

# VMS at the Heart of Converged Security

BY LING-MEI WONG

Video surveillance systems today remain steadfast sentinels, but people can learn so much more from the video. Looking for the shady character lurking about two weeks ago? Just pull up the footage with the search function, instead of wading through reels of videotape. As the DVR revolutionized storage by shifting it to a digital medium, video management software (VMS) brings separate devices into a single cohesive network.

VMS expressly manages video, which often is the largest and most complex system in security. While access control and building automation protocols are largely universal, video control protocols and compression depend on the maker. Smart edge devices come loaded with VCA, which is uniquely coded

by each vendor and not always compatible with the VMS.

VMS can be categorized as stand-alone and hardware-based. A stand-alone VMS is pure software, managing third-party hardware through server-client architecture. The hardware-based VMS runs off a storage platform — a DVR or NVR — designed with specific functions in mind and manages video systems from its maker or approved partners.

We examine the two large categories of VMS in the following coverage. *A&S* talks to vendors and installers on what distinguishes stand-alone from hardware-based VMS, what makes a VMS solution good and how it will get better in the future.

Management tools are poised for strong growth. While the market for physical security information management software is expected to reach US\$200 million in 2014, the combined video management software (VMS) and access control software (ACS) market will top \$1 billion by 2014, according to IMS Research forecasts. VMS has become standard for security installations as camera counts have grown. A management interface extracts more data from video, providing users with value. This first of three articles examines dedicated software solutions, selection criteria and key developments.

Finding an effective VMS solution can be daunting. "There are only a few features that really set some VMS apart as being good, but there is a long list of things that can make them bad," said Jacob Loghry, Systems Engineer II, Adesta (a G4S company).

The checklist for VMS below includes architecture, device support, ease of use, integration and scalability.

**TECHNOLOGY DIFFERENTIATORS ARCHITECTURE**

VMS can be examined by five metrics. The first is the platform's architecture. "The primary difference between dedicated VMS and hardware-bundled VMS is that the dedicated VMS will work on any standardized, commercially available, off-the-shelf (COTS) server or workstation, and the bundled VMS will only work on a proprietary black box from the vendor," Loghry said. "This is a critical difference depending on the type of

environment the system is going to be placed in."

The type of architecture affects system stability, which is critical in mid- to large-scale projects. "Being able to work with COTS equipment generally allows for a much more IT-friendly and enterprise-class solution," Loghry said.

Selecting best-of-breed hardware demands network maintenance. "The downside to a COTS-based solution is usually that the system is more complex, requiring trained IT staff with knowledge of enterprise-class servers and complex corporate networks," Loghry said. "We typically use this solution for all of our larger installations or anything required to meet corporate IT standards."

**DEVICE SUPPORT**

As architecture determines system stability and size, a second metric for VMS is processing power. "Processing power indicates how many servers and edge devices the VMS can support, which determines the system's scale," said Alf Chang, Senior Consultant for A&S magazines and a former installer.

As an HD camera recording at 30 fps will tax a system, processor efficiency will affect the system's

device support, Chang said. Different compression formats are more processor-intensive — H.264 requires twice the decoding power of MPEG-4. Installers can check VMS device load by seeing how many channels can be viewed simultaneously without lag or dropped frames. Bandwidth management and transcoding should also be noted, Loghry said.

**EASE OF USE**

Users may be overwhelmed by VMS playback, configuration and recording options. "A user-friendly interface affects purchase decisions," Chang said.

Support for different user profiles, along with ease of administration and maintenance, are good for customers, Loghry said. The number of simultaneous users is another factor, as guards and system administrators will both access the VMS.

**INTEGRATION**

As VMS manages dozens of devices, ease of installation and setup can save installers precious time. Backward compatibility with analog devices is differentiator — VMS that seamlessly integrates all cameras, D/NVRs and video servers



▲ Airports deploy cameras in the hundreds to thousands, requiring scalable VMS to manage all video devices.

will maximize the user's existing investment, Chang said. As support for more systems is expected, VMS that can integrate with access control, fire and building automation will win points for flexibility.

Customers will put vendor claims to the test. "In Russia, the user will test VMS from different manufacturers so they can see how it works," said Alexey Mayorov, PM at Axxon. "If the VMS is more flexible, scalable or easy to use, the customer will install it for their project."

**SCALABILITY**

A good VMS should meet a customer's current and future needs, Loghry said. More vendors believe a scalable solution must have a simple licensing plan along with an open platform, Chang said.

