

www.securityupdate.in

# SECURITY Update

THE SECURITY & FIRE SAFETY TECHNOLOGY MAGAZINE

For Security &  
Fire System  
Manufacturers,  
Distributors, Dealers,  
Integrators, Installers,  
IT Systems Integrators &  
VARs, Consultants &  
Enthusiasts.

Vol. 14 No. 08 | September 2024  
Price ₹ 150 | Pages 52

WiFi Halo: Revolutionising IoT  
Applications



## CLOUD ADOPTION TRANSFORMING PHYSICAL SECURITY

Serving The Mission Critical Requirements  
Of The EdTech Market With A Broad Range  
Of Smart Technologies, Including Security

Cybersecurity Should Be A Part Of A  
Business Strategy For You



# BEST SECURITY INDUSTRY PUBLICATION



**ON 28TH NOVEMBER 2018, SECURITY UPDATE WAS AWARDED  
AS THE 'BEST SECURITY INDUSTRY PUBLICATION'  
BY THE HON'BLE UNION MINISTER OF COMMERCE &  
INDUSTRY AND CIVIL AVIATION  
SH. SURESH PRABHU  
DURING THE 28TH IISSM GLOBAL CONCLAVE IN NEW DELHI.**

# HIKVISION®

See Far, Go Further



## VIDEO DOOR PHONE (INTERCOM)

VIEWS LIVE VIDEO OF DOOR STATIONS AND LINKED CAMERAS



### DS-KIS603-P

- Night Vision
- WDR
- HikConnect App
- Alarm Output

7-Inch Colourful Touch Screen, Display Resolution: 1024\*600



Standard  
PoE



Alarm  
In & Out



Wi-Fi  
Supported



32G  
SD Card



Auto  
Capturing  
Pictures



Plug &  
Play

 /HikvisionIndiaOfficial

**Prama Hikvision India Private Limited**

 /HikvisionIndiaOfficial



**Registered Office:**

Office No.1-4, 2nd Floor, Siddhivinayak Arcade, Akurli Cross Road No.1,  
Near Kandivali Station, Kandivali (E), Mumbai - 400 101, India.

**CIN: U36100MH2009PTC190094**

**Corporate Office:**

Oberoji Commerz II, International Business Park, 18th Floor, Near Oberoi Mall,  
Off. W. E. Highway, Goregaon (East), Mumbai - 400063, India.

**Board No.:** +91-22-4041 9900, +91-22-6855 9900 | **Web:** www.hikvisionindia.com



**Technical Support:** +91-22-6822 9999, +91-22-3322 6060  
**Email:** support@pramahikvision.com



**Sales:** +91-22-6822 9944, +91-22-4041 9944  
**Email:** sales@pramahikvision.com



**RMA Support:** +91-22-6822 9977, +91-22-3322 6070,  
+91-250-663 6677 | **Email:** rma@pramahikvision.com



**Toll No.:** 18602100108



COVER  
STORY

16

## CLOUD ADOPTION TRANSFORMING PHYSICAL SECURITY

The physical security industry is swiftly adopting cloud-based solutions, fueled by advancements in AI and cybersecurity. Despite ongoing concerns about migration and network reliability, the benefits—scalability, cost savings, remote management, and real-time AI analytics—are significant. Security leaders agree that cloud technology is essential for future-proofing operations, and delays in adoption could leave organizations vulnerable. In this article, Kunal Bhogal examines the opportunities and challenges of cloud-based security, emphasizing the urgent need for businesses to modernize their security strategies.

### WISE THOUGHTS 8

#### AI, Analytics & Machine Learning— What's The Difference?

In an era where the term “AI” dominates discussions across various industries, distinguishing between its different forms—particularly within the security sector—has become essential. Peter Giacalone, explores the distinction between Narrow AI and General AI, emphasizing how Narrow AI applications like facial recognition, object detection, and anomaly detection are revolutionizing security practices. With many companies claiming to leverage AI, understanding its true capabilities is crucial for navigating this rapidly evolving landscape.



### 10 INDUSTRY UPDATE

### 22 CASE STUDIES

General Information

SECURITY UPDATE welcomes manuscripts, news items and photographs, however SECURITY UPDATE is not responsible for loss or damage incurred while in transit or in our possession. SECURITY UPDATE is published monthly on the 28th day of every month. Editorial deadlines are three weeks before this date.

## 26 SU GYAN



### WiFi Halo: Revolutionising IoT Applications

WiFi HaLow (IEEE 802.11ah) is revolutionizing video surveillance with its long-range, low-power capabilities tailored for IoT applications. It offers efficient and scalable solutions for modern surveillance, enhancing safety in both residential and commercial settings.

## 28 BIZ BUZZ



### Cybersecurity Should Be A Part Of A Business Strategy For You

The article emphasizes integrating cybersecurity into business strategy due to increasing cyber threats. It highlights the importance of measures like multi-factor authentication and leadership commitment to protect sensitive data and maintain customer trust. A proactive approach is essential for mitigating risks and safeguarding organizations from potential breaches.

## 36 PRODUCTS UPDATE

## 44 INDUSTRY SPOTLIGHT



### Serving The Mission Critical Requirements Of The EdTech Market With A Broad Range Of Smart Technologies, Including Security

The article explores the evolving EdTech market, highlighting its benefits like remote learning and personalized education. It emphasizes the integration of security technologies, such as cloud-based access control and AI surveillance, to enhance campus safety. Hikvision's solutions are presented as vital tools for ensuring secure and interactive educational environments.

## 30 TECH TALK

- Hanwha Head Of Product And Marketing On The Future of AI
- Frost Predicts Rapid Growth In Corporate Cloud Protection Market

## 32 FIRE CHAT

- The Rising Importance Of Fire Safety And Protection Risks
- Bull Products introduces new LFX Lithium-Ion Fire Extinguishers
- Minimising fire risks in recycling plants through video analytics and real-time verification systems

## 50 EVENTS CALENDAR

# EDITOR'S NOTE



**Dear Reader,**

In my April 2019 Editorial, I noted that “CCTV cameras have become a part of our daily lives. There is no longer any mystery surrounding how they work or what they do. In fact, millions are being installed worldwide, both privately and publicly, to detect and prevent crime, as well as to enforce laws.” However, in India, the rapid deployment of cameras in recent years often occurs without a proper assessment of the purpose they are meant to serve, with key elements of professional ‘System Design’ frequently overlooked.

By May 2022, I addressed the active promotion of public surveillance cameras in Chennai, which led to a significant increase in CCTV installations across the city. The then-police commissioner was a strong advocate of video surveillance and urged citizens to support law enforcement by installing cameras in their homes, shops, and buildings. He even pushed for the civic authorities to mandate CCTV installations as a requirement for new building plan approvals.

By forging a public-private partnership, Chennai Police had managed to get the shopkeepers, traders and several resident welfare associations to pitch in with their contributions to bring the entire city under the surveillance system. Perhaps, this was the reason behind the amazing incident, where a nine-year-old girl had contributed ₹1.5 lakh from her life savings to fix CCTV cameras in the city!

However, I had also cautioned then, and which holds true till today, this investment and efforts shall be in vain if a robust plan to maintain these systems was not


simultaneously put in place. A section of residents had soon thereafter claimed that the CCTV cameras would be of no use if they failed to detect and resolve crimes, due to poor maintenance and dysfunctional cameras.

I have long emphasised the critical need to maintain installed systems to ensure optimal performance. In a recent 2024 ruling, the Hon’ble Madhya Pradesh High Court underscored this by mandating proper upkeep of CCTV cameras in police stations to safeguard citizens’ fundamental rights. Justice Subodh Abhyankar, presiding in Indore, declared that from now on, any failure to provide CCTV footage from police stations will lead to disciplinary action against the responsible Station House Officer and other relevant officials.

This order has come in the wake of the Hon’ble Supreme Court of India order of 2020, where the court had ordered the installation of CCTV cameras in all police stations and central investigation agencies. The court had also directed that the recordings be kept for at least a year. The court also established Oversight Committees at the state and district levels to ensure the installation and maintenance of CCTV cameras.


While it’s unfortunate that it takes a court orders to ensure the upkeep of public security cameras—something that should be the responsibility of the custodians to maintain, given these systems are funded by taxpayer money—it is a reality that many such installations fall into disrepair, creating a false sense of security for citizens. However, I am pleased that this precedent has been set to hold system owners accountable for their neglect. Hopefully, this will lead to improved performance in the future.

Till we meet next month, Stay Safe and Keep Others Safe.

