IHS Markit™

Video surveillance:

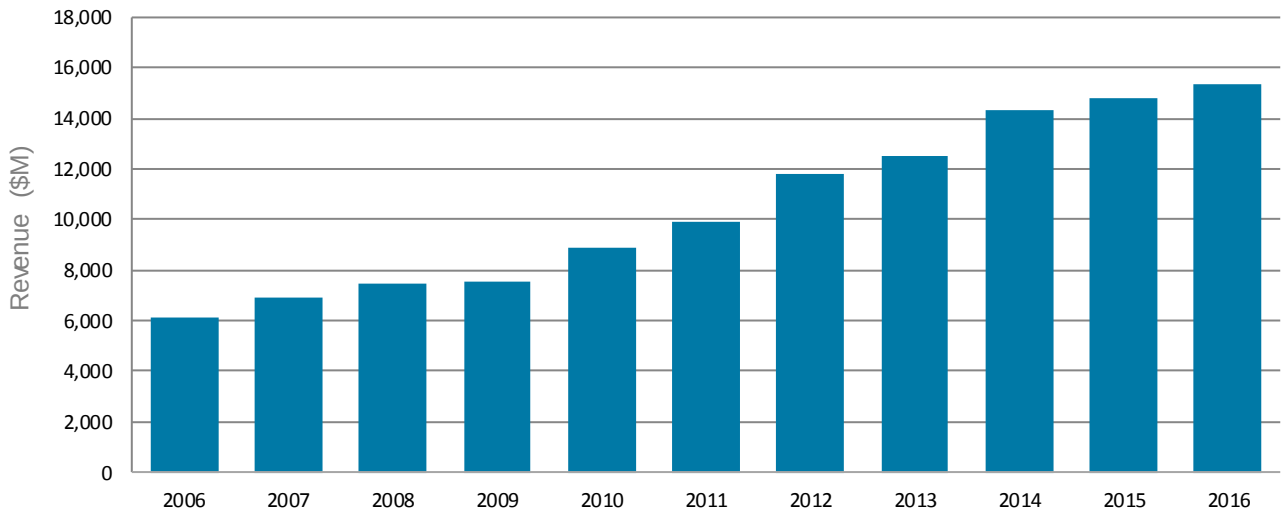
How technology and the cloud is disrupting the market

Table of Contents

Executive Summary: How technology and the cloud is disrupting the video surveillance market

Demand for surveillance cameras has grown quickly during the last decade; and is forecast to continue growing in the coming years. It is estimated that 9.9 million professional surveillance cameras were shipped globally in 2006 and that this grew to 106.4 million in 2016. At the same time, the global market for professional video surveillance grew from $6.7 billion to $15.4 billion in 2016. It is forecast to grow to $19.7 billion in 2020 (a compound annual growth rate (CAGR) of 6.5% from 2016 through to 2020).

Global professional video surveillance market growth ($M)



Source: IHS Markit

The main drivers of this market growth have been:

- The transition from analog equipment to networked equipment; leveraging networking developments in the broader ICT market and the trend to the Internet of Things (IoT).
- The decline in average selling prices for video surveillance equipment driven by increased shipments and aggressive new entrants to the video surveillance market, predominantly from China.

These trends have changed the video surveillance market dramatically, such that eight of the top ten suppliers (in revenues) from 2006 had lost market share by 2016. However, the question remains, which technology trends and market evolutions will drive the video surveillance market of the future?

This white paper aims to highlight some of the critical drivers relevant for the video surveillance market in the coming years. These include:

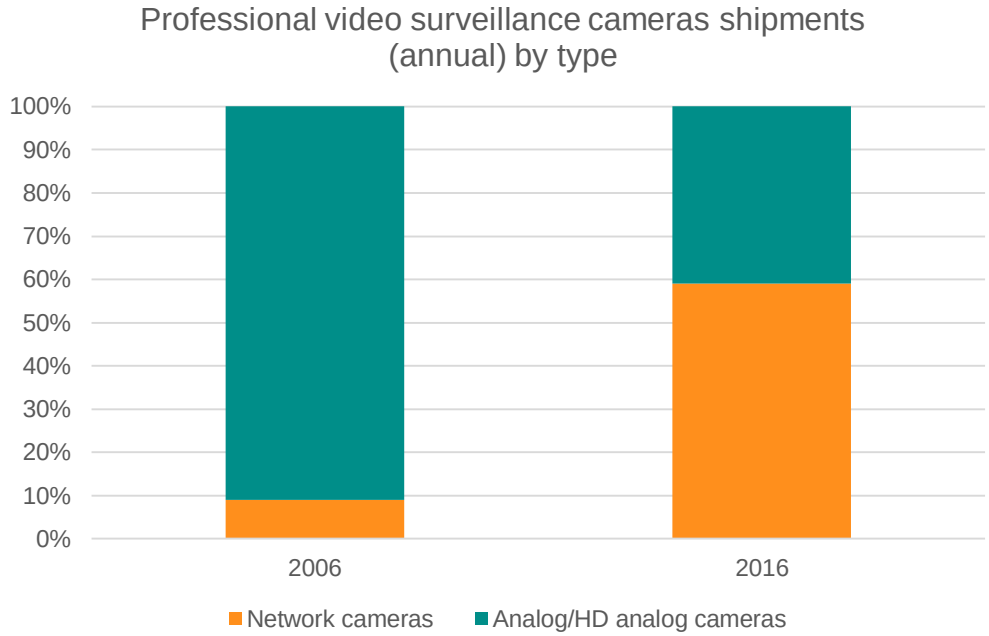
- Technology developments - specifically the application of video analytics in security cameras, back-end equipment, and in the data center – which will drive broader and more valuable use-cases in the video surveillance market.
- The increasing connectivity and application from cloud architecture which will support new business models and enhance the markets ability to leverage resources such as compute power and storage assets.

