IHS **Technology**

September 2014

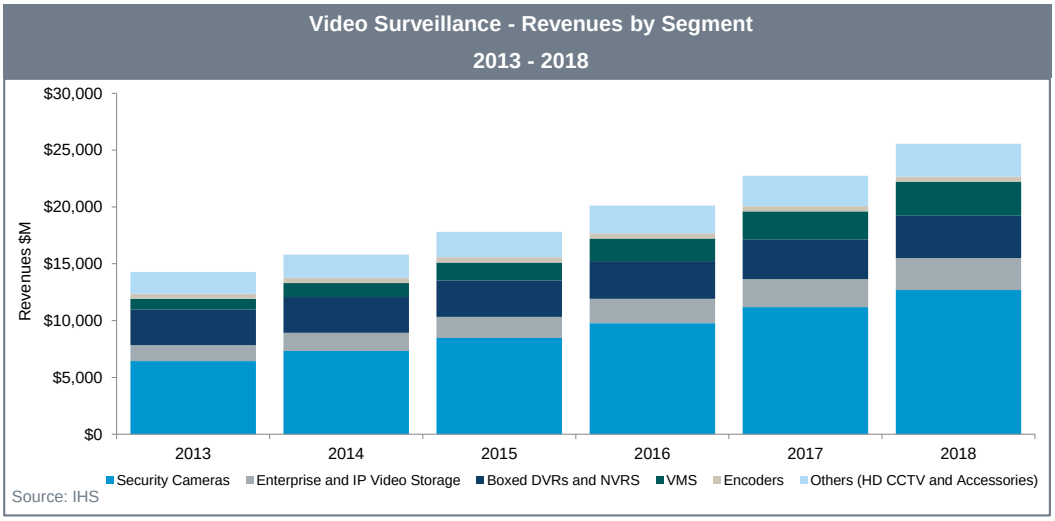
Video Surveillance & Storage

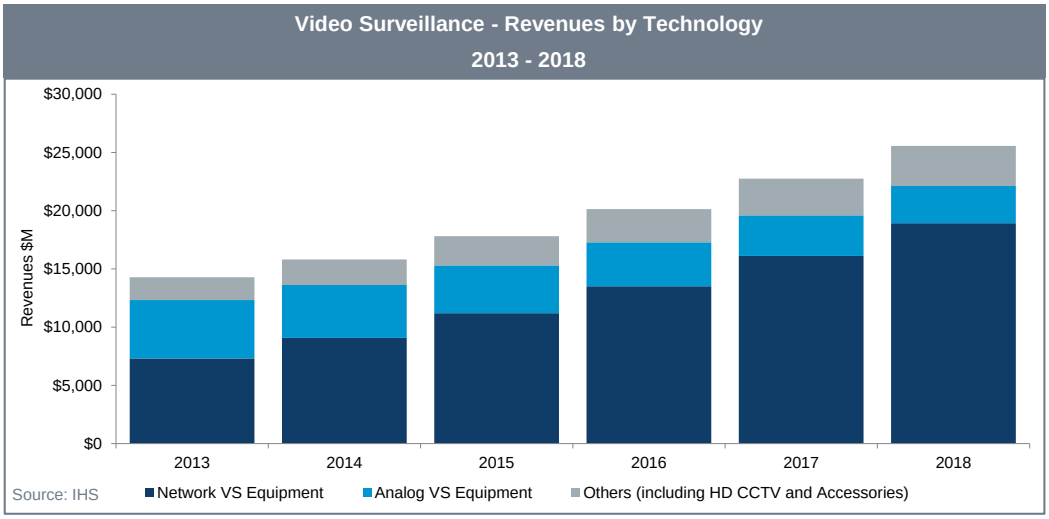
Opportunities at the Intersection of IT & Physical Security