Openness is a hurdle for purchase decisions. "There is no typical selection process," said Jumbi Edulbehram, VP of Business Development, Next Level Security Systems. "To simplify life, an integrator takes one or two products and only sells this or that VMS. If

the customer wants another VMS, he might have to go to another integrator."

**EASE OF USE**

Ease of use for VMS is superior compared to analog video. "I will admit that some systems are harder to use than others, and usually this is because they just have too many features and can be a bit overwhelming," Loghry said. "By and large, I would say that most VMS offerings are relatively easy to use and if you learn one, then you understand them all."

Training time depends on the operator's knowledge of video surveillance and computers. "We typically spend two or three days of hands-on training with the operators and offer follow-up sessions if needed," Loghry said. The installer will tailor the VMS according to the requests for proposal.

Good VMS should be configurable. "Each of the VMS GUI applications offers the full configurability of the layout elements: what elements are displayed, along with their position

and size," said Nik Moissiadis, President of Adtech Network Media. "All can be controlled on-the-fly by the application operator, or defined and locked down by an administrator."

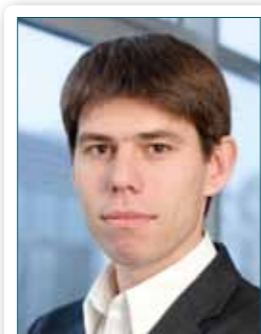
Axxon adapts its software to applications in retail, transportation and city surveillance. "We only provide one application, but it can be used for many different applications depending on the customer's requirements," Mayorov said.

Other interfaces can be customized by each user — features can be hidden, exposed or dragged and dropped. "From a flexibility standpoint, maybe I only care about reports or I only care about alarms," said Marc Holtenhoff, CEO of Aimetis. "As an IP administrator, I don't care about cameras but care about the IP network tree."

Some VMS solutions offer individualized clients by authorization. "Expanding the use of profiles further, every user can belong to a specific profile group, dictating how their interface looks and feels, as well as the system devices and functionality that they have access to," said David Aindow, Product and Technology Director for Synectics (a Quadnetics company).

VMS options can fine-tune user rights down to single devices or cameras. "A doorman, for example, may only have user rights and control panels for live view and PTZ control," said Rolf Senger, CEO of SeeTec. "For the special needs of vertical segments such as the logistics industry, SeeTec offers particular solutions tailored to specific needs."

Genetec's task-oriented concept is designed for ease of use, displaying different functions by credential and software package. "All user



Alexey Mayorov, PM at Axxon



Nik Moissiadis, President of Adtech Network Media



Marc Holtenhoff, CEO of Aimetis

interfaces are based on tasks," said Francis Lachance, PM at Genetec. "In the security market, people tend to stack as many functions in the same UI. We bring a lot of functions to users without overwhelming them."

The company goes to market through system integrators, who must be certified to install the solution. "This is how we ensure the deployment goes as smooth as possible," Lachance said.

Browser-based solutions require no software installation apart from the server, letting users and administrators set up quickly. "The VMS offers a number of easy-to-use features such as auto discovery of network cameras and a definable UI," said Steve Lewis, COO of ipConfigure.

**CULTURE**

Accounting for local preferences makes a system easier to learn. "Milestone has fully documented online help for its user interface in 22 languages — and that's just one facet of making the VMS easy to use," said Christian Bohn, VP of Marketing and Head of Product Development for Milestone Systems.

Software preferences are far from universal. "Sitting in your lab or factory, customer requirements are

not exactly the same," said Tuhin Bose, Chief Engineer of Videonetics. "Making something work in Europe or the U.S. is not the same as making it work in India."

**INTEGRATION**

Dedicated software platforms utilize third-party hardware, offering users best-of-breed solutions. These noble ideas are trickier in real life, with different control protocols and video compression formats requiring individual integrations.

Standards such as ONVIF and PSIA are easing integration. "We are completely open, so we already integrated about 400 different devices: not only network cameras, but access control and fire alarm systems as well as third-party software," Mayorov said.

Genetec offers multiple integration levels, with simple integration taking a day. "What we tend to see in the industry is the camera maker provides the API, and it's on the VMS developer to integrate cameras," Lachance said. "We have created the Genetec protocol and provide it to third-party camera vendors, so they can integrate protocols in their camera to be compatible with our software."