The evolution of technology and changes in the competitive environment will all impact the video surveillance market of the future.

Professional video surveillance cameras are increasingly being connected to the network

Governments and private organizations often deploy video surveillance equipment as a crime prevention tool. While research into the effectiveness of video surveillance as a tool to reduce crime is somewhat inconclusive, most would agree that it reduces the fear of crime, which in itself is an attractive proposition for most governments.

This has led to organizations installing video surveillance as a proactive measure to prevent crime. Moreover, the threat of terrorism in many regions of the world is high and has led to increased government spending on public-space video surveillance. Video surveillance is a cost-effective and high-profile method of increasing security at likely terrorist targets; hence governments are investing heavily in this technology.



The mix of camera types sold has changed greatly over the past decade.

It is estimated that just **9%** of surveillance cameras sold in 2006 were network cameras but this had grown to **59%** in 2016.

At the same time, there has been an ongoing trend towards these cameras having a higher resolution. While resolution is just one aspect of video quality, the key benefit of higher-resolution cameras is to offer sharper and more clearly defined pictures.

It is estimated that less than **2%** of network cameras sold in 2010 featured embedded video analytics but this had grown to over **40%** in 2016.

There is also an ongoing trend to these network cameras having more advanced features. For example, an increasing proportion of network cameras come with advanced low light functionality, wide dynamic range, and embedded video analytics.

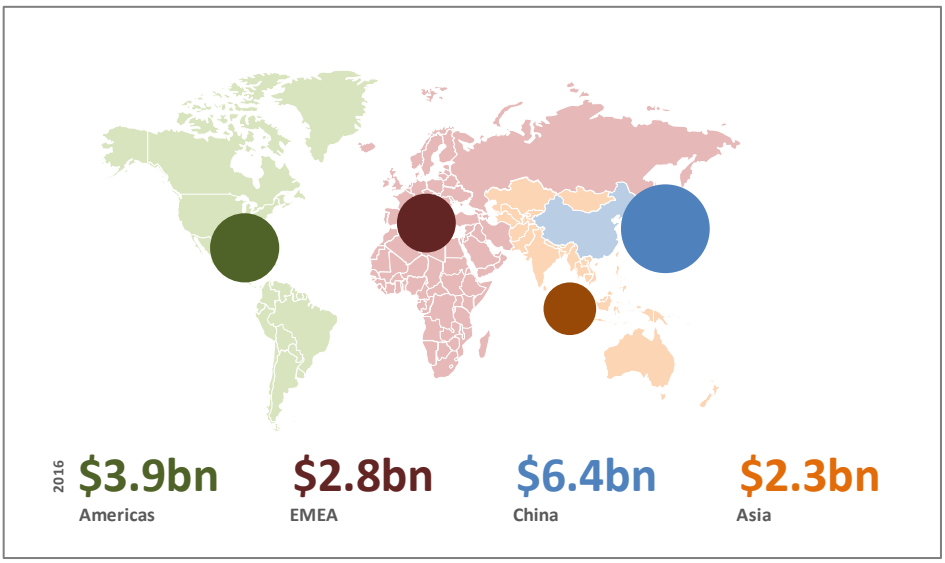
China represents the largest video surveillance market; however, growth is coming from emerging markets.

China is the world's largest country market for video surveillance equipment and accounted for **41%** of world revenues in 2016.

The Chinese market has grown quickly this decade. Unit shipments of surveillance cameras grew by **29.6%** in 2013, **38.5%** in 2014, and **34.6%** in 2015.

However, growth has started to slow with unit shipments growing just **2.3%** in 2016.

The lower rate of growth reflects the high installed base of cameras in China. Demand for cameras in future will be increasingly for replacements rather than new installations.



There is also a high penetration of installed video surveillance cameras in countries like the USA, the UK, Japan, South Korea, and much of Western Europe. Again, demand in these countries is often for replacement cameras rather than new installations.

Demand is growing faster in other regions like India, South East Asia, and Latin America where the installed base of cameras is not as high. In many cases, the lower price of equipment is opening up these emerging markets, making video surveillance a more affordable option.