Optimizing Performance for Video Surveillance Storage

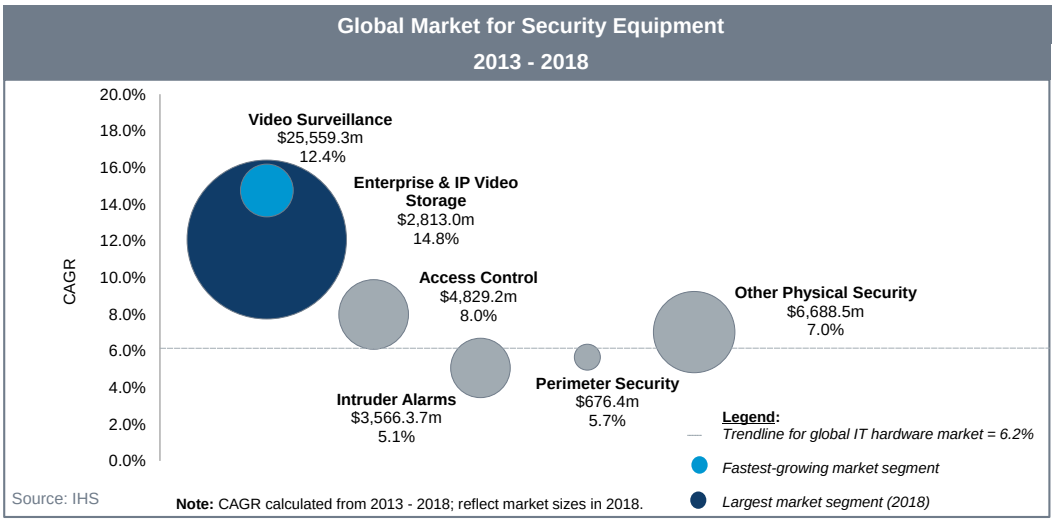
Protecting people, property, and other assets is a serious business. This fact can cause the physical security industry to take a conservative stance when it comes to adopting new technologies. In many cases, the security market will, in effect, follow in the footsteps of others—often the defense or IT industries—only after a product or technology has proven itself to be both effective and reliable. While this can cause frustration for technology companies hoping to penetrate the space, ***it can also mean that when other markets begin to flag, security is poised for growth***.

This phenomenon is currently taking place in the world market for video surveillance solutions, where the wider trends of digitization and IP-enablement are just now reaching critical mass. This has caused robust growth in recent years, which is forecast to continue at rate of 12.4% per annum to $25.6 billion in 2018. It has also created significant opportunities for IT providers, even as the greater market for IT spending has moderated.





Video is of course one of the most storage-intensive application workloads around. Thus, as high definition, megapixel network cameras have declined in price and begun to proliferate, the need for reliable and scalable storage space has risen in-kind. As a result, the market for enterprise storage solutions in security is forecast to grow by a 14.8% compound annual growth rate (CAGR) over the next five years; the market for IT hardware is slated to grow by a more modest CAGR of 6.2% during this time.

