Trends, opportunities and challenges in **Video Surveillance**

An eBook from

IFSEC GLOBAL

Contents

Introduction

So often the focal point of new tech trends and practices in the security industry, the world of video surveillance continues to undergo change. No longer viewed as simply a deterrent or a grudge purchase to review incidents, the advancements in technology have somewhat 'shifted the goalposts'. Alongside numerous other benefits, deep learning algorithms, video analytics, edge processing and cloud-based systems have provided professionals with valuable devices and platforms to not just 'protect', but prevent real-time threats from becoming security incidents in the first place.

It's not just security professionals who are making the case for modernised, IP surveillance cameras in their facilities, either. Intelligent functions, displayed on easy-to-understand platforms, enable more data-driven business operational planning and decision making – across industries from logistics and manufacturing, to education and retail.

It is quite clear, however, that technological change will always bring about unforeseen challenges. Just look at the debate over social media platforms as a prime example of this. How will automated facial recognition and additional biometric data capture from surveillance systems fare in a world where the public is becoming increasingly aware over privacy rights – particularly in regions such as Western Europe and North America? Moreover, how do end-users, integrators and consultants keep up with the technological page of change being set by vendors and software providers? Education will be required to ensure security professionals fully understand how best to utilise new tech.

Cyber security, too, is of greater alarm than before as IP-based physical security solutions become a potential vulnerability in organisational networks.

In this eBook from IFSEC Global, we seek to clarify some of the key themes from those pioneering the transformation of video surveillance. We surveyed and spoke with several key vendors in the sector to gauge their thoughts on the opportunities and challenges they're witnessing within the industry – both from their own point of view, and from the conversations they're having with customers on a daily basis.

What are the questions they're being asked from security professionals? And, considering they are at the forefront of new product and solution development, where do they see industry trends really heading? Here, we summarise the anonymous responses to such questions, with some thought-provoking quotes thrown in for good measure.

We'd like to thank all the companies listed to the right who found the time to speak with us and offer their unique perspectives in what has been a challenging start to 2021 for businesses of all sizes. We hope this provides readers with a useful overview of common themes and developments in the video surveillance industry looking ahead to the coming years. And, for those looking for views from industry professionals – such as security managers, systems integrators and consultants – IFSEC Global's latest trend report which surveyed over 700 professionals may provide further insight:

CLICK HERE > The Video Surveillance Report 2020

AXIS COMMUNICATIONS

EAGLE EYE NETWORKS

Genetec

Hanwha Techwin

HIKVISION

IDIS One Solution. One Company.

milestone

OMDIA

Summarising the key trends in video surveillance

The development of artificial intelligence, the growth of surveillance for non-security applications, migration to the Cloud, 5G and cyber security are some of the big themes to come out of this year's survey.

AI and analytics

Many respondents saw the increasing use of AI as key to the development of camera functionality. More specifically, machine learning – a subset of AI – is fuelling new standards and use-cases for surveillance systems, as devices learn from data they're taking in, process it and then use it to improve their future capabilities and decisions. For example, a system or camera can be "trained" to distinguish between humans and other animals, or between a vehicle and a bicycle, and the learning improves as the device is subjected to more scenarios.

This technology is being propagated by being available at the camera end, also known as the edge of a network. Applications such as facial recognition, ANPR, movement and non-movement detection, people-counting and heat-mapping are built into the camera, allowing these sophisticated sets of analytics to be readily available and affordable to many more surveillance system users. In addition, multi-sensor technology such as thermal imaging, humidity, fire and smoke detection and radar have provided greater perception capabilities, bringing an increased level of situational awareness. Accuracy of detection and recognition has now significantly increased with a consequent reduction in false alarms.

Not only do edge analytics provide for more intelligent functions to take place on devices such as cameras, but by being on the edge of the network, they also allow for substantially reduced levels of bandwidth. Only images which have been processed as being of interest (defined by the algorithms that make up the analytics functions) are sent to the control and monitoring station at the centre of the network. The advantages of this are especially apparent in the case of remote monitoring of cameras or with a cloud-based system. There is also an increasing level of importance placed upon how insights and data are presented, such as in centralised video management system platforms.