Technology trends also vary by country and region. Following are some examples:

- **The penetration of network cameras into the overall security camera market is much higher in China than in the American market.** Similarly some markets are more likely to purchase software and server-based recording, while other regions will more commonly buy boxed recorders. As mentioned, China is the largest video surveillance market by some distance; it is also rapidly transitioning to cloud video surveillance architecture.
- **Many of the large safe city deployments are being distributed across numerous data centers to share resources, analysis and data.** This means city authorities can be more integrated which works well in the large camera count projects deployed in the country.
- **Outside of China, cloud has been more successful in smaller camera count projects in the commercial and retail markets.** Here, the bandwidth costs remain a barrier to larger camera systems and many projects are not sufficiently large to require private data centers; principally because each security or government departments is independent and does not integrate with each other. How this develops will depend much on the success of cloud projects in China and other emerging markets.

Video analytics, cloud and connectivity will all shape the market of the future

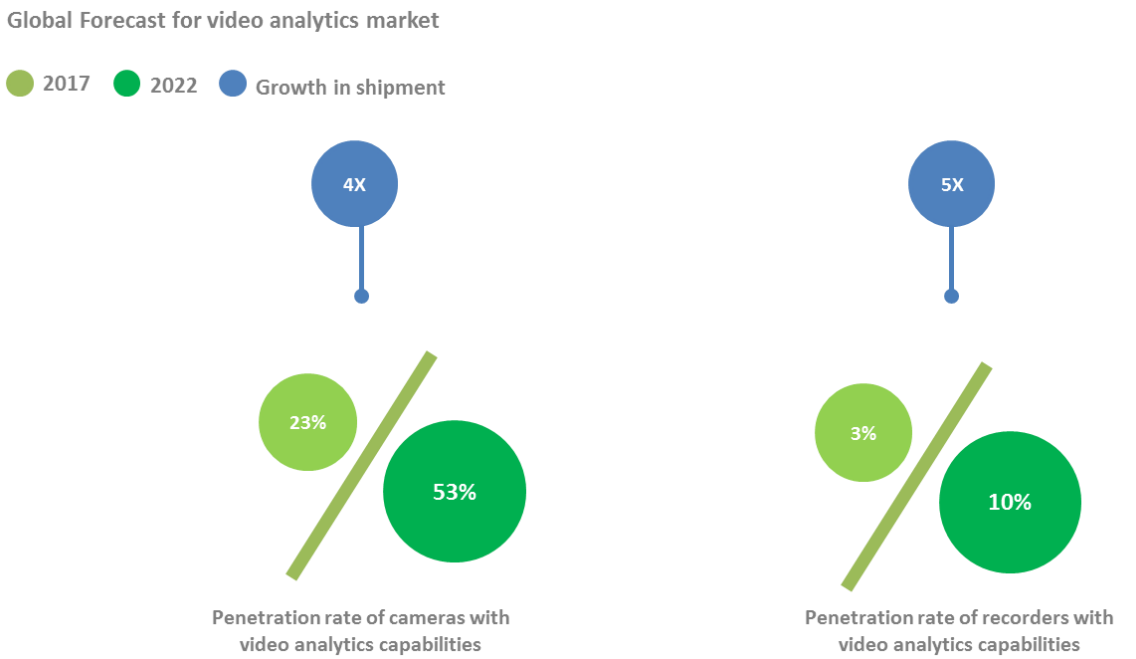
Video analytics and deep learning

Video analytics can be applied to:

- Retrospective analysis of archives (archive management, search, triage, forensic investigation).
- Real-time analysis of live video streams (situation awareness and alerting, encoding, compression).
- Predictive analysis leveraging both live video streams and archives as well as data from other related domains (prediction based on the past and present, event/activity prediction, anomaly detection).

Video analytics software analyses live or recorded video streams to detect, classify and track predefined objects and behavior patterns. It is used as a means to automate the monitoring process and can be particularly effective in proactively identifying events as they happen or extracting information from recorded video.

The software can either be priced independently as a distinct purchasable product or embedded on a piece of video surveillance equipment, prior to reaching the end-user (typically at the point of manufacture). In the second case, the analytics software is normally amortized in the price of the equipment although there is sometimes a separate charge. The algorithm can either be embedded on the camera, where the compute power is lower but where savings can be made on bandwidth, or embedded on the central device, where compute resources are higher.



Security cameras with video analytics capabilities accounted for **17 million** shipments in 2017; this is forecast to rise to over **70** million shipments by 2022. Similarly, the number of recorders with video analytics capabilities is predicted to rise by a factor of **5** between 2017 and 2022.

Much of this growth is being driven by leading Chinese equipment vendors such as Hikvision, Dahua and Huawei. These suppliers have been integrating video analytics into their surveillance products for a number of years now. For example, Hikvision and Dahua has introduced face and vehicle recognition on its high-end products. Huawei is also focused on providing more video analytics functionality and each of these three companies is leading the move into deep learning-based analytics.

Outside of China, Bosch has decided to provide analytics on all but its basic line of camera products and other vendors, such as Avigilon and Hanwha Techwin, have a strong focus on providing video analytics as a differentiator. A number of retail-focused algorithm suppliers have emerged and since been acquired by traditional video surveillance vendors. Examples include Cognimatics, a software company specializing in retail-focused video analytics which was acquired by Axis Communications in 2016; and ShopperTrak, a company specializing in video analytics for retail, which was acquired by Tyco in January 2016. These established companies target retail market which is aligned with their core competences.