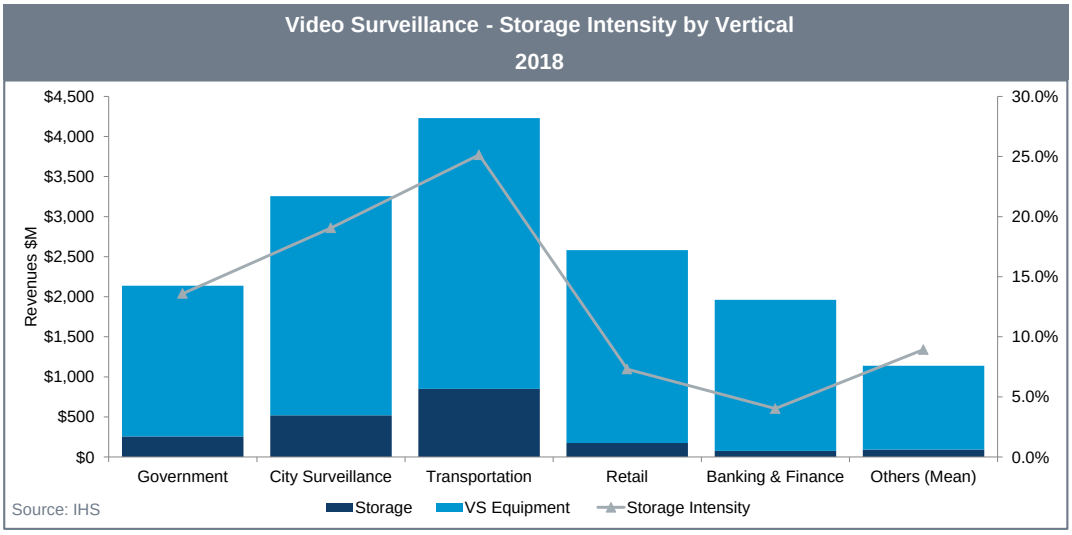


Storage Intensity by Vertical

While there is much opportunity for leading IT vendors in video surveillance, it is greatly concentrated within a handful of vertical segments. As recent research from IHS Technology has revealed, there are striking differences in the degree to which various end-users of video surveillance systems rely on storage solutions. These differences are captured in the relative *storage intensity* ratios of each vertical; i.e. the amount each spends on enterprise storage compared with that for all video surveillance equipment. Of the 17 end-user verticals analyzed, IHS forecast that three in particular—Government, City Surveillance, and Transportation—will account for 58% of all storage expenditures in 2018. Furthermore, these three key verticals will exhibit storage intensity ratios of between 13.6% (Government) and 25.1% (Transportation), while the average for the market is projected to be 8.9%.

"Of the 17 end-user verticals analyzed, IHS forecast that three in particular—Government, City Surveillance, and Transportation—will account for 58% of all storage expenditures in 2018."

- IHS Technology



The differences in storage intensity can be explained by the uniquely rigorous requirements for enterprise-class features and functions found in these three verticals. Surveillance systems in these settings are typically very large and complex. They may include hundreds or even thousands of cameras ("edge devices" or "edges") dispersed over vast distances, and connected via secure IP networks. The underlying assets being safeguarded, whether they are high profile government buildings, densely populated urban corridors, or critical transportation networks, may be considered high-risk targets for terrorist acts. Increasingly, the risks posed by natural disasters are also driving purchases. As a result, video data is regarded as a treasure trove of information that can be utilized—both in real-time and after-the-fact—for the purposes of situational awareness, predictive analysis, and forensic investigation.

For these reasons, the data is typically stored for much longer periods of time than in more commercial applications such as retail or banking. Average retention times may also increase during periods of heightened threat. Likewise, rigorous measures are taken to ensure the integrity and security of the underlying data. Because of the sensitivity and importance of the data, end-users tend to prefer that it be kept on-premise (though they may want the flexibility to move it off-site at a later time). Even more so, it is critical that the entire infrastructure upon which the security system is built be both open and flexible. A prime example of this is scale-out storage, which allows the entire system to be expanded or contracted as needed and without disruption to daily operations.

Of the three verticals where data storage is critical, video content analysis (VCA) is particularly well suited for transportation. In these settings, a team of operators will typically monitor video streams from hundreds of cameras, and any automation of the system (e.g. using incident detection, motion detection, or facial recognition software) has the potential to reduce operational costs significantly. In other words, while there is a limit to the number of cameras that a human operator can effectively monitor, this number can be augmented by employing analytics software. For these reasons, VCA projects can be found in many high profile transportation projects around the world including JFK airport in New York, the Port of Singapore, and the Beijing metro system in China.

Lastly, and in marked contrast to most other verticals, the effectiveness and reliability of equipment will often trump considerations of its price for government and transportation buyers. This is not to say that tenders and competitive pressures are not present here—they are quite prevalent and extensive in fact. But on the whole, there is simply a greater willingness and ability of this group to pay up for performance. This speaks to the availability of capital to fund these purchases, as well as the gravity of potential consequences from system downtime. It is also worth noting that with physical security in particular, the issue of system malfunction is not limited to the failure to detect threats. To be sure, systems that generate repeated false alarms can be just as dangerous if they come to be ignored altogether.

Edge-to-Core Architecture

The migration from analog to network surveillance cameras has caused parallel changes in the system architectures that underpin them. Historically, analog cameras have been used mostly in centralized, *core* deployments; the distance between camera nodes in a given system was constrained by the scalability of the underlying infrastructure. With IP network cameras, core architectures continue to be used in situations that call for them, e.g. in airports, but are now noted for their performance, scalability, and ease of management. It is also possible to build distributed, *edge* systems with vast distances between cameras. Edge systems are characterized by their relatively low-cost, simplicity, and ability to plug-and-play. Furthermore, an *edge-to-core* model has evolved to address the multifaceted needs that are common in government, city surveillance, and transportation. These systems are highly distributed, and often have high channel and camera counts. The edges are managed via a core deployment that enables data movement to and from the core, provides overall system status, and acts as a repository for data mining and analytics.

