

TIME TO SWITCH

Luke Harley examines the advantages in making the move to IP: the evolution of video surveillance

In today's increasingly uncertain world, video surveillance has become essential to monitor security threats, deter theft and protect our homes, workplaces and more. The global video surveillance market is expanding so fast that according to a study carried out by Research and Markets, it is expected to grow at a rate of 15.4 percent, reaching \$106.98-billion by 2026.

But the days of slow, clunky and blurry CCTV are long gone. It's no surprise that security cameras have advanced in line with the latest developments

in technology. As our lives and our workplaces become more digitised than ever, the need for advanced digital security has led to greater demand for more sophisticated network cameras. It's been 23 years since the launch of the first-ever network-capable surveillance camera and we've now reached a tipping point. Today, Internet Protocol (IP) cameras make up around two-thirds of the total security camera market. Given that consumers can now pick up IP home security camera devices like Ring and Blink on the high street, it's time for network installers and system integrators to embrace the future of IP surveillance.



Internet Protocol cameras now make up around two-thirds of the total security camera market

During the initial phase of surveillance technology, analogue cameras were used. However, the market is witnessing a change with many people shifting from CCTV to IP surveillance cameras as a more advanced security solution. This evolution is driven by factors such as increased safety, time, cost efficiency and convenience for the end user.

FLEXIBLE FRIEND

IP surveillance is flexible and can be used in a number of different settings, such as banks, shops, offices and other public areas. In fact, video surveillance has been an essential tool for retailers, primarily used to monitor physical security threats and deter theft. Meanwhile the technology has steadily progressed to reveal new possibilities. The rise of cloud computing, the Internet of Things (IoT) and Artificial Intelligence (AI) has transformed an IP video camera from a security tool to a business opportunity that can provide much more than protection against crime, with real-time insights into retail store activity and footfall.

Video surveillance can help to increase profitability and gain advantage over competitors in retail by providing previously unreachable insights into customers' behaviour and the effectiveness of in-store marketing activities. Understanding the way shoppers behave in-store can be leveraged to identify and fix operational issues, such as congested fitting rooms or poor floor layout. In the long-term this can help significantly improve customer experiences.

It is in the best interest of any business in need of surveillance to implement IP technology as it can be combined with other tech for advanced processing and insight, while also providing high levels of security for the business premises. To truly unlock these benefits and ensure ideal performance of video monitoring and quality footage, businesses first need to establish a strong network that will provide the required connectivity, security and bandwidth optimisation.

The new power-over-ethernet (PoE) surveillance cameras offer the next generation of security features including HD image quality – even in low light – the ability to pan, tilt and zoom and store archive footage without the need for a stockroom's worth of tapes. In addition, the installation and maintenance of traditional cameras can often be a complicated process that requires separate cabling for both power and data, driving up costs. However, Power-over-Ethernet (PoE) cabling simplifies IP camera installation with both power and data carried over a standard network cable.

With IP surveillance cameras, smart analytics and alerts can be sent straight to the user's smartphone, making businesses aware of any unusual activity or motion, so they don't always need to pay for a large-scale security team to watch the footage. Some cameras even offer object recognition – so the system can determine between a potential burglar or a stray cat passing the camera.

But what happens if something goes wrong with the surveillance network? Organisations are no longer comfortable shutting down their whole system to repair a fault with a camera or to carry out updates on software. Being able to work on the network, without having any fear of turning off the cameras is now an expectation not a 'nice-to-have', from small offices to campus-wide settings.

The easiest way to monitor this is with the addition of IP surveillance-specific network switches, making it easy to maintain surveillance networks without extensive support teams. Such switches can monitor each camera's status, auto-reboot any third-party camera or install upgrades without cutting power to the cameras or system.

Through the use of smart switches, an operator can manually control the camera at anytime from anywhere on the network. The operator doesn't need to be in the same location as the camera, or in the same room as the PoE switch, therefore helping to save both time and money. IP surveillance technology allows users to view cameras live and monitor and review recorded video footage from any remote device such as a laptop, smartphone or tablet.