It is clear that video analytics are becoming increasingly important to the video surveillance market. Suppliers that can provide well developed, accurate algorithms – alongside a regular update cycle – and support the high compute requirements that these algorithms demand will be well placed to grow their share of the market.

The video analytics market is emerging from a challenging period

Markets for new technologies often follow a recognized pattern of initial growth. This pattern starts with over-enthusiasm and inflated expectations. There may be some successful applications, but there are typically more failures. This is followed by disillusionment as limits to the technology are realized and growth fails to meet expectations. Typical of this stage, is that the technology becomes unfashionable and the press abandon the topic. After this stage of disillusionment, prospects for the market gradually pick up as a more realistic set of expectations are set. The market then enters the final stage of this initial growth phase as the technology becomes increasingly stable and enthusiasm for it returns. Its benefits become widely demonstrated and accepted. This final stage sees second and third generation products enter the market.

The video analytics market has so far followed this pattern closely. Ten years ago there was over-enthusiasm and inflated expectations with suppliers to the market forecasting triple digit growth for many years to come.

Two years later, and a combination of market factors and the global economic downturn lowered expectations significantly. High false alarm rates, difficult installations, and a limited number of successful installations dented growth. There was general disillusionment with the technology. Prospects for the market have picked up since that time and a more realistic set of expectations has generally been set by suppliers.

Furthermore, deep learning and artificial intelligence promise to deliver next generation products with enhanced performance.

Deep learning is the next step for video analytics

Deep learning is a technique for the implementation of machine learning that has existed since the 1980s. A key element that distinguishes deep-learning from traditional computer vision technologies is that it uses artificial neural networks in order to mimic the human brain.

Its algorithms are able to learn from examples and training and then apply that knowledge in interpreting new data, all the while continuing to refine the ability to interpret and infer.

Deep learning appears to be able to offer a level of accuracy and reliability in object classification and face recognition that not only enables video analytics to finally deliver on some of the lofty but as yet unrealized claims made in the past, but pushes capabilities far beyond them.

There are two main areas of benefit to video analytics from deep learning:

Accuracy

A long held complaint levied against traditional video analytics products was that the algorithms were unable to distinguish between objects and behaviors that a human would have no problem classifying. This lack of intuition on the part of computer vision algorithms would often result in missed security breaches or false alarms. The ability of deep learning algorithms to view a scene intuitively, in the same way a human would, means there is a greater potential for object and event detection accuracy, while false alarm rates should decline. This is a significant development for the video analytics industry. Although some end-users may not need an analytics solution that is 100 percent accurate all of the time, many use cases require that the security system be as close to infallible as possible. Users in the critical infrastructure and transportation sectors, for instance, cannot afford to miss a breach in their security; and can spend significant sums of money responding to and investigating false alarms. In many security scenarios, a few percentage points of accuracy can be the difference between a successful video analytic, and the user turning the solution off due to the extra work created from false alarms.

Capability

As discussed, deep learning has the potential to increase the accuracy of object and behavior classification. It also has the potential to improve the effectiveness of the overall analytic solution. The processing and analysis of video footage can be completed in a fraction of the time that previous analytics would require, and at much higher volumes.

Companies like Face++, SenseTime and IronYun, are now marketing analytics that leverage deep learning to turn vast amounts of video footage into usable information quickly. This also includes video processing software with modern user interfaces and natural language search terms to reduce the time it takes to find relevant footage in an archive.

Advanced computing power and big data are the two trends driving the evolution and success of deep learning video surveillance analytics.

1. Computing Power

Deep learning video analytics promise improved performance, but also require significantly higher computational power when compared to traditional video analytics products.

To start with the deep learning model requires a large amount of image samples to do the training. In the past, hardware devices were incapable of processing complex deep learning models with over one hundred layers.

For example, in 2011, Google's DeepMind used 1,000 devices with 16,000 CPUs to simulate a neural network with approximately 1 billion neurons.

Today, only a few GPUs are required to achieve the same sort of computational power. The rapid development of image processing, cloud computing and other high performance hardware platforms have enabled the rise of deep learning analytics.

2. Big Data

As this connectivity increases, network cameras are creating, storing and sharing ever more data. The big data collected through connected cameras can be used to feed the deep learning training models which output much more accurate results and enable the creation of applications to new scenarios.

For example, deep-learning video analytics could be an essential facilitator delivering on the safe city concept. Data generated from the thousands of sensors deployed across a city can be analyzed and assessed to provide predictive analytics. Reliable analytics, that are capable of making inferences on a more abstract level than tradition machine vision algorithms, in a wider variety of weather conditions, will be essential to reduce false alarms and hence the number of operators required to monitor video feeds.

A key element of the safe city concept is the integrated system operating efficiently and in real time, with much of the process being automated. Deep learning has a significant part to play in this evolution.

Apart from deep learning and artificial intelligence, other future trends which are likely to impact the video analytics market include:

- Use the cloud to run video analytics. This allows users to take advantage of the large virtualized processing power available to them.
- Make use of increased processing power in cameras. In some cases, this is enabling algorithms to be entirely embedded in cameras. In other cases, this increased processing power is being used to relieve data stream workload and save back-end computation capacity.
- Make video footage easier to search through. In the same way that search engines created mass appeal for the internet, searchable analytics is making it quicker, easier and more cost-effective to find the correct frames of video surveillance.

