The Video Surveillance Report 2023

IFSEC INSIDER

Sponsored by

IDIS One Solution. One Company.

Contents

Introduction

Welcome to the 2023 Video Surveillance Report from IFSEC Insider, where we once again seek to analyse major trends in the sector and shed light on what lies ahead.

The impacts of rising inflation, geopolitical events and supply chain issues have been keenly felt by governments, businesses and organisations across the globe. These are macroeconomic events – but so too is the evolution of technology. The proliferation of cloud-based platforms and AI usage has continued at pace, with the latter arguably set to be a defining topic of this generation.

While there is an immediate link to be drawn between the technology trends outlined above and video surveillance systems, the sector is by no means protected from those macro issues before it, either.

Rising inflation has resulted in a cost-of-living crisis that is having profound consequences on frontline security – a report in May revealed that around one in 10 young adults had admitted to stealing from supermarkets this year.[1] Meanwhile, geopolitical tensions continue to impact supply chains and influence the face of a global video surveillance market set to be worth $38.2 billion in revenue by 2027.[2]

Video surveillance remains a fundamental piece of the jigsaw in securing people, places and assets – but it is now so much more than that. As we've explored in the previous two market reports, a large percentage of systems are now also being used to solve operational challenges, or provide additional business intelligence, due to the sheer volume of data cameras and their corresponding analytical functions collect.[3]

As a result, we've seen use-cases change, evolve and adapt over the many years we've been running our annual reports.

This year, we'll begin by examining the current state of the video surveillance industry. Here, we take stock of the overall market outlook and whether projects have been affected by rising costs, or whether the sector remains as robust as ever. We also set the scene for the tech currently in place in the market, exploring levels of adoption for IP-enablement, edge-based processing and the VMS systems cameras are, or are not, attached to.

While we've covered the uptake of Artificial Intelligence (AI) analytics for several years, it would be remiss of us to not dive a little deeper in the 'year of ChatGPT', as 2023 has played witness to an explosion of generative AI. Use cases continue to grow as vendors tout their ever-expanding list of application solutions, but what do the professionals actually using and buying AI-based applications really think? Is it making their jobs easier, or are they increasingly worried about its development? What barriers remain to adoption and what are they hoping to achieve by using AI?

Report written by
James Moore
Managing Editor, IFSEC Insider

[1] The Metro, One in 10 young people admit shoplifting due to cost of living crisis, **https://metro.co.uk/2023/05/10/one-in-10-young-people-admit-shoplifting-due-to-cost-of-living-crisis-18761170/**
[2] Omdia, Video Surveillance & Analytics Market Report 2023, **https://omdia.tech.informa.com/products/video-surveillance--analytics--2023**
[3] IFSEC Insider, Video Surveillance Report 2022, **https://www.ifsecglobal.com/downloads-resources/the-video-surveillance-report-2022/**

Cloud technology is now so ubiquitous across our daily lives that many of us don't even recognise, or comprehend, how much we're using it. Security remains a little behind the curve of adoption – and many would argue sensibly so – but this year we have found over half of respondents are either installing and recommending it, or actively using it for video surveillance purposes. So that forms the basis for chapter three.

We also take a closer look at a few different vertical sectors, to better understand how surveillance systems are being used to manage unique requirements and challenges. This year's survey asked those actively working within or who have worked on projects in the retail, construction and public sector, to analyse how industry-specific trends are manifesting in these areas, from curbing retail losses to enhancing construction site safety and bolstering public security.

As ever, we would like to extend our gratitude to the 500+ professionals in security, facilities and IT who provided their responses and opinions to our survey. Whether you have a role in specifying, installing, maintaining, operating or influencing decisions on video surveillance purchases, your opinions form the basis for our trend reports – they would not be possible without your contributions.

We hope the results outlined here provide you with greater insight into the current adoption of video surveillance technology and key trends ahead to inform future plans and decisions.

And thank you to our long-time sponsor, IDIS, whose experts also provide additional insight into trends at various points throughout each chapter.

About IFSEC Insider

IFSEC Insider – formerly IFSEC Global – is a leading news and online content provider for the security and fire safety markets. Alongside daily articles covering the latest in the sectors, IFSEC Insider also delivers valuable insight and analysis on market trends via webinars, podcasts and trend reports for the global security and fire communities.

About IDIS

IDIS' end-to-end video solutions benefit installers with plug-and-play installation, and reliable support for every project, while end-users' advantage from an industry-leading low total cost of ownership. Video tech from South Korea's largest in-country manufacturer benefits a range of sectors including banking, retail, logistics, government, education, and commercial offices. IDIS delivers cyber-secure surveillance with an impressive choice of NDAA-compliant cameras, recorders, servers, accessories, and a choice of VMS and scalable AI video from software to pre-configured AI boxes. These are all powered by the in-house developed IDIS Deep Learning Engine to meet the security and intelligence needs of businesses large or small.

Executive summary: 5 takeaways from the 2023 Video Surveillance Report

1. AI is actively supporting security – but there is demand for regulation and guidance

2. Over half of respondents are now using the cloud for video surveillance

3. Demand for video surveillance remains strong, but tougher times ahead?

4. Buyers of video surveillance technology are actively considering sustainability credentials

5. Video surveillance systems will have a central role to play in smart building and city development

Video surveillance – State of the market

Demand for video surveillance projects remain strong

The economic challenges over the past 12 months have been vast, and certainly have not been unique to one particular region or country. Though some have suffered worse than others, interest rates on the whole have risen to numbers not seen since the financial crash of 2008, as central banks have been forced to respond to high inflation levels. Though there are positive signs on the horizon at the time of writing, markets are by no means stable.

This has an inevitable impact on business costs. To keep up with inflation which has sparked a cost-of-living crisis, wages have risen significantly in 2023 – regular pay grew by 7.3% in the UK compared to last year's figures.[4] Meanwhile, property rates have increased significantly as mortgages, rents and utility bills have all been hit by the economic situation.

Last year, we asked whether economic challenges had affected video surveillance upgrade plans. While 50% said that it had caused a reassessment and delays, projects were still going ahead – only 10% stated their plans had been cancelled as a direct result.[5]

Given the economic situation has only worsened, we asked this question again. We can see a slight increase to 13% in those who have said projects have been cancelled as a result of the economic situation. Despite this, the majority said they had continued, and there was a rise in those who said they had been unaffected altogether, from 20% last year to 29% in 2023.

Have wider economic trends affected video surveillance upgrade plans?	
Yes, it's caused reassessment and delays, but projects are still happening	39%
No, we've carried on as normal	29%
No, it's been a consideration but hasn't affected the physical security budget/projects	19%
Yes, upgrade plans/projects have been cancelled as a result	13%

We also delved a little deeper, specifically asking those supplying video surveillance products and services – such as installers, vendors and consultants – what they have witnessed in 2023.

The good news for the video surveillance supply chain is that demand for new projects remains strong. 70% of those who install, consult or provide products to the market answered that they had witnessed an increase in demand for new projects in the past 12 months. While 23% said no, only 7% said they had seen demand fall.