  
**G B Singh**  
Group Editor

 [gbsingh@1stasset.org](mailto:gbsingh@1stasset.org)

 [@gbsingh9](https://www.linkedin.com/in/gbsingh9)

 [@EditorGB](https://twitter.com/EditorGB)

All rights reserved. No part of this publication may be reproduced in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise without the prior written consent of the publisher. Opinions expressed in articles or advertisements appearing in SECURITY UPDATE are those of the authors or advertisers and do not necessarily reflect those of the publication, or of its publishers.

Printed, published and edited by G B Singh on behalf of 1st Academy of Security Science Education & Training Pvt. Ltd. Printed at Ask Advertising Aids Pvt. Ltd. 88 DSIDC Sheds, Okhla Indl. Area Ph-I, New Delhi 110020 Published at “Security House”, 24-B, Udyog Vihar-V, Gurugram 122016, Haryana, INDIA.

[info@1stasset.org](mailto:info@1stasset.org)

presents

**SECURITY TODAY**  
www.securitytoday.in

# KNOWLEDGE SUMMIT SINCE 2006 2024

**REGISTER NOW**



**GRAND HYATT GURGAON**



Knowledge Partner:



Media Partner:



The Knowledge Summit presented by SECURITY TODAY has gained universal recognition for providing in-depth coverage of leading edge technical and security management issues facing Protection Professionals.

For details, visit our website:

<https://securitytoday.in/knowledgesummit/> | E-mail: [events@1stasset.org](mailto:events@1stasset.org)

# AI, Analytics and Machine Learning—What’s the Difference?



**Peter Giacalone**

The author is the President of Giacalone Associates, an independent security consulting firm.

Over the past few years — and especially this past year — the term “AI” has become one of the most discussed (and possibly most misunderstood) of our time.

Artificial intelligence, or AI for short, has had a lot of hype on so many levels and on countless channels. Given the stated power of the new capabilities that its use enables, it is no wonder that so many are compelled to learn more and even engage.

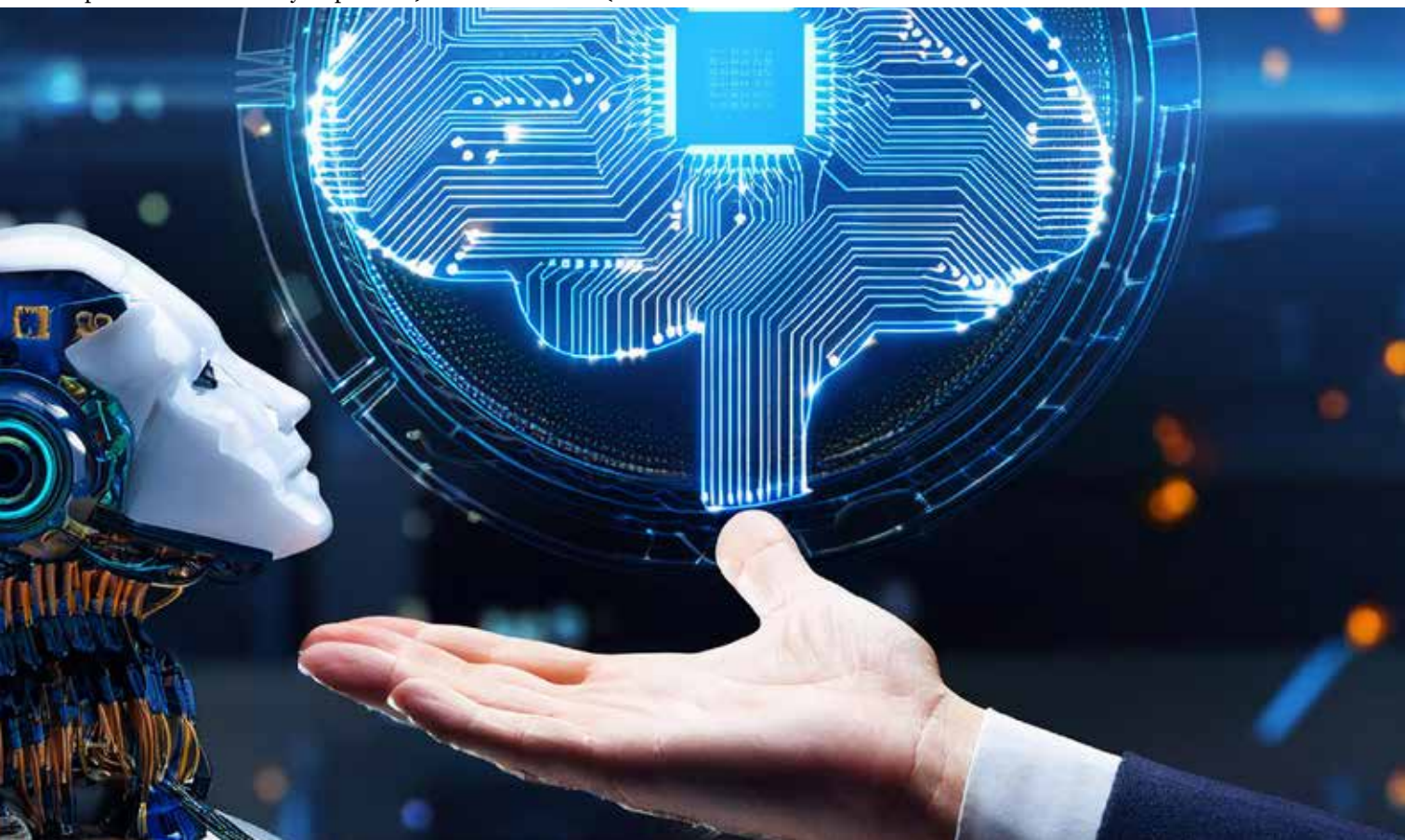
Because of all this buzz, it’s often hard to differentiate what’s real from what’s not. Every company nowadays claims to have some sort of AI. But what does it mean for the security industry?

At the highest level, there are two main types of AI: “Narrow AI” (an AI that is trained to solve one specific problem as accurately as possible) and “General AI” (an

AI that can solve any generic problem and can think critically and reason about any topic like a human would).

All mainstream applications of AI today are Narrow AI, no matter how much they may look like General AI. For example, ChatGPT can take any written textual input and generate human-like text responses to the prompt. However, ChatGPT is a subclass of AI called “Generative AI,” which is trained on an input dataset (i.e., all text that humans have written on the internet) and taught to do a specific task (i.e., respond to a text input with a relevant text output).

ChatGPT appears at first glance to be General AI but lacks the generic reasoning necessary to garner that distinction. Instead, it’s most accurately classified as Narrow AI. As of today, a true General AI has yet to be





created. However, we have been able to solve a lot of real-world problems with Narrow AI.

Internet search is amazingly accurate; your navigation directions and ETA to destination are accurate within minutes; self-driving cars are starting to reach a threshold of being nearly as safe as (or even safer than) human drivers; and, perhaps most importantly, through a variety of available tools, we can generate pictures of some really strange things that don't actually exist.

There are also some really important applications of Narrow AI in the security industry.

Here are a few security industry applications that are particularly compelling:

**Facial recognition in video:** This is, to date, one of the best applications of narrow AI in the security industry. As of today, it still has some key real-world limitations, but we expect improvements to continue to open new opportunities for its application.

**Object recognition in video:** Having a computer "watch" a video and be able to identify which specific objects are in the video (e.g., animal, person, vehicle, weapon/gun, open door, closed door, fire, smoke) is an extremely valuable capability for security.

**Optical character recognition (OCR) in photos and video:** Being able to tell from a photo what text is in the field of view (i.e., being able to automatically read a license plate) has been revolutionary for many security applications.

**Speaker/voice recognition in audio:** This opens the door to many interesting applications. Speech-to-text has existed for quite a while, but some companies are making advancements in their capacity to detect who is speaking based on their voice.

**Detection and identification of common sounds (e.g., the ability to automatically detect a gunshot, glass breaking or another event of interest that emits a lot of sound) is hugely powerful.**

Interestingly, many voice-recognition platforms and facial-recognition platforms face many of the same challenges (e.g., accuracy of the technology, privacy concerns, the need to have a monitored area completely blanketed in the technology in order to realize its benefits).

**Anomaly detection:** This is a broad term with many

potential applications, but there are a few key examples in the security industry that jump out.