From AI edge to AI cloud

Increasingly, a hybrid approach is being developed where analytics workloads are more distributed using a mix of smart cameras at the edge combined with centralized servers and cloud based analysis. This means some analytics can be run at the camera, for example crowd monitoring, counting and object detection with the aim of saving bandwidth and relieving the computing capacity at backend. More powerful centralized analytics could be used to run processor intensive applications such as feature extractions of human / vehicle and object searching. This approach has gained particular interest in the Chinese market, where AI deployments have been greatest and where projects are large and can benefit from the distribution of compute and analytics most.

Video analytics software can either be priced independently as a distinct purchasable product or embedded on a piece of video surveillance equipment, prior to reaching the end-user.

*Supply of the first type is fragmented with the top ten vendors accounting for just over **60%** of global revenues in 2016 and no individual vendor having a market share greater than **14%.** There are also many small vendors with a share of this market.*

When it comes to the second type, many video surveillance equipment vendors now embed video analytics software in their equipment. Often, there is no separate price for the video analytics software, it is simply included in the price of the equipment. In fact, some vendors now sell only devices with embedded analytics software.

Of the world's five largest vendors of network surveillance cameras, all five of them offer cameras with embedded analytics.

Large equipment vendors and small ISVs (Independent Software Vendors) both supply the market

Related to this, next generation video analytics using deep learning technology is now being introduced. Some big vendors develop the algorithms by themselves while the middle to smaller video surveillance vendors can embed the deep learning video analytics software from ISVs. At the other end of the channel, data center providers are facilitating small ISVs (Independent Software Vendors) with the technology and processing required to develop algorithms. This could be an important step for the competitive market as it will help smaller companies to catch up as they only need a few developers on staff to work with deep learning solutions. While they will need to partner with larger equipment vendors, this will also provide routes to market for those vendors that have not started to develop analytics in-house.

In the competitive video analytics market, the advantages of established equipment vendors include mature sales channels, vertical-focused know-how and big data collected from a range of verticals. By leveraging these advantages, large equipment vendors tend to offer bundled sales of hardware and software (OEM or branded) to end users. However, the ISVs are often faster to upgrade their algorithms and can be more competitive in innovative product releases.

System integrators and end users are seeking ways to combine best in class video analytics software with reliable video surveillance equipment. The challenge is to decouple the software and hardware so that the integrators and end users can freely choose the established hardware combined with advanced software which could be provided by a less well-known brand. Therefore, open platforms which have the compatibility across different video analytics software, independent from the hardware infrastructure, will be an increasing trend in the video surveillance ecosystem.

IHS Markit estimates that City Surveillance is the largest end user market for total video surveillance revenues with an **11.5%** share. City surveillance is also the fastest growing end user segment with CAGR of **11%** from 2016 to 2021.

Cloud for cities surveillance

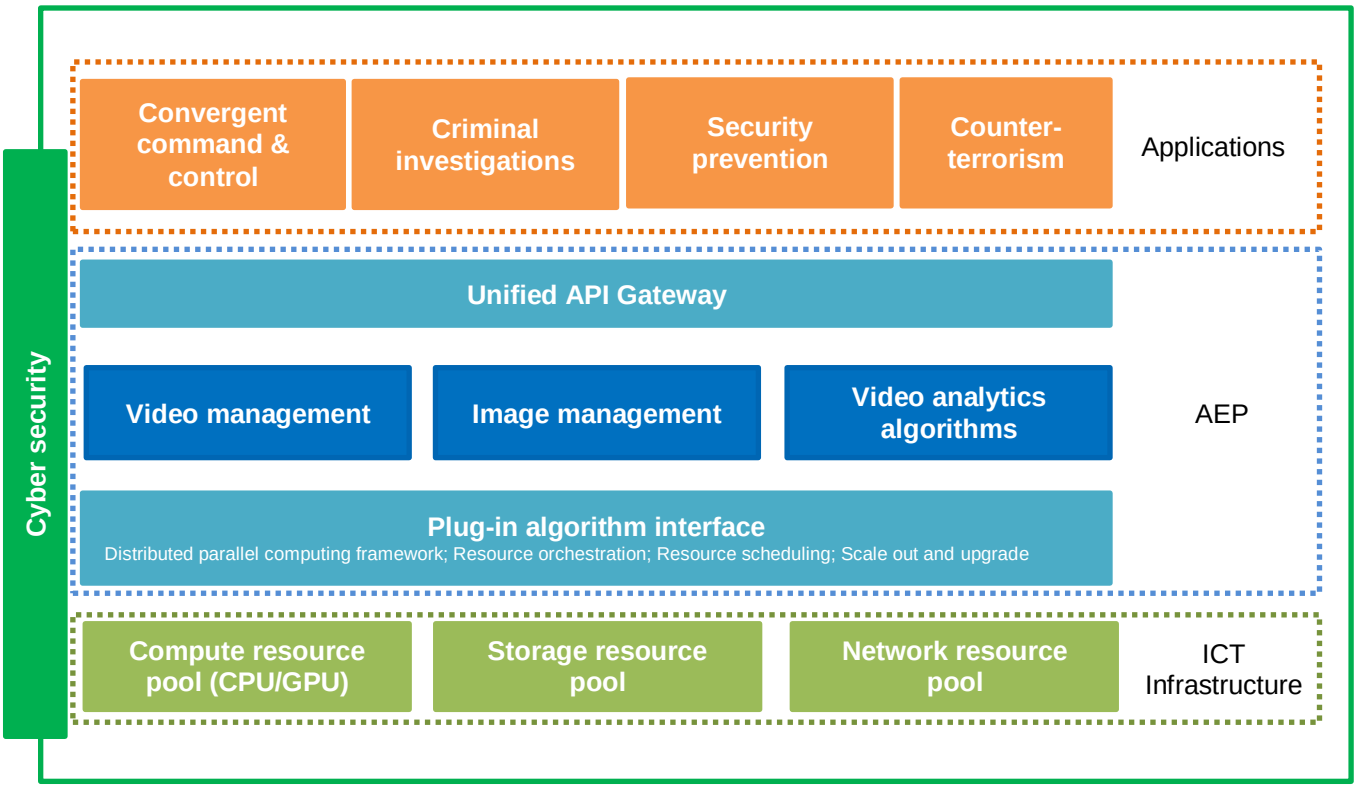
Cloud architecture is already widely used in many industries. It is also being gradually adopted in the video surveillance applied in safe cities. With the number of installed video surveillance cameras constantly increasing in cities, it is important to intelligently manage the footage they generate.