Overall then, demand for video surveillance projects has remained strong over the past 12 months. While rising

70%

of those supplying video surveillance products or services have witnessed an increase in demand for new projects in 2023

[4] BBC News, Record pay rises fuel fresh inflation fears, **https://www.bbc.co.uk/news/business-66156713**
[5] IFSEC Insider, Video Surveillance Report 2022, **https://www.ifsecglobal.com/downloads-resources/the-video-surveillance-report-2022/**

costs have likely hit organisations' profit margins and bottom lines, the necessity of video surveillance systems to security and general organisational resilience is clear.

External reports indicate that advertising budgets and 'non-essential spending' have been cut, but that investment in technology stands firm. Cloud investment and IT spending, budgets which IP- and cloud-enabled CCTV systems may now fall under, has actually grown over the past 24 months across the wider business landscape.[6]

In many ways, increasing value may be placed on physical security systems to combat the new threats occurring from challenging economic conditions.

The UK's Office for National Statistics (ONS) figures published in July showed police recorded crime in the year ending March 2023 had exceeded pre-pandemic levels, including crime against people, households and businesses.[7] Crime rates in Europe are also on the rise against a backdrop of hardened economic conditions.

Perhaps it is of no surprise then than organisations continue to invest in security measures, with video surveillance acting as a visible deterrent and reporting mechanism. Indeed, systems are increasingly used as proactive and predictive tools when integrated with audio or analytics technology.

There are positive signs ahead, too. In research undertaken by Omdia with the International Security Management Association (ISMA) earlier in 2023, 84% of Chief Security Officers (CSOs) surveyed expected their budgets to match or exceed 2022.[8]

IP versus Analogue

We also sought to understand what type of technology is currently in place. For this section, we focused on end-user responses, and covered Internet Protocol (IP) enablement levels, adoption of edge-based technology and whether cameras are connected to Video Management Systems (VMS) platforms.

Respondents were also asked about AI and cloud adoption, but we interrogate these answers further in the two chapters that follow.

While the general consensus is that the security industry has mostly transitioned to connected and IP-enabled devices, commentators highlight that analogue systems still have their place, and will remain for several years to come.[9]

Our survey results reenforce this very point. According to our respondents, on average 74% of video surveillance devices on their CCTV networks are IP-enabled. This is the overall average of nearly 300 respondents, many of whom are likely to have very different requirements, but it is noteworthy that 45% of those who surveyed answered that 90% or more of their systems were IP-based, while 32% of respondents said that 100% of their network was IP-enabled.

Uptake is therefore high, and of those who have installed or upgraded to IP-enabled cameras, a significant proportion have done so almost system-wide. Legacy systems no doubt remain in place where there is no pressing requirement to upgrade, and not all organisations require the latest tech – analogue systems remain a cheaper option – but the many features

3/4

of video surveillance cameras in use are IP-enabled

[6] CIO Dive, Budget cuts will spare IT heading into 2023, **https://www.ciodive.com/news/recession-cuts-spare-IT-budgets/632777/**

[7] ONS, Crime in England and Wales: year ending March 2023, **https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2023**

[8] IFSEC Insider, 84% of leading CSOs expect 2023 physical security budget to match or exceed 2022, **https://www.ifsecglobal.com/corporate-security/leading-csos-expect-2023-physical-security-budget-to-match-or-exceed-2022/**

[9] Security Informed, Is Analog dead, or how Is it viable in today's security systems? **https://www.securityinformed.com/insights/analogue-dead-viable-today-security-systems-co-227-ga-co-1645-ga-co-1756-ga-co-4022-ga-off.1689849467.html**

provided by today's digital systems will continue to drive further IP adoption, it appears.

Jamie Barnfield, Senior Sales Director, IDIS Europe, adds: "There's still a significant amount of analogue technology still in use and many larger end-users are reluctant to replace equipment until the end of its lifecycle.

"To reduce waste, the complexity of managing multiple systems and improve control room capabilities, many are adopting a cost-effective Video Management System that doesn't come with a significant price tag or ongoing maintenance fees for integrating legacy cameras.

"Due to demand, IDIS recently launched an NDAA-compliant, 8-channel encoder that digitises various brands of analogue camera signals to provide excellent HD image quality. This ensures end-users can continue to support older cameras, use a mix-and-match analogue and IP approach, or manage phased upgrades to full network surveillance."

IDIS 8-channel DP-DE2108 HD encoder digitises various third-party analogue cameras

Adoption of edge-based, SOC technology

At IFSEC 2023, Omdia's Physical Research and Analysis Manager, Oliver Philippou, identified System on Chip (SOC) technology as one of the key areas of growth ahead for the sector. The proliferation of SOCs in cameras has allowed the deployment of deep learning analytics to explode, he explained, given this enables processing to take place on the camera itself – or at the 'edge' – significantly reducing bandwidth and storage requirements.

Thanks to edge processing, video data can be processed and analysed on the camera itself, removing the need to send all the footage to a centralised server, database, or even to the cloud. And, as Phillipou outlined, this is made possible thanks to SOC technology. Whereas 30% of network cameras deployed today have an advanced SOC processor built in, by 2026 this will be closer to 70%, predicts Omdia.[10]

Given these statistics, we asked the level of adoption of edge-based cameras to both those operating or purchasing cameras. 28% cited that they hadn't as edge technology wasn't necessary for their video surveillance purposes, while another 24% said no due to cost or for other reasons. The remaining 48% however was split between either 'steadily upgrading to' or 'installing more' edge-based systems.

Acknowledging that not every camera in each site is likely to have the same level of technology, there is a clear demand for processing at the edge to take place, with almost half of respondents installing or upgrading to cameras capable of doing so.

48%

are upgrading to or installing edge-based video surveillance cameras

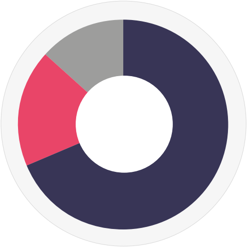
[10] IFSEC Insider, Omdia Insights – Trends in the video surveillance market, https://www.ifsecglobal.com/video-surveillance/omdia-insights-trends-in-the-video-surveillance-market/

Video management system platforms

While touched upon in previous reports, this year we also wanted to understand how many cameras are connected to a Video Management System (VMS). Designed to manage and control video surveillance cameras and to act as a central hub for feeds and alerts, VMS software platforms are evolving in much the same way as their camera device counterparts.

As well as edge-based processing on the cameras themselves, VMS platforms feature their own analytics software to provide valuable insight, as well as providing alerts and event management capabilities to provide users with real-time situational awareness from all their feeds.

VMS platform providers offer increasingly scalable solutions, too. While on one-end there might be an enterprise-wide system with hundreds or even thousands of cameras feeding in, organisations with a relatively small number may still benefit from a central platform to manage and analyse footage.



Are your video surveillance cameras connected to a VMS system?

