



FLEXIBLE WORKING

Martyn Ryder, looks at the capacity for the cloud to unlock critical insights and help manage costs for business that support flexible working

When the global pandemic took hold in spring 2020, the closing of business premises saw those who were able to turn to homeworking. Organisations that had already embraced digital transformation and the use of cloud-based infrastructure would have found the administration and coordination of such a setup straightforward. In contrast, those businesses that still relied on older systems on-premises will have had to quickly resource a homeworking setup from scratch.

As restrictions fluctuated and some went back to the office, it became apparent that the new and wholly

more flexible model was preferable for those who could work in such a way with ease. Some now found the restrictions of the 9-5 office too stifling, and its considerable overheads an unnecessary financial burden. Conversely, the attraction of a 100 percent homeworking setup began to wane with many reporting a lack of face-to-face contact or opportunity for collaboration with colleagues. Part home, part office, or 'flexible' working, therefore, offered a solution.

But there are challenges associated with an increased number of people coming and going from a site, and patterns of movement that are difficult to

The intelligence generated from VSaaS insights can be used to inform many aspects of decision making

predict. The demand for flexible working is prompting many managers to look to technologies that can help them not only ensure the security of their premises and the people within, but also help them keep track of office use and ensure appropriate health and safety measures are in place. Making this feasible while retaining staff and delivering growth, demands a scalable futureproof solution.

CCTV cameras have long been a common sight across many industries, used to secure buildings both inside and out. Now, as technology continues to advance, digital infrastructure supports cloud-enabled alternatives to these legacy analogue-based systems. The internet of things (IoT) makes it possible for security devices to be connected to a network, increasing their use beyond the purposes for which they were originally intended. Connecting IoT devices and sensors, rather than running them in isolation, makes them much more powerful in terms of their increased scope and the outputs that a combined system can provide.

Video surveillance as-a-service (VSaaS) is a managed service that harnesses the power of data and represents the next generation of physical security. VSaaS makes the connection of cameras to cloud platforms easy to facilitate, and the wealth of insights that can be generated using analytics and AI results in a smart business and security solution that can be customised and scaled to meet individual requirements – all monitored from a single platform. The intelligence generated from actionable insights can be used to inform many aspects of decision making. For example, people-counting and queue-monitoring capabilities allow managers to check the number of visitors on site and make decisions about controlling flow around the building based on real-time visitor demand.

Historically, access control was commonly part of a building or office manager's responsibility and often a simple box-checking exercise. With the traditional model, if a key card is presented, a door will open, regardless of who is trying to gain access. Managing the system and looking for potential security breaches is a manual task, and often a low priority on the list of prime security concerns.

ACCESS ALL AREAS?

This is where access control as-a-service (ACaaS) comes in, facilitating the smarter automation of entrance and exit points with full visibility and control over confirmation of user identity and the granting or denying of admission. Now, an access control device can give access to anyone who, for example, has pre-booked a desk at a co-work facility, simply by presenting a QR code on a mobile phone. Video surveillance can provide a second factor of authentication to confirm the identity of the member entering the premises, minimising the chances of attempted access for malicious endeavour.

We also know that demand for both VSaaS and ACaaS is on the rise. In a 2019 independent survey of 1,000 IT decision makers conducted by Morphean, 84 percent of IT managers stated that they were currently using (48 percent) or considering using (36 percent) a cloud-based video surveillance or access control solution. Of those considering VSaaS and ACaaS, 79 percent anticipated introducing these solutions to

their business within 12 months. Indeed, the VSaaS market alone is expected to experience huge growth, rising to a projected \$4.7-billion by 2025 at a CAGR of 16.0 percent.

Better security is just one element of what VSaaS and ACaaS can offer. Through the use of collected and analysed security data intelligent insights about how the business operates can be used to inform decision-making processes, leading to more efficient operations and even cost savings. As an example, efficiencies can be made around the use of energy, lighting and heating during quieter periods according to data from the access control system and other interconnected devices.

