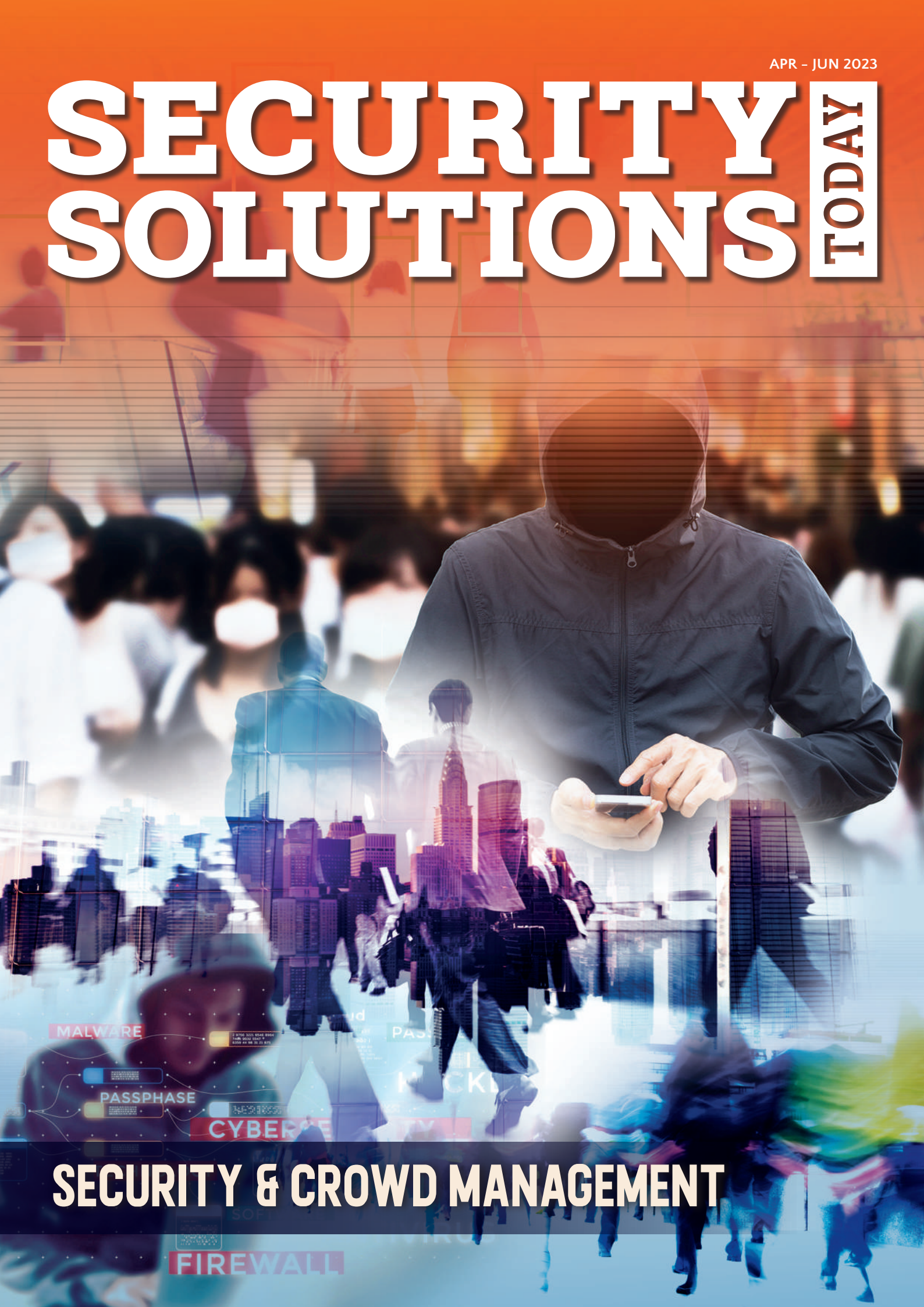
APR – JUN 2023

# SECURITY SOLUTIONS TODAY




## SECURITY & CROWD MANAGEMENT

# IN THIS ISSUE


4 **In The News**
Updates From Asia And Beyond

26 **Cover Story**
+ Applications of Video Surveillance Implementation for Crowd Management

32 **Calendar Of Events**

# CONTACT

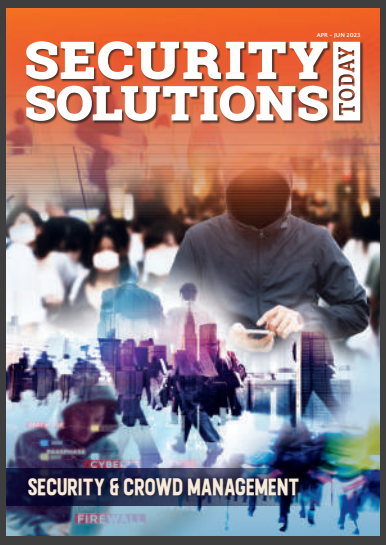

**ASSOCIATE PUBLISHER** Eric Ooi (eric.ooi@tradelinkmedia.com.sg)

**EDITOR** Navkiran Kaur (sst@tradelinkmedia.com.sg)

**MARKETING MANAGER** Felix Ooi (felix.ooi@tradelinkmedia.com.sg)

**HEAD OF GRAPHIC DEPT / ADVERTISEMENT CO-ORDINATOR**
Fawzeeah Yamin (fawzeeah@tradelinkmedia.com.sg)

**CIRCULATION** Yvonne Ooi (yvonne.ooi@tradelinkmedia.com.sg)


Vectors/Images Credit: Freepik.com
*Designed by Fawzeeah Yamin*


**SECURITY SOLUTIONS TODAY**
is published quarterly by Trade Link Media Pte Ltd (Co. Reg. No.: 199204277K)
1 Paya Lebar Link, #04-01, Paya Lebar Quarter 1 (PLQ 1), Singapore 408533
Tel: +65 6842 2580
ISSN 2345-7112 (E-periodical)



Disclaimer: The editor reserves the right to omit, amend or alter any press release submitted for publication. The publisher and the editor are unable to accept any liability for errors or omissions that may occur, although every effort had been taken to ensure that the contents are correct at the time of going to press.

The editorial contents contributed by consultant editor, editor, interviewee and other contributors for this publication, do not, in any way, represent the views of or endorsed by the Publisher or the Management of Trade Link Media Pte Ltd. Thus, the Publisher or Management of Trade Link Media will not be accountable for any legal implications to any party or organisation.

Views and opinions expressed or implied in this magazine are contributors' and do not necessarily reflect those of Security Solutions Today and its staff. No portion of this publication may be reproduced in whole or in part without the written permission of the publisher.

For advertising interests, please email us at **info@tradelinkmedia.com.sg.**

# ASIA'S MOST ANTICIPATED I&T EVENT

**12-15/4**
Hong Kong Convention and Exhibition Centre

**12-22/4**
Click2Match

**REGISTER NOW FOR FREE ADMISSION**

Tel : (852) 1830 668 | Email : exhibitions@hktdc.org
App : HKTDC Marketplace | Web : innoex.hk

# GEOPOLITICAL TENSIONS ENABLED INCREASED HACKTIVIST CYBER THREATS IN 2022

*New report from FS-ISAC highlights opportunity for cyberattacks against public and private institutions*

**Singapore –** FS-ISAC, the member-driven, not-for-profit organisation that advances cybersecurity and resilience in the global financial system, today announced the findings of its annual Global Intelligence Office report, Navigating Cyber 2023.

The latest report showcased the effect that Russia's invasion of Ukraine had on the global cyber threat landscape, sparking a flood of ideologically driven "hacktivism" that continues to this day. Driven from both sides of the conflict, the threats have increased substantially within the financial services sector, particularly for institutions in countries that Russia considers hostile. These threats can come from hacktivist groups or directly from the nation-states themselves.

In Asia-Pacific (APAC), FS-ISAC members in the first half of the year reported rising concerns around the cyber impact of the Russia-Ukraine War and around state-sponsored attacks by China and North Korea. In the second half of 2022, members reported an increase in cyber incidents involving impersonation of specific individuals. According to a mid-December survey of members, APAC members consider ransomware to be a major threat, along with reports of rising cyber insurance premiums and exemptions for ransomware. The APAC region, home to a significant number of small and medium-sized enterprises (SMEs) with limited resources and insufficient cybersecurity measures, has been particularly vulnerable to these attacks.

"Unfortunately, the growing involvement of non-state actors attacking on an ideological basis and the manipulation of information by malicious actors will continue to sow uncertainty across the landscape in actual and perceived security threats," said Steven Silberstein, CEO of FS-ISAC. "The best tool available for financial institutions to combat this is intelligence sharing, allowing collaboration across the global industry and ensuring better cyber preparedness. Cyber threats often evolve faster than the tools we use to combat them, but our strength is in our community."

The report also highlights that some of the more traditionally common cyber threats, such as DDoS attacks and ransomware, are becoming more sophisticated and the suite of tools at a malicious actor's disposal continues to develop.

Looking ahead into 2023, some of the key drivers of change in the threat landscape include:

- **A growing market for malware-as-a-service:** As threat actors become specialised in specific aspects of the kill chain and offer their services in skills and code for sale, cyberattacks become easier to orchestrate, less attributable, and of lower risk. Supply chain threats proliferate as key software, authentication, technology, and cloud service providers are increasingly targeted.
- **The accessibility of AI helping attackers, and defenders:** The emergence of new AI-technology lowers the barrier for hacking, allowing threat actors to use tools like ChatGPT to design ever more convincing phishing lures. However, those same tools will be leveraged to strengthen defences as well.
- **Cryptocurrency offers a prime target for cybercriminals:** Cryptocurrency and digital assets are becoming more integrated into global financial infrastructure, generating a complex regulatory environment for multinational firms. In addition, threat groups will continue to finance their operations using cryptocurrency, highlighting the need for better oversight and asset class protections.

*Image by Freepik*

*continue on page 6*

# ACCESS + POWER SIMPLIFIED.

Altronix Trove™ access and power integration solutions easily combine Altronix power distribution with the leading access brands to streamline system design and deployment. Simplify board layout and wire management, while reducing installation and labor cost- increasing profits and ROI.

**TROVE™MAX**
Maximum Density Solutions,
24-Doors with Power or 36-Doors without

**TROVE™ PLUS**
Pre-configured Kits include
Power Distribution and
Wire Management

**TROVE™ RACK**
2U Rack Mount Drawer Supports
up to 8-Doors with Power

Altronix®

YOUR LEADER IN **ACCESS & POWER INTEGRATION**

"Cyber criminals are endlessly inventive and aided by technological advances," said Teresa Walsh, Global Head of Intelligence at FS-ISAC. "The emergence of new technologies and malware delivery tactics will require institutions to ensure they keep up with evolving cyber threats on a continuous basis and focus on resilience so they can keep operating no matter what happens."

The threat landscape is rapidly changing, and organisations face key challenges of increasing regulation around the world, seismic shifts in the cyber insurance market, and cybersecurity talent shortages. Facing massive changes in their operational environment, the financial services sector must navigate pressures to reduce costs without compromising the ability to continuously evolve defences and enhance operational resilience.