- ■ **(68%)** Yes
- ■ **(18%)** No
- ■ **(13%)** No, but expect to implement in next two years

According to our survey, the majority of today's organisations have their cameras connected to some form of VMS system at 68%, while another 14% expect to implement them in the next two years. Just under one in five (18%) don't have a VMS platform in place.

Cost and license free IDIS Center VMS for up to 1,024 devices

The majority of those who answered that they did not have cameras connected to a VMS system were from either small or medium sized companies, despite larger companies making up the significant proportion of respondents to this year's survey.

Jamie Barnfield, IDIS Europe, expands on these findings: "The small to medium sized market for video surveillance is significant and makes up a considerable amount of run rate business for integrators and installers.

"Most SMEs don't need the functionality or cost of a sophisticated, enterprise-class VMS platform. So, it's worth integrators and end-users looking out for solutions that come with totally cost-free client software that is easy to use for non-security operatives, which they can also operate via mobile apps to ensure their premises, staff, and assets are safe and secure out of hours and on the move."

Of those organisations using VMS, server-based systems remain the dominant method, at 47%. 19% are being managed via Network Video Recorders (NVRs), 26% are hybrid systems and 8% are managed specifically in the cloud by the same supplier as their surveillance cameras.

"Server and NVR-based systems continue to be in high demand as they offer the most cost-effective and secure method of storage. They also make system design and retention calculations quick and easy. And unlike cloud they give end-users the assurance that if they want to upgrade to higher resolution cameras or extend retention periods they are not faced with spiralling costs," concludes James Min, Managing Director, IDIS Europe.

Eye on AI – Its use and future use in video surveillance systems

A subject that has been in mainstream media outlets as much as it has in security publications, the proliferation of Artificial Intelligence (AI) has in many ways, defined 2023.

Open AI launched its ChatGPT natural language model chatbot with significant backing from Microsoft in late November of last year, swiftly followed by Google rolling out a major expansion to its rival Bard product. Meanwhile, Amazon has announced it is set to invest as much as $4 billion in Anthropic in its own efforts to also become a major player in the generative AI space.[11]

Before we get too carried away, it is important to note that video surveillance systems have been using AI-based algorithms and programmes for video analytics purposes for several years now. ChatGPT and its fellow chatbots that have hit the headlines are based on a different subset of AI to that which we've been examining, and will continue to explore, in the video surveillance sector – for the time being, at least.

Generally, analytics in surveillance cameras are based on machine or deep learning – an evolution on traditional analytics, as AI algorithms learn without human interference what is the right and wrong output.

Ultimately, these are being used to support security teams do what they already do, just at more speed, with greater accuracy and with the ability to comprehend huge data sets to provide users with actionable insights in a more streamlined way.

While uses in security may not have significantly changed – at least not as much as the rate of generative AI chatbots – this year we felt the need to further investigate not just the adoption rate of AI-based analytics in surveillance cameras, but also the perceptions of those professionals actively using, installing or recommending the technology.

Adoption of AI

Given a significant proportion of video surveillance devices in active use will be legacy systems, or those used for relatively straightforward video capture, deterrence and evidential purposes, we should not expect uptake to be overwhelming. Though it should be acknowledged that our respondents work in security, facilities, or IT backgrounds, and so likely represent the more sophisticated end of the overall market.

Asking respondents for a rough percentage of their video surveillance systems, or those that they install, that have some form of AI-based software embedded or added onto them (cameras, AI boxes, VMS etc.) only 31% answered zero. This leaves the majority of those professionals we surveyed having had some form or significant interaction with AI-based technology in camera systems.

46%

of security professionals say AI is actively supporting their team to carry out their roles

39%

of security professionals say AI–based video surveillance is actively supporting other business functions

[11] Fortune, Amazon to invest up to $4 billion in ChatGPT rival Anthropic as it plays catch-up in Generative AI, https://fortune.com/2023/09/25/amazon-invest-4-billion-chatgpt-rival-anthropic-generative-ai/

The main reasons for adoption varied, though intrusion detection was selected by three quarters of respondents. Subsets of this application also featured – virtual line crossing (39%), object classification (32%), loitering detection (26%) – indicating that primary security purposes remain the most important reason for investment.

Meanwhile, critical event search for evidential or post-event analysis purposes was third on the list (42%), while facial recognition (38%) also scored highly.

Security professionals are also attuned to use-cases outside of their traditional field, however. People counting (45%) was the second most popular driver of adoption, while ANPR-based AI for licence plate recognition was selected by 42%. Though the latter can also relate to security purposes, both have strong connections to facilities and estates management when integrated to building management platforms or access control systems.

5 Top reasons for implementing AI in video surveillance systems

1	Intrusion detection
2	People counting
3	Critical event search
4	Reducing false alarms
5	ANPR purposes

This is also in line with last year's findings, where 49% of respondents cited that video surveillance analytics were being used for operations outside traditional security purposes.[12]

Provided with some general positive and negative statements around AI – the latter of which we will explore shortly – and asked to select the three they most agreed with, the majority held a positive outlook for the technology's use.

46% said that AI was actively supporting their teams in carrying out their duties, while another 39% said that it was being used to support other business functions and helping to showcase security's evolving role in their organisation. 25% also cited that customers were keen to implement AI and were asking regular questions around the topic.

All this sounds great – but what barriers remain?

Acknowledging that AI-based video surveillance applications aren't required for every video surveillance system in active use, more prominent barriers remain to adoption. These haven't significantly changed in recent years with upfront costs (61%) and camera upgrade requirements (37%) remaining as two of the biggest hurdles for end-users.

[12] IFSEC Insider, Video Surveillance Report 2022, https://www.ifsecglobal.com/downloads-resources/the-video-surveillance-report-2022/

What are the 5 biggest challenges for installers, integrators and consultants when selling AI applications?	
1	Price
2	Concerns over data privacy
3	Lack of understanding of the benefits
4	Responding to different customer demands
5	Lack of education from vendors to support sales

While almost a third (30%) of end-users remain unsure about the accuracy of AI in creating false alarms, this option was significantly lower when asked to those selling AI applications (16%). This may indicate that installers, integrators and consultants in more tech-minded roles don't perceive this traditional challenge to be quite as much of a barrier anymore. Given the key selling point of machine or deep learning AI over traditional analytics is accuracy, this perhaps isn't too surprising.

In contrast however, there is demand for more education for those selling AI-based video surveillance applications. 29% cited that vendors' lack of training or education programmes to support application sales was a challenge, while the same number of end-users answered that they remained unsure of the return on investment.

Across the board, ethical and data privacy concerns were highlighted as barriers to adoption. Many of these worries will depend on the intended use-case, of course. AI-based facial recognition systems continue to come under scrutiny, with such an application infringing on privacy far more than a people counting system, which wouldn't actually require any biometric data.

Indeed, 31% of respondents outlined that while they believed AI was improving security processes, they were unsure about the potential data privacy and ethical implications of its use.

It may be that an underlying barrier to adoption, which could factor in all of the selections made, is an inherent unrealistic expectation from AI models, too. Like any technology, including video surveillance itself, the use of its accuracy and capabilities will be dependent on how it is sold and marketed, and whether it is specified for the right situation in the first place.