Anything that can be measured over time and plotted on a line chart can be trained into an anomaly-detection model. Computers are capable of noticing regular patterns in the behavior of critical metrics and alerting you if there are major deviations from patterns that have been seen in the past. Applications include predictive maintenance on critical security equipment, crowd



behavioral patterns and temperature/humidity/noise fluctuations in a monitored area.

Increasingly, novel presence-detection technologies are creating computer-readable insights about who is coming and going from a monitored premise. These behavioral patterns can train AI models to elevate new insights about normal and abnormal presence of devices and individuals in critical areas.

Anomaly detection is also particularly useful in cybersecurity. "Normal behavior" and "normal access patterns" can often be quantified, and AI models then can tell you when there is access or behavior that looks abnormal. For instance, your number of "friend requests per second" on Facebook is an easily measurable quantity. Facebook regularly employs AI models to detect if an account is suddenly sending a far larger than normal number of friend requests. If so, it can automatically block that account and flag it as hacked/spamming. ■

## Vivotek Enhances AI Security Solutions with Realsight Engine



“Realsight Engine further improves image clarity in various scenarios, ensuring key images are accurately captured, providing clients with crucial evidence,” said Louis Liao, Director of Product Planning at Vivotek.

Realsight Engine’s key benefits include:

- Reducing motion blur and enhancing facial detail.
- Capturing clear night images without manual adjustments.
- Improving facial clarity in backlit conditions by balancing brightness.

Vivotek has launched the Realsight Engine, an advanced AI feature that significantly improves image clarity in challenging lighting conditions. This technology enhances facial images even in backlit or low-light environments, optimizing operational efficiency in areas like dimly lit galleries and parking lots. The feature is designed for easy activation, eliminating complex setup processes.

This feature is now available in selected AI network cameras and will soon expand across Vivotek’s product line.

Vivotek also highlighted that the global AI camera market, valued at \$8.2 billion in 2023, is projected to reach \$67.4 billion by 2033, emphasizing the growing importance of AI in security technology.

### Assa Abloy Cumulus wins innovation initiative award

Abloy Cumulus, a keyless mobile access solution from Assa Abloy Opening Solutions EMEA, has been named the 2024 winner of ISJ’s Leaders in Security Award in the Innovation Initiative category. ISJ praised Cumulus for its ethical design and operational flexibility.

Cumulus replaces traditional keys with encrypted mobile credentials, allowing users to unlock any authorised device via their smartphone. It simplifies access management, offering quick authorisation changes and audit trails for enhanced security. The system works even in remote locations without continuous network coverage.

“Abloy Cumulus was built API-first, making it easy to integrate with various systems,” said Hanna Sillanpää, Head of Abloy Digital Solutions. The range includes outdoor-ready padlocks, key deposits, and a Bluetooth-enabled Cumulus Controller that works with any electric or electronic lock.

### Sensormatic recognised with sustainability award

Sensormatic Solutions has been awarded a bronze Stevie in the 21st Annual International Business Awards for its hard tag recirculation programme, recognized in the Sustainability Initiative of the Year category. This programme helps retailers reduce environmental impact by recirculating, recertifying, and reusing security tags, lowering costs and minimizing plastic waste.

Over the past two years, the initiative has recirculated 2.5 billion tags, saving 45.8 million pounds of plastic and 551,000 MWH of electricity. One judge noted, “By reusing and recertifying tags, they reduce waste and minimise emissions.”

Sensormatic also introduced its Sustainable SPX AM Label, made from over 90% plastic-free materials, helping retailers meet environmental goals while using existing EAS systems.





# IS THIS HOW YOU GO INTO THE MARKET **LOOKING** **FOR CUSTOMERS?**

Let your customers find you  
@ **SECURITY UPDATE**

Advertise in **SECURITY UPDATE**  
and exhibit your product/service  
line for meaningful business.

**SECURITY UPDATE** is the best read channel publication brought exclusively to you by the most read and followed magazine in the Industry - **SECURITY TODAY**.

If you are a Security & Fire Systems Manufacturer, Distributor, Dealer, Integrator, Installer, IT Systems Integrator or VAR, then **SECURITY UPDATE** is just the right medium to advertise in and augment your business via our print and digital publications and web portal.

**Why wait?**

Contact us today @ **9811549545**  
or **info@1stasset.org**



Note: To subscribe to our print and digital editions log on to <https://www.securityupdate.in> or Scan this QR Code and choose your tenure and mode of delivery, fill your contact details make your payment on our secure gateway using your credit/debit card. Alternatively, you may even tear and physically fill the subscription form available in this magazine, and courier it to us along with your payment.

## Identiv receives official authorisation for \$145 million asset sale

The Committee on Foreign Investment in the United States (“CFIUS”) has now approved Identiv’s transaction to sell its physical security business and assets to Vitaprotech, the security solutions provider that also acquired British manufacturer, TDSi in 2019.

The Identiv sale was originally announced in April this year, but was subject to regulatory approval under the Hart-Scott-Rodino (HSR) Act and to approval from the Committee on Foreign Investment in the United States (CFIUS).

On August 15, 2024, Identiv received notification of approval from the Department of Treasury, on behalf of the Committee on Foreign Investment in the United States. CFIUS determined that there were no unresolved national security concerns; therefore, action under

Section 721 with respect to the transaction was concluded.

Having met all regulatory requirements and received shareholder approval of the transaction, all regulatory and statutory conditions for closing have been satisfied. Both parties are now proceeding to close the transaction promptly. Based on the anticipated time needed to complete the actions required to close, Identiv and Vitaprotech expect to close the transaction within 30 days following CFIUS approval.

Upon closing of the transaction, Identiv will receive a cash payment of \$145 million, subject to customary adjustments. The proceeds from the sale will significantly strengthen Identiv’s financial position, providing capital to pursue growth opportunities for its specialty IoT solutions business.

## Gunnebo earns bronze EcoVadis status for sustainability

Global security solutions specialist, Gunnebo has achieved the prestigious bronze EcoVadis status, affirming its dedication to evolving sustainable business practices and corporate responsibility.

EcoVadis is a globally recognised sustainability rating platform that assesses the environmental and social performance of companies across various industries. It evaluates a company’s performance based on four key categories: Environmental Impact, Labour & Human Rights, Ethics, and Sustainable Procurement.

In 2024, Gunnebo was awarded a score of 62, reflecting a significant improvement from its 2023 score of 48. This enhanced rating is a clear indicator of Gunnebo’s progress on its sustainability journey.

Stefan Syrén, President and CEO of Gunnebo comments, “We are on a journey to establish a robust and sustainable business model that ensures solid long-term profitability. Our improved EcoVadis rating demonstrates we are on the right path. While we are still in the early stages of this transition, I am confident this Bronze Medal represents just the beginning. We will continue to do all we can to strengthen our efforts for a better future.”

Gunnebo has been intensifying its sustainability efforts

with a focus on building a resilient business that delivers long-term profitability. A cornerstone of these efforts is the Company’s commitment to achieving net-zero carbon emissions by 2045 under the Science Based Targets Initiative. This ambitious goal aims to decarbonise Gunnebo’s entire business model.



The Company is dedicated to creating safe and diverse workplaces where employees are empowered to innovate and deliver top-quality products for customers and partners. The notable improvement in Gunnebo’s EcoVadis rating not only highlights the progress made but also provides valuable insights into areas where the Company can further enhance its sustainability practices.

Per Hökfelt, Head of Sustainability at Gunnebo adds: “I am pleased with our progress in improving our rating from last year and also acutely aware of the continued need for improvement. I firmly believe in a long-term approach to sustainability, which involves laying the groundwork for future profitability by steadily moving towards net-zero emissions.” As Gunnebo continues to advance on its sustainability journey, the Company remains committed to making meaningful progress and setting new standards for sustainability in the security industry.

## BRINC & Echodyne partnership brings new abilities to first responders

BRINC, a pioneer in drone technology for first responders, has entered into a strategic partnership with Echodyne, a leader in ground-based radar systems. This collaboration will integrate Echodyne's advanced MESA radar technology into BRINC's purpose-built Drone as First Responder (DFR) solution.

The strategic relationship enables a path toward beyond-visual line of sight (BVLOS) operations without visual observers, advanced airspace awareness for safer operations, and lowers the barrier to entry for public safety agencies looking to start or expand DFR programmes.

Drone as First Responder (DFR) systems significantly lower emergency response times and enable more informed decision-making for first responders. Current FAA regulations require a visual observer onsite for drone operations to monitor flights. The onsite visual observer rule limits drones' flexibility and operating times for emergency response operations.