People-counting capabilities lets managers know exactly who is on site and helps build up intelligence around its regular use. Having such insights about the number of people and their movements within the premises may be important for insurance purposes to ensure the required levels of security/fire protection are adhered to. Such intelligence can also benefit users by improving online scheduling, simplifying the choice to work from home or to book office space as requirements dictate, based on real-time occupancy and usage figures.

THE VSAAS MARKET ALONE IS EXPECTED TO RISE TO A PROJECTED \$4.7-BILLION BY 2025

Of course, with rising costs a concern, it's critical that any security solution proves to be cost effective. Based on an as-a-service model, VSaaS and ACaaS are paid for monthly as an operational expense, meaning that there is no requirement for up-front capital. Moreover, cloud infrastructure then opens up remote management capabilities to enable device monitoring at the touch of a button. Technicians are able to perform maintenance remotely, offering businesses faster response times and the ability to update software and upgrade firmware without the need to be physically present; this helps avoid costly callouts and reduces travel/fuel costs for the installer.

This model facilitates simple scalability as part of a fluid modern solution, evolving in-line with the business. For example, such a system enables the automation of pre-set procedures, including the triggering of alerts and alarms via digital (IP) audio speakers in response to an incident, such as a fire or even criminal attack. All staff and clients can be directed to safe zones by a completely automated process without the need for human intervention, and managers can have confidence in the technology to manage such situations swiftly and safely.

If fluctuations in Covid-19 infection rates return and in doing so become a cause for concern, building owners and managers will understandably be anxious about what this could mean for their sites over the longer term. This places them under pressure to maintain a clean, infection-free environment that people will be confident and comfortable to keep using. For the co-work facility, a loss of clients means a loss of revenue, so making sure

▶ that people keep returning to use their facilities is mission critical. At the front entrance, touch-free or contactless access control technology can be implemented to remove the need to touch shared surfaces, thereby minimising infection risk. Once inside, IP audio speakers, connected to the video surveillance system, can automatically trigger messages as required to promote safe practices. With government rulings around such measures no longer in place, alerts could be for advice only, but the technology and the capability are there to be used and tailored for any future event where important health and safety messages may need to be conveyed.

VSAAS MAKES THE CONNECTION OF CAMERAS TO CLOUD PLATFORMS EASY TO FACILITATE

Making the right choices about partners and technology is business critical to ensure that services and solutions can be trusted. Connecting any physical security technology to an IT network is not without risk, so it's imperative to consider the cybersecurity of each device. Unsecured systems which are not manufactured in accordance with cybersecurity principles can be easily used as a backdoor to gain access to a wealth of information;