AI solutions to suit businesses and budgets of any size

IDIS has developed its AI solutions to ensure that businesses of any size, scale and scope can reap the benefits of deep learning analytics using the in-house developed and up to 98% accurate IDIS Deep Learning Engine, without the associated AI price tag.

IDIS' 4-channel retail and surveillance compact AI boxes are simple, licence-free, plug-in devices that pack a punch with essential AI functions ideal for small to medium businesses. In retail, the DV-1304 is being used to gain actionable customer behaviour and in-store insights often integrated with ERP software to boost profits, while the DV-1304-A allows smaller organisations to take a far more proactive approach to security and safety that was once the domain of large enterprises.

The IDIS latest range of 5MP Edge AI cameras has enabled phased AI adoption. For example, customers are deploying them to eliminate false alarms caused by conventional analytics or to target high risk areas such as entrances, perimeters, stock rooms and car parks.

Larger customers can choose from a powerful AI-ready DV-3200 series of servers opting for the AI and metadata tools they need, while multi-site customers that need centralised monitoring can opt to use IDIS Deep Learning Analytics as a service module within IDIS Solution Suite VMS, which comes with a single one-off license fee.

AI and future regulation

As we've seen from the responses to this year's survey, security professionals tend to side with the positives of AI – at least for where it can automate or significantly quicken manually repetitive tasks. Critical event search, where operators can search for specific terms such as 'man in red jumper', or 'blue car' across hundreds of hours of footage, is the obvious example of this.

It would, however, be remiss of us not to highlight the more holistic concerns with Artificial Intelligence. If tech leaders such as Elon Musk and Steve Wozniak are calling for a pause on AI research – and let's be clear, Musk isn't exactly known for his caution – there are likely inherent risks carried by its continued use and development.

What do these risks look like in security, though? As already discussed, ethical and data privacy implications are a concern for many, but wider regulation appears to be an underlying wish. Almost half of respondents stated that they believed regulation is urgently required for the use of AI-based video surveillance.

One in 10 went further, agreeing with the statement that usage of AI should be significantly restricted as we don't know enough about the consequences of its use.

What form such 'regulation' may take is another question altogether, and is not something we asked in this year's survey. The European Union's AI Act appears to be the first attempt of this, with the aim of regulating AI "to ensure better conditions for the development and use of this innovative technology". [13]

The security industry hasn't completely shied away. Guidance is already available from associations such as the BSIA on facial recognition alongside specialist consultancies beginning to provide regulatory advice in the field, but AI is more than simply facial recognition.[14]

Many applications exist and are likely to be developed in the coming years. As we have witnessed with the rise of 'Big Tech' companies such as Google, Amazon and Facebook, technology transcends national boundaries and is difficult to put back in the box once it's out, making tight regulation difficult at best. What is clear, is that those using the technology are calling for further guidance on the subject, given it's capacity for the unknown.

Deepfakes – the next frontier?

Deepfake technology is a form of AI that uses deep learning algorithms to create highly convincing, often deceptive, fake videos or audio recordings. It involves superimposing the likeness and mannerisms of one person onto another, often resulting in realistic but entirely fabricated content.

For full transparency, ChatGPT provided this definition. While we don't know the full extent of what AI will enable, we are beginning to understand the challenges culminating from deepfakes.

A quarter of respondents believe that deepfake technology is a major threat to trust in video surveillance – a fairly alarming but unsurprising number, given the coverage the issue is beginning to receive. TV programmes like the BBC's *The Capture* brought deepfake technology into the mainstream, while the

44%

believe regulation is urgently required for the use of AI-based video surveillance

1 in 10

believe AI usage should be significantly restricted

[13] European Parliament, EU AI Act: first regulation on artificial intelligence, https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

[14] IFSEC Insider, Three-way security partnership launches FaceComply to offer expert advice on facial recognition use, https://www.ifsecglobal.com/video-surveillance/security-partnership-launches-facecomply-offer-expert-advice-facial-recognition-use/

[15] Thomson Reuters, Practice Innovations: Seeing is no longer believing – the rise of deepfakes, https://www.thomsonreuters.com/en-us/posts/technology/practice-innovations-deepfakes/

proliferation of AI and its ability to produce realistic, but highly manipulative digital media, has added to the conversation in 2023.[15]

Thieves used voice-mimicking software to imitate an executive from a British energy company earlier this year, stealing more than $240,000 in the process. Meanwhile, a deepfake video was shared on social media in March 2022 appearing to show Russian President, Vladimir Putin, declaring peace.[16] Though quickly spotted as a fake, how long before the technology improves to a point of genuine realism?

The ramifications for those operating and owning video surveillance systems, who have always previously depended on video footage as indisputable evidence, are strong. It is yet another example where physical and cyber professionals will be required to cooperate to ensure cameras and their networks remain protected from attack or manipulation.

Dr Peter Kim, Global Technical Consultant at IDIS explains: "If not mitigated, deepfakes have the potential to compromise video's credibility as evidence and its value as a deterrent. In court, we are increasingly likely to see defence teams challenging the veracity of video evidence as they seek to cast doubt on its chronology and authenticity.

"Watermarking or chain of custody can't solve the risk entirely, although both technologies are essential. Yet techniques and deepfake tech are rapidly evolving. So, users need to ensure they are seeing, recording, and using as evidence is coming from legitimate video sources, and recorded on legitimate video recorders.

"End-to-end systems that use certificate-based mutual authentication and proprietary protocols are one of the safest surveillance tech options to ensure cyber security. Certificate information is exchanged during camera registration with an NVR, which must be authenticated when the NVR communicates with the camera for the system to operate. This means there is a guarantee that the video feed is coming from an IP camera paired with an NVR. It's cyber security working behind the scenes, without the need human interaction."

A human in the loop

It was encouraging to see that only 13% of respondents were concerned about the potential implications of AI for their job. After all, reports earlier this year indicated that millions of jobs could be lost to AI if it is to live up to its hype.[17]

Yet security has been using video analytics systems for several years now. AI is making these applications stronger, more accurate and quicker, but the importance of a human decision in the loop has yet to be degraded.

Deep learning algorithms can spot patterns and absorb vast data sets quickly, but context and human assessment from trained security professionals is viewed as essential if AI is to be utilised in an ethical and responsible manner.[18]

Delivering network security through a powerful mutual authentication

[16] BBC News, Deepfake presidents used in Russia-Ukraine war, **https://www.bbc.co.uk/news/technology-60780142**

[17] Forbes, Goldman Sachs Predicts 300 Million Jobs Will Be Lost Or Degraded By Artificial Intelligence, **https://www.forbes.com/sites/jackkelly/2023/03/31/goldman-sachs-predicts-300-million-jobs-will-be-lost-or-degraded-by-artificial-intelligence/?sh=46cfb1b8782b**

[18] IFSEC Insider: AI in physical security: Uses, myths & responsibilities, **https://www.ifsecglobal.com/video-surveillance/there-should-always-be-a-human-in-the-loop-ai-in-physical-security-uses-myths-responsibilities/**

The cloud and video surveillance

The move to the cloud continues to be identified as a key trend from industry reports and analysts. While many other business applications transferred their operations to cloud platforms to support remote working and access, improved efficiencies, reduce the risk of data loss, and more, the uptake from the security sector has always remained a little behind the curve.