### Methodology

The Navigating Cyber 2023 report is sourced from FS-ISAC's thousands of member financial firms in 75 countries and further augmented by analysis by the Global Intelligence Office. Multiple streams of intelligence were leveraged for the curation of the round-up, which examined data from January 2022 to January 2023. The publicly accessible version of the report can be found here. The full report is only available to member financial institutions.

### About FS-ISAC

FS-ISAC is the member-driven, not-for-profit organisation that advances cybersecurity and resilience in the global financial system, protecting the financial institutions and the people they serve. Founded in 1999, the organisation's real-time information-sharing network amplifies the intelligence, knowledge, and practices of its members for the financial sector's collective security and defences. Member financial firms represent $100 trillion in assets in 75 countries. ■

## ACTIVE INTELLIGENCE'S ASTRA™ ANOMALY DETECTION SOLUTION CAPTURES GLOBAL ATTENTION

*Integrations with Leading VMS Solutions to be Demonstrated at ISC West in Booth 30057*

**Port Charlotte, FL –** Active Intelligence, innovator of anomaly detection software for physical security and business intelligence applications, is building on the momentum of its successful official launch, which took place this past November. The company's ASTRA™ Autonomous Video Anomaly Detection solution proved to be an eye-opener at ISC East by demonstrating how the solution provides the unique ability to detect any anomalous activity in a video feed without the restrictions of conventional rules-based video analytics systems. "ASTRA is already in the final stages of on-site beta testing with several clients," said Ken LaMarca, CEO, Active Intelligence. "The global reaction to ASTRA has been even better than we anticipated, with inquiries coming from a wide range of private business and public organizations."

To further validate ASTRA's effectiveness, Active Intelligence is offering a free 30 day trial to qualified users. "The best way for us to provide proof of performance is to let prospective customers take ASTRA for a test run on their own video system," said LaMarca. "There have been so many claims made about video analytics by so many companies over the years, we want to definitively prove to potential customers that ASTRA delivers on its promise." Active Intelligence will be showcasing ASTRA at ISC West booth 30057 in Las Vegas. Visitors can witness the potential of this proprietary anomaly detection solution and apply for the free 30-day demo in person. Integrations with

Milestone XProtect, Qognify Ocularis, and Genetec Security Center will be featured.

Active Intelligence's ASTRA takes a modern approach to video security, detecting both known and unknown threats by identifying statistical anomalies in video feeds. The software, powered by AI and Machine Learning algorithms, first learns what is normal in a specific camera's field of view over a short period of time, and then detects abnormalities and alerts security operators when an anomaly is present.

Unlike conventional rules-based video analytics, ASTRA's anomaly detection offers infinite detection capabilities, including events like a person in distress, physical violence, fire and smoke, pedestrians walking in front of moving vehicles, theft, vandalism, traffic jams, wrong way driving, and much more. The unlimited detection capabilities also make ASTRA ideally suited for a wide range of commercial and industrial business intelligence applications. ■

# BOSCH CLIMATE SOLUTIONS IS HELPING EBM-PAPST DEVELOP A COMPREHENSIVE SUSTAINABILITY STRATEGY

International technology specialist ebm-papst is putting its trust in the expert consultancy services offered by Bosch Climate Solutions as it develops a climate neutrality strategy. Over a period of around five months, the two companies worked together to analyze the energy needs of the ebm-papst Group's international sites and draw up a roadmap for reducing emissions by over 47,000 metric tons of CO2 in Scopes 1 and 2. In other words, direct emissions from sources owned or controlled by the reporting company and indirect emissions associated with the generation of electricity, steam, heat, and cooling purchased by the company. Scope 3 emissions were also analyzed, thus creating transparency in relation to emissions produced by upstream and downstream activities in the value chain, such as in relation to purchased goods and services, or the use of sold products.

"We understand sustainability and climate protection as strategic challenges that cover all areas of life and work as we seek to successfully tackle the challenges of climate change. By working together with the Bosch team, our aim is to interweave this understanding of sustainability into our corporate strategy," explains Klaus Wittmann, Head of ESG at ebm-papst. "In the context of this collaboration, we can draw on our expertise in cutting $CO_2$ emissions to provide the world's leading manufacturer of fans and motors with optimum advice and support as they advance toward climate neutrality. Together, we can make many changes," says Lisa Reehten, Business Lead at Bosch Climate Solutions. This independent consultancy company, which was established after the Bosch Group successfully became climate neutral (Scope 1+2), now primarily shares its expertise with other manufacturing companies.

## The aim – to achieve $CO_2$-neutral production by 2025

At ebm-papst, there is a major scope for reducing both direct emissions caused by the burning of fossil fuels in the Group's own plants (Scope 1) and emissions associated with purchased energy such as electricity (Scope 2). On the basis of an "avoid and reduce" policy, measures designed to conserve resources and boost energy efficiency will now follow, with the aim of further increasing the $CO_2$ savings identified. As one of these measures, ebm-papst will be switching to green energy as the source of its purchased electricity in Germany by the end of 2023. It will also be investing around 1.5 million euros a year into its own electricity production.

The two companies are also working together to identify Scope 3 measures and incorporate them into the roadmap. The aim of these measures is to reduce indirect $CO_2$ emissions that occur in the supply chain as a result of purchased goods and services or business travel, for example. The operationalization is being supported by a newly formed sustainability department at ebm-papst. "We are delighted that ebm-papst is traveling this road with us. Sustainability is not a barrier to economically successful business operations, on the contrary, it is actually a prerequisite," says Reehten.

ebm-papst is a world-leading manufacturer of fans and motors that are used in a multitude of sectors. The family-owned company employs some 15,000 members of staff at 29 production plants and 51 sales locations. ■

# CARNAVAL DEL PAÍS: DAHUA TECHNOLOGY HELPS SECURE THE LONGEST CARNAVAL IN THE WORLD

Celebrated in the city of Gualeguaychú in Argentina, Carnaval del País is a vibrant and exciting celebration that spans two months. It holds the distinction of being the world's longest carnival. The festivities are filled with lively events, featuring samba dancers in sequins and feathers, and parades showcasing colorful, exquisitely crafted floats. To accommodate this spectacular event, the city constructed its very own Sambadrome, called the Corsódromo, which is the first of its kind in Argentina. This impressive venue stretches over 500 meters in length, with a track width of 10 meters, providing seating capacity for up to 38,000 spectators.

## Challenges

Implementing an outdoor video monitoring solution that can cover a capacity of 38,000 people was a massive challenge and not an easy task for the entire team. The client required a surveillance system that can monitor the crowd's security; from the moment they enter the stadium, watch and enjoy the show, until they leave the premises. Recorded video footages must also be readily available for further analysis in case of an incident.

## Solution

The team deployed several types of Dahua cameras around Corsódromo to monitor the situation during the carnaval. A dozen 4MP IR Vari-focal Bullet WizMind Network Camera (IPC-HFW5442H-ZHE) were deployed to cover various areas of the venue. Aside from providing clear and vivid images, this intelligent camera is also equipped with deep learning algorithms that enable intelligent functions such as video metadata, smart object detection, people counting, and more. It has IP67 waterproof rating and IK10 vandalproof rating, making it durable and reliable for outdoor applications. Other cameras installed include 4MP 32x Starlight IR WizSense Network PTZ Cameras (SD5A432XB-HNR), 2MP 33x Starlight+ Laser WizMind Network PTZ Camera (DH-SD6AL233XA-HNR), and Integrated Solar Monitoring System (DH-SD6C3432XB-HNR-AGQ-PV).

After each show, the situation at the entrance are also being analyzed through the recorded footages (via NVR5216-8P-I/L) in order to reduce waiting/queuing time in the future. It also helps in deploying security personnel in the right location to avoid unauthorized entry, theft, or any misdemeanor. What's more, cameras with integrated alarm system were strategically installed in crucial zones and are supervised by dedicated personnel on regular basis. All cameras are checked one day before each event to make sure their optimal condition and performance during the event.

## Results

The Dahua video monitoring solution deployed in Corsódromo for the Carnaval del País is a technological step forward from what it had in previous years. Through this new monitoring system, the management of the venue can efficiently monitor the situation inside the stadium and make necessary adjustments if needed. It helps optimize the entry time of spectators to avoid congestion and assists in assigning security personnel at crucial points around the venue to prevent incidents from happening; all of which contribute to the enhanced on-site experience of every spectator and improved security measures of Corsódromo.

## About Dahua Technology

Dahua Technology is a world-leading video-centric AIoT solution and service provider. Based on technological innovations, it offers end-to-end security solutions, systems, and services to create values for city operations, corporate management, and consumers. With more than 22,000 employees (over 50% engaged in R&D), Dahua has deployed its products, solutions, and services in 180 countries and regions, covering key industries including smart city, traffic management, retail, banking & finance, energy, etc. Since 2014, Dahua Technology has been estimated to be the world's second largest supplier of video surveillance equipment, and has been ranked 2nd on the a&s Security 50 list for 5 consecutive years. ■

# GALLAGHER SECURITY REACHES FOREFRONT OF DATA PROTECTION WITH SOC2 TYPE 2 CERTIFICATION

Award-winning global security leader Gallagher today announced that they have achieved System and Organization Controls (SOC2 Type 2) certification for the cloud-hosted services of their flagship security solution—Command Centre.

Gallagher has achieved the revered compliance standard for service organizations, which provides the highest level of reassurance that client data is securely processed and stored.. It is maintained by the American Institute of Certified Public Accountants (AICPA) and demonstrates stringent internal controls for information security and privacy.

The SOC2 Type 2 certification rounds out an impressive suite of standards and certifications achieved by Gallagher Security, including ISO27001, CAPSS 2021 and EN50131-4—making it the only physical access control manufacturer, worldwide, with this set of credentials.

Mark Junge, Global General Manager, says the company welcomed the opportunity to undergo an external audit as part of the certification process:

"Any business with cloud-hosted solutions that is serious about their data protection and privacy measures should be prepared to undergo this type of scrutiny," Mark says. "At Gallagher, our customers place a huge amount of trust in our people, and our security solutions – the onus is on us to demonstrate we are worthy of this trust."

SOC2 Type 2 certification also lays the foundation for the imminent move of Gallagher's Command Centre from an on-premise to cloud-based solution. Guy Irvine, who is leading this development for Gallagher Security says: "This certification is evidence that the future of our enterprise security solution has cyber security and data ethics at its core."

There are five principles in the SOC 2 framework: Security, Availability, Processing Integrity, Confidentiality, and Privacy. A business can be audited against any combination of these principles. During the audit process, all systems are reviewed by a trusted external third party to ensure they comply with the AICPA trust principles. This audit captures how a company safeguards customer data and counters the risk of cyber-attacks.