More importantly, it adds an extra staffing burden when public safety agencies across America are understaffed. As evidence of the staffing shortage, the Police Executive Research Forum's 2023 study on police staffing found that police resignations have increased over the last 4 years, alongside a 5% decrease in sworn-in officers over the same period.

DFR requires extended range and operation in obstructed environments and inclement weather. Beyond Visual Line of Sight (BVLOS) waivers are essential for successful DFR implementation. The partnership with Echodyne will add a layer of safety and reliability while providing a path for BRINC's customers to meet the stringent Federal Aviation Administration (FAA) requirements for BVLOS operations without a visual observer.



## Carrier agrees to Sell Fire Business for \$3 Billion

Carrier Global Corporation has agreed to sell its Commercial and Residential Fire business to Lone Star Funds for an enterprise value of \$3 billion. This move is part of Carrier's transformation into a more focused, high-growth company.

"This sale marks a defining step in our journey to become a pure-play company focused on sustainability," said Carrier Chairman & CEO David Gitlin. The company has now completed over \$10 billion in divestitures in about a year, achieving a mid-teens EBITDA multiple.

The sale is expected to close by the end of 2024, following regulatory approvals. Carrier plans to use the \$2.2 billion in net proceeds from the transaction for share repurchases.

"By combining BRINC's drone technology with Echodyne's advanced radar, we are creating a safe, robust, and reliable solution for first responders to deploy 911 response drones autonomously to emergencies," said Blake Resnick, BRINC CEO.

Echodyne's radar systems offer continuous monitoring and real-time data on the drone's surrounding environment, including the location of other aircraft, obstacles, and dynamic changes that can occur at a moment's notice.

"Echodyne radars have been used for years by UAS centres of excellence, as well as FAA and NASA testing programmes," said Eben Frankenberg, Echodyne CEO. "DFR represents a unique opportunity to introduce widescale BVLOS operations, and radars are the ideal sensor to provide detailed and accurate airspace situational awareness."

As part of BRINC's comprehensive DFR offering, BRINC Integrates Echodyne's hardware to send radar readings to an agency's connected Liveops account. From Liveops, agencies can simultaneously view their drone operations, ADS-B data, airspace advisories, weather conditions, and radar data. The Echodyne addition provides a comprehensive, all-in-one view of the surrounding airspace, enabling automated Liveops triggers to inform pilots of potential dangers. It also enables the automated grounding or rerouting of drones to avoid air traffic.

## Genetec renews FIPS certification for Security Center

Genetec’s Security Center 5.12 now complies with FIPS 201 and is approved by the Federal Identity Credential and Access Management (FICAM) conformance programme.

With this certification, government entities can trust that Genetec software meets stringent federal security standards to ensure that only authorised individuals are provided access to sensitive data and facilities.

This certification extends the list of supported FICAM access control hardware within Security Center Synergis. The Genetec access control platform is now certified to offer an end-to-end FICAM-compliant solution with HID Piv Class readers, HID Signo readers, Veridt readers, as well as Assa Abloy integrated locks and

server cabinet locks.



FIPS 201-certified products undergo rigorous testing, resulting in fewer vulnerabilities and robust security features, ensuring that federal organisations’ sensitive data are protected.

In a market often constrained

by proprietary systems, Synergis stands out by offering multiple open architecture systems that efficiently validate Personal Identity Verification (PIV and PIV-I) credentials for federal employees and contractors. This allows federal agencies and organisations to choose from a diverse range of certified and secure access control solutions, ensuring greater flexibility and interoperability.

“With this updated FIPS 201 certification and expanded support, federal customers can benefit from the latest generation of access control solutions,” said Thibaut Louvet, Product Group Senior Director at Genetec Inc. “Genetec is committed to providing the most up-to-date interoperability and options for FICAM-certified products.”

## Pye-Barker Fire & Safety acquires Safety Plus in Kansas

Pye-Barker Fire & Safety has acquired Safety Plus First Aid & Safety, a life safety equipment provider and servicer in Kansas. This addition extends Pye-Barker’s customer base in the Midwest and complements its full suite of code compliance services for commercial customers.

Safety Plus First Aid & Safety, headquartered in

customers with first-aid kits, AEDs, CPR kits and other safety equipment needed in case of a workplace injury or emergency. The company also conducts emergency response training and workplace safety assessments to ensure customers are compliant with local and federal regulations and can remain open and operational.



Wichita, helps businesses protect their employees and

“Safety Plus has always been a family-run business, dedicated to building trusting relationships with our customers and local community,” said Max Brown, President at Safety Plus. “Joining forces with Pye-Barker, a company that shares our commitment to local operations, will help us enhance the ongoing services we provide our customers.”

“Safety Plus complements our full-service safety offerings and is a natural fit for the growing Pye-Barker family,” said Bart Proctor, CEO of Pye-Barker Fire & Safety. “We are happy to have them aboard as we embark on this next chapter together.” The dedicated team at Safety Plus will continue to serve customers in Kansas, with support from Pye-Barker.

# Want to Unlock Expert Insights and Cutting-Edge Technology Updates Every Month?

## Subscribe to SECURITY UPDATE & Know The Latest:

- ✓ Industry Trends
- ✓ Technology & Products
- ✓ Industry Expert Interviews
- ✓ Insider knowledge & More....



INDIA'S LEADING PUBLICATION ON SECURITY & FIRE SAFETY TECHNOLOGY



ORDER FORM



I want to subscribe to

**SECURITY Update**  
THE SECURITY & FIRE SAFETY TECHNOLOGY MAGAZINE

Signature \_\_\_\_\_

Date \_\_\_\_\_

This subscription is for  personal /  office use \_\_\_\_\_

**Complete your details**

PLEASE USE CAPITAL LETTERS TO FILL THE FORM

Name (Mr./Mrs./Ms.) \_\_\_\_\_

Job Title \_\_\_\_\_ Organisation \_\_\_\_\_

Address \_\_\_\_\_

Town \_\_\_\_\_ District/State \_\_\_\_\_ Country \_\_\_\_\_

PIN/Zip/Postal Code \_\_\_\_\_ Tel/Mobile \_\_\_\_\_ Email \_\_\_\_\_

### SIMPLE STEPS TO SUBSCRIBE NOW:

- 1 Fill up the form above
- 2 Click a picture of the form
- 3 WhatsApp it to our team at: +91 98115 49545

# Cloud Adoption **Transforming** Physical Security!

Are you missing valuable opportunities by delaying large-scale migration to the cloud?

BY **Kunal Bhogal**



The author is the Business Head and Chief Design Officer - Design and Technology Services of IIRIS Consulting Pvt. Ltd.





In recent years, the realm of physical security has experienced a significant transformation, with cloud-based solutions becoming the prevailing trend. As organizations pursue systems that are more scalable, flexible, and secure, traditional on-premise security models are gradually being replaced by cloud-based infrastructures. This shift is primarily fuelled by the swift advancement of cloud technologies, the incorporation of artificial intelligence (AI), and an increased emphasis on cybersecurity.

Cloud (including Cloud computing, and Cloud storage) as we know it, isn't a new concept in Physical security. It has been amongst us since the early 2000s, and have slowly yet steadily become mainstream over the years. Though largely adopted by companies and large organisations in the West (thanks to excellent broadband services and availability of widespread data centre infrastructure), today it finds companies all over the world as adopters in equal proportions.

In a recent survey, over 90% of the surveyed security leaders agree that the future lies in the advancement of cloud infrastructure, and purpose built applications will gain traction much faster; and the businesses that delay the adoption will only fall behind in an industry that is rapidly moving towards a centralised, AI driven world. In the same survey, less than 25% of organizations are looking to fully transition to the cloud, while the majority prefer either an on-premise setup or a hybrid approach, with over two-thirds of their assets installed on-premise.

This migration of physical security to the cloud can also be attributed to digital transformation across industries, vast improvement in compute and communication speeds, adoption of AI and related new-gen technologies, as well as situations like the COVID-19 pandemic – that clearly highlighted the need for managing people, processes, assets and infrastructure – remotely.

The global cloud market, with its steadfast growth of CAGR 18%, has given organisations a huge impetus to think towards adoption of Cloud for Physical Security.

Although the shift to cloud solutions is already in progress, many organizations remain equally hesitant to revise their security strategies and incorporate cloud technologies into their physical security operations. The primary concerns revolve around infrastructure challenges in certain areas, the potential risks of transferring sensitive data to the cloud, and the complexities of migration. This article aims to examine whether these apprehensions are justified or if companies are missing valuable opportunities by delaying large-scale migration to the cloud. We will discuss the challenges associated with transitioning to a cloud environment for physical security, highlight the benefits of cloud-based technologies, and outline how

organizations can effectively leverage cloud migration for enhanced security.