Analytics have now become automatic and ingrained in workflows. The use of analytics during the pandemic – for example, with body temperature detecting cameras and software which can detect whether a subject is or is not wearing a mask – has also led to an uptake of this technology.

Real-time surveillance

All this has contributed to video surveillance systems increasingly being used in real-time rather than being activated for investigation 'after the event' or alternatively needing 24/7 human monitoring. And when investigations are made into recorded events, the quality of metadata (literally data about data) now available means that searches can be made of multiple cameras using multiple criteria, enabling a significant increase in the speed of investigations.

Others cautioned that with all this data being generated by systems, the industry has a responsibility to ensure that there are sufficient safeguards and guidelines in place to handle all the data, which we will discuss in more detail later on in this eBook.

Non-security surveillance

The growth in use of multiple sensors has resulted in the widening of scope for surveillance systems beyond conventional security purposes. Examples of these are people-counting enabled cameras for retail management of footfall, ANPR for traffic and parking management, and a range of applications in health and safety, manufacturing and construction.

The question that arises is how does the security profession embrace this expansion? Perhaps the answer is greater collaboration between teams to promote enterprise security risk management.

The increased sophistication of video surveillance systems has also led to integration and convergence with other systems. These include facial recognition enabling contactless access control, fire detection, intruder alarms and emergency management. Increasingly these systems are merging onto a central platform.

> ***"From a security perspective, the top priority for the deployment of deep learning analytics is to reduce false positive alarms caused by harmless factors which traditional 'blob type' analytics cameras are susceptible to."***
>
> **Jamie Barnfield,**
> *Senior Sales Director, IDIS*

The rise of 5G

There are many potential benefits for video surveillance resulting from the rollout of 5G networks. The technology allows for higher quality images and lower latency due to substantially greater bandwidth, and should result in more edge devices being connected in remote locations.

The Cloud

Respondents pointed to the acceleration in the uptake of the Cloud based systems, due to the flexibility in operation, deployment and management these can provide. Benefits include: remote operation and maintenance, software updates, scalability, and no need for the operation and maintenance of local servers. When combined with AI, these systems can provide sophisticated surveillance solutions without the need to support a recording and storage infrastructure on site.

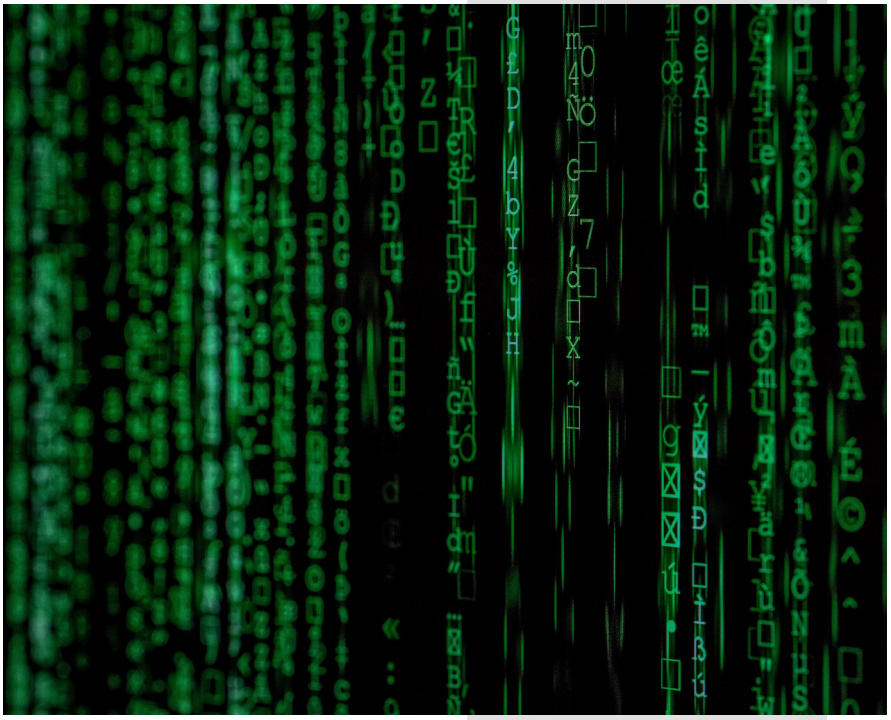
Respondents mentioned cyber security as an essential requirement, either locally on site or in the cloud, where providers should be competent at maintaining security and securing data. One respondent mentioned the blurring of lines between physical and cyber security, with several others emphasising the need for improved protection against cyber-attacks has never been more essential.