Chart 1 (next page), provides a high-level cloud architecture for city surveillance as well as large scale projects.

The chart refers to the differentiated features and functionality that the application developer creates using the functions of the Application Enablement Platforms (AEPs), integrated with API (Application Programming Interface) Gateway. Essentially, this cloud architecture (some combination of AEP, typically along with cloud hosting, cybersecurity, and professional services from various vendors and providers), provides the application developer with pre-made capabilities to manage needs that are common to video surveillance-focused applications. The application developer can then focus development effort and investment on those areas that are unique to their application. **The core purpose of AEP platform is to enable device management, data management, and facilitate application development.**

ICT infrastructure is the foundation of the cloud architecture. It provides computing and storage resources, together with the ICT management software.

Chart 1: Cloud architecture for city surveillance



The cloud architecture can provide a useful solution for doing this in a number of ways.

- The cloud architecture can be used to have video data shared across a wide geography and the hierarchy of public agencies which used to be isolated from one another. For example, with the cloud architecture, the police department can use shared video surveillance data captured by cameras installed in different provinces to chase down a suspect who runs across these provinces.
- The cloud architecture is able to reduce repeat ICT construction with unified platform serving different agencies. Resources can be managed more efficiently and can be flexibly assigned based on the demands of tasks.
- The cloud architecture is designed to provide an open AEP which provides more options to system integrators and end users. In traditional city surveillance projects, some major vendors tend to pre-embed the video management software and video analytics software in the hardware as a bundle sale to the system integrator or end users. If the end users want to change the algorithms, they have to change the entire system. In a world where technology and features change quickly, this approach is not practical because it limits an end user's ability to try new technology and requires a substantial financial commitment to specific manufacturers and proprietary interfaces. The AEP is able to integrate various software and data source by decoupling software from hardware and metadata from applications, so the end users can easily upgrade or replace the applications or algorithms.

Connectivity

Connectivity enables the creation of complex information systems which are greater than the sum of the individual components. There has been a gradual trend from analog to network video surveillance cameras during the last decade and this trend is forecast to continue. With more network cameras connected to the internet, the ability to network and manage these devices will become more important.

The network camera market has been enjoying a high growth rate with a CAGR of **65.7%** from 2013 to 2016 in terms of shipments. In China, it is estimated that there are **66.5** million network cameras installed as of the end of 2016.

The benefits of connectivity:

- Connectivity enables the video surveillance data be accessed directly, or via the cloud, and enables data sharing across geographies and entities.
- Connectivity enables remote viewing on laptops, tablets and mobile handsets and has become an important feature as security managers responsible for many sites demand immediate access to their video images, often from remote locations.
- Unique scenario-based solutions could be created through the application of complex analytics and big data collected from a number of connected video surveillance cameras in large projects.

Connectivity also brings challenges to video surveillance suppliers:

- It requires the unified communications protocols between different physical security and video systems. Industry alliances are expected to take the initiatives in promoting the standards and protocols (e.g. GB/T28181, Profile S by ONVIF and SIP) to drive the realization of connectivity.
- It requires the capability to minimize the latency of data transmission in a remote distance, which is an important factor to users' satisfactions.
- It requires network infrastructure to manage more connected devices and systems. For example, for a province level of city surveillance project in China, the video surveillance solution is required to connect 10 million scaled surveillance cameras with various protocols. In some projects, the end users will require the integration of video surveillance system and video conference system.

This means:

- Suppliers with capabilities in networking large scaled devices and integrating heterogeneous platforms will be more competitive.
- Device suppliers need to understand the networking side of the market and ensure they meet any obligations related to the security of the network.