With over 15,000 security customers worldwide, Gallagher solutions are trusted to simplify life on campus within the education sector, keep staff and patients safe in healthcare, ensure the highest security requirements are met for government sites in the Five Eyes alliance, safeguard critical infrastructure within the utilities industry, and ensure uninterrupted movement for transport and logistics. ■

# HOW ARE UNIVERSITIES TAKING ADVANTAGE OF THE LATEST TECH TO IMPROVE SECURITY?

*The Association of University Chief Security Officers (AUCSO) Vice Chair (and Chair from April 2023), Oliver Curran, talks about the latest security technology in universities. Just how is this technology helping to protect students, the workforce, and the wider communities?*

Protecting university communities is of paramount importance for all those responsible for the Safety and Security of all Higher Education Institutions (HEIs). And AUSCO provides a valuable forum based on knowledge and experience to help our members. Here at AUCSO, we will use every method available to us in order to achieve safety for our communities, alongside our aim to protect our workforce whilst providing the best campus experience for all.

Our security teams will always be supplemented with the most up-to-date technologies, in order to provide a fully functional, integrated security service. Technology is integral to how we work.

Traditional security such as CCTV, access control, alarm monitoring, radios, parking tech (ANPR) and personal body cameras are an absolute given in most higher education operational activities today. The higher education sector is taking things to the next level by utilizing advanced technologies to improve support for the large and diverse communities they serve. This also helps ensure the safety of both staff and students.

## Personal safety and mass communication apps

One of the more widely used solutions, now utilised across most institutions is Personal Safety Apps, which can be used by our security staff, academic staff and students alike. Examples of some of these safety apps include SafeZone, CallMy and Horus Eye.

Take SafeZone for example – This is a campus safety app designed to assist universities in providing help to

**A student using the SafeZone app from CriticalArc**

students while on campus. Once downloaded, students can easily call security for assistance or help through the app.

Callmy Alert helps ensure safety on campus, making it a safe place for both work and study. It is available for free download by the community, provided that the university supports the technology. The app sends alerts to both students and staff in case of significant threats to life or safety on campus, such as major fires, toxic chemical or gas leaks, or terrorism-related incidents.

Should an incident occur, students receive a simple message in real time informing them of the incident location and which areas to avoid. Firearms or weapon attacks on UK campuses are extremely rare, but should the unthinkable happen, establishments have the technology to help protect students.

Horus Eye takes a broader geographical view. It provides students with essential timely information on elements such as crime hotspots, protests, rallies and other major events that are happening in and around their location. With an easily accessible network or 24/7 information, it helps students assess the situation and make informed decisions.

There is also a 'watch me closely' feature which alerts watchkeepers to keep a close eye on their location and offer 1-2-1 assistance where needed.

These apps can provide many services for the user, such as immediate 'call-for-help' buttons, lone-working monitoring, mass-communication, overseas travel

*continue on page 11*

monitoring/advice, wellbeing signposting, and more. It is all about 'risk mitigation' and ensuring safety in every aspect of a student's day – whether while studying or at leisure.

### Using smart security technologies smartly

Given the large communities of people who study, work, and socialize on university campuses, many institutions have been utilizing smart technologies for quite some time to assist their teams.

Artificial Intelligence for our video surveillance systems continue to grow in the sector and the benefits and results are often shared around the AUCSO members to promote knowledge and experience sharing.

Our current two-way radio solutions look very different to what we were using only five years ago, with a smartphone replacing the traditional walkie-talkie appearance. These new radios not only give us a better service in two-way communications, but can interact with our other security services, such as patrol systems, incident reporting, and safety apps. They can also be linked into our institution so we can access staff directories (and call anyone from anywhere) and campus maps. This not only enhances our customer service but makes our team present a more professional approach.

Lastly the use of incident report software (ICR) continues to grow in our sector as this is the best way for an institution to keep track of incidents and know where their risks are.

ICR is a simple mobile app that prompts staff to respond effectively to incidents. It gives details of what to do in an incident, prompting them with a step-by-step plan as to how to deal with a specific case. Each step of the emergency response process is supported with relevant documentation, such as evacuation routes, and contact numbers for key personnel, including nurses, emergency services, and embassy information for overseas students. This information is available both on and off-campus, providing accurate reporting in case a review is necessary and capturing a wealth of valuable information.

ICR's connectivity has been enhanced to complement other technologies, and it can now connect with mobile smart technology even in areas with no network coverage. Additionally, it can handle multiple incident responses, providing a single source of information for effective crisis management.

Higher education campuses can face numerous security risks, and it is crucial to know where to focus our resources. By leveraging the right technology, we can identify and prioritize our greatest risks and deploy the appropriate solutions to address them.

We are also able to demonstrate our value to our institutions by showing these trends and the work we do to mitigate and eliminate risk.

AUCSO (The Association of University Chief Security Officers) is the leading organisation for security professionals working in higher and further education around the world.

Oliver Curran has a wealth of experience in the security industry, spanning over 27 years. He started his career in Contract Security in the corporate sector, and for the past 15 years, he has served as an In-House Security Manager at UCL (University College London), focusing on the higher education sector.

Oliver Curran not only serves as the Chair Elect at AUCSO (taking over as Chair from Les Allan in April 2023), but also holds several other non-executive roles. He is a Security Commonwealth Board Member and Co-Chair of the SyCom EDI Group. ■

# ICO CLEARS LIVE FACIAL RECOGNITION SYSTEM FROM FACEWATCH AS LEGALLY COMPLIANT

*Following a formal assessment by the Information Commissioner's Office (ICO), the use of Facewatch's live facial recognition technology in retail stores has been cleared as compliant with data protection legislation.*

In July last year, privacy campaigners had mounted a formal complaint against the use of Facewatch's system in 35 Co-Op branches across the south of England. The campaign group, Big Brother Watch, had described the use of live facial recognition as "Orwellian in the extreme".

The investigation by the ICO ultimately concluded that no further regulatory action was required, and that it was "satisfied the company has a legitimate purpose for using people's information for the detection and prevention of crime".

Facewatch specialises in live facial recognition systems in the retail sector. It maintained throughout the process that its system complied with the Surveillance Camera Commissioner's Secured by Design protocols and is fully GDPR compliant.

## A "balancing act between privacy rights and crime prevention"

In a post on the ICO website, Stephen Bonner, the ICO's Deputy Commissioner for Regulatory Supervision, noted the need to weigh the use of facial recognition to prevent and detect crime against the privacy rights of the individual.

He noted how the ICO had raised areas of concern, which Facewatch then "made, and continues to make, improvements to its product". These improvements included reducing the personal data they collect by focusing on repeat offenders or individuals committing more serious offences; appointing a Data Protection Officer; and protecting those classified as 'vulnerable' by ensuring they didn't become a subject of interest.

The ICO concluded that based on these improvements, it was "satisfied the company has a legitimate purpose for using people's information for the detection and prevention of crime" and that no further regulatory action was required.

It did, however, issue a word of warning to the wider industry, saying that the decision does not give a "green light to the blanket use of this technology". Each use should be considered on its own merits, and must always balance individual privacy rights with crime prevention.

## Surveillance Camera certification for Facewatch live facial recognition system

The ICO judgement followed the recent awarding of the Surveillance Camera Commissioner's certification mark to the Facewatch system for meeting the Surveillance Camera Code of Practice for the use of live facial recognition.

Commissioner Fraser Sampson, said: "By successfully engaging with the professional accreditation bodies and my certification scheme, an organisation, and more importantly the public, may be reassured that surveillance camera systems which intrude upon their privacy are being demonstrably operated ethically and legitimately to an appropriate standard.

"The certification scheme goes above and beyond the basic requirements of data protection and is designed, as is the government's Surveillance Camera Code, to enable operators of surveillance camera systems to make legitimate use of available technology in a way that the public would rightly expect and to a standard that maintains public trust and confidence. I acknowledge your excellent and most commendable commitment in that regard arising from your engagement with this process."

Facewatch Chairman, Nick Fisher said: "The ICO judgement and Biometrics Commissioner award underlines our commitment to best practice, both to prevent crime and protect staff and customers. The public and our subscribers can continue to have confidence in our systems and privacy safeguards." ■

# IFSEC IS BACK! WHAT CAN YOU EXPECT FROM THE UK'S LARGEST AND LONGEST-RUNNING SECURITY EVENT AS IT CELEBRATES ITS 50TH ANNIVERSARY?

*Following a hugely successful in-person comeback in 2022 after three years away due to Covid, IFSEC, in partnership with the British Security Industry Association (BSIA), returns to ExCeL London from 16-18 May this year. A packed expo hall, topical seminar programme, live demos, new Distributor Network and a partnership with charity Mates in Mind awaits!*

Thousands of senior security professionals are expected to attend, keen to explore innovative solutions and collaborate with the entire community, including over 250 exhibiting companies and key security associations.

This year also marks IFSEC's 50th anniversary and the show has changed considerably since it launched in 1973, as Gerry Dunphy, IFSEC Event Director, explains: "ISEC, as it was then called, was quite a charming and modest gathering of burglar alarm suppliers that got together at the Royal Lancaster Hotel in London."

The event has come a long way since then and is now the UK's longest and largest running security event. "I have been thinking about how IFSEC has achieved such longevity, and it's purely down to industry appetite and demand against an ever-changing backdrop of technology and suppliers."

"IFSEC brings buyers and sellers together and creates and enhances partnerships by uniting people from the same industry. It's a place where they can collaborate, network, meet face to face, discover new technology and be part of a huge global industry. The fact that it has been running for 50 years is testament to the appetite for progression and evolution."

## New distributor network

New for 2023, the Distributor Network recognises the essential role distributors play in the security market. In bespoke distributor hubs on the show floor, 11 of the UK's leading distributors will meet and greet the installer audience and invite them to VIP sessions and meet suppliers.

Distributors involved include ADI Global, DTS.Solutions (U.K), Dynamics CCTV, DVS, CIE-Group, COP, Dynamic CCTV, MAST Digital, Nimans, Oprema, and PureTech.

## Live demo areas

Visitors to this year's IFSEC can look forward to two live areas on the show floor:

- **The Converged Security Centre,** in partnership with Advancis, is collaborating with several vendor partners to showcase the benefits of open, integrated security management platforms. Visitors can see, hear and experience the technology in real-time and meet with the experts behind the technology.
- **The LPCB Attack Testing Zone** puts a range of highly engineered security equipment to the test by attacking them with hammers and wire cutters. Commenting on the feature, Gerry said, "I'm delighted that the very dynamic and energetic LPCB Attack Testing Zone is back, this is without doubt the most popular feature we have ever been involved with."

## Seminar programme

This year's seminar sessions on the show floor will cover the biggest topics affecting the security industry, including the impact of big tech on access control, the changing world of alarm signalling with the introduction of Move to All IP, use of body cams to make the workplace a safer space, and more.

In addition, a one-day session focusing on the introduction of Martyn's Law, a new piece of anti-

**The packed-out LPCB Attack Testing Zone at IFSEC 2022**

*continue on page 14*

terrorism legislation, will talk about how the high-profile campaign led the UK government to assess and legislate on security measures adopted by venues in the wake of the Manchester Arena attack in 2017.