Data protection, privacy and ethics

Survey participants mentioned the importance of balancing public security and safety with protecting the privacy of individuals. This is a challenge, as technology moves at a faster pace than policy and regulation.

Questions include the role of AI and machine learning, human versus machine interventions, and what constitutes personal data. The EU has taken a lead on this, with the GDPR data protection legislation and hints of the potential regulation of the use of AI. Some highlighted, however, that there needs to be a greater awareness of how AI is being used within the industry. Security professionals are not asking the technology to make decisions on their behalf, for example, but instead using machine learning to generate data that supports decision-making processes and actionable events.

> ***"The reliability of wireless transmission via 5G is likely to revolutionise the currently wired video security market, thanks to the proliferation of wireless cameras and the ability for more edge devices to be connected in remote locations."***
>
> **Hikvision**



Challenges for the video surveillance industry

To paraphrase the mantra of Tony Blair and New Labour, the top three challenges for the video surveillance industry are: 'education, education and education'. Several vendors agreed that video surveillance systems have become so technology driven, that it is easy to lose people in the mass of high-tech specifications and technical jargon – which is not readily comprehensible to many or most end-users.

Respondents to the survey indicated that end-users need to be educated so that they understand the genuine benefits of new technology, rather than the minutiae of the tech specifications. Secondly, vendors themselves need to understand the challenges for end-users and the benefits and outcomes they are looking for. Vendors need to act less like salespeople and more like consultants. Indeed, both manufacturers and consultants may benefit from taking a step back and asking what the 'true challenges' of their customers are? And how can the technology solve these?

There was also a feeling that too few engineers have the technical skills needed in the industry today.

One specific area which respondents highlighted as requiring more and better education is about the cloud. Integrators and installers need this knowledge to properly inform their customers, and also understand the potential added value it offered them.

Respondents also pointed to the lack of cyber security awareness and

poor cyber security practices, in the face of rising volumes and levels of sophistication of cyber-attacks on physical security systems. Several highlighted they were under greater scrutiny as to what cyber security measures they had in place to protect their products. Expanded questions in this field also revolved around who has access to their systems, the integrity of recorded and exported video data solutions, and multi-layered security.

One participant noted that cyber security priorities have risen from the bottom to the top of customers' questions. Perhaps this is no surprise when the cyber threat has only grown in the face of a pandemic. As part of this, deepfake images being used to alter video and affect the reliability of footage was also cited as a concern.

Specifically looking at the United States, federal agencies are also requiring physical security devices and their related components that are being installed and specified to be NDAA (National Defense Authorization Act) approved. If they have not been, then they cannot be procured for any government installation or federally funded project under this act.

Getting back to face-to-face dealing and standard business practices after lockdown and the pandemic was another challenge identified by participants. This will entail a more flexible approach in the way we work and building more meaningful relationships with customers and end-users. It will also involve security providers supporting customers by advising them on analytics/software that they can use in helping to create safer workspaces, believed vendors.

Finally, while customers continue to request surveillance systems that can be used for other, non-security related business operations, there will likely be more involvement from other departments. What was previously considered the realm of the security manager, may now involve several opinions – not least the IT and cyber security team who will want to ensure any devices being added to the network are not going to create new vulnerabilities. Again, this links with the move towards video tech being integrated with other parts of an organisation – will this result in departmental conflict? Or will this result in greater importance being placed on the security department, who may have enhanced organisational influence?