Cloud-based physical security utilizes cloud servers to oversee access to facilities while safeguarding data associated with access control, video management, and alarm monitoring. This approach enables security teams to monitor their premises from any location with an internet connection.

Through this article, I intend to bring about a realistic canvas discussing opportunities and challenges of using Cloud for the physical security industry, and perhaps address some ground realities when adopting a cloud-focussed strategy.

### Why should an organisation think about Cloud?

Security hardware, such as cameras, access control Like any critical application or function, Physical security often necessitates costly servers that entail significant upfront investments and ongoing management. These servers are responsible for processing video feeds from security cameras to identify noteworthy events in addition to alarms coming from hundreds and thousands of sensors, readers and electronic components. In contrast, a cloud-based model can efficiently handle substantial computational demands. Additionally, security companies provide regularly updated software, ensuring that users always have access to the latest version. Another reason to shift to cloud-based systems are features that allow organizations to swiftly adjust to evolving security needs and effectively manage their infrastructure.

Some common challenges in traditional / conventional systems could be: A camera could be broken after a security breach, thereby producing no video, or system failure due to compatibility issues arising because of outdated firmware. Many of these problems are addressed through a well purposed cloud strategy, and organizations are likely to favour hybrid cloud solutions, which combine various environments, such as on-premises systems with public or private cloud options. These hybrid models can deliver the advantages of both approaches.

Through the cloud platform, we can oversee and manage security equipment remotely, eliminating the need for on-site visits. This capability is particularly advantageous for businesses that operate across multiple regions or have distributed locations, as it helps reduce labor and time costs while enhancing overall work efficiency.

Going back to the data from the survey: Significantly, 70% of respondents anticipate raising their expenditures on physical security systems in 2025.

This trend corresponds with the fact that 75% of security leaders intend to migrate to cloud solutions within the next year, and over 90% aim to finalize this transition within the following 18 months. This urgency underscores the critical need to modernize physical security infrastructures.

Cloud technology provides numerous advantages compared to on-premises systems, including flexibility, scalability, enhanced security, ease of maintenance, and future-proofing. However, not all cloud camera solutions are created equal. While some traditional systems may be retrofitted to accommodate cloud technology, fully integrated end-to-end systems—where the NVR, VMS, and camera functionalities are available out-of-the-box without the need for additional integration—lead to a more advanced, scalable, and adaptable security solution.

### Adopting Cloud for Physical Security: Advantages at a Glance



**Secure by Design:** Cybersecurity and network security are significant concerns regarding IoT devices, including cameras. There are various security aspects to consider with camera systems, ranging from the privacy of the video content to reducing the risk of cyberattacks. Frequently, security camera systems remain vulnerable due to their complexities, which can hinder effective maintenance.

**Scalability:** Scalability is arguably the most significant benefit of cloud-based systems. Traditional security setups often necessitate costly hardware upgrades and physical installations when expanding a security network. In contrast, cloud systems enable organizations to easily scale their operations up or down, adapting to evolving security needs without the need to completely revamp existing infrastructure. This flexibility is especially crucial in industries with variable security demands, such as retail, healthcare, and large event venues.

**Remote Management:** One of the most compelling

advantages of cloud-based security is centralized management. For large organizations or those with multiple locations, a unified platform enables security administrators to oversee all sites from a single dashboard. This feature is particularly beneficial for geographically dispersed businesses, such as retail chains, hospitals, or multinational corporations, where security threats can emerge at various locations simultaneously. Remote access is another significant benefit, allowing security teams to monitor and control their systems from anywhere in the world. Whether addressing a local threat or coordinating security across international sites, centralized management ensures that all data is accessible and actionable in real-time. Remote management is a crucial factor driving the transition to cloud-based security systems. In traditional on-premise setups, security personnel often need to be physically present to manage or troubleshoot systems, which can be time-consuming and inefficient—especially for organizations with extensive operations or limited resources. In contrast, cloud-based systems offer remote access capabilities that enable security teams to monitor feeds, manage devices, and receive alerts from any location with an internet connection. This functionality allows businesses to respond more quickly to security incidents, minimize downtime, and ensure continuous surveillance even during local technical issues. Additionally, remote management can reduce labor costs, as security personnel can oversee multiple sites simultaneously without the need for travel. This not only streamlines operations but also enhances the overall security posture by providing real-time visibility into potential threats. For instance, a company with multiple locations can implement a cloud-based solution that centralizes management, allowing security personnel to monitor all sites from a single platform. This approach simplifies operational complexity and facilitates timely responses to security threats across geographically dispersed locations.

**Cost Effectiveness:** Another significant advantage of cloud-based systems is their cost efficiency. On-premise systems often entail high upfront costs, requiring considerable investments in hardware, installation, and maintenance. In contrast, cloud-based solutions generally operate on a subscription model, enabling businesses to pay for the services they require on an ongoing basis without incurring large initial expenses. This subscription model also offers greater predictability in budgeting, allowing organizations to adjust their security investments based on current needs. This flexibility simplifies long-term cost management and helps avoid the financial burden associated with upgrading or replacing outdated systems. Furthermore, cloud-based systems facilitate the seamless integration of various security devices—such as cameras, alarms, and access control systems—into a single platform. This integration minimizes the need for multiple vendors and complex infrastructure, further streamlining

management and reducing overall costs.

**Strategic Importance of AI:** Artificial intelligence is increasingly becoming an integral part of cloud-based security systems. AI-driven functionalities, including video analytics and predictive modelling, enable security teams to proactively identify potential threats. The incorporation of AI is regarded as vital for sustaining a strong and proactive security stance. Artificial Intelligence has emerged as a transformative force in cloud-based physical security, introducing a level of sophistication that surpasses traditional systems. The integration of AI enables security platforms to execute tasks such as automated alerts, predictive modelling, and video analytics, which enhance organizations' ability to detect threats with increased speed and precision. Three-quarters of security leaders acknowledge the influence that AI-driven features can exert on a company's strategy for physical security. As security systems advance, integrating AI analytics will be essential for delivering actionable insights and maintaining an edge over sophisticated threats.

**Real-Time Detection:** One of the most significant contributions of AI to cloud-based security systems is its ability to analyze vast amounts of data in real-time. For instance, AI-driven video analytics can automatically identify unusual behaviours or unauthorized access, providing security teams with immediate alerts and reducing response times. Key features such as facial recognition, object detection (including weapons or suspicious items), and behavior analysis (like loitering, running, or fighting) empower organizations to proactively address potential security incidents. AI-powered systems can simultaneously analyze footage from multiple cameras, tracking individuals of interest as they move across different areas within a facility. This capability significantly improves the management of large spaces, such as airports, campuses, or retail environments, where security threats can arise unexpectedly.

**Data Encryption:** In the current digital landscape, encrypting all data is essential to safeguard sensitive information from malicious actors. Organizations that fail to properly encrypt data are vulnerable to breaches, lawsuits, and substantial fines. A well-designed cloud solution encrypts data by default, relieving integrators and customers of this responsibility. Consequently, organizations become more cyber-secure, as they can reap the benefits of enhanced security without having to implement it themselves. On-premises solutions, however, face the risk of not being regularly updated due to software limitations and a lack of proper manpower, exposing organizations to potential security and data breaches.

**Faster and Updated:** Cloud-based solutions maintain

a constant connection to the internet, allowing them to receive updates in real-time. This means that organizations automatically benefit from the latest software and hardware capabilities as soon as updates are released. Furthermore, the cloud mitigates on-premises server bottlenecks that can cause slow performance, inconsistent output, and delays in software updates. Most organizations lack dedicated cybersecurity personnel who specialize in addressing cybersecurity threats. Hiring IT resources can be costly, and existing IT staff may be preoccupied with other organizational risks, leaving physical security systems vulnerable. Cloud-based access control solutions enable organizations to reduce the time spent on managing associated cybersecurity risks. Well-designed cloud-based access control systems allow organizations to outsource the security of their systems to the technology provider. This not only frees up internal resources but also enhances cybersecurity best practices through the provider's expertise, enabling teams to more effectively prevent cyber-physical attacks.