But as we come towards the end of 2023, has this now changed? Omdia analysts indicate that the growth of Video Surveillance as a Service business models will be one of three big trends to impact the market following a growth in providers and flexible offerings.[19]

Our survey shows that over half of installers and consultants are recommending cloud-based platforms, though there is still some level of caution, with 42% only installing or recommending on-premise systems. Meanwhile, asking a similar question to the end-user audience, 28% answered that they use on-premise and are not considering a move towards the cloud.

While we haven't seen significant change to overall uptake from previous years, one in five (20%) are actively considering moving some, or all of their operations to a cloud model in the next two years.

Vendors, suppliers & consultants – Have they installed or recommended cloud technology in the last 12 months?	
No, I only install/recommend on-premise systems	42%
Yes, I have installed/recommended the cloud for video storage purposes	41%
Yes, I have installed/recommended a hybrid system	25%
Yes, I have installed/recommended the cloud for video analytics purposes	19%
Yes, I have installed/recommended the cloud for VMS purposes	18%
Yes, I have installed/recommended end-to-end VSaaS solution	7%

End-users – Are they actively using cloud-based video technology?	
Yes, I use the cloud for video storage purposes	32%
No, I use on-premise and am not considering the cloud for video surveillance purposes	28%
No, I use on-premise but am considering moving some/all of our operations to a cloud model in the next two years	20%
Yes, I use a hybrid system	16%
Yes, I use the cloud for video analytics purposes	12%
Yes, I use the cloud for VMS purposes	9%
Yes, I use a full end-to-end VSaaS solution	2%

Note, these results total more than 100% as respondents were able to tick more than one answer. For instance, they might use the cloud for both video analytics and VMS purposes, but not storage.

[19] IFSEC Insider, Omdia Insights – Trends in the video surveillance market, https://www.ifsecglobal.com/video-surveillance/omdia-insights-trends-in-the-video-surveillance-market/

It's also worth noting that we provided more specific options in our survey this year than in 2023, and consequently have an improved picture of the current market adoption. As far as end-to-end VSaaS cloud-based operations go – where the same vendor's cameras, storage and VMS is installed and run purely on an operational expenditure model – uptake remains relatively low, with 2% of end-users selecting this, and 7% of installers or consultants saying they'd recommended it as an option.

A hybrid approach is therefore most common, with some operations running on-premise, and others running on the cloud. 32% of end-users cited they were using the cloud for video storage purposes, 12% for video analytics, and 9% for VMS.

What are the barriers to adoption?

If uptake is yet to significantly increase, it would suggest that barriers to widespread adoption remain. Cyber security and data protection concerns were cited as the major barrier, according to 59% of respondents.

Data centres form the physical storage facilities where data sent to the cloud is held, meaning it is removed from the traditional storage method of an 'on-premise' server and outside the direct control of that organisation. Data centres do experience cyber-attacks, with two major Asian data centre firms having login credentials stolen and a Danish company falling foul of a ransomware attack just this year.[20]

Yet, cloud proponents would argue that these incidents are far less likely to happen compared to cyber-attacks on individual companies, given the physical and cyber security resources spent on protecting data centres. Specialist personnel, perimeter and physical security protection, and insider threat mitigation plans form a fundamental marketing and selling point for data centre companies, for instance.

Top 3 barriers to cloud adoption	
1	Cyber security data protection
2	Poor internet connection or bandwidth/ latency restrictions
3	Monthly recurring costs (Prefer to pay upfront for costs)

Poor internet connection or bandwidth restrictions were a close second in the most referenced barriers to adoption. 56% of respondents appear to have experienced this issue – whether directly or received feedback from customers – which will have an impact on the quality of video footage streamed back to cloud-based video management systems.

Experiences may depend on the location of the video surveillance systems being installed, of course. Though 5G network coverage is on the rise, there are significant regional variations with China and North America by far seeing the highest adoption rates.[21] Given the evolution of bandwidth-hungry video surveillance system technology – especially when live footage is expected

[20] Computing, Data centre hacks affect Apple, Microsoft and more, https://www.computing.co.uk/news/4076451/centre-hacks-affect-apple-microsoft; Data Center Dynamics, Danish hosting firms lose all customer data in ransomware attack, https://www.datacenterdynamics.com/en/news/danish-hosting-firms-lose-all-customer-data-in-ransomware-attack/

[21] Ericsson, 5G network coverage outlook, https://www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/network-coverage

to be viewed on VMS platforms remotely – this barrier may remain in place for many camera systems for a little while yet.

Several other challenges also exist, though it is worth noting that 'lack of understanding about the cloud' was selected by only one in four respondents this year – in 2021, it was selected by almost one in three. In addition, 3% fewer believe that the supply chain, such as integrators or their customers simply weren't ready to move to the cloud, in 2023 (20%) compared to 2021 (23%).

A standard cloud operating model moves one-off, upfront fees for on-premise storage facilities to an OpEx model of monthly recurring subscription costs. Though often highlighted as a benefit, 36% of respondents say they or their customers aren't necessarily keen on such a move.

Only 5% of those surveyed said that they had used or recommended the cloud before, and it didn't deliver. This could indicate that the vast majority of those who have used or recommended it as a solution, were satisfied with the outcome.

IDIS' Jamie Barnfield notes: "We're still some way off to seeing surveillance fully transition to cloud. Demand for end-to-end video solutions is increasing globally yet we're witnessing growth as users move away from a mix-and-match approach to on-prem solutions that come with all the hardware, software, AI-powered analytics, and network accessories to design and deploy a complete video system. For end-users that means a low total cost of ownership thanks to lower installation and maintenance costs with lower VMS fees too, plus single point of contact for the lifecycle of their surveillance infrastructure.

"We're increasingly seeing more customers opting for hybrid models and IDIS solutions can offer customers simultaneous edge, local NVR, and cloud configuration and storage. Plus, today's mobile apps put enterprise-class VMS functionality at security operatives' fingertips.

"Cloud can also spell bad business for integrators when partnering with a VSaaS vendor where recurring revenue benefits the manufacturer far more than the integrator. Customers can easily renew contracts or simply switch to new lower cost competitors to upgrade, since there's less need for technical services.

"End-users also get tied into long-term licence agreements which can lead to spiralling costs once users adopt analytics and integrations, and it's that OpEx cost which soon eats up annual security budgets, preventing or delaying other projects and upgrades."

What is driving adopters towards the cloud?

All this said, the vast majority (77%) of security, facilities and IT professionals do see benefits or opportunities to be gained from utilising the cloud for video surveillance purposes.

Remote accessibility of systems was cited by 54% of respondents, alongside flexibility to upgrade and adapt if more cameras or storage are required, by 48%. Ultimately, these two reasons generally underline the fundamental benefit of cloud-based technology – that of convenience.