Looking ahead – the 'five-year view'

Respondents were asked to look ahead over the next five years and identify the main developments they expect. First, they were asked to set out what end-users will 'look like' in five years' time.

As already discussed, they expected that IT departments would play an increasingly important role in decisions involving the specification and procurement of security systems, with other departments also having an influence. Organisations will become less siloed, as more business operations saw the value of surveillance systems, though to what extent this will happen will vary among different businesses. But whatever happens, security departments will need to involve IT from early on, otherwise there will never be a fully cyber-secure process.

IT departments are also increasing their influence as information security and physical security converge. When installing video management systems (VMS) for example, IT departments want them integrated with their own information management systems. Increasing collaboration, however, does depend on breaking down the traditional barriers between departments such as IT, security and facilities management.

Intelligent and connected buildings will drive the need for increased cooperation, with cameras becoming elements in a whole host of 'super sensors' within a building or buildings.

Video analytics

The uptake of video analytics is expected to continue its growth in the coming years. This is partly due to the reduction in the cost of analytics, and partly due to improved algorithms. Video analytics are increasingly found in edge-based products such as cameras, reducing the need for expensive servers and decreasing the need for bandwidth to process live video. In addition, the growing uptake of the cloud also means there is less need for physical servers.

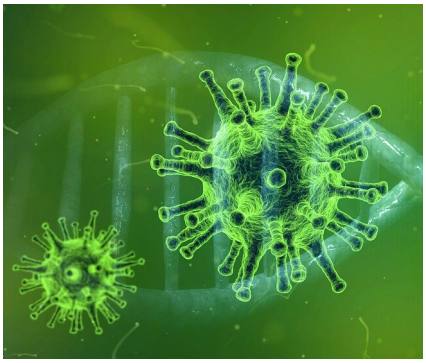
> ***"Physical security professionals must partner with their counterparts in IT to understand the true limits of the security perimeter and mitigate against risk."***
>
> **Nick Smith,**
> *Regional Manager, Genetec*

The accuracy of analytics has also improved significantly, partly due to machine learning, as well as organisations such as the UK Government's Centre for the Protection of National Infrastructure (CPNI) being involved in benchmarking analytics systems. More metadata is being captured, giving context to video with more insights to increase operational efficiency.

Video analytics mean that there is an increasingly proactive approach to security and other business objectives – it's no longer just about forensic analysis. Additional business benefits flow from the increasingly rich data from features such as heatmapping, people counting and body language detection. It can be said that there is now a genuine return on investment from security systems, whereas previously they may have been considered a 'grudge purchase'.

COVID-19 implications?

There was a general consensus among participants that it was difficult to predict the long-term effects of the COVID-19 pandemic on the video surveillance market. The increasing adoption of video analytics was already happening before COVID struck, but it is difficult to say whether we will see specific deployments to support future safety measures.