Figen Murray, who has spearheaded the campaign, will be one of the speakers during the session. Figen is the mother of Martyn Hett, who died in the attack.

## Session highlights – IFSEC Tech Talks Theatre

With inspirational speakers, including Lee Odess (Access Control Expert), Blake Lekowitz (Axon Enterprise), Peter Kelly (Mates in Mind), Oliver Philippou (OMDIA) and many more, this year's seminar sessions on the show floor will cover the biggest topics affecting the security industry. What is the impact of big tech on access control? Where are we at in the move to All IP and its impact on alarm signalling? And, how can body cams make the workplace a safer space?

All this will be discussed, alongside plenty more. We've picked out a few highlights below:

<u>Tuesday 16 May</u>

- **OMDIA Insights – trends in video surveillance (11:30-12:00):** Speaker: Oliver Philippou, Senior Research Manager Security Technologies, OMDIA
- **Mental health and wellbeing in the security sector (12:15-12:30):** Speaker: Peter Kelly, Head of Programmes, Mates in Mind
- **Enhancing technical security solutions with behavioural analysis (13:00-13:30): Speaker:** Blake Lekowitz, Director of Enterprise Marketing, Axon Enterprise Inc

<u>Wednesday 17 May</u>

- Big tech and global trends impacting access control (11:30-12:00): Speaker: Lee Odess, Access Control Expert
- **Futureproofing your CCTV network (15:00-15:30): Speaker:** Peter Mason, Consultant

<u>Thursday 18 May</u>

- **Benefits of engaging security consultants with an engineering background for projects within the built environment (11:30-12:00):** Speaker: Gary Thomas, Consultant

There's plenty more to watch live on the show floor over the three days, too!

## Mates in Mind – bringing mental health to the forefront

This year IFSEC has partnered with mental health and wellbeing charity, Mates in Mind. Gerry explains: "We are delighted to partner with Mates in Mind this year since they launched in 2017. Mates in Mind have been committed to improving mental health across the construction industry.

"Their target is to reach 75% of the industry by 2025 and we are thrilled to be working with them to help spread their message within what has been a traditionally very difficult audience to break into."

## Meet leading suppliers

IFSEC offers tens of thousands of visitors an unrivalled opportunity to meet hundreds of leading security suppliers across access control, video surveillance, perimeter protection, intruder detection and more.

"This year's IFSEC is fantastic because we've seen a lot of previous companies returning after COVID. Some headliners include the likes of Uniview, who are a major camera manufacturer who couldn't attend last year due to the restrictions in their own country, so it is brilliant to have them back again. We've also got the likes of ASSA Abloy, Provision ISR, BT Redcare, CAME BPT, Hikvision, HID, and Texecom," added Gerry,

"We are on course to welcome between 250 to 270 companies this year to IFSEC alone, so it is going to be an unmissable event."

## Exhibitor launchers and demonstrations

Several exhibitors will be showcasing brand new products at IFSEC this year, including:

**Police Crime Prevention Initiatives (IF.3440) – showcasing Secured by Design (SBD)**
Police CPI will be showcasing Secured by Design (SBD), the official police security initiative that works to improve the security of buildings and their immediate surroundings to provide safe places to live, work, shop and visit. Visitors to the stand will also be able to discover best practice around crime prevention, as well as find out more about the Police Preferred Specification product accreditation scheme for products that can prevent and deter crime.

**CLD Physical Security Systems (IF.6045) – showcasing its latest innovations**
CLD, the manufacturer and supplier of rigid mesh fencing and security gates, will be showcasing its latest innovations including off-grid on-ground, agile security products, that are said to deliver true sustainable solutions. Product demonstrations will be available all day, every day on the stand, including the new non-metallic SR range of GRP solutions, SR rated temporary hoarding solution and off-grid access control range.

**Igloocompany (IF.3449) – showcasing the new iglooco Padlock 2E**
Igloocompany, a smart access

*continue on page 15*

solutions provider, will be showcasing its iglooco Padlock 2E (SP2E). Designed to be used in extreme conditions, surviving harsh cold and heavy rainfall, Padlock 2E is a heavy-duty IP68 insurance-grade Padlock at IF.3449.

**Henry Squire & Sons Limited (IF.6040) – demoing inigma, smart technology bike locks**
Lock maker Henry Squire & Sons Limited will be showcasing further developments with its inigma product. These Bluetooth operated bike locks feature one of the world's most secure smart operating systems.

**WiBase Industrial Solutions Inc. (IF.4837) – demoing smart dashcam and body-worn camera**
WiBASE specialises in developing IoT communication devices, including in-vehicle systems, rugged handheld terminals, and wearable IoT devices. At IFSEC, WiBase will be demoing its smart dashcam and body-worn camera with functions such as SOS, live streaming, push-to-talk, location service and more.

**Innovative Contractors for Advanced Dimensions (ICAD) (IF.4020) – showcasing new Visetec security cameras**
ICAD provides system technology services for facilities such as: airports & airlines, metro rail and bus, hospitality and events, healthcare, government, stadiums, public venues, educational, residential infrastructures and more. At IFSEC, ICAD's I-Defense division and i3s will be launching and showcasing its new Visetec security cameras and video analytics system (PSIM).

**Terracom SA (IF.3012) – showcasing QR-Patrol and MyLoneWorkers**
Terracom SA, a provider of guard tour solutions for modern businesses and enterprises, will be showcasing the latest version of its most successful products, QR-Patrol and MyLoneWorkers, including new features, such as Face Verification, Dynamic Guard Groups, and the addition of a vast library of Business Intelligence reports.

**Provision ISR (IF.3410) – launching new products**
Continuing to showcase its embedded cyber solution from Check Point, Provision ISR will be launching three new products at IFSEC: a new integration with Tyco alarm system – Visonic, DSC, Bentel, an intercom series and thermal cameras.

**Cento Personnel Ltd (IF.2630) – launching Cento Sustain**
Cento we will be launching 'Cento Sustain' at IFSEC. Using its offsetting platform, Cento will plant a tree for every visitor to the stand meaning the carbon footprint for visiting the show will be offset. This initiative will then continue to be rolled out throughout 2023 at all Cento events, meetings and beyond.

**Delta Telecom Sound & Security (IF.5001) – launching new Torus key cabinet**
Delta Telecom Sound & Security will be launching its new Torus key cabinet at IFSEC. Torus keeps keys safe and secure, whilst monitoring usage for auditing in real time, according to the manufacturer.

**Webro Cable & Connectors (IF.5015) – demoing Eyenor cameras**
Webro has partnered with Norden to launch the Eyenor range of NDAA-compliant CCTV solutions, including cameras and NVRs. Webro has also expanded its CPR-compliant range of cables for improved fire safety.

**Suprema Systems UK Ltd (IF.4615) – demoing BioStation 3 and Airfob Space 2.0**
Suprema, the global provider of access control, time and attendance, and biometric solutions will be showcasing its BioStation 3 Face Recognition device. It will also showcase the Airfob Space 2.0, a fully hosted access control solution.

**SKIDEEV INDUSTRIAL (IF.5020)**
Skideev Industrial Co. Ltd will be demoing the following products at IFSEC:

- Full intercom affordable "ULYSS" system with 4G, APPs and wired monitors that can be used with smartphones only and/or as traditional system
- Connected keypads 12 and 13 keys (with companion App)
- End users RFID tags self-programming
- Two wires Ethernet

**CAME BPT UK Ltd – demoing CAME Connect**
At IFSEC, CAME BPT UK will be demoing its CAME Connect cloud based remote operating system, as well as displaying a wide range of CAME OZAK speed gates, turnstiles and road blockers.

*continue on page 16*

### Elizabeth Line – Travel to London's ExCeL now easier than ever

The launch of the brand-new Elizabeth Line means visitors can now access ExCeL direct from as far away as Reading, Heathrow and Shenfield. "The Elizabeth Line is now open and visitors can travel to ExCeL from central London in under 13 minutes, and direct from Heathrow in 45. It's an absolute game changer," concluded Gerry.

### Four shows in one

IFSEC and its three co-located events – FIREX, Facilities Show and Safety & Health Expo – are all free to attend. Visitor registration is open now.

- **FIREX,** Europe's leading annual fire safety event, exclusively in partnership with the Fire Industry Association (FIA), supports and reinforces third-party approved solutions and is the only event in the UK which makes accreditation a condition of exhibiting.
- **Facilities Show** is the dedicated facilities management event where visitors can prep for the future of the workplace and explore solutions for making them smarter, more efficient and more sustainable.
- **Safety & Health Expo** welcomes thousands of health and safety professionals to connect with peers and discover solutions to combat safety risks in the workplace and keep up to date with mental health initiatives. ■

### Register today for IFSEC 2023

***16-18 May 2023, ExCeL London | IFSEC 2023: Recognising the past, embracing the future***

Join thousands of likeminded security and risk professionals at IFSEC 2023 in May, as the UK's largest and longest running security event looks ahead to what's next in the sector as it celebrates its 50th birthday. This year will see the launch of the IFSEC distributor network, while London's new Elizabeth Line makes travel to the venue easier than ever!

You'll find hundreds of leading exhibitors from the physical and integrated security sector, showcasing all the latest in video surveillance, access control, intruder detection, perimeter protection and software solutions. Join the community and secure your ticket today!

## VIVOTEK LAUNCHES FIRST EDGE-COMPUTING FACIAL RECOGNITION CAMERA FD9387-FR-V2

VIVOTEK, the leading global IP surveillance provider, strives to provide comprehensive security solutions and launches first-ever facial recognition camera that integrates edge computing to help enterprises to quickly identify the gender and age of people in the video on edge, as well as those who are wearing masks. The camera has a built-in memory card with facial data storage up to 10,000 profiles and achieves a 99% accuracy rate of detection. The camera can also target specific images for real-time alarming and its software and hardware meet the standards of U.S. National Defense Authorization Act, building an environment people can live in with a peace of mind.

The FD9387-FR-v2 Facial Recognition Camera from VIVOTEK includes the SAFR Inside AI facial recognition platform developed by SAFR from RealNetworks, LLC., which is integrated with the camera's robust edge-computing capacity to enhance analysis efficiency significantly. The camera's functions include real-time facial detection and tracking; early warning of strange faces; and image privacy mode for sensitive areas, avoiding sharing of the video with a third party. Moreover, the camera is equipped with strong cybersecurity protection capability with fully encrypted data storage and transmission, safeguarding user privacy.

The VIVOTEK FD9387-FR-v2 Facial Recognition Camera is ideal for building automation and access control systems in banks, retailers, and buildings. The camera's built-in system can be integrated with business intelligence (BI) services, especially for customer service in luxury retail. The camera can send real-time notifications when VIP customers enter the store, improving service quality and standards. Additionally, the camera effectively tracks and detects traffic in and out of buildings, making it a crucial aspect of smart buildings. Through list management, unauthorized visitors will be reported and recorded for future investigations. **For more information, please visit: https://www.vivotek.com/fd9387-fr-v2** ■

# SMALL BUSINESSES CAN NOW REAP THE BENEFITS OF THE CLOUD WITH ZYXEL'S NEW EASY-TO-USE SWITCH

*Zyxel's new GS1915 series maximizes efficiency and agility in an affordable way, to offset the scaling network management challenges of prosumers, small businesses and chain stores.*

**Hsinchu, Taiwan** – Zyxel Networks, the leader in delivering secure and cloud-powered networking solutions, today launched its compact and affordable cloud-based GS1915 series 8-port PoE and Non-PoE Switches enabling more agile network connectivity, seamless multi-device management, and an easier transition to the cloud for small businesses.