Top 3 drivers for cloud-based video adoption	
1	Remote accessibility of systems
2	Flexibility to adapt if more storage or cameras required
3	Cyber security managed externally

The ability for security professionals to have active oversight over potential alerts without requiring an on-sight presence, and be able to monitor feeds remotely, is a reassuring one. Meanwhile, if the cloud is used for storage purposes, end-users know that footage can be stored remotely, reducing the risk of on-site tampering or removal of video feeds by criminals.

Moreover, the convenience of less hardware to purchase means that the video surveillance operation can be scaled quickly and easily. Storage retention periods, camera feeds, and additional analytics features can all be added to subscriptions without requiring on-site installations or impacting on budgets with a heavy one-off purchase.

The third most-cited reason for adoption also relates to convenience, and runs directly against the 59% of respondents who saw cyber security as a barrier. 35% of professionals see cyber security being managed externally, either by the service provider or at the end of the supply chain by the data centre, as a benefit.

Additional drivers included moving to an OpEx model (20%), lower upfront costs (18%), and preferring to have the whole CCTV system provided by one vendor (16%).

Vertical focus – Retail, construction and the public sector

We decided to follow on from last year's vertical segment focus, repeating one (retail) and exploring two more - construction and the public sector.

We repeated retail due to the continual challenges the sector is being faced with, as shoplifting numbers and violence against frontline workers are both on the rise.[22] Construction hasn't been immune to the economic impact, with high value tools and building materials targeted - so much so that legislation has been created around it in the UK.[23]

We also sought to understand a little more about projects in the public sector, such as infrastructure, transport, healthcare or local government video surveillance installations. How do procurement processes and budget constraints impact requirements for CCTV?

We asked broadly the same questions for each, including qualifying questions of whether the respondent either worked or had consulted, installed or specified work in each sector. If 'no' they were excluded from the data set. Numbers of respondents for these sections are therefore lower, but more focused.

Only those providing or supplying video surveillance products and services, such as installers, integrators, consultants, resellers and vendors were asked about the level of demand they were witnessing in the sector. All relevant professionals were asked about video surveillance requirements most important to that specific market.

There were some broader trends across all three sectors worth noting. Demand for integration of video surveillance with both other physical security systems and building management platforms was cited as important by at least 40% for each market, while the use of AI-powered analytics was also popular across the board.

Retail

Current demand in the retail sector is strong according to our findings. 38% said they were seeing a rising demand for video surveillance projects, 30% said it was high but not necessarily increased, and 18% said there was demand but it was relatively static. Only 8% cited demand being low or decreasing.

These were very similar findings to last year's results, though those seeing demand increasing was 4% higher this year than in 2022.

Top 5 requirements for AI video surveillance applications in retail

1	Loss prevention & security purposes
2	Customer and in-store intelligence
3	Facial recognition
4	People counting
5	Object detection

[22] IFSEC Insider, Tackline the retail crime epidemic with technology – Are body-worn cameras the answer? https://www.ifsecglobal.com/video-surveillance/tackling-retail-crime-epidemic-are-body-worn-cameras-the-answer/

[23] Equipment Theft (Prevention) Act 2023, https://bills.parliament.uk/bills/3192

Regarding the types and uses of video surveillance cameras most required in retail projects, 'simple surveillance for loss prevention' was considered as most important by 64% of relevant professionals. This has risen sharply since last year's survey, where 45% selected this. We also asked about AI-based analytics and what is most in demand from such software - 66% selected AI-powered analytics for loss prevention, security and safety.

A significant proportion were or have already explored more advanced crime prevention capabilities. AI-based facial recognition was considered important by 59%, for instance. This is not without its implementation challenges, especially in regions that have stricter data protection laws, though is being increasingly explored by retailers. The Co-Op's use in 35 stores in the UK last year provides a clear example of the benefits security professionals see, as well as the challenges involved from a privacy perspective.[24]

For anyone following news stories in the UK at least, this would be of no surprise, with a surge in shoplifting being described as an 'epidemic' affecting retail stores and supermarkets across the board.[25]

Video surveillance as a deterrent, and AI-powered applications to support reporting and evidential processes, are therefore viewed as vital for the retail sector's future. As the high street continues to feel the heat from e-commerce platforms and lower footfall, loss prevention is extremely important to protect profits and mitigate the risk of falling victim to targeted theft.

Remote management and viewing capabilities were also considered important by 55% of respondents, indicating security managers and teams are increasingly turning to cloud-based platforms to ensure stores can be monitored at all times.

Retail is perhaps the most widely cited use-case for video analytics software applications in video surveillance systems outside of pure security. Demand for customer and store layout or footfall intelligence remains, it would seem. 61% of those surveyed regarded analytics for customer and in-store intelligence as important, while 35% also selected analytics for customer behavioural analysis.

The add-on AI Box for Retail (DV-1304) is installed across 1000s of stores globally, delivering local and centralised customer and in-store intelligence from existing IDIS DirectIP® security cameras.

[24] IFSEC Insider, UK retailer Co-Op's use of facial recognition cameras faces legal challenge from privacy campaigners, https://www.ifsecglobal.com/video-surveillance/co-op-facial-recognition-cameras-face-legal-challenge-privacy-data-protection/

[25] Reuters, Britain faces epidemic of shoplifting as Primark profits hit, https://www.reuters.com/business/retail-consumer/britain-faces-epidemic-shoplifting-primark-profits-hit-2023-09-12/

Construction

Demand is also strong in construction, though not quite as much as in retail, according to our respondents. 31% cited they were seeing rising demand, 33% that it was high but not necessarily increasing, and 18% that there was demand but relatively static. 15% responded that demand was either relatively low or decreasing.

Like retail, simple surveillance for loss prevention purposes was the most important underlying reason for video surveillance projects in the construction sector (64%). Over half (54%) also cited specialist mobile surveillance units to protect construction sites, which is a relatively sector-specific demand. Such mobile surveillance units are often built to withstand tampering or attack by would-be criminals, so it is no surprise that almost a quarter (22%) selected vandal resistant cameras as being in demand, too.

Construction sites go through several stages of design and layout making them difficult to patrol, while key entry points to buildings such as doors and windows aren't necessarily in place for much of the construction process. Perhaps this is why video surveillance that links directly to alarms, audio systems and access systems is imperative to ensuring holistic security across the site. 52% cited integration with other physical security systems as one of the most in-demand features when installing CCTV systems.

