.' The ability to offer visual and personalized verifications, guard tours or video escorts enables companies to leverage this kind of technology as a way to be all places 'on demand' without the costs associated with manning multiple stations or locations."

In Edulbehram's view, the industry can provide and develop stronger revenue-sharing models with the security channel and help system integrators further build recurring monthly revenue (RMR) models. "Also, we can increase integration with traditional central stations or monitoring centers to help build business efficiencies and customer security."

Indeed, while the concept sounds great, dealers want RMR and users do not want to buy security or manage assets remotely. There is still a lack of defensible use cases with white papers and TCO comparisons, Lohse observed.

"We often find in video services that the toughest part is not the hardware and software configuration," Paul



▲ Surveillance footage holds an incredible amount of information and potential to drive improvements across different departments within an organization.

said. "The toughest part is clearly understanding the customer's expectation of what we do with the video we see and then document that in a way that an operator can act on it."

Carlos Perez, VP of Product and Marketing at Envysion, agreed. "While our application offers many benefits and much flexibility, I am not suggesting that it does everything. Instead, I am suggesting that we communicate very effectively what we can do and work very hard to understand what prospective customers need from a solution to ensure that we can deliver."

Surveillance footage holds an incredible amount of information and potential to drive improvements across departments. The trick is getting to the video that matters quickly and in a cost-effective manner. MVaaS makes this possible. "Departments across the organization, including marketing, operations, human resources and risk management, can benefit from access to relevant video. These areas remain relatively undeveloped, but there is enormous potential to add services to existing offerings or develop completely new ones," Steinfort projected.

With growing 3-G and 4-G coverage and improved bandwidth, Mill also sees MVaaS potential in transportation, e-government, manufacturing and medical applications. "Our ultimate goal is to create public awareness about mobile surveillance and incorporate this service as part of their mobile lifestyle." Take Asia for example. The Chinese market consists of 350 million mobile subscribers, reaching 25 percent of its population. Taiwan has a 100-percent mobile penetration rate of about 22.5 million people. Malaysia currently has 14.6 million subscribers, out of a population of 27 million. "In total, the estimated global market size could be as high as \$800 million," Mill concluded.