Other vendors do not integrate by

device. "This is all based on open standards," said Hans Schipper, GM of Security Management, Education and Locker Management Systems, Nedap. "We don't use camera drivers; we follow ONVIF camera controls and standard compression."

**SOFTWARE INTEGRATION**

While adding cameras is straightforward, the consensus was VCA integration took longer. "Analytics are a challenge because there are no standards," Lewis said. "Even with the framework, there is so much interaction between the VMS UI and the analytic algorithms that it takes months to integrate. That is why the majority of dedicated VMS vendors use their own basic analytics such as video motion detection."

March Networks does not integrate third-party VCA, offering its own analytics instead. "It's very different how metadata is overlaid for ObjectVideo and how we do it," said Jesse Frye, Product Line Manager, IP Video Management Systems, March Networks. "The development cycle takes months to integrate."

SeeTec emphasizes deep integration for devices and applications. "Standards like ONVIF and PSIA may make life easier in the future, but they currently offer only the least common denominator of features," Senger said. The company's solution is fully integrated with algorithms from ObjectVideo and offers a standard interface for third-party applications.

**SCALABILITY**

Big, bigger, biggest — video installations aren't shrinking. Keeping up with all those devices requires robust VMS. "There's a growing demand for VMS," Frye said.



Rolf Senger, CEO of SeeTec



Steve Lewis, COO of ipConfigure



Christian Bohn, VP of Marketing and Head of Product Development for Milestone Systems



**Éric Fleming Bonilha**, Technology Director of Digifort



**Hans Schipper**, GM of Security Management, Education and Locker Management Systems, Nedap



**Tuhin Bose**, Chief Engineer of Videonetics



**Jesse Frye**, Product Line Manager, IP Video Management Systems, March Networks

“Even with financial institutions that currently use DVRs, they’ll use video management. They’re not using stand-alone DVRs, but a video management system to manage all DVRs from a corporate network.”

Modular “building-block” solutions are suited for scaling up, along with the use of a distributed database with no single point of failure, said Phil Ridgeon, VP of Sales for Vigilant Technology.

SeeTec’s concept is based on real client-server architecture, making it easy to add servers for more sites or a larger number of cameras. “Starting with a basic package containing five camera channels, SeeTec systems can be extended up to several thousand cameras,” Senger said.

Munich Airport deploys Aimetis’ solution, which runs 1,800 cameras

on six servers. “Aimetis is strong in scalability, which is interesting for bigger customers,” Holtenhoff said. “Each server manages not just camera feeds from HD cameras, but more than 1,000 I/O devices with alarms, as well as 5,000 clients all running on six servers.”

## COMPONENT REQUIREMENTS

VMS requires sufficient processing power from its components. However, processor performance depends greatly on system size and the device count. “Requirements vary depending on the size of a surveillance instal-

lation: how comprehensive the VMS is being used, how many cameras, whether they are megapixel, HD, H.264, whether there are analytics being used and more,” Bohn said. “We have a server estimator to help customers and partners define the hardware requirements for a given installation.”

Efficient solutions mean users do not need to buy new hardware. “That’s something we can do over the competition, which is use one processor for fewer cameras,” Lachance said. “It’s the processor, bit rate and cameras. The metric to calculate is usually the bit rate.”

Standard PC processors from AMD and Intel are sufficient for PC-based solutions, while DSPs are used for boxed VMS requiring recoding.

## CHALLENGES

The future of VMS will see greater integration. “The challenges for VMS are convergence, standardization and embracing access control models,” Schipper said. “In video management, there’s an increasing need for access control system models, like role-based access and compliancy rules.”

Software providers must keep up with a growing range of equipment. “Hardware support is a challenging area, since each day new hardware is released and we must support all of it,” said Éric Fleming Bonilha, Technology Director of Digifort. “In the future we expect that ONVIF and PSIA will change this, so we can focus on feature development.”

Keeping integration from being overwhelming will be a concern. “Though it is practically possible, integration of everything — access control, video analytics, fire alarms and building management — may be too complex to maintain and lacks user friendliness,” Bose said. “Some interfacing standards need to be defined, and then the integrated system will emerge more effectively.”

As IP video standardizes, VMS companies will struggle to differentiate themselves. “For some companies, that may mean a price leader strategy; some may focus on special applications or industries, while others will be forced to leave the market,” Senger said.

Having a clear value proposition will give vendors an edge. “We all do same thing — capture video, events and trigger alarms,” Frye said. “Frankly, who cares? The customer doesn’t see the value in a feature or function, he sees value in how to solve problems.”