The GS1915's effortless deployment and easy management makes it simple for prosumers, small businesses and chain stores to deploy without a dedicated IT team.

## Agile networks, easily managed

The GS1915 series features complimentary Nebula cloud management via an intuitive web interface or the Nebula mobile App. Users can enjoy a streamlined experience from network installation to management without the additional costs of a software or hardware controller. There is also a typical standalone mode available for even more flexibility.

The Nebula App provides an easy way to onboard new devices to the platform, check the network status overview, remotely control your network, and block unauthorized clients anywhere, anytime.

Prosumers, small businesses, and chain stores can take advantage of Nebula ecosystem to access real-time network information and to centrally and remotely manage the GS1915 series of switches along with access points, security firewalls, and 5G/LTE mobile routers with a simple and unified network experience.

## Making daily work easier

The PoE model GS1915-8EP comes with a full 8-port PoE+ and supports a 60W power budget, ideal for setting up multiple APs and cameras within homes and small businesses. With the Nebula App it's easy to reset an abnormal camera by power cycling it, even when you're away.

The intuitive LED indicators on the GS1915 series switches' front panels make it easy for users to check the switch status immediately. Designed without a fan, the switches operate silently, blending perfectly into any working environment without disturbing fan noises.

"Fast, stable, secure connections shouldn't solely be the luxury of huge enterprises that have big budgets and dedicated IT teams. The expansion of our switch and Nebula portfolio is a sign of our commitment to smaller businesses and prosumers, giving them the flexibility to scale their networks, and make the transition to the cloud when they're ready, without the need to replace hardware. By removing these stresses, and making network connectivity simpler, they can spend more time focusing on what they need and do best - running their business," comments Crowley Wu, Vice President of Sales and Marketing at Zyxel Networks.

## About Zyxel Networks

Zyxel Networks has unlocked people's potential by connecting businesses and home users for over 30 years. Headquartered in Taiwan, we are one of the few leading brands in the world that has in-house R&D capabilities across home networking, LAN switching, WLAN, to security solutions.

Zyxel is the only networking company named among Best Taiwan Global Brands with an unrivaled international presence in 150 markets and a proven track record of being among the top 5 leading brands in the SMB segment in EMEA and worldwide. We've shipped more than 100 million devices and are trusted by over 1 million businesses, all working smarter with Zyxel solutions. We're building the networks of tomorrow and meeting the needs of the modern workplace – powering people at work, play, and life.

**For more information about the switch range please visit: https://www.zyxel.com/products_services/8-port-GbE-Smart-Managed-Switch-GS1915-Series/** ■

# THE GROWTH OF THE EDGE ECOSYSTEM REAFFIRMS NEED FOR PROACTIVE SECURITY

*A cross-functional collaboration to safeguard digital assets is a critical element to secure organizational information assets.*

As the digital world continues to transform and develop, there are new cybersecurity threats that business leaders need to be aware of and protect against. This is even more important as computing continues to move toward the edge. According to a recent survey, 76% of security professionals expect fully new threats to emerge because of an expanded attack surface. Take the recent example of the ransomware group BotenaGo being able to attack vulnerable IoT targets without relying on any human activity.

Adversaries are targeting the expanding attack surface at the edge and taking a proactive stance is crucial for edge innovators. The stakes are too high for reactionary security decisions or security controls prescribed based primarily on past experiences or practices. Sensors and data are everywhere, and networks are always available.

SecurityInfoWatch.com recently had a conversation with former Gartner analyst and Head of Cybersecurity Evangelism at AT&T Business, Theresa Lanowitz, who spoke to existing cybersecurity controls and the cost benefits of those controls as companies move toward the edge. She also discusses the need for cross-functional collaboration to safeguard digital assets, build a resilient business, and drive operational efficiency of security budgets to deliver stronger outcomes.

**SecurityInfoWatch.com (SIW): Edge computing is a term that has been circulating in the industry for a while. How exactly do you define edge computing?**

**Theresa Lanowitz:** The term edge means different things to different people depending on where they are in the ecosystem. For example, vendors selling edge solutions will skew the definition towards their technology stack. Organizations implementing edge will skew towards

*continue on page 19*

the technology stack they are using. However, looking at edge computing through the lens of three essential characteristics seems to help clarify the topic. Those three essential characteristics for edge computing which provide a consistent framework are:

- A distributed model of management, intelligence, and networks
- Applications, workloads, and hosting closer to the users and assets that are generating or consuming the data, which can be on-premises and/or in the cloud
- Software-defined

It's important to keep in mind the above characteristics in order to truly help define what is occurring with edge computing.

Edge use cases are evolutionary, not revolutionary. Edge use cases are pervasive, and many apply existing connectivity, networking, and security elements. As use cases evolve, resilience gains importance and the competitive advantage that edge applications provide can be fine-tuned. Future evolution will involve more IoT devices, faster connectivity and networks, and holistic security tailored to hybrid environments.

Some of the top edge use cases we've uncovered in different industries through our research include:

- Finance – concierge services
- Retail – loss prevention
- Healthcare – consumer virtual care
- Manufacturing – video-based quality inspection
- Energy and utilities – remote-control operations

### SIW: As organizations across all industries move to edge computing, what must happen to ensure an edge ecosystem is being adopted properly and what benefits will organizations begin to see as a result?

**Theresa:** This question really hits on the decades-old silos that have been erected inside any business. For successful implementation and with security at the core, those silos need to erode. Over the past four to five decades, we've seen silos such as networking, IT, quality assurance, operations, and application security become isolated from one another. Moving to a computing paradigm that is more experiential and based on near real-time data and observations, there has to be more cross-functional work, roles, and communication. The edge is calling for collaboration across the business as a whole, and this entails putting together an extensive plan for moving toward the edge, as well as bringing in trusted third-party advisors to help.

Those trusted advisors have the experience needed to bring about this evolution in computing. For example, businesses may work with a telco to help with the network component of edge computing, a global systems integrator to help with application integration, or with a managed security service provider (MSSP) to provide endpoint security. According to recent data from the annual AT&T Cybersecurity Insights Report, 65% of survey participants are working with a third party for designing and deploying new architectures for edge use cases.

**Theresa Lanowitz, Head of Cybersecurity Evangelism, AT&T Business**

As teams begin to move to edge computing, we will see computing experiences move the user away from the traditional input/output of monolithic applications. The move to experiential computing offering a digital experience with near real-time information will be the norm. For example, look at the top edge use case for manufacturing – video-based quality inspection, this allows defects to be remediated at the point of insertion almost immediately. Using a system of cameras and sensors, teams are alerted immediately and appropriate adjustments can be made.

### SIW: What emerging threats concern businesses the most in relation to edge computing?

**Theresa:** Research shows that 75% of global survey respondents from the AT&T Cybersecurity Insights Report are on a journey to the edge with use cases either in full or partial implementation – this is a powerful indication that the market is on its way to introducing new computing paradigms that go beyond monolithic applications. With that said, another 74% of respondents say a security compromise is very likely with a high impact on the business as a result of the compromise—this is indicative of the fact that organizations now understand the inextricable link between business outcomes and security as a business function vs. a technical problem. We probably would not have seen this connection between a security incident and the realization of a business impact five years ago. Across the board, businesses are savvier about what security risks mean to the business and the need to build a resilient business.

Adversaries adapt and look for new ways to interrupt businesses. In late 2021, malware named BotenaGo was able to attack vulnerable IoT

*continue on page 20*

targets without relying on any human activity. This indicates that the advancement of edge computing and the expanded attack surface is something adversaries are moving toward, which calls for a proactive stance on security for all enterprises that are innovating at the edge. The stakes are too high for reactionary security decisions or security controls prescribed based primarily on past experiences or practices. Sensors and data are everywhere, and networks are always available.

Fortunately, organizations are moving to combine cybersecurity controls and network functions in the cloud (for example, SASE). While manual security activity has proven to be less useful in edge use cases, multifactor authentication is specifically indicated as one of the leading cybersecurity controls for the edge ecosystem

**SIW: What advice do you have for business professionals to best secure the edge?**

**Theresa:** As organizations across all industries move to edge computing, it is important to evaluate existing cybersecurity controls and the cost-benefit of those controls. It is also critical to evaluate what new edge use cases require for security. Each organization has to make the call on what cybersecurity controls they should continue to use with new computing types and which to leave with legacy computing for maintenance purposes. Overall, there is quite a bit to be optimistic about. Yes, cyber adversaries are determined, but defenses are moving to be holistic vs. reactive. Today's line of business understands the criticality of security, and organizations are planning and investing properly. This includes

collaboration among the line of business, network teams, application development teams, security teams, and third-party trusted providers.

Edge use cases represent the future with digital trust being at the core of businesses of all types. Further securing the edge will be a matter of working with an internal and external ecosystem to safeguard digital assets, build a resilient business, and drive operational efficiency of security budgets to deliver stronger outcomes. ■

## AVIOTEC – PRODUCT OF THE YEAR IN THE FIRE DETECTION CATEGORY TOP INDIAN INDUSTRY AWARD GOES TO VIDEO-BASED FIRE DETECTION FROM BOSCH

The safety and security sector is once again quite literally all fired up about Aviotec, the video-based fire detection with pre-installed AI algorithms that uses video analysis to detect smoke and flames directly at their source. At the Finest Skills & Talents (FIST) Awards 2022 in the Indian capital Mumbai, this innovative technology from Bosch was recently named Product of the Year in the Fire Detection category and presented with the renowned FIST Award – India's number one fire safety and security accolade. "Bosch Aviotec is the latest and fastest way of detecting fire as compared to any traditional fire detection system. The AI-based algorithms enable detection of flames and smoke in no time, resulting in the saving of lives and assets," says Pankaj Dharkar, who is on the panel of judges and

**The attached photo(s) may only be published in conjunction with this newsflash. Any further use of the photographic material is only permissible with the prior consent in writing of Bosch Building Technologies.**

a member of the Advisory Council of the Fire and Security Association of India (FSAI). This organization presents the awards annually, together with the PwC auditing and consulting firm.

*continue on page 21*

### Seven and counting

The FIST Award 2022 takes the number of prestigious awards Aviotec has received to seven. This particular achievement is considered the highlight in terms of international accolades, and has given the responsible team a significant boost.