NETWORK SWITCHES CAN INSTALL UPGRADES WITHOUT CUTTING POWER TO THE CAMERAS OR SYSTEM

IP networks also integrate many features such as facial recognition, motion detection and low-light or night vision. This information is backed up using cloud-based storage to protect mission-critical data and prevent data loss. A network management system can monitor all networked devices – including cameras, switches, access points and storage devices – and automatically generate alerts or notifications if issues are detected.

But, as much as IP surveillance cameras make the security process easier, faster and more reliable, they are not without their challenges. As these new camera devices get more complex, they need more power. This can start to challenge the boundaries of normal Ethernet cabling, which usually has a 100m range. To extend this, installers would traditionally add a booster to the camera network because the further away from the power source, the less power a network will have. But in a large enterprise building or a hotel resort, for example, system integrators prefer longer reach networks without adding additional equipment.

To counteract this, IP surveillance switches, which offer the flexibility of PoE power ranges without having to install electrical cabling, are beneficial. These provide a far longer 250m-range support for PoE devices and the ability to scale from 15.4W power (802.3af), to 30W power (802.3at) and even up to 100W (802.3bt), providing flexibility for a range of devices. This reduces costs to the installer and offers greater power to handle pan, tilt and zoom cameras or the next generation of devices.

Given the quality and size of HD footage, data storage is another big issue. The advancement in IP technology has meant security teams are often streaming large file-size images from multiple security cameras across a shopping mall or office building. Retailers and banks can store footage for up to six months to monitor archive footage. Yet inadequate storage can leave a system unfit for purpose and can ultimately restrict users from reaping the benefits of new technologies.

To prevent issues with data storage, security installers should make sure they implement a surveillance infrastructure based on switches capable of parsing a high bandwidth, that will migrate all footage to the cloud. With the recent advances in cloud technologies, cloud storage solutions allow security teams to remove the need for costly dedicated on-site servers and IT maintenance. By moving security footage to the cloud, disaster recovery, automatic backup and software updates

THE RAPID RISE OF AI HAS TRANSFORMED IP CAMERAS FROM A SECURITY TOOL TO A BUSINESS OPPORTUNITY

can be managed across the whole network remotely. This is particularly beneficial as it allows any camera errors or glitches to be registered and fixed remotely, while also enabling the problem to be resolved quickly to prevent outages. Additionally, by running software updates while the camera is recording, users are able to avoid any gaps in footage.

Cybersecurity has become a growing concern for many consumers and companies in every sector, and the surveillance industry is no exception. There is growing concern among many enterprises around IP surveillance and it's mainly a fear of hacking – that a potential cybercriminal could access the main company network through the surveillance system. Many businesses invest large amounts of money to deploy physical security technology, with little thought given to the security of the hardware and the impact on the business network. Security systems, such as cameras, can often be a back door

into IT networks, making them a prime security risk to an organisation. This potential vulnerability has led many to create a whole new isolated network just for surveillance equipment. A duplicate network not only costs more, but is more work to install and manage.

SENSE OF SECURITY

With a web-managed network, the system can be monitored in real-time from anywhere, alerting users to unusual activity. This enables customers to consolidate their surveillance on to one central network, more affordably, with less hassle and a greater sense of security.

Increasing concern about public safety and security, growing adoption of IP cameras and rising demand for wireless cameras are the factors driving the growth of video surveillance. The industry is likely to be influenced by future trends such as the adoption of multi-sensor cameras, implementation of IoT-based video analytics, integration of Artificial Intelligence and cloud computing.

However, with the growth of IP surveillance, the security industry is no longer just about cameras. As these capabilities increase, security customers are pushing for faster, more streamlined networks to adopt the surveillance systems of the future. This means there are growing opportunities for security and network installers who embrace these latest IP technologies to provide increased user experience, detailed analytics and more power in surveillance networks.

Just as you need a motorway to take the fast traffic while driving, fast lanes are now becoming mandatory for high-powered security networks too. By integrating network-capable surveillance systems with switches that have been specially designed with high power cameras and security in mind, the industry will be able to speed towards the power of IP surveillance ●

Luke Harley – EMEA Market Development Manager Switch at Zyxel Networks – has worked in the IT industry since 1997. In 2018 as Market Development Manager EMEA Channel for Home solutions, LTE and CPE he worked to create more awareness for his product groups before becoming Market Development Manger EMEA in 2020.

IP surveillance technology allows users to view cameras live