"The transition of the video surveillance market from analog to network systems has caused a convergence of the IT and physical security sectors. This has in turn led to pronounced changes in the way that way that security projects are conceived, built, and managed."

- IHS Technology

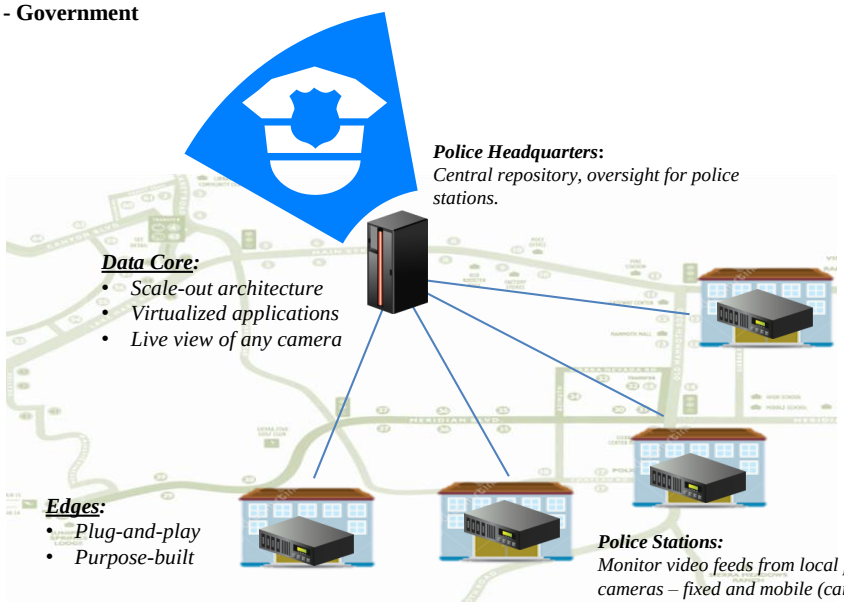
A key advantage of incorporating a data core into a distributed system is the ability to perform powerful, data-heavy VCA applications that are impractical to run downstream. The data core also allows system operators to assess event patterns that might be unfolding across multiple cameras deployed in positions throughout the surveillance system network. These capabilities are increasingly important given the rise in VCA applications being used to parse video data for elusive insights—often on a streaming, real-time basis. Though still nascent, this segment of the video market has drawn tremendous interest from governments, law enforcement agencies, and investment groups alike, and it is growing rapidly. Some of the most successful applications to date include license plate recognition (LPR), facial recognition, intelligent scene analysis, population and traffic counts, and a host of business intelligence (BI) applications. While edge analytics—at the level of the camera, encoder, or record—have become more cost-effective and prevalent, they are still limited to more simplistic algorithms, and to filtering functions designed to manage upstream data transmission.

Another advantage of having an integrated data core is the ability to employ virtualized platforms for compute and storage. Virtualization can provide significant reductions in the total cost of

ownership (TCO) for compute and storage resources as less hardware is required to perform multiple roles in a system. Virtualization also enables streamlined consolidation and scalability as the surveillance system grows or is otherwise modified.

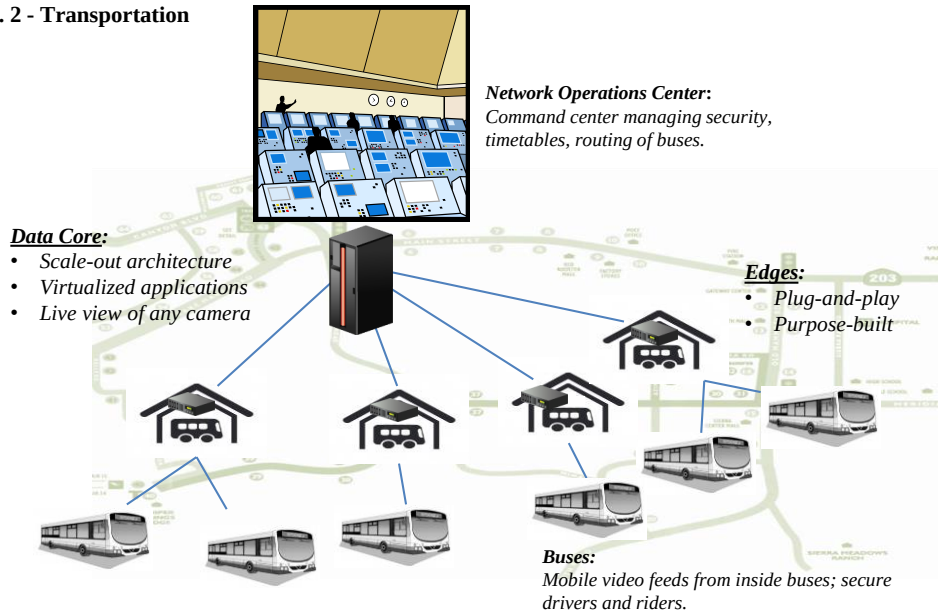
Edge-to-Core Deployment:

Ex. 1 - Government



Edge-to-Core Deployment:

Ex. 2 - Transportation



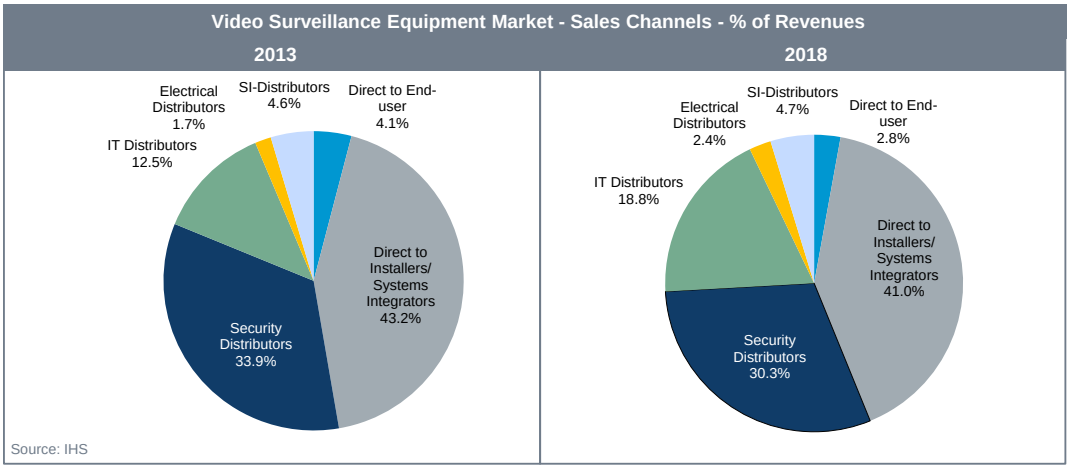
As seasoned end-users and systems integrators will attest, the process of building-out an enterprise security system is ongoing. For this reason, it is important that the underlying infrastructure on which it is built be simultaneously open, flexible, and cost-effective. As customers look to integrate disparate system components (e.g. video surveillance, access control, intrusion detection, etc.) into a single, "system of systems," these considerations become critical. This trend is being led by the adoption of Physical Security Information Management (PSIM) systems in the enterprise security segment. PSIM provide users with a single application in which to interface, visualize, automate, and audit all the physical security systems that might protect a given asset.

The general trend to merge disparate systems and share data has been accelerated by the desire of organizations to leverage security data for business purposes. For example, retailers are using video obtained from their security cameras to optimize staffing and inventory decisions, reduce theft, and mitigate risk from accident-related lawsuits. Interestingly, alternative applications such as these tend to cause organizations to extend the time they retain video surveillance footage. The net effect of these developments is an increase in the need for storage space by end-users. In other words, as the perceived value of video data increases, this leads to a corresponding increase in the demand for storage space.

The Convergence of IT and Physical Security

The transition of the video surveillance market from analog to network cameras has caused a convergence of the IT and physical security sectors. This has in turn led to pronounced changes in the way that security projects are conceived, built, and managed. From the standpoint of security end-users, internal IT personnel have gained significant influence when it comes to the procurement and, in many cases, the day-to-day oversight of surveillance technologies. They have also helped to accelerate the adoption of IT best practices by security personnel—not the least of which has been the virtualization of storage infrastructure.