"Awards for our technology reflect the recognition and appreciation of the markets and are therefore a reliable indicator for decision-makers," says Theresa Kramer, Aviotec Global Business Developer at Bosch. Its speed and accuracy make Aviotec a reliable and innovative smoke and flame detection solution, even in difficult conditions such as industrial environments with high fire loads, vast buildings with high ceilings, and protected outdoor

areas. This is possible thanks to video analysis controlled by AI algorithms that visually detects smoke and flames directly at their source. As a result, Aviotec reacts much faster than conventional ceiling-mounted fire detectors where the smoke has to rise far enough before the alarm is triggered. This speed is a vital advantage when every second counts. Safety and security personnel can verify the alarm in the video image and pinpoint the exact location of the fire. "Aviotec will revolutionize fire detection in applications involving high ceilings and open spaces," insists FSAI Vice Chairman C. K. Asher.

### Award-winning and certified solution

Besides winning various awards, Aviotec is also the first VdS-certified product of its kind. VdS Schadenverhütung GmbH is an independent, internationally recognized institution for corporate security that establishes international guidelines based on agreed regulations. VdS approval carries great weight and is a key criterion when it comes to making an investment. ■

## SHOOTER DETECTION SYSTEMS TO SHOWCASE WORLD-LEADING GUNSHOT DETECTION SOLUTIONS AND NEW INITIATIVES AT ISC WEST 2023

*Show Attendees Will Be First to Experience Latest in Active Shooter Intelligence™*

Shooter Detection Systems (SDS), an Alarm.com (NASDAQ: ALRM) company and provider of the world's leading gunshot detection solutions, will be displaying the latest developments in Active Shooter Intelligence™ along with several new product and business initiatives at ISC West 2023 in Las Vegas, NV. ISC West attendees visiting Shooter Detection Systems booth #26049 will get a first-hand look at many of the company's latest technology innovations scheduled for release over the course of 2023.

"Shooter Detection Systems is poised for continued growth and innovation in 2023 with many new technology and business developments on the horizon" said Joe Byron, VP of Sales, Shooter Detection Systems. "We never stop innovating to save lives threatened by gun violence, and we are excited to unveil new solutions and partnerships that speak directly to this commitment."

One of the latest developments SDS will demonstrate at the show is an advanced emergency response solution that enhances situational awareness for first responders during active shooter incidents. The solution goes beyond E911 by leveraging the Noonlight platform to expedite the continuous transmission of shot location information to law enforcement responding to the event. The solution also enables the 911 call taker, responding officers, onsite security and building managers to communicate and share information in real-time and view critical contextual data, including the building, room, and floor location of gunshot events. In keeping with SDS' commitment that every citizen deserves the right to the highest protection against active shooters, these new capabilities will be included with the standard SDS software package for existing SDS software users. Attendees can receive demos of the SDS gunshot detection and 911 alerting solution at SDS SDS booth #26049.

SDS and Alarm.com will also be offering an inaugural demonstration of "SDS Powered by Alarm.com". This new solution pairs the proven accuracy of the SDS indoor gunshot detection sensor with the fully integrated Alarm.com for Business platform. "Introducing solutions to serve

*continue on page 22*

the small to mid-sized commercial market was important to our service providers," said James Reno, Vice President of Commercial Sales for Alarm.com. "Offering them the only unified cloud platform with shot detection enhances not only the capabilities of the Alarm.com platform, but it also gives our service providers the ability to offer broader, more comprehensive security solutions that help their customers address the changing landscape of modern-day threats." Currently in development, "SDS Powered by Alarm.com" will soon be released for beta testing. ISC West attendees can receive demos of the new Shooter Detection Powered by Alarm.com integration at Alarm.com booth #16039.

SDS Advisory Board member and retired FBI Special Agent Jin Kim, recognized as one of North America's leading active shooter experts, will present his latest analysis on the increasing sophistication of active shooters at a special SDS event held on Thursday, March 30. Space is limited, attendees can register in advance to secure a seat here.

At the upcoming show, the company plans to showcase several new initiatives. These include the introduction of its new branding, upcoming improvements to the business model that will benefit SDS reseller partners, and the latest developments in total-building gunshot detection solutions, which will now include exterior perimeter protection.

**To learn more, please visit shooterdetectionsystems.com or visit us at ISC West 2023 booth #26049.** ■

## INTRODUCING 3D FLASH+: TBS SWITZERLAND'S ADVANCED BIOMETRIC FACIAL RECOGNITION SOLUTION

*TBS Touchless Biometric Solutions in Switzerland has just announced their latest product, 3D FLASH+. This new facial recognition product is one of the most advanced on the market today, with the ability to recognize registered users from up to four meters away. It also features a unique walk-through method that allows for verification of a person's identity by walking past a camera. With its many cutting-edge features, 3D FLASH+ offers unmatched convenience and security.*

TBS is excited to announce our latest product, 3D FLASH+. This facial recognition product is able to recognize registered users from up to four meters away, making it one of the most advanced algorithms for facial recognition and verification available on the market today. The 3D FLASH+ also features a unique walk-through method that allows to verify person identity by walking past a camera. This makes it ideal for use in high-security areas where traditional methods of identification may not be feasible. Utilizing sophisticated algorithms for face identification and walk-through verification techniques, 3D FLASH+ generates an exclusive mathematical representation of each person's distinct facial features. The authentication process via walking through takes merely one second and can be adjusted according to your preferred starting point – making it perfect for locations like buildings or airports where touchless biometric validation is crucial.

"We are confident that 3D FLASH+ will revolutionize the security industry and provide peace of mind for users around the world", said Stefan Schaffner, CEO TBS. "3D FLASH+ is the newest facial recognition device from TBS. It features cutting-edge 3D algorithm for facial verification and has an anti-spoofing capability against photos, videos, as well as face masks – rest assured that the individuals entering through the gate are indeed who they claim to be", explains Stefan Schaffner further.

The 3D FLASH+ is designed for indoor installation and can be used in a variety of settings, from airports to manufacturing facilities. It has a large database capacity, able to store 10,000 faces in identification mode and 100,000 faces in verification mode (dual-factor verification). The biometric solution also possesses the ability to seamlessly combine various techniques for two-factor authentication, including card-based systems, personal identification number (PIN) codes or mobile access options.
The 3D FLASH+ is an exceptional product that offers numerous advantages and benefits, making it a valuable asset in various industries.

### About TBS

Touchless Biometric Systems (TBS) is a Swiss company that is internationally renowned for its innovative biometric systems. In particular, in the areas of access control and workforce management, TBS has created various solutions together with its partners and implemented them at customer sites. Based on the patented touchless 3D fingerprint technology and the powerful BIOMANAGER Enterprise software platform, TBS provides its customers with unique system components that can be easily integrated into existing solutions and guarantee that only authorized persons have access. Even complex workflows can be represented by extended integration and customization options of the system. TBS has a global presence with 100 partners in over 40 countries, including Siemens, Honeywell, Dormakaba, Interflex/ Allegion and Nedap. TBS touchless biometric solutions are used in airports, banks, hospitals, governments and other organizations. ■

# SUPREMA SHOWCASES INTEGRATED SECURITY SOLUTIONS AT ISC WEST EXHIBITION IN LAS VEGAS

**SEOUL, South Korea** – Suprema, a global leader in access control and biometrics, participated in ISC West 2023 in Las Vegas, where a range of integrated security solutions are showcased. The largest annual security exhibition in the United States, ISC West is held from March 29 to 31.

At the event, Suprema is exhibiting a number of security solutions comprising access control devices managed by BioStar 2, an integrated security software platform. BioStar 2 links all of Suprema's access control terminals and supports multiple credentials seamlessly including RFID and mobile, QR codes, barcodes, facial recognition, and fingerprint recognition. BioStar 2 offers a very flexible system architecture where the system can be deployed in both a traditional panel-based topology in a centralized system with its intelligent controller, the 'CoreStation', and a distributed system by connecting the edge readers directly to the server.

First official launch at ISC West is the 'BioStation 3', the first of its 3rd generation readers. Apart from being an access terminal that supports multiple credentials such as facial recognition, RFID, mobile and QR codes, this device also supports VoIP Intercom and real-time video monitoring features to make it a truly multi-functional reader. Its state-of-the-art facial recognition is processed by deep learning AI-based engine inside a Neural Processing Unit (NPU) making it the most powerful engine in an embedded device with the strongest anti-spoofing detection technology.

The demo stations at the booth have been setup to provide live demos of how BioStar 2 with Suprema readers can offer the best user experience in terms of seamless issuing and management of different credentials and how easy and fluid the authentications are at the readers.

In addition, Suprema demonstrates how it will build its partner ecosystem by enabling integration of Suprema devices with third-party systems through Open APIs and SDKs. Also, a newly introduced cloud-based integration option offers a simple way for any cloud-based 3rd party platforms to make use of Suprema-hosted, managed devices over the cloud.

"Suprema continues to be the technological leader rolling out the most innovative and intelligent security solutions," said Bob McKee, President of Suprema America, "Having a reputation of a top 50 global security company for the last 12 years requires commitment to technology and our services. We are committed to build our brand and invest in the North American market." ■

# STATE OF SECURITY 2023 REPORT REVEALS INCREASE IN DATA BREACHES AND OUTAGES DUE TO CYBERSECURITY INCIDENTS

*Global research shows over half of organisations have had a data breach, and 62% suffer from unplanned downtime on a monthly basis*

**Singapore** – Splunk Inc., the cybersecurity and observability leader, in collaboration with Enterprise Strategy Group, today released the State of Security 2023, an annual global research report that examines the security issues facing the modern enterprise. More than 1,500 security leaders participated in the survey, revealing they've continued to see an increase in cyberattacks and unplanned outages.

*Images by Freepik*

According to the report, over half (52%) of organisations say they have suffered a data breach in the past two years, an increase from 49% in 2022 earlier and 39% in 2021. In addition, 62% of respondents report that their business-critical applications have suffered from unplanned downtime due to a cybersecurity incident on at least a monthly basis, an increase from 54% in 2022.

Key Singapore findings from the report include:

- **Companies are increasing investment in security at a lower rate than their peers:** Just 27% say that their organisation will increase spending significantly over the next 12-24 months (vs 59% across the rest of the world).
- **Local companies are less likely to report software supply chain security as a top area of focus for the coming year** (23% vs 33% in the rest of the world).
  - Only 38% of Singapore organisations say they've significantly increased their focus following recent software supply chain attacks (vs 70% of respondents in the rest of the world).
- **The implementation or increased investment in key controls to assist with ransomware is less likely to be reported by companies.**
  - Only 17% implemented ransomware detection rules (vs 26% in the rest of the world)
- **Companies across the APAC region prioritise investment in staff training and commercial security controls to overcome talent challenges.**

Globally, the report has also found:

- **Bad actors are going unnoticed on corporate networks for extended periods of time.** On average, respondents report over two months **(2.24)** go by from when a bad actor gains access to when appropriate parties are aware of it.
- **The mean number of outages an organisation faces is ~22 per year.** The costs of this downtime consumes roughly **2.7% of annual revenue.** According to Splunk's recent Resilience Pays Off global research report, this downtime can cost organisations roughly $365,000 per hour.
- **Security incidents are an existential threat.** Over a third **(39%)** of the respondents say cybersecurity incidents have directly harmed their competitive position. In addition, 31% say cybersecurity incidents have reduced shareholder value.