Other technology trends

Cybersecurity and product hardening remains a challenge

The cybersecurity of IoT devices, video surveillance cameras and associated networked systems has become increasingly important. Networked devices are at risk of being "hacked". Hacking through networked video surveillance equipment has generally been to gain access to other parts of networks (rather than to view or manipulate video surveillance live feeds or recorded footage).

There have been a number of recent high profile cyber-attacks through installed video surveillance equipment. These have included DDoS (distributed denial of service) attacks taking some of the world's most popular websites offline and the Washington DC police surveillance system being hacked with ransomware shortly before President Trump's inauguration.

Many of the initial vulnerabilities could be characterized by poor practice of password protection by manufacturers and/or installers. Examples of this include device firmware which does not require passwords to be changed upon installation, or firmware which does not sufficiently hide passwords.

No product can be 100% cyber-secure; but it is important for manufacturers to take a more active approach to cybersecurity.

Some examples of active approaches to cyber security include:

- A pre-defined process in dealing with and responding to identified vulnerabilities.
- Effective vulnerability notifications and software patch delivery.
- Offering advice on best practices to installers/integrators (many vendors have produced cybersecurity hardening guides).
- Camera product features related to cybersecurity include encryption at the camera and certification by third parties.

Semiconductor developments are driving many video surveillance trends

Many video surveillance equipment manufacturers are developing equipment to use the next generation of compression codecs. Cameras with enhanced versions of H.264 are already common. However, H.265 or High Efficiency Video Coding (HEVC), is also starting to be used. HEVC is approved as a standard by the International Telecommunications Union (ITU-T) and compared with first generation H.264, HEVC has the potential to use 30–40% less bandwidth for a video stream of the same quality.

Similarly, developments in CMOS image sensor technology have helped facilitate many of the improvements in video surveillance image quality such as higher resolution, advanced low light functionality, and wide dynamic range. Suppliers of image sensors for the video surveillance market include PIXELPLUS and Sony Imaging.

The emerging deep learning market is also being built on semiconductor developments. The high rate of image calculations required in deep learning training and inference algorithms is well suited to GPUs (Graphics Processing Units) and NVIDIA has been active in working with video surveillance vendors to develop these solutions. Likewise, Movidius, acquired by Intel, can provide similar functionality on the security camera, albeit with less processing power. These technologies will support the increased deployment of improved video analytics in the surveillance market.

The competitive eco-system is evolving

As the video surveillance market evolves, embracing video analytics, deep learning and cloud-based solutions, the cloud-based video surveillance eco-system is being created with new entrants and incumbent suppliers all competing for business.

Facing a number of vendors with differing offerings, end users often look for a unified and open platform which is able to integrate different software and ensure processed data is accessible to all application software.

Benefits of an open platform in the ecosystem:

- Smaller software vendors will likely find open platforms the most beneficial because they essentially level the playing field between large and small vendors. This can eliminate the need for proprietary protocols between suppliers for communications between different components of a system.
- End users don't need to buy solutions with bundled sales. For example, end user can choose specialized, high-end computing servers from one manufacturer to use with a deep learning algorithm that is perhaps lesser known, but that provides what the end user needs when it comes to management and reporting.

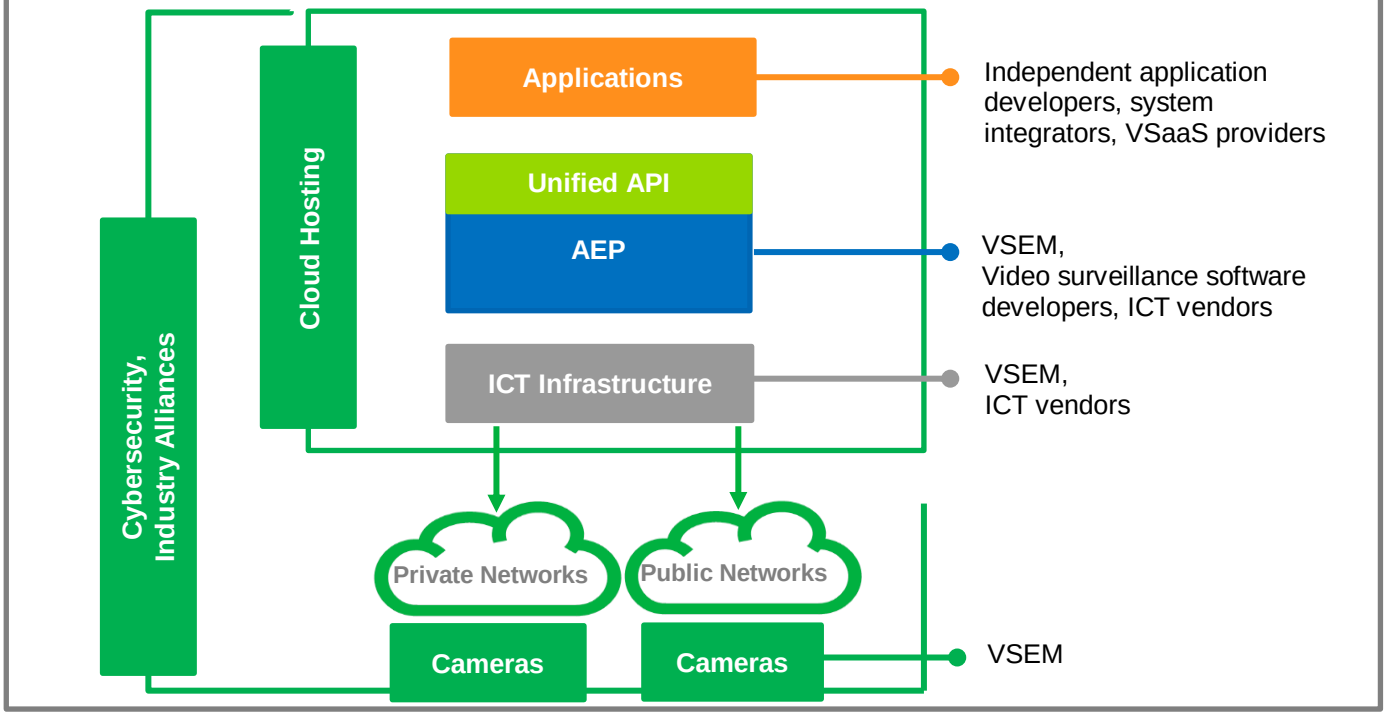
Chart 2 (next page) provides a high-level structure of the cloud based video surveillance ecosystem in enabling video surveillance applications.