On the supply side, IT integrators are gaining a growing share of the video surveillance market, especially within the most storage-intensive verticals. They are undertaking these projects both as sub-contractors to physical security integrators, and increasingly, as direct contractors themselves. What is particularly interesting is the degree of interdependence that has developed between both IT and physical security integrators. As technology, and security practices grow increasingly specialized, a knowledge gap has emerged at the intersection of these two disciplines. There is a scarcity of professionals with robust experience in both these domains, and as a result, IT and physical security integrators have found it beneficial to partner with one another in order to bridge this gap. This phenomenon can currently be observed in even the largest and most established professional service practices for both IT and security firms.



A further effect of the convergence between security and IT markets has been the growing importance of product certifications and validations to the systems integration community. Certifications are not as widely used in the security industry as in IT. However, as systems have grown increasingly large and complex—particularly among government and government-related end-users—the risks associated with incorporating an unknown or unproven product into a project have grown in parallel. Consequently, integrators have become highly selective in determining which vendors and products in which to work with. When evaluating new products, they tend to rely on manufacturers and/or third parties to perform rigorous and large scale testing. The joint testing of systems is also preferred–especially as it relates to the interoperability of systems—and helps to reduce the time-to-market for SIs.

The previous points notwithstanding, the physical security industry has significantly lagged the IT sector when it comes to the testing and certification of products such as cameras and VMS. This may be due in part to the fragmentation of the security market; many different products would need to be certified, which is to say that the cost to manufacturers, integrators, and end-users could

"As systems have grown increasingly large and complex—particularly among government and government-related end-users—the risks associated with incorporating an unknown or unproven product into a project have grown in parallel."

- IHS Technology

be prohibitively high. That said, end-users are demanding open APIs to allow systems to be integrated seamlessly with best-of-breed components. This has given rise to standards-based alliances for product interoperability, including the Open Network Video Interface Forum (ONVIF) and the Physical Security Interoperability Alliance (PSIA).

Movement to Lifecycle Budgeting

While they acknowledged the need for it, many organizations have historically viewed the purchase of security equipment begrudgingly. For that reason, the same end-users were likely to handle system and component upgrades on ad hoc basis. This "rip and replace" mentality involves minimal anticipatory planning and coordination, and can result in higher overall capital expenditures than would be warranted under a more thoughtful, regimented approach. It is analogous to the "break-fix" model that characterized the IT industry prior to the development of managed services.

But as IT systems and practices become more embedded within the security industry, it is causing end-users to grow increasingly conscious of the return on investment (ROI) and total cost of ownership (TCO) implicit in their security systems. This is in contrast to simply looking at the initial cost to procure the equipment. Recently then, security departments have begun to move toward the type of lifecycle model to systems procurement and management that is espoused by their counterparts in IT. This movement is being led by the storage-intensive verticals, and entails practices such as the usage of enterprise-class hardware, the development of system roadmaps, and regular performance refresh planning.

"Recently…security departments have begun to move toward the type of lifecycle model to systems procurement and management that is espoused by their counterparts in IT."

- IHS Technology

A further consequence of lifecycle planning by security end-users has been their migration away from the "appliance model" of purchasing. That is to say that instead of looking to buy entire solutions from one provider (e.g. cameras, VMS, encoders, storage, etc.) they will source best-of-breed components from multiple vendors. Diversifying in this way allows them to avoid the need for costly rip and replace upgrades as well as unfavorable service contracts tied to proprietary equipment. Last but not least, it underscores the need to build their systems atop an open, flexible architecture that will accommodate the equipment upgrades and change-outs that will inevitably follow.

Conclusion

The widespread adoption of network cameras in the video surveillance market has accelerated its convergence with the IT industry, and ushered in a period of robust expansion. This has caused a surge in demand for enterprise storage solutions, particularly for the storage-intensive verticals of Government, City Surveillance, and Transportation. Surveillance systems in these settings require a new form of open, flexible infrastructure to operate successfully. This infrastructure is increasingly being built upon an edge-to-core architecture that combines centralized storage and compute capabilities with distributed video feeds. In order to address these requirements, a major shift is taking place in the way that security systems are designed and built. It has caused systems integrators to rely heavily on manufacturers for guidance and product certifications. These collective changes have, and will continue to create unprecedented opportunities for both physical security and IT providers to grow rapidly in the years to come.

Further Information

For further information pertaining to this topic, please contact Niall Jenkins, Research Manager, Video Surveillance & Security Services at +44 1933 402255 or niall.jenkins@ihs.com.