**Increased Reliability:** Storing data off-site may seem insecure to many, with concerns about potential data loss in the cloud due to hacking. However, the reliability and security of contemporary cloud resources significantly surpass those of traditional



servers and infrastructure. Cloud providers prioritize data security, employing dedicated teams of experts to manage it and ensure regular updates for essential security patches. They implement a range of protective measures, from encrypting all data to providing employees with multi-factor authentication, to guarantee safety. Additionally, by working with various clients, cloud service providers can learn from their experiences. When vulnerabilities are identified, they adapt their security and operational models to enhance protection for all clients.

**Smart Analytics and Automation Capabilities:** Customers seek to gain valuable business insights for informed decision-making, which is why the demand for AI-based analytics is on the rise. Cloud computing empowers organizations to utilize real-time video analytics and leverage AI to manage large volumes of

data online, extracting meaningful business intelligence. With cloud technology, employees can access their data and applications from anywhere in the world, utilizing communication and collaboration tools for seamless sharing and mobile computing. This capability is particularly crucial during times like the pandemic when many employees are working remotely. AI also plays a vital role in automating routine security tasks, allowing human resources to focus on more strategic initiatives. Automated alerts can notify security teams of potential risks, while predictive modelling analyses historical data to forecast future threats based on behavioural patterns or past incidents. For example, AI algorithms can scrutinize video feeds to identify unusual activities, such as someone tampering with a security camera or trying to access a restricted area. These systems can then trigger automatic alerts or responses, such as locking down a building or dispatching security personnel, before a threat escalates. Additionally, predictive analytics enables businesses to stay ahead of potential risks by identifying patterns that may signal security vulnerabilities. This proactive intelligence helps organizations adopt a more forward-thinking approach to security, preventing incidents before they happen.



**Not so easy Migration:** Transitioning physical security to the cloud is a challenging endeavour, particularly for companies that have invested years in developing their security systems and infrastructure. This complex process requires time and incurs additional costs. Rushed migrations can heighten the risk of insecure data transfers and compliance issues. Nonetheless, companies are increasingly interested in adopting cloud solutions—whether private, public, or hybrid—to take advantage of the benefits offered by the cloud. With a surge in available tools designed to facilitate the move to the public cloud, organizations can expect a smoother transition and ongoing support for their operations.

**Cybersecurity Concerns:** The transition to cloud-based systems introduces a new array of cybersecurity challenges. Many organizations express concerns about

the security of sensitive data stored off-site and the risks of breaches during data transmission. However, the report also highlights a shift in attitudes toward cloud security. Most respondents believe that cloud security has improved significantly over the past five years and will continue to progress, offering enhanced protection against emerging threats. To mitigate these concerns, cloud-based security providers are making substantial investments in encryption technologies, multi-factor authentication, and regular security updates to ensure data is safeguarded at every stage. This evolving cybersecurity landscape is helping to alleviate some of the apprehensions that have historically hindered cloud adoption. While cloud environments can be susceptible to cybersecurity issues, especially if an account is not properly configured, this should not deter stakeholders from moving sensitive information to public servers. No organization is immune to hacker attacks. However, when it comes to cloud architecture providers, cybersecurity is their top priority. Cloud services have dedicated teams working diligently to stay ahead of new threats. They keep up to date with the latest best security practices, install patches, and perform regular updates to prevent breaches. This makes clouds more secure and effective than most on-premise solutions. Nevertheless, users of cloud computing also have a responsibility to ensure they comply with the cloud provider's security guidelines and properly secure their accounts.

**Infrastructure Challenges:** Traditionally, security solutions have been implemented on hardware located on-site, designed to be secure and protect sensitive information. However, these systems come with limited access to data and restricted capabilities. As a result, if companies wish to scale their operations, they must invest in new servers, computer hardware, software, network services, backup systems, and more. Maintaining this infrastructure presents another challenge, requiring ongoing technical support, regular updates for hardware and software, and performance optimization—all of which can lead to significant additional costs. For small businesses or those with limited budgets, these expenses can be prohibitive. Cloud computing alleviates budgetary pressures by removing the need to purchase and maintain hardware. It offers the convenience of scaling resources up or down as needed while reducing the time required for infrastructure maintenance. A cloud service provider handles technical support and ensures that technologies are updated and configured according to users' actual needs.

**Network Reliability and Uptime:** Another common concern is network reliability. Since cloud-based systems rely on internet connectivity for real-time monitoring and management, any disruption can create potential security blind spots. In the widely referenced survey, 27% of respondents highlighted their worries about the reliability of their internet

connections and the possible impact on their security infrastructure. However, many cloud providers are addressing this issue by implementing failover systems and backup protocols to ensure that security systems remain operational even during network outages. These solutions enhance reliability, allowing businesses to maintain security continuity despite connectivity challenges. Cloud computing necessitates a stable internet connection, so bandwidth issues can pose significant obstacles, particularly in remote areas with unreliable connections. Without consistent internet access, it's difficult to depend on cloud technologies, especially for security solutions. On a positive note, internet connectivity is continually improving, and the rollout of 5G is expected to boost cloud adoption. With 5G, internet speeds will significantly increase while latency decreases, enabling cloud services to manage large volumes of data with ease.

### How fast is the adoption happening?

Citing the survey reference, a good 86% of respondents who have not yet fully transitioned to the cloud plan to do so, with 90% of those using entirely on-premise setups and 85% with hybrid systems indicating their intention to migrate. This demonstrates a clear momentum toward cloud adoption. Notably, 70% of respondents anticipate increasing their spending on physical security systems in the 2026-27 timeframe. This aligns with the finding that 75% of security leaders plan to transition to the cloud within the next 12 months, and 96% aim to complete this transition within the following 18 months. This urgency highlights the critical need to modernize physical security infrastructures.

### Importance of Centralisation

In total, 85% of security leaders consider it very or extremely important to integrate multiple physical security products—such as door access control, alarm systems, and video surveillance—into a single centralized system. This underscores the emphasis on system integration and management efficiency. Attitudes toward physical security systems differ significantly based on existing setups. However, organizations universally agree that cloud-managed systems are easier to maintain, can scale very rapidly, and manage across multiple locations. Despite concerns regarding cybersecurity, most believe that cloud systems are safer than ever and express confidence in ongoing improvements over the next five years. While cybersecurity is recognized as the primary barrier, respondents strongly agree that the cloud is more secure now than it was five years ago and will continue to enhance its security in the coming years, reflecting a general optimism about advancements in cloud technology security.

### Key Takeaways

The swift transformation of the physical security industry

towards cloud-based systems means that organizations delaying adoption will encounter increasing risks and rising costs. Cybersecurity threats are becoming more sophisticated, and traditional on-premise systems often lack the necessary flexibility and scalability for effective adaptation. Without the centralized management, automated updates, and predictive analytics offered by cloud solutions, organizations remain vulnerable to breaches, non-compliance, and the higher expenses associated with outdated technology.

Postponing this transition can lead to extended downtime, slower incident response times, and costly recovery efforts. Organizations that hesitate to adopt cloud security risk falling behind as competitors utilize advanced cloud features for a more proactive security stance. As a recent survey suggests, more than 85% of those not fully transitioned are considering cloud systems, highlighting the strategic direction of the industry. Moreover, nearly all respondents planning this transition aim to do so within the next 18 months.

Organizations that are slow to adapt may miss opportunities to enhance operational efficiency, streamline monitoring across multiple sites, and facilitate seamless collaboration. Security leaders must act promptly to leverage the significant advantages that cloud-based systems offer. The survey concludes that about 60% of the companies view this transition as a high priority, with most intending to fully transition within the next 18-24 months. It is generally regarded that the future of physical security lies in cloud solutions, underscoring the urgency for immediate action.

Key drivers of this transition include system scalability, improved integration, and efficient remote management, enabling organizations to meet evolving security needs while maintaining a comprehensive defense strategy. Budget forecasts indicate a strategic focus on investments in cybersecurity, cloud storage, and AI-driven automation. With most companies expecting to increase their physical security budgets in 2025, there is a growing consensus within the industry regarding the urgency of adopting modern security practices.

By shifting to cloud-managed systems, businesses can ensure seamless integration of physical security products, facilitating effective scalability and comprehensive protection. Ultimately, security leaders should view the transition to the cloud not merely as a technological upgrade but as a strategy for future-proofing their operations. With AI integration, advanced analytics, and predictive modelling, organizations can proactively identify and respond to emerging threats with agility and accuracy. Cloud-based systems provide centralized management that reduces manual tasks and optimizes security resources across geographically diverse areas. Immediate adoption is essential for ensuring resilience, maintaining compliance, and achieving a strategic advantage in the rapidly evolving security landscape. ■

# Oskar Strøm's Arctic Expedition Security Solutions by Ajax

**Introduction:** Oskar Strøm, a renowned expedition leader and documentary filmmaker, is known for his groundbreaking expeditions to the Arctic, focusing on capturing polar bears in their natural habitat in Svalbard. His crew lives in extreme conditions, facing threats from polar bear intrusions and environmental hazards like carbon monoxide buildup and fire risks from generators. To ensure their safety and protect valuable equipment, Strøm required a reliable, comprehensive security solution capable of functioning without internet connectivity.