For similar reasons, night-vision/infrared technology may have scored higher than other markets. 43% deemed such technology as important for video surveillance projects, highlighting the challenges involved with securing an ongoing construction site where heavy tools, equipment and plant machinery are likely left overnight with significantly fewer people around to act as a deterrent.[26]

Top 5 requirements for video surveillance technology in construction	
1	Loss prevention, crime & anti-social behaviour
2	Mobile surveillance units
3	Integration with other physical security systems
4	Night vision/infrared technology
5	AI-powered video analytics

[26] Pbctoday, Construction site crimewave: 9 in 10 tradespeople have been victims of theft, https://www.pbctoday.co.uk/news/planning-construction-news/construction-site-crimewave-9-in-10-tradespeople-have-been-victims-of-theft/129183/

Public sector & government projects

Acknowledging that the types of public sector and government projects can vary substantially - from critical national infrastructure projects through to one-off local council CCTV installations, there remains significant demand for video surveillance projects. 43% of respondents said that they were witnessing rising demand, while another 27% said it was high, but not necessarily increasing. Only 7% said demand for video surveillance was either low or decreasing.

We also asked which areas were specifically experiencing demand. Public safety such as local government projects in towns was the most popular response (63%). Healthcare, power generation, transportation projects, criminal justice and education systems were all selected by over 40% of those surveyed, too.

For public sector projects, integration with other physical security systems was particularly high at 70%. In fact, this was the most popular response when asking respondents what video surveillance technology was most important to government or public sector projects. 45% also selected integration with other building management systems.

A driver behind these responses may be the push for a more joined up approach to security and safety within public sector projects. Smart city projects, where video surveillance systems are part of a wider data network feeding into central intelligence platforms are on the rise as we explore In the next chapter, while transport hubs and infrastructure sites will be required to have high-security processes.

Demand for video analytics and AI is also high (45%), indicating projects are future proofing and investing into more sophisticated systems for security and operational purposes.

70%

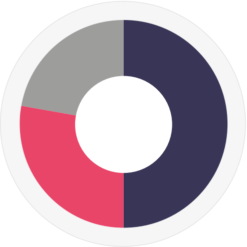
believe integration with other physical security systems is critical for public sector video surveillance projects

What's next? The role of video surveillance in sustainable and smart ecosystems

What's next for video surveillance, then? As we've examined throughout this report, uptake of new technology continues to grow as video surveillance systems increasingly contribute towards overall business objectives, alongside their traditional roles of safety and security.

Our first chapter highlighted that demand for upgrade projects and new installations has remained strong in the past 12 months. As we've now moved through a period of further economic instability however, will this continue?

We specifically asked end-users whether they were expecting to upgrade or add to their video surveillance system in some capacity – be it hardware or software – as we move into 2024. Exactly half (50%) of respondents cited they expected to upgrade or add to their video surveillance system in the next 12 months. 28% were considering it, and 22% said they were not expecting to do so.



Do end users expect to upgrade or add to their video surveillance systems in the next 12 months?

- ■ (**50%**) Yes
- ■ (**28%**) Considering
- ■ (**22%**) No

Though predictions are always likely to be a little more reserved and these figures don't account for new businesses or projects opening up, with one in five indicating they wouldn't be undertaking new projects, suppliers may need to prepare for a tougher year ahead.

Will sustainable credentials play a bigger role in procurement decisions?

There is little doubt that sustainability is an increasingly important metric to track and report on for organisations. As 2030 Net Zero goals loom closer, organisations – especially those larger companies reporting to shareholders – are under pressure to demonstrate their sustainable credentials.

According to McKinsey, more than 90% of S&P 500 companies in the US now publish ESG (Environmental, Social and Governance) reports in some form, and this is beginning to go beyond simply their direct emissions.[27] Though sustainability initiatives like the UN Global Compact Supply chain acknowledge the challenges of extending sustainability principles because of the "scale and complexity of many supply chains", reporting requirements are only likely to be extended. Certainly this is the case for new build projects, where environmental credentials are now factored into the building's architecture and design from the very start. Sustainability is being 'baked in' to contracts when out for tender, including when specifying video surveillance systems.

[27] McKinsey, Does ESG really matter – and why? **https://www.mckinsey.com/capabilities/sustainability/our-insights/does-esg-really-matter-and-why**

We therefore asked respondents whether they considered sustainability credentials in their choice of video surveillance provider. The majority (66%) said yes. Only 13% answered no, and the remainder (21%) admitted they weren't sure what impact video surveillance plays in the sustainability agenda.

Perhaps this serves as an important message then, to the sector's hardware and software providers. Given sustainability output could include a variety of elements, such as manufacturing processes, distribution and packaging systems, and the energy efficiency of the products themselves, there is an opportunity to educate their buyers of any sustainable credentials they may have.

Smart ecosystems

To end this year's report, we thought we'd look ahead and provide several overarching statements on video surveillance to understand the wider perspectives from security, facilities and IT professionals.

The results make for interesting reading. There is a clear perception by over half of respondents (51%) that video surveillance systems are already playing an important role in developing smart buildings, while 36% believe that they will play a role in the future.

Moving another step on this journey, 40% also cite their belief that systems are playing a role in developing smart cities in today's landscape, with 26% believing that they will in the years to come as well.

In addition, almost a third of professionals see greater collaboration and integration between public and private video surveillance operators – a move that will no doubt be beneficial to those tasked with public safety and security, but questioned by data protection and rights campaigners. Certainly, if this trend does come to fruition, proper oversight and proportionality will need to be factored in.

Video surveillance and the smart ecosystem

Video surveillance systems are already playing an important role in developing SMART BUILDINGS	51%
Video surveillance systems are already playing an important role in developing SMART CITIES	40%
Video surveillance systems will play a role in SMART BUILDINGS but we're not there yet	36%
Public and private video surveillance operators will increasingly partner and feed into central databases	30%
Video surveillance systems will play a role in SMART CITIES but we're not there yet	26%

There are indeed a growing number of use-cases for video surveillance systems being used to create smarter building, or city-wide ecosystems. The Digital Catapult initiative is working with businesses in London to boost digitisation adoption, which it ultimately hopes will drive innovation in city infrastructure, traffic, transport and energy management.

Meanwhile, law enforcement agencies are turning towards technology in New York, where the ShotSpotter

66%

consider sustainability credentials in their choice of video surveillance provider

project is optimising a gunfire detection system via sensors that can integrate into preexisting public video surveillance devices.[28]

And we haven't even started on the Vision 2030 roadmap outlined by the Kingdom of Saudi Arabia (KSA) for smart city projects such as Neom and 'The Line'.[29]

What perhaps separates the responses is the definition of 'smart'. The term has become ubiquitous to describe IoT devices such as home cameras sending alerts to users' phones, to feeding actionable data into a fully autonomous building management system, and everything in between.[30]

While the start of the 'smart' spectrum is in play on a daily basis, it is likely we haven't quite yet found where the other side ends.

Whichever definition you decide, opportunities for all those in the video surveillance supply chain are abound, because what isn't in doubt is the essential role cameras are set to play in the evolution of smart ecosystems in the future.