This ecosystem framework corresponds to the cloud architecture displayed in "Cloud for cities surveillance". However, this framework highlights the participants across the ecosystem.

The participants include:

- Applications: independent application developers, system integrators and providers of Video Surveillance as a Service.
- AEP: video surveillance equipment manufacturers (VSEM), video surveillance software developers and ICT vendors
- ICT Infrastructure: ICT vendors and VSEM

Chart 2: Cloud-based video surveillance ecosystem



Video surveillance equipment manufacturers (VSEM)

These organizations develop and produce equipment used for video surveillance applications. This includes security cameras, recorders, encoders, controllers and keyboards, housings and security camera mounts. Most video surveillance equipment manufacturers now offer cameras and/or recorders with embedded video analytics. A limited number of them have started to offer these products with deep learning based video analytics. The success of deep learning technology will be ultimately driven by how some of these leading suppliers meet market expectations, both in terms of the quality of the analytic and the price that can be achieved.

Some video surveillance equipment manufacturers also actively participate in the VSaaS (Video Surveillance as a Service) and cloud markets. One challenge that faces video surveillance equipment manufacturers is the relative unfamiliarity of the recurring monthly revenue (RMR) business model associated with the VSaaS market. Another is the ICT knowledge that leveraging cloud architecture requires. Another trend is that some VSEMs start to offer ICT equipment due to the increasing demands of ICT products for video surveillance use from large scale projects. However, participants in this group are motivated by the prospect of increasing hardware sales. They are also motivated by a desire to maintain access to the total addressable market for video surveillance equipment.

Video surveillance software developers

Software used in video surveillance applications includes: video management software (VMS), video content analysis (VCA), physical security information management (PSIM), and software used by central monitoring stations (CMS).

The VSaaS and cloud user interface and the VMS user interface are very similar. Also, most VMS solutions provide free remote access via an internet-connected device. Some VMS software developers already offer VSaaS solutions. One example is Genetec, a VMS developer that launched a VSaaS solution in partnership with Microsoft. More recently, one of Genetec's main competitors, Milestone, announced that it would launch an enterprise-class VSaaS solution called Arcus Global. These companies are well placed to benefit from the market moving to a SaaS (Software as a Service) model and the emerging trend of deep learning video analytics, even if it is primarily through partnerships.

Independent application developers and system integrators

Both video surveillance application developers and system integrators could provide application software. Independent application developers only provide application software with focus on some verticals. Apart from application software, system integrators also provide consulting services, equipment and installation services. However, lack of IT knowledge can be a barrier for some traditional security systems integrators. The ability to work with ICT equipment and infrastructure will be increasingly valuable to these companies as the network complexity advances; those that do not keep up will likely lose market share to dedicated application developers.

ICT vendors

With more and more large-scale video surveillance projects such as safe city projects in place, ICT infrastructure is gaining more weight in project implementation. ICT vendors with video surveillance tailored solutions are well placed to support many of the new trends driving video surveillance. It is also observed that some ICT vendors are moving up to provide AEPs which in most cases are pre-embedded in ICT equipment. The capability to provide an open platform which enables big data analysis technology and connectivity with thousands of cameras will be a factor in their success.

The bottom line

The video surveillance market is becoming increasingly intertwined with other industries. Where there was dedicated security distributors and integrators, now there is ICT and telecoms suppliers competing for business. Where there was traditional analog cabling between devices, now there is advanced ICT infrastructure integrating numerous IoT devices across the network.

Fundamentally, companies which embrace emerging technology, especially in the video analytics market, and develop leading infrastructure and networking skill-sets, will be well placed to win business as the video surveillance market continues its evolution to greater networks, better technology, and higher quality solutions.