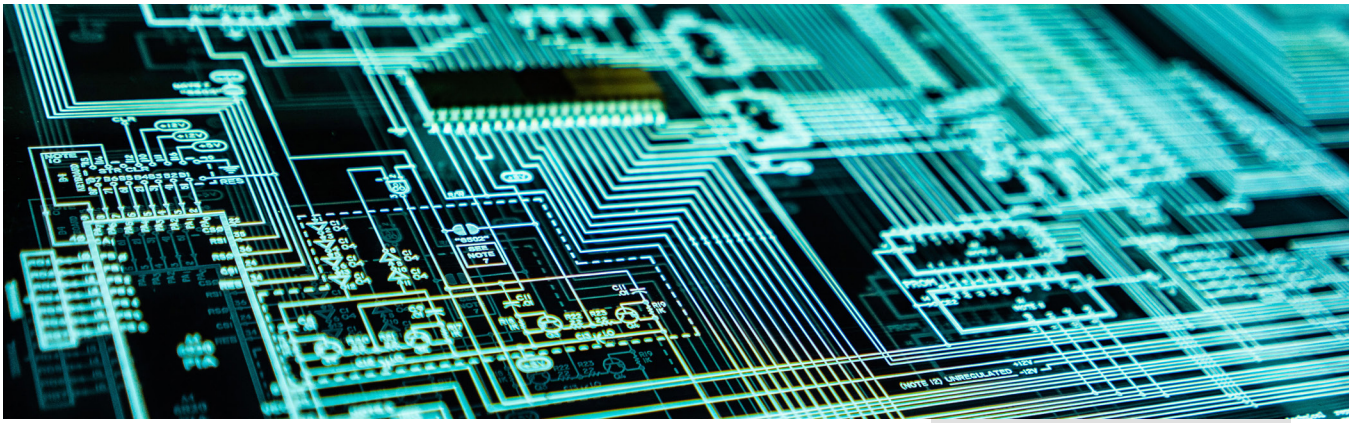


Potential effects at present include:

- Surveillance systems being used to facilitate contactless experiences
- Local authorities and the police may look to use systems to monitor crowds and enforce social distancing – may influence further growth in the provision of 'smart' cities
- Remote access to systems may grow as more people aren't based in the office/hub – this will require more accountability of access
- The pandemic may drive adoption of analytics in video surveillance systems to enhance public safety

One respondent said there may be an increased appetite for public safety apps which may be enhanced through integration with video/audio.

> ***"Smart Buildings are not around one application, it is about the integration of various applications that can work together and jointly deliver valuable information for tenants and owners of buildings. An open platform will be essential to contribute to and expand this ecosystem."***
>
> **Rishi Lodhia,**
> *Managing Director, Eagle Eye Networks EMEA*



Integration

Integration with other systems appears to be at the forefront of security professionals' minds. Interoperability and openness are on the agenda, with several vendors citing questions on topics such as:

- ONVIF compliance? (ONVIF is the forum that provides and promotes standardised interfaces for effective interoperability of IP-based physical security products)
- Standardised in terms of communication
- Capable of working with end-users' cloud roadmaps
- Capable of operating as part of a unified building management process

Respondents said that the potential to integrate video surveillance with other security and/or building management systems was a growing trend. Driven by the requirement from end-users for an increasing number of business operations being integrated onto one platform, sensors within video surveillance systems can now provide further actionable intelligence, working in tandem with access control and intruder detection.

Several vendors noted that open platforms and APIs (Application Programming Interfaces) were important to have when aiming for integrated solutions on a unified platform. Standardised platforms, it was argued, will ultimately make it easier for integrators, installers and end-users to assimilate new devices and systems together, for the benefit of the wider industry.

Many believe that this is all part of the 'natural evolution' of security, which no longer operates in traditional siloes, but instead is managed and analysed as an overall integrated solution that can help justify expenditure and demonstrate a clear return on investment.

> ***"Closed protocol, proprietary systems are a thing of the past. As the influence of IT departments becomes more prevalent, the adoption of industry standards will become the norm and closed systems will find it very difficult to compete in a world where their customers desire choice."***
>
> **Steven Kenny,**
> *Manager, Architect & Engineering Program, EMEA, AXIS Communications*

Cyber security – now a critical consideration?

All participants in the survey said that cyber security was a continual concern, especially considering that IP cameras are essentially IT devices on a network. Although physical security professionals are now more aware about the risk of cyber-attacks, there needs to be continual investment in cyber security as threats continue to grow and 'back-door' attacks are possible.

No one wants to be responsible for the weakest link of an IT network. It is essential to keep end-users' confidential data safe, and control who has access to video and data. With this in mind, collaborating with IT departments is an important step to improving the cyber security credentials of physical security devices, highlighted several vendors.

The rise of deepfake videos – where images are digitally manipulated so that, for example, a person in an existing video is replaced with someone else's likeness – are also a concern. Not only is there the disruptive potential of deepfakes, but the credibility of genuine surveillance footage may start to be questioned.

Respondents said that cyber security was the shared responsibility of the whole supply chain, from manufacturers through to integrators and end-users. Due diligence of everyone involved can help combat the 'insider threat', and manufacturers, integrators/installers and end-users need to trust and communicate with each other.