While enterprises face major cybersecurity obstacles, many organisations are taking steps to address these challenges:

- **Security teams are spending more. 95%** of the respondents say their security budgets will increase over the next two years, with 56% saying their budgets are increasing "significantly."
- **Cybersecurity is a team sport. 81%** of organisations say they are converging aspects of their security and IT operations together. Respondents believe that this convergence will help with the overall visibility of risks in their environment (58%) and that they will see improved cooperation in threat identification and response processes (55%).
- **Organisations focus on protecting their supply chain. 95%** of respondents say they have increased their focus on third-party risk assessments.
- **Data is the answer. 91%** of respondents agree that better capture and analysis of detection data is one of the most effective tools to prevent successful ransomware attacks.

"In the organisations we've worked with, resilience has been strongest with a collaborative approach in everything, from software development and infrastructure monitoring to business continuity planning," said Ryan Kovar, Distinguished Security Strategist for Splunk and Leader of SURGe. "This approach brings everyone to the table, including security leaders with IT and business leaders, so they all can focus on protecting the organisation."

**For more insights and recommendations from the State of Security 2023, please visit: https://www.splunk.com/en_us/campaigns/state-of-security.html** ■

# ALTRONIX LIGHTS UP ISC WEST 2023 WITH INNOVATIVE PRODUCTS FOR NEW APPLICATIONS

**Las Vegas, NV** – Altronix is showcasing new solutions for emergency communications and occupancy monitoring at ISC West in booth #11073. These additions further enhance the company's expanded portfolio of access, surveillance, security, and fire products that are on display at the event. New additions include Altronix new OA2 Occupancy Alert System, and COMMBATT™ Power and Backup for Emergency Responder Communication Enhancement Systems.

"Altronix continues to offer new products that make professional security installations easier, faster and more cost-efficient. This year at ISC West, we are further expanding our portfolio with new products that ensure sustained emergency communications and help facilities reduce risks and liabilities in public facing secured areas. We are also displaying new enhancements to our leading lines of products for critical security applications," said Alan Forman, President, Altronix Corporation.

Altronix OA2 Occupancy Alert System provides notifications when unauthorized activity or loitering occurs in up to two protected areas. This stand-alone solution is ideal for deployment in public facing areas such as restrooms in convenience stores, retail establishments, restaurants, universities, sports and recreation venues, etc.

Altronix is also previewing COMMBATT™ Power and Backup for Emergency Responder Communication Enhancement Systems. This provides power and back-up for bi-directional amplifiers (BDA) and other critical system components, while monitoring a wide range of internal supervisory conditions, including BDA health. An optional annunciator facilitates remote status monitoring.

An updated LINQ™ Dashboard enables remote power management of virtually unlimited Altronix LINQ enabled products throughout multiple sites. This feature provides comprehensive remote power diagnostics and reporting, as well as several new features. Dashboard v12 is backward compatible with existing LINQ enabled devices, ensuring a smooth transition when upgrading.
Additionally, Altronix is displaying a host of enhanced products, including:

**NetWay Spectrum PoE and Fiber Solutions** support the latest 802.3bt devices in remote locations with or without local power. Hardened PoE switches and media converters accommodate fiber, hybrid, and structured cable for a wide range of indoor and outdoor applications. NetWay Spectrum models are also available with embedded LINQ Network Power Management.
**NetWay™ PoE Adapters** enable deployment of up to two PoE+ devices over a single cable. Units are also capable of providing PoE+ (30W) and 12VDC simultaneously powering a camera along with an external microphone, and more. NetWay PoE Midspans/Injectors also support multiple 802.3bt devices and offer embedded LINQ Network Power Management.

**Pace™ Long Range Ethernet Adapters** transmit power and data up to 500m over structured cable or 1000m

over a single pair for deploying IP devices at longer distances. It is ideal for citywide surveillance, elevator communications, HVAC applications, and more.

**Tango™ PoE Driven Power Supply/ Chargers** utilize 802.3bt PoE to simultaneously deliver 12VDC and 24VDC. This eliminates the need for a dedicated AC power circuit, saving time and labor using low voltage installation and wiring methods.

**Trove™ Access and Power Integration** enhancements include expanded high- capacity wall and rackmount models to accommodate more access control hardware with or without Altronix power. Other additions include power supply protective covers and external wiring and battery cabinets for cleaner and more streamlined installations. Pre-configured kits including power distribution and wire management are also available with customized private labeling upon request.

**For more information on Altronix's extensive line of products e-mail info@altronix.com or visit www.altronix.com.** ■

# Applications of Video Surveillance Implementation for Crowd Management

*Images by Freepik*

Crowd management is vital to business operations, events, and public gatherings. It's essential in crowded places such as shopping malls, airports, train and bus stations, and sports stadiums. To ensure a safe and secure environment, managing and controlling crowds effectively is critical. This is where the use of video surveillance comes in.

Video surveillance can help with crowd management by providing a comprehensive overview of an area. As a result, this allows security personnel to identify areas of overcrowding, potential safety risks, and any suspicious activity. Also, video surveillance can be used to monitor the movements and behaviour of people so that appropriate action can be taken in the event of an emergency.

Video surveillance depends on facial recognition and artificial intelligence video analytics. The estimated growth of global facial recognition market size will be $12.67 Bn by 2028, with a growth rate of 14.2% from 2021 to 2028. Therefore, it's vital that we learn about the applications of video surveillance in crowd management. From managing sports stadiums to shopping malls, video surveillance is necessary to enhance security.

## atest Trends in Video Surveillance

Here are the latest trends rapidly making their way into video surveillance.

- Artificial Intelligence: Use of computer software with specific coding and machine vision. These can analyse various images and audio in different categories.
- IOT For Systems Integration: IOT can simplify operational data when analysing the relevant information for security and crowd management.
- Cloud To Cloud Integration: Remote saving of the videos and audio in archives is accessible all the time, saving the need for hard drives and several computers.
- Machine Learning: Using machine learning and deep learning to assess videos and audio. AI trains the systems just like humans to acquire new skills as needed. This adds new features and alert notifications while assessing the archives.
- High-Definition Cameras: Ultra HD 4K IP cameras offer 27 times the resolution of conventional analog cameras, hence better identifiable pictures. A high-resolution image will be easier to assess.
- Contactless Screening: Apart from a face recognition system, using camera body temperature screening and mask/equipment detection algorithm. Systems like ANPR and thermal screening devices are becoming popular for no-contact screening.

## Current Challenges for Video Surveillance Implementation

These are some of the challenges for video surveillance Implementation that must be addressed for smooth operations in the future.

### Hacking Threats

A video surveillance system faces the risk of hacking as it's connected to the internet. So anyone who hacks into the Wi-Fi camera system may steal important information while changing the surveillance system software or completely shutting it off.

**A video surveillance system faces the risk of hacking as it's connected to the internet. So anyone who hacks into the Wi-Fi camera system may steal important information while changing the surveillance system software or completely shutting it off.**

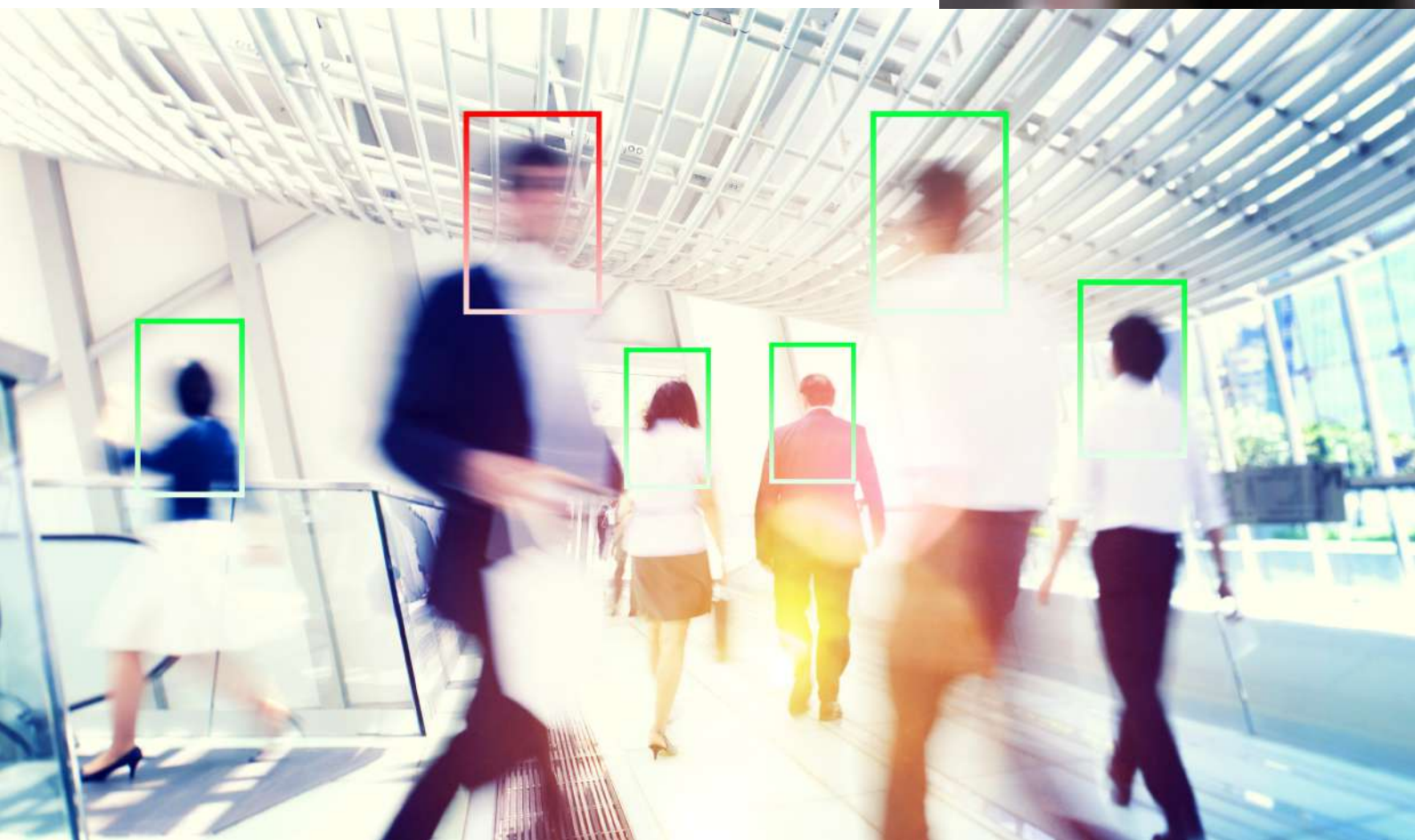
**Privacy Concerns**
It's crucial to balance security needs with privacy concerns and ensure that surveillance is used in a responsible and ethical manner. However, video surveillance everywhere does not ask for individual permissions and may use that data anywhere.