[28] IoT World Today, The definitive list of smart cities projects taking the world by storm, **https://www.iotworldtoday.com/smart-cities/the-definitive-list-of-smart-cities-projects-taking-the-world-by-storm**

[29] IFSEC Insider, Opportunities abound for the security sector in Saudi Arabia? **https://www.ifsecglobal.com/corporate-security/opportunities-abound-for-the-security-sector-in-saudi-arabia/**

[30] For a closer examination of the 'smart' environment, see: IFSEC Insider, Podcast: Episode 15 – Why physical security is integral to the smart building ecosystem, **https://www.ifsecglobal.com/podcasts/episode-15-why-physical-security-is-integral-to-the-smart-building-ecosystem/**

About the respondents

The analysis and data outlined in this report come from a survey sent out by IFSEC Insider over the summer period of 2023 – beginning in mid-July and closing in early September.

This year's survey was open to a range of roles in security, as well as those who manage, or are responsible for managing building systems and facilities. IT and facilities professionals were consequently encouraged to provide their viewpoint, given the overlap in responsibilities for estates and IP-connected technology.

Anyone who selected 'not in the security/facilities profession' was automatically excluded from taking the survey. We also removed any duplicate entries, or those that were deemed to be disingenuous, where answers did not corroborate or open field questions were clearly not filled in appropriately.

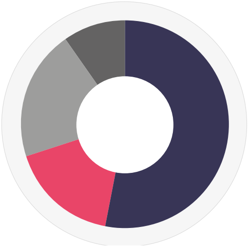
In total, the 2023 Video Surveillance Report is based on the answers of 566 unique respondents. It should be noted that not all 566 filled out every question, while logic was assigned early on to ask those providing products/services (such as installers or consultants) slightly separate questions to end-buyers (such as in-house security managers and directors).

Demographics of respondents

The responses were open to a global audience to provide an overarching perspective of the video surveillance market. For a thorough and detailed breakdown of regional variations, we would recommend our sister Informa research and analyst brand, Omdia.[31]

The vast majority of responses came from the EMEA region, totalling 84%. 45% came from the UK, 15% from the rest of Europe, 18% from countries across Africa and 6% from the Middle East. An additional 6% of respondents were based in India, and 3% from the United States.

We provided a range of different job role options to select from so that we could better target specific questions more relevant to those roles. 9% of respondents selected 'other' and another 6% held roles in vendors, manufacturers or distributors, we were able to group those remaining into three broad but defined categories.[32]



Job roles of respondents to the 2023 Video Surveillance Report

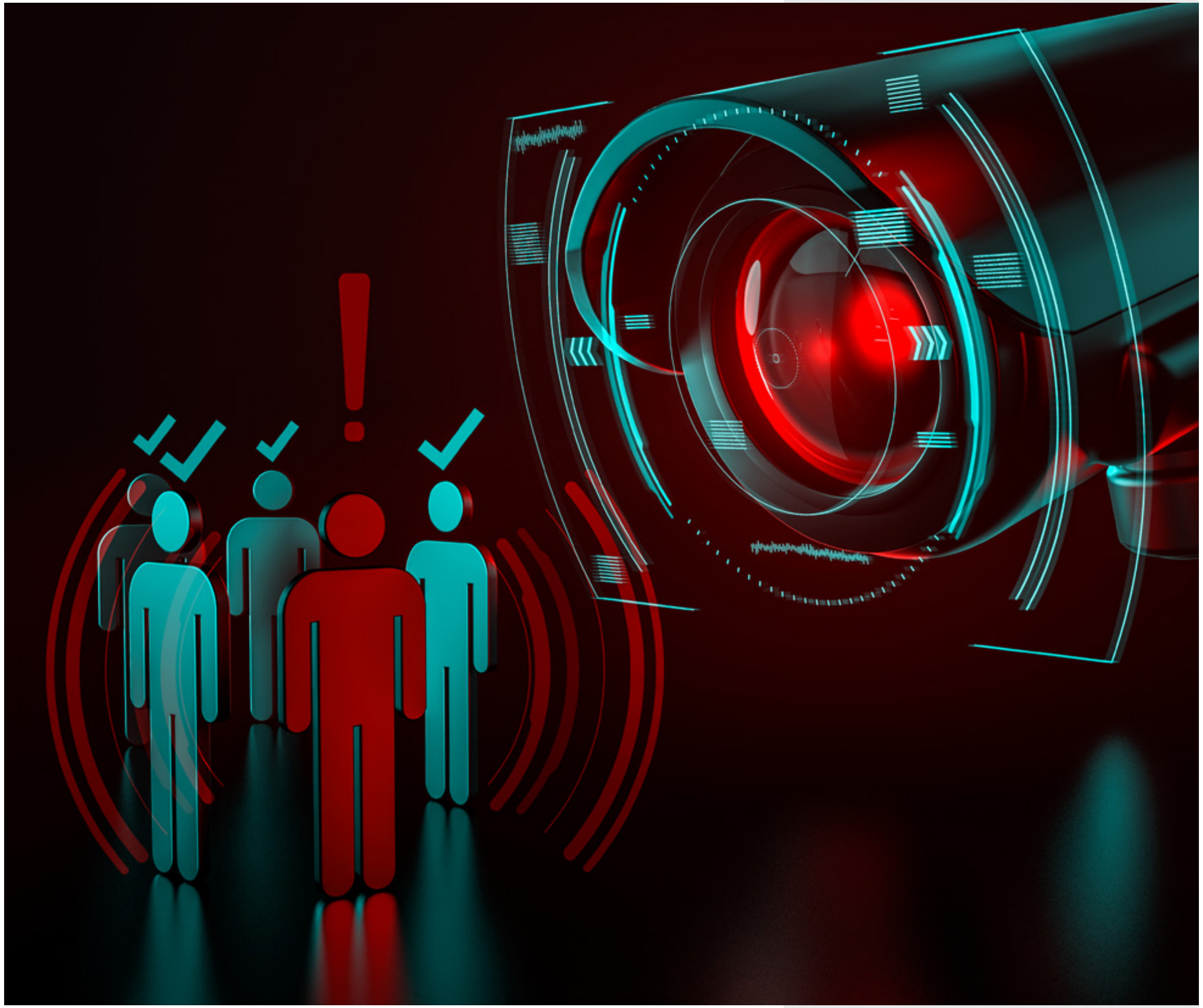
- ■ (**50%**) End-users
- 🟥 (**16%**) Consultants
- ▨ (**19%**) Installers/Engineers/ integrators
- ▨ (**9%**) Other

[31] Omdia, Video Surveillance & Analytics Market Report 2023, **https://omdia.tech.informa.com/products/video-surveillance--analytics--2023**

[32] Respondents' roles when selecting 'other' included security systems designers, heads of safety and estates, architects and security tech developers.

Defining anyone who has an in-house security, facilities or C-suite role as an end-user, these respondents made up 50% of the total.[33] 19% of those surveyed classed themselves as installers, systems integrators and technicians, while 16% were either security or IT consultants.

We segmented end-user industries a little further. Key sectors respondents worked in included government or public sector (16%), manufacturing/engineering (11%), construction (10%), and distribution/supply/logistics (7%), alongside representatives from retail, education, healthcare, finance and banking, residential housing, hospitality and critical national infrastructure.



[33] For the purposes of this report, we also included 'business owner/senior executive' in the end-user category, though we are aware this may include some installers, integrators or consultants who run their own businesses.