Points to take into consideration comprised:

- Commercial grade cameras are capable of being hacked – not just IoT home security devices. There's still a lack of acknowledgement that a camera is a device that can give access to a corporate network
- People need to start assessing the inherent cyber security of cameras before the operational performance
- Don't feel threatened by IT teams, but work with them as part of a holistic approach to security management
- The risk of cyber security loopholes increases with larger installations
- The pressure of installing products from several different vendors can open loopholes

> ***"With data increasingly being captured, stored and secured at the edge as part of a smart factory, smart office, smart retail store or on a larger scale, a smart city solution, the need for protection against cyber-attacks has become an even more essential requirement."***
>
> **Uri Guterman,**
> *Head of Product & Marketing for Hanwha Techwin Europe*

The view from respondents generally indicated that although the industry is catching on, there is some way to go. In the UK, the BSIA has recently released cyber security codes of practice and guidance for manufacturers and installers, but there is a consensus that the industry is still playing catch-up and more is needed. Other suggestions for improving the cyber protections for surveillance devices included:

- Third party certification. The UL Cybersecurity Assurance Program (UL CAP), for example, assesses potential cyber issues and levels of risk from hackers in respect of network-connectable hardware devices and software
- Secure by Design and Secure by Default: Although these can reduce the need for in depth training if products are secure 'out of the box', they rely on self-certification
- Third-party penetration testing is important, but businesses are not penetration-testing their devices.

Developments with the cloud and AI are fast-moving and disruptive, so there is a requirement for the industry to ensure such technology is balanced and remains cyber secure - ultimately, it's a public safety issue.

But it's not just the issue of secure software and hardware – employees need to be educated on how to mitigate cyber risks and procedures need to be more secure. Default passwords should be abolished and multi-factor authentication should be enforced, it was highlighted. Both of these processes have recently been encompassed into UK legislative plans to improve the cyber security of consumer IoT devices.

Opportunities arising from cloud-based systems

Several respondents pointed to the growing uptake of cloud-based solutions and Video Surveillance as a Service (VSaaS). While it is referred to as a 'natural evolution' and the majority of participants believe cloud services are the future – since businesses are used to storing other data on the cloud – there is a consensus that not all are ready to adopt fully cloud-based video surveillance solutions just yet.

As such, there is a role for hybrid solutions comprising a blend of local, on-premise storage with cloud storage. This allows users to become better accustomed to it before fully committing, providing a transition to a full cloud solution.

Although VSaaS offers a full range of remote capabilities and flexibility without the need for internal servers, video can be slightly more challenging than other security systems, such as access control. For migration to continue without interruption, the sizeable amounts of bandwidth required for video transfer may require some improvement in infrastructure.

While there was an acknowledgement that the industry remains wary of VSaaS due to cyber and data concerns, the majority of vendors highlighted that cloud-based services often far surpass the security systems in place for on-premise storage. Data centres are likely to have high levels of physical and cyber security processes in place, and are required to be fully compliant with data protection legislation.

There was a consensus that cloud-based services are not always fully understood by 'traditional' security integrators or their customers, pointing once again to the need for further education. There's also potentially a smaller range of cameras on offer by cloud vendors, and then there is the issue of licensing fees, though there is a belief that the data centre market will become more competitive and storage costs will fall in the near future.

In spite of the many advantages of cloud solutions, a few participants emphasised that the industry needs to ensure that it is promoting and using them for the right reasons, ensuring that they actually solve problems for end users. Demand is growing, it appears, but vendors must listen to their customers to ensure they provide a solution that is appropriate for their needs, to help erase some of the confusion in the sector.

> ***"Defining the actual infrastructure and process challenges is critical to truly evaluate if a particular cloud-based system is the right solution. Technology should help you rise to meet the challenges you have; the technology should not constrain the challenges you're able to solve."***
>
> **Alex Knapik,** *Competitive Intelligence Lead, Milestone Systems*

The role of regulation and data protection in surveillance tech

As the use of video analytics and AI-based software continues to develop, there is a growing awareness from the public and campaigners that tools like facial recognition may be encroaching on people's privacy. These circumstances significantly differ between regions – there is more of an acceptance of public surveillance tools in parts of Asia, compared to that of Europe for instance, where stricter data regulation such as GDPR is in place. Meanwhile, in the US there is varying legislation and regulation between states, with some areas restricting or even banning the use of automatic facial recognition.