**Power Failure**
Lack of ample power, sudden grid failure, or poor Wi-Fi signal may lead to compromised video surveillance.

**Inaccuracies**
Although artificial intelligence and machine learning are evolving, some limitations remain. Some inaccuracies may exist, such as false reports while identifying humans, animals, or different races.

## Applications of Video Surveillance Analytics

Here are all the significant applications of video surveillance analytics.



*Images by Freepik*

**Facial Recognition**
Modern facial recognition software uses algorithms to analyse facial features and compare them to a database of known individuals. This can be particularly helpful in situations where there is a large crowd or when security personnel is trying to identify a specific individual.

For example, facial recognition can be used to track specific individuals' movements, such as suspects in a criminal investigation. Law enforcement agencies may use facial recognition to track suspects' movements and identify their whereabouts. This can help investigators gather evidence and build a case against the suspect.

**Object Detection**
Video surveillance analytics can detect and track objects of interest, such as cars, bags, or specific products, in a retail store. For example, retailers may use analytics to determine which products are most popular and which store areas attract the most traffic. These analytics will serve as a blueprint to detect theft or other suspicious behaviour, such as a customer attempting to shoplift a product.

In outdoor environments, video surveillance analytics can be used to track the movement of vehicles or people. For example, law enforcement agencies can use analytics to track the movement of a suspect's vehicle and monitor their activities. This can help investigators gather evidence and build a case against the suspect.

**Sports Stadium and Tournaments**
Video surveillance analytics can be used in sports stadiums and tournaments to track player movement, detect and prevent unauthorised access, and monitor the behaviour of fans. One primary use is that video analytics can track player positioning, speed, and movements during a game.

This can be used for performance analysis and to improve coaching strategies. Analytics may also be used to detect and prevent unauthorised access, such as fans trying to enter restricted areas or individuals attempting to sneak into the stadium without a ticket.

Analysing fan behaviour in large crowds can be successfully done using video surveillance. For example, analytics can detect large crowds or congestion, alerting security personnel to potential safety concerns. Analytics can also be used to identify fans who are engaging in any sort of disruptive or violent behaviour.

In addition, video analytics can be used to manage parking lots, analyse traffic flow, and monitor parking violations. This can help improve traffic flow and reduce congestion, making it easier for fans to get in and out of the stadium.

Many large tournaments and associations are moving towards using artificial intelligence video surveillance. One such example is the French National Assembly approving the use of artificial intelligence video surveillance at the Paris 2024 Olympics. This makes France the first European Union country to approve the use of a wide-reaching AI-powered surveillance system.

*continue on page 30*

**Shopping Malls and Retail Spaces**
Video surveillance analytics can be used in shopping malls and retail spaces to track foot traffic, monitor shopper behaviour, and detect theft. Moreover, it may predict rush hours by analysing the usual traffic. This can benefit in effectively managing crowds and using ample measures to avoid chaos.

Retailers can use this information to optimise store layouts, improve product placement, and enhance the shopping experience. This may also help retailers prepare for peak shopping by ensuring they have enough staff and inventory to handle the increased traffic.

Video analytics can also be used to monitor shopper behaviour and detect suspicious activity, such as shoplifting. Retailers can use this information to intervene before a theft occurs, improving loss prevention efforts.

**Offices and warehouses**
There will be an influx of people in a big corporation or office. A warehouse will have delivery personnel, security, and other staff to handle operations. Video surveillance is a big help in these spaces.

They may track the movement of employees, machines, technical assets, and working hours. Moreover, it may detect lunch breaks and employees' absences from the office. If an employee takes an extended break, the system can notify that.

If anyone leaves work early before the set working hours, a similar notification will help to find the person. The management won't rely on manual labour for this task.

**Hospitals**
Video surveillance analytics can be used in hospitals to monitor patient behaviour, track the movement of medical staff, and prevent unauthorised access to sensitive areas. If a patient is in intensive care, the monitoring may be more manageable. The presence of medical staff and the working of machines may be detected using video surveillance. In case of an emergency, the staff can be immediately disposed of.

**Airport security**
Airport security is of utmost importance for any country. The global airport security market will grow by 26 Billion by 2030. With AI video surveillance, we can improve security measures and enhance the airport experience for passengers.

AI video surveillance involves using artificial intelligence and machine learning algorithms to analyse real-time video footage and identify potential security threats. One way AI video surveillance can be used in airports is to detect suspicious behaviour. For example, AI algorithms can analyse the movements and behaviours of individuals and identify patterns that may indicate potential threats, such as someone attempting to sneak into a restricted area or tampering with security.

AI video surveillance can also be used to identify lost or unattended items, such as bags or suitcases, that may pose a security risk. The system can detect and alert security personnel to the presence of unattended items, allowing them to investigate and take appropriate action if necessary.

Another use of AI video surveillance in airports is to enhance the passenger screening process. For example, AI algorithms can analyse passenger behaviour and identify those who may require additional screening, such as someone who is nervous or acting suspiciously.

AI video surveillance can also be used to monitor airport traffic, both inside and outside of the terminal. This can help airport authorities identify areas of congestion or potential safety hazards, such as a vehicle parked in a no-parking zone or a crowd blocking an emergency exit.

*Images by Freepik*

**Video analytics can also be used to monitor shopper behaviour and detect suspicious activity, such as shoplifting. Retailers can use this information to intervene before a theft occurs, improving loss prevention efforts.**

## Video Surveillance for Emergency Response

One of the significant goals of video surveillance is to offer an emergency response in crowded areas. Time is vital in such situations, and analysing real-time video may help create a plan to manage crowds. The staff can access crucial life-saving risk assessments and measures without wasting precious minutes in an emergency.

After the emergency is under control, video surveillance can be used to identify any additional potential threats or sketchy behaviour. It may be used in the following ways.

**Monitoring for Suspicious Activity:** With a simple program of facial expression detection and body language, video surveillance systems can detect and analyse patterns of activity that may indicate potential threats. These activities include people loitering in sensitive areas, vehicles parked in unusual locations, or abandoned bags or packages.

**Facial Recognition:** Video surveillance can identify individuals who pose a threat or are on a watchlist. Some venues may ban a particular activity or people and prevent them from entering the premises. Some areas may prohibit excessive drinking and may prevent crowd gathering doing so.

**Alarm Triggers:** When an unauthorised person enters a restricted area, the surveillance system triggers alarms and sends signals to manage that situation.

**Quick Response:** With real-time monitoring, security personnel can respond to potential threats when they are detected. This can help prevent incidents from escalating into massive emergencies.

**Evidence Collection:** In an emergency or crime, video surveillance can provide valuable evidence to law enforcement agencies. The footage can help investigators identify suspects, track their movements, and gather relevant information.

## Parting Words

Now we know the applications of video surveillance and current trends that enhance the security system. In addition to helping with crowd management, video surveillance can help with safety monitoring, public event management, and business operations. This will significantly detect dangerous behaviours, and deter theft and vandalism. The videos and audio may then provide evidence for prosecution.

Overall, video surveillance for crowd management is an integral part of ensuring everyone's safety and property protection. ■

# COMING SOON

**APR 25 – 27 2023**
**The Security Event 2023**
Birmingham, United Kingdom
https://www.thesecurityevent.co.uk

**APR 27 – 29 2023**
**Secutech India 2023**
Mumbai, India
https://secutechindia.in.messefrankfurt.com

**APR 26 – 28 2023**
**Secutech Taiwan 2023**
Taipei, Taiwan
https://secutech.tw.messefrankfurt.com

**AUG 16 – 18 2023**
**Secutech Vietnam 2023**
HCMC, Vietnam
https://secutechvietnam.tw.messefrankfurt.com

**SEP 11 – 13 2023**
**GSX 2023**
Dallas, USA
https://www.gsx.org

**OCT 3 – 5 2023**
**Intersec Saudi Arabia 2023**
Riyadh, Saudi Arabia
https://www.intersec-ksa.com

**NOV 1 – 3 2023**
**Secutech Thailand 2023**
Bangkok, Thailand
https://secutechthailand. tw.messefrankfurt.com

*Security Solutions Today is available on issuu!*

issuu.com/securitysolutionstoday

*Or download our e-magazine at*

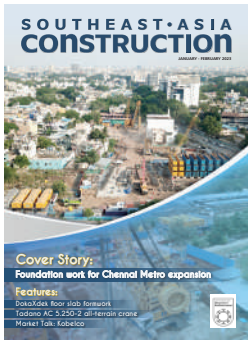
sst.tradelinkmedia.biz

# SUBSCRIPTION FORM

Email your order to:
**yvonne.ooi@tradelinkmedia.com.sg**

## PRINT

☐ **Southeast Asia Building**
*Since 1974*




☐ **Southeast Asia Construction**
*Since 1994*

### *1 year (6 issues) per magazine*

| | | |
|---|---|---|
| Singapore | ○ | SGD$70.00 |
| Malaysia / Brunei | ○ | SGD$120.00 |
| Asia | ○ | SGD$180.00 |
| America, Europe | ○ | SGD$220.00 |
| Japan, Australia, New Zealand | ○ | SGD$220.00 |
| Middle East | ○ | SGD$220.00 |

## DIGITAL

Please (√) tick in the boxes.

☐ **Bathroom + Kitchen Today**
*Since 2001*

☐ **Lighting Today**
*Since 2002*

***Bathroom + Kitchen Today***
is available on digital platform.
To download free PDF copy,
please visit:

**http://bkt.tradelinkmedia.biz**

***Lighting Today***
is available on digital platform.
To download free PDF copy,
please visit:

**http://lt.tradelinkmedia.biz**

☐ **Security Solutions Today**
*Since 1992*

***Security Solutions Today***
is available on digital platform.
To download free PDF copy,
please visit:

**http://sst.tradelinkmedia.biz**

**Personal Particulars**

Name: _____

Position: _____

Company: _____

Address: _____

_____

Tel: _____ E-Mail: _____

**IMPORTANT**

Please commence my subscription in
_____ (month/year)

Professionals (choose one):

☐ Architect ☐ Landscape Architect ☐ Interior Designer ☐ Developer/Owner
☐ Property Manager ☐ Manufacturer/Supplier ☐ Engineer ☐ Others

☐ Bank transfer payable to:
**Trade Link Media Pte Ltd**

**Bank Details**

| | |
|---|---|
| **Account Name:** | Trade Link Media Pte Ltd |
| **Account Number:** | 033-016888-8 |
| **Name of Beneficiary Bank:** | DBS Bank |
| **Address of Beneficiary Bank:** | 12 Marina Boulevard, DBS Asia Central, Marina Bay Financial Centre Tower 3, Singapore 018982 |
| **Country:** | Singapore |
| **SWIFT Address/Code:** | DBSSSGSG |

☐ PAYNOW to:
**Trade Link Media Pte Ltd**

PAYNOW option is applicable for **Singapore companies only**.

**Company Registration Number:** 199204277K

* GST inclusive (GST Reg. No: M2-0108708-2)

# ADVERTISE WITH US TODAY!

Email us at info@tradelinkmedia.com.sg.

Scan to visit our website