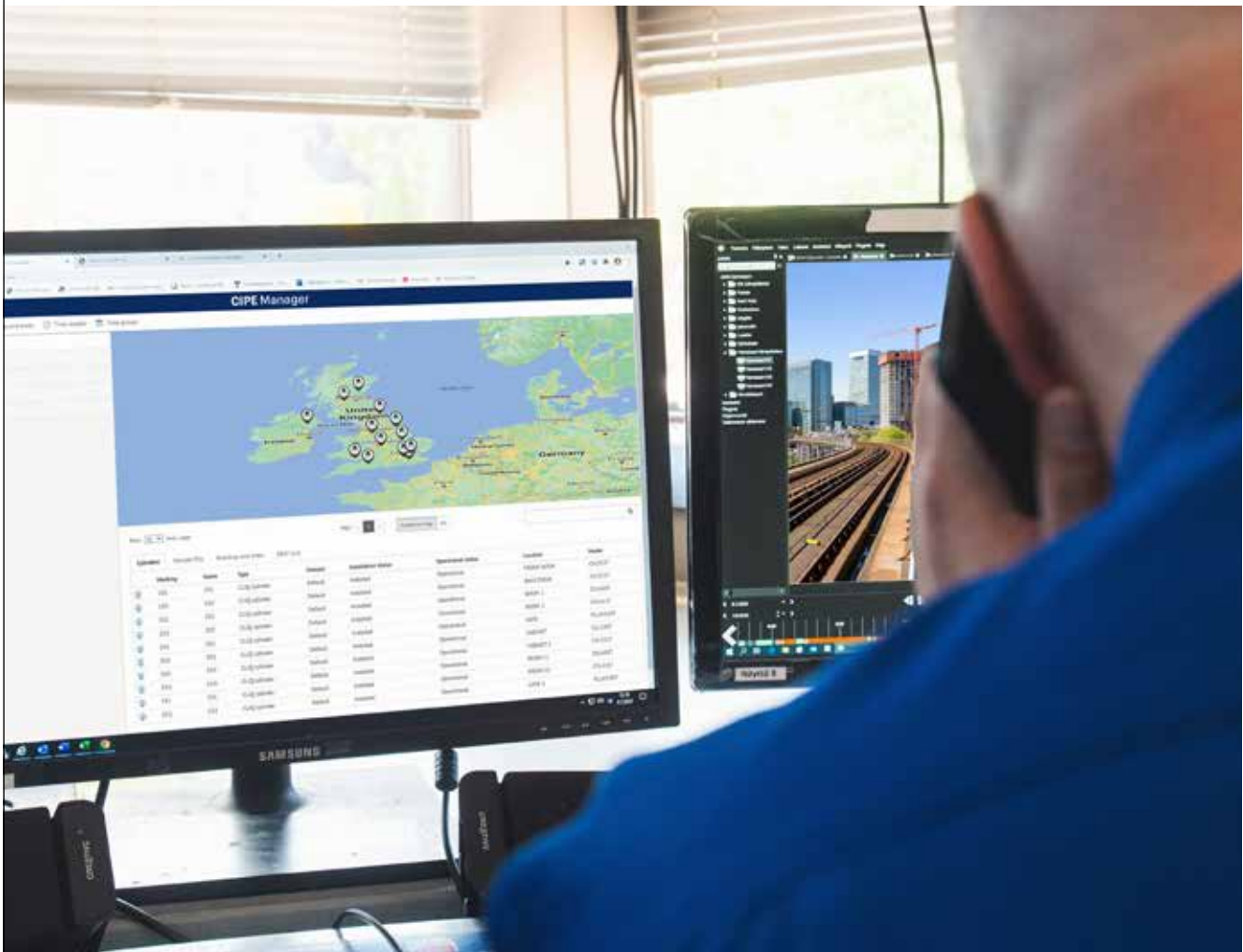
for example, using a vulnerability in a security camera or sensor to attack a customer database.

When it comes to modern cloud-enabled physical security solutions, businesses who have not thoroughly checked the vendor credentials cannot be wholly confident that their valuable surveillance data is secure. This places their business at risk, where data breaches, cyber attacks and even terrorist activity can have a devastating impact. According to the IBM Cost of a Data Breach Report 2021, the average cost of a stolen data record now stands at \$161, and the average overall cost of data breach incident stands at \$4.24-million. When downtime is factored in, plus the long-term damage to brand and reputation, it can have a devastating impact.

When seeking out appropriate tools and technologies, it is all too easy to use devices that have been manufactured cheaply and brought to market quickly, often hastily produced in countries with low levels of quality assurance and with poor transparency of labour laws. It is essential, therefore, to partner with a trustworthy provider that has a track record of success, as well as adhering to ethical practices and codes of conduct that are common across the EU. Such partnerships will provide assurance of corporate governance and allow closer scrutiny of manufacturing processes. Cloud physical security technologies, delivered in partnership with a trustworthy solutions provider, can offer a futureproof and highly scalable system to support the success of the flexible working model in an ever-changing world ●

Martyn Ryder is VP Sales and Marketing at Morphean SA

Access control as-a-service facilitates smarter automation of entrance and exit points with full visibility and control over granting or denying of admission



Picture credit: Ablouy UK