The general view among respondents was that more – or at least better – regulation is needed, so that public and private organisations can feel more confident they are doing the right thing. Referring to the UK specifically, in relation to automatic facial recognition, participants said that there needs to be better alignment between the Information Commissioner's Office and the Surveillance Camera Commissioner, with a clearly defined framework on who can and can't use the technology.

The debate continues to be divisive, with vendors raising several questions. Where do we draw the line? Should private-sector organisations be able to capture biometric data without permission? It is no doubt imperative that we have the right safeguards and standards in place, and cyber security is equally part of the equation.

Questions that need to be asked by end-users may include:

- Who has access to the surveillance?
- How is it being used? How do you compare use-cases when private companies are capturing biometric data for marketing purposes, compared to government/police forces using it for preventative and public safety measures?
- What about the issue of potential racial and gender bias in AI and automatic face recognition systems?
- Is the data being captured proportional? Users should only be capturing data that is required for an appropriate purpose.

These unresolved issues are viewed as risks by potential users of automatic facial recognition and therefore may be acting as a brake on the wider adoption of the technology, which can ultimately better protect the public and increase security processes, it is believed. In the field of AI as a whole, the EU is exploring further regulation for the sector. Whether this significantly impacts on uptake of AI-based solutions in the security sector is yet to be seen, though the argument that much of the tech used in security can be more closely attributed to machine learning – ultimately, the end-users still make decisions, not the technology itself – will becoming increasingly important.

It was emphasised, therefore, that the security industry needs to be prepared for the debate over accountability and the usage of the technology, before the control over the narrative is lost.

Vertical markets – growth areas and use cases

Finally, we asked vendors whether there were any clear growth areas from different verticals. Perhaps unsurprisingly, this generated quite a varied response, with different vendors having different perspectives on which sectors offer opportunities.

One clear area that continues to witness demand for surveillance cameras is the retail sector. No longer simply a security measure, video analytics solutions now provide store owners with actionable business intelligence, such as footfall analysis, to better understand customer behaviours and attitudes. Vendors now even have specific applications and solutions for retail operations.

Smart cities were also mentioned as a potential area of growth, particularly in Asia and the Middle East, with demand being driven by several factors, according to respondents:

- Local authorities are seeking smarter solutions
- The growing use of multiple sensors
- The rollout of 5G capability in cities
- Traffic and pollution monitoring
- Monitoring of street lighting
- Increased focus on public safety

Allied to smart cities are transport hubs, where security, health and safety and tackling anti-social behaviour are priorities.

Respondents said there's been a growth in demand for data centres, which require a high level of surveillance and physical security as well as cyber security. Many of them are independently certificated, and robust security is a substantial part of this.

Utilities – where infrastructure can be fragmented over large geographical locations – were also identified as potential areas for growth.

Logistics was highlighted as another sector with potential for growth. With the relentless rise of e-commerce and online shopping, there is continued investment in new logistics centres in the UK and Europe. And, since the outbreak of the COVID pandemic, there has been a renewed emphasis to further strengthen supply chains. In addition, analytics such as footfall monitoring or behavioural analysis can help increase efficiencies and improve health and safety processes – if a worker falls to the ground, the camera can recognise this and produce an automatic alert, for instance.

Other sectors identified for potential growth included commercial offices, sports and stadia, education facilities and the banking sector.

IFSEC GLOBAL

www.ifsecglobal.com

THE NUMBER ONE SOURCE OF ONLINE CONTENT FOR SECURITY AND FIRE SAFETY PROFESSIONALS

IFSEC Global is the leading provider of news, exclusive reports, industry thought leadership, webinars, whitepapers and more.

Join the IFSEC Global Newsletter community and receive weekly industry news and updates to keep you at the forefront of the industry.

informa markets