**Challenge:** The expedition's main challenges included:

1. **Wildlife Threats:** Polar bears often wander into camps in search for food, posing risks to crew and equipment.
2. **Remote Environment:** The lack of infrastructure and limited internet meant the system needed to operate autonomously.
3. **Environmental Hazards:** Carbon monoxide buildup and fire risks from generators posed significant dangers in their tightly sealed sleeping pods.

The solution needed to be wireless, easy to install, detect polar bear movements, detect fire and carbon monoxide, and be functional in extreme temperatures as low as  $-45^{\circ}\text{C}$ .

**Solution:** DesignAlarm, a security system integrator, chose Ajax systems for their flexibility, reliability, and ease of installation. The Ajax ecosystem provided a complete range of solutions to address the expedition's unique

security needs.

1. **Wireless Operation:** The Ajax system's wireless nature allowed for flexible placement of devices around the camp without the need for cables or internet connectivity, making it ideal for the remote Arctic location.

2. **Hub 2 Plus Jeweller Control Panel:** This panel acts as the heart of the system, using Ajax's proprietary Jeweller radio protocol for reliable communication between devices without relying on internet access. It also functions on low-voltage power, making it perfect for environments with no traditional power grid.

3. **Perimeter Detection:** Four DualCurtain Outdoor Jeweller detectors were placed around the camp to detect polar bear intrusions. These detectors cover up to 30 meters in total and send alarms to both indoor and outdoor sirens if any movement is detected. To reduce false alarms from snow or small animals, the system uses a sophisticated software algorithm to analyze signals.

4. **MotionCam Outdoor (PhOD) Jeweller Detectors:** These detectors provide a second layer of defense by capturing images when motion is detected, offering visual verification of alarms. The crew can see these images in the Ajax app, allowing them to track the bear's movements in real-time when internet connection is available.

5. **Alarm and Sirens:** Indoor and outdoor sirens (HomeSiren and StreetSiren Jeweller) were installed to alert the crew of security breaches and deter polar bears with high-pitched sounds up to 113 dB.

6. **Fire and CO Detection:** FireProtect

2 Jeweller detectors were installed to provide 24/7 monitoring for fire, heat, and carbon monoxide. These detectors are always active, offering immediate alerts in case of danger, even in the absence of internet or power.

**Results:** The Ajax system exceeded expectations by delivering reliable protection against polar bears and environmental hazards in the harsh Arctic environment. It operated effectively in Arctic temperatures, with only minimal battery drainage, pre-warning users of low battery levels to ensure timely replacements. Even without continuous internet connectivity, the Hub 2 Plus Jeweller maintained seamless communication between all devices, autonomously processing and responding to alarms. The system's ease of installation and mobility were standout features, allowing a single person to install and configure it quickly using the Ajax app, without the need for specialized tools, making it adaptable to the expedition's dynamic needs.

**Conclusion:** Ajax systems provided a versatile and reliable security solution for Oskar Strøm's Arctic expedition, safeguarding both the crew and valuable equipment in one of the world's most inhospitable environments. By combining advanced motion detection, fire and CO monitoring, and wireless functionality, Ajax delivered unparalleled security, enabling the crew to focus on their mission of documenting polar bears in their natural habitat.



# Leading Casino Operator Enhances Operations With Future-Proof Security

**Client:** Merit International, a leading casino operator in the Balkans, with a portfolio of hospitality and gaming resorts valued at over USD \$1 billion, spanning Northern Cyprus, Croatia, Bulgaria, and Montenegro.

**Objective:** As part of the launch of its new luxury Starlit Casino and Hotel Resort in Budva, Montenegro, Merit International aimed to set new standards in security, customer service, and operational efficiency. The goal was to deploy a scalable, future-proof video surveillance solution that would not only safeguard the property but also enhance customer experience and provide actionable business intelligence.

**Solution:** In collaboration with Volga Electronics Ltd., Merit International installed an end-to-end Idis video surveillance solution across the entire Starlit resort. The system consists of more than 90 NDAA-compliant Idis cameras, including 5MP IR domes and compact PTZs, as well as four 64-channel Idis Solution Suite (ISS) servers equipped with dual power for redundancy. The video management system (VMS) also integrates with the casino's ERP software, enabling real-time monitoring and overlaying transaction data on recorded video for streamlined incident investigation.

**Key Features:**

- **Comprehensive HD Coverage:** The solution provides full video coverage of gaming tables, slot machines, and surrounding areas, ensuring real-time monitoring of all activities.

- **Centralized Management:** Through ISS federation services, Merit can monitor and manage multiple casino locations from a central hub, enhancing situational awareness and streamlining operations.

- **AI-Powered Analytics:** Merit has begun testing AI-based features such as people counting and heat maps, which provide insights into customer behavior, footfall, and dwell times. These analytics are designed to improve resource allocation, customer service, and operational efficiency.

**Results:**

- **Future-Proof Security:** The modular Idis system allows Merit to deploy new AI-driven functions with ease. This enables real-time analysis of customer movements and patterns, which can be used

to optimize the placement of gaming tables and staff resources.

- **Business Intelligence:** Heat maps generated by the surveillance system provide actionable insights into customer behavior, allowing management to align staff deployment and promotional efforts with customer spending patterns.

- **Operational Efficiency:** The system's integration with the ERP software simplifies incident investigations by linking video footage with transactional data. This capability supports faster and more accurate responses to security breaches or disputes.

**Client Feedback:** Koray Ozyildirim, Idis Türkiye Country Manager, highlighted the adaptability and future-proof design of the Idis solution, stating that it opens up new possibilities for leveraging AI-powered video analytics to enhance resource allocation and security strategies. Similarly, Malik Oğuz, Surveillance Director at Merit International, praised the system's flexibility, expressing satisfaction with its performance and the ability to seamlessly integrate new AI functionalities as their security and operational needs evolve.

**Conclusion:** The advanced Idis video surveillance system has transformed operations at Merit International's Starlit resort, offering robust security and valuable business intelligence. With its scalable infrastructure and AI-readiness, the solution positions Merit to continue enhancing its operations and customer experience in the years to come.



# Sharry Enhances Physical Security and Workplace Experience at PATRIZIA London Hub



**Client:** PATRIZIA, a global real estate investment manager

**Location:** Endell Street, Covent Garden, London

**Technology Partners:** Sharry, Gallagher Security, Trigr

## Overview:

PATRIZIA, a global leader in real estate investment, embarked on a significant transformation of its London headquarters to create a state-of-the-art, future-focused workspace. The project involved the comprehensive refurbishment of a Victorian building, turning it into a sustainable, smart office that emphasizes both security and employee experience. As part of this transformation, PATRIZIA partnered with Sharry, a global workplace experience platform, to enhance access control and operational efficiency through the integration of digital solutions.

## Challenge:

With 200 employees based in the new London hub and frequent visitors from other global offices, PATRIZIA sought a state-of-the-art security solution that could provide seamless mobile access while enhancing both physical security and the overall employee experience. The company wanted to eliminate the need for traditional plastic access cards, streamline visitor management, and provide real-time insights into building occupancy and environmental controls. As an innovative workspace, the hub needed an integrated platform that would not only offer secure access but also improve operational efficiency and adaptability to modern, flexible work conditions.

## Solution:

Sharry delivered an integrated workplace experience platform built around mobile access. Leveraging Gallagher Mobile Connect credentials, the system



was fully integrated with the Gallagher Command Centre access control system. This integration allowed PATRIZIA employees and visitors to unlock doors with their smartphones, eliminating the need for physical badges and improving both security and convenience.

The workplace experience platform also introduced features like reservations for shared workstations, service requests, and guest passes, all accessible through the PATRIZIA App. In addition, the system enabled real-time data analysis on workplace occupancy and resource usage, powered by Trigr's building operating system (BOS).

### Key features and Benefits:

**1. Touchless Mobile Access:** Employees can generate mobile access badges through the PATRIZIA App, providing seamless, touchless entry to the building. This system enhances both security and convenience, as there is no need for physical cards or manual badge issuance. Employees visiting from other PATRIZIA offices can quickly generate access in seconds without additional requests.

**2. Integrated Access Control and Workplace Management:** Sharry's platform integrates with Gallagher's Mobile Connect credentials and Command Centre, ensuring robust physical security. Office managers can remotely revoke access to any mobile or plastic badge via the PortalWX, while employees can easily report lost cards and suspend access.

**3. Enhanced Workplace Experience:** Beyond security, the PATRIZIA App offers users a variety of workplace management features, including:

- **Reservations:** Employees can reserve workstations or book Health Club access.
- **Service Requests:** Users can request maintenance or services directly through the app.
- **Guest Passes:** Employees can invite visitors and send them digital guest passes with essential building information.

**4. Data-Driven Decision Making:** Real-time data on occupancy and resource usage is collected through Trigr's BOS, which is integrated with Sharry's platform. This data empowers PATRIZIA's facility managers to

make informed decisions about space and amenities, ensuring optimal use of the office environment. The system also allows for real-time control of lighting, temperature, and CO2 levels.

**5. Sustainability and Smart Building Integration:** The hub's design aligns with PATRIZIA's sustainability goals, incorporating energy-efficient building systems and smart technology. Through Trigr, the office's environment can adapt in real time, optimizing energy use and creating a more comfortable workspace for employees.

### Results:

The integrated platform from Sharry, Gallagher, and Trigr has significantly improved both the physical security and workplace experience at PATRIZIA's London hub. Employees now enjoy touchless, mobile access, eliminating the need for physical badges, and managers benefit from powerful access control and data insights. The hub has become a flagship workspace for PATRIZIA, combining flexibility, technology, and sustainability to embody the "office of the future."

### Client Testimonial:

Shreya Sheth, Associate Director of Building Technology & Sustainability at PATRIZIA, commented, "PATRIZIA's employees in London and those visiting from our other offices can enjoy seamless and touchless mobile access to our new international hub. This innovative approach saves time while strengthening security policy."

Ondřej Vodňanský, Head of Sales EMEA at Sharry, expressed enthusiasm for the project: "We are very excited to support PATRIZIA with their smart workplace app and integrated access control solution. Their commitment to creating a future-proof workspace is truly inspiring."

### Conclusion:

PATRIZIA's collaboration with Sharry, Gallagher, and Trigr has resulted in a highly secure, flexible, and efficient workplace. The successful integration of mobile access, smart building systems, and real-time data analytics has positioned the London hub as a model for future offices. This case exemplifies the benefits of combining physical security with enhanced digital workplace experiences, ensuring both safety and productivity in the modern work environment. ■

# WiFi Halo: Revolutionising IoT Applications

As technology continues to evolve, the security industry consistently seeks new ways to enhance surveillance systems. One of the most exciting developments in this field is the emergence of WiFi HaLow, a low-power, long-range version of WiFi, officially known as IEEE 802.11ah. WiFi HaLow (pronounced “Halo”) is making waves across various sectors, but its impact on video surveillance systems is particularly noteworthy. In this article, we’ll delve into the benefits of WiFi HaLow for CCTV applications, its key features, and how it addresses the evolving needs of modern security infrastructures.

WiFi HaLow is an innovative technology designed to provide long-range, low-power connectivity ideal for IoT applications, and which was specifically designed for long-reach, battery-powered IoT applications. It has far greater reach than conventional Wi-Fi due to several factors.

Unlike traditional WiFi, WiFi HaLow operates in the sub-1 GHz frequency band, offering extended range and improved penetration through walls and obstructions. With its ability to connect thousands of devices, and apart from its advantageous usage for connecting CCTV cameras, Wi-Fi HaLow is poised to transform various sectors, from smart cities and agriculture to logistics and healthcare.

New Wi-Fi HaLow devices are designed to meet the growing needs of various industries and applications, including:

- **Smart City Solutions:** Enhancing urban living with smart lighting, parking, and waste management systems.
- **Smart Building Solutions:** Improving automation in buildings with accurate people counting and enhanced coverage.
- **Smart Retail:** Enhancing customer experience and engagement with valuable insights.
- **Agricultural Applications:** Revolutionising farming with remote monitoring and precision agriculture tools.
- **Logistics and Asset Tracking:** Ensuring efficient and secure tracking of assets and inventory.
- **Healthcare Innovations:** Improving patient care with remote monitoring and telemedicine solutions.

## WiFi Halow and Video Surveillance

Security camera systems with 24/7 real-time monitoring are vital for both public and private sectors, yet 75% of surveillance failures are due to network issues like poor connections, especially in the home market where smart

cameras are rising in popularity. With 20% of U.S. homes now equipped with security cameras, and the market growing 18% annually through 2030, these systems enhance safety, reduce break-ins, and may even lower insurance premiums.

While wireless CCTV systems are popular for their ease of installation, traditional WiFi limits range and power efficiency. WiFi HaLow solves these issues, offering extended range, low power consumption, and better performance for IoT-connected devices.

The home security camera market, encompassing wired, wireless, and wire-free cameras, is projected to reach \$25 billion by 2030.

Wired cameras offer clear signals but are costly and difficult to install due to wiring needs.

Wireless cameras use Wi-Fi for data transmission but still require a power source.

Wire-free cameras operate on batteries and offer easy installation, ideal for renters or temporary setups.

WiFi HaLow presents a more efficient solution, addressing connectivity and power challenges in modern surveillance systems.

## Benefits of Wi-Fi Certified HaLow

Wi-Fi HaLow differs significantly from the conventional Wi-Fi we’re familiar with, offering a distinct advantage in range, especially for CCTV systems.

### *Extended Range for Surveillance Coverage*

Wi-Fi standards like Wi-Fi 4, 5, and 6 operate at higher radio frequencies—2.4 GHz, 5 GHz, and 6 GHz, respectively. The higher the frequency, the shorter the distance the signal can travel in open spaces. In contrast, Wi-Fi HaLow operates in the sub-GHz range (902 MHz – 928 MHz in the U.S.), allowing signals to travel much farther due to the lower frequency.

For security cameras, this means Wi-Fi HaLow cameras can transmit video over significantly greater distances than Wi-Fi 4, 5, or 6 cameras, which typically lose connection after a few hundred metres. Wi-Fi HaLow’s range, which extends up to 1 kilometre, makes it ideal for covering large properties or outdoor spaces without the need for additional signal boosters or network infrastructure. This is particularly beneficial for large commercial properties like warehouses, factories, and malls, residential complexes that require perimeter security, and agricultural or rural

settings where securing vast expanses is crucial.

This extended range simplifies the deployment of outdoor surveillance cameras and ensures that even remote areas of a property are adequately covered.

### ***Improved Signal Penetration for Indoor and Outdoor Security***

Sub-GHz signals have a much better ability to penetrate objects like walls, windows, and doors compared to conventional Wi-Fi. As a result, Wi-Fi HaLow signals are much less impacted by building structures and can easily reach outdoor areas.

Wi-Fi HaLow's capacity to pass through obstacles such as walls, trees, and other barriers allows it to maintain a strong, consistent signal even in difficult environments. Traditional Wi-Fi cameras often experience degraded signal quality or connection loss due to thick walls or multiple floors within a building, which can disrupt video transmission. Wi-Fi HaLow resolves this issue by providing a stable connection, enabling continuous surveillance, even in multi-story buildings or densely constructed areas. This advantage allows security teams to monitor feeds without concerns about network interruptions or the need for extra hardware like extenders or repeaters.

### ***Lower Power Consumption for Remote Cameras***

Another challenge with traditional WiFi cameras is the power consumption. Cameras running on traditional WiFi tend to consume more power, which can be problematic in remote locations or where battery-powered systems are preferred.

WiFi HaLow's low-power capability makes it ideal for battery-operated CCTV systems, allowing cameras to run for extended periods without requiring frequent maintenance or battery replacements. This feature is particularly useful for cameras installed in hard-to-reach areas, such as high walls, rooftops, or secluded outdoor spaces.

### ***Cost-Effective and Scalable Surveillance Solutions***

Security installations in large complexes often require a significant number of cameras to ensure full coverage. The scalability of WiFi HaLow allows a single access point to connect thousands of devices, making it an ideal solution for large-scale deployments. This translates into lower installation and operational costs since fewer network devices are needed to cover vast areas.

Moreover, the extended range and reliability of the HaLow signal mean that fewer access points are required to cover the same area compared to traditional WiFi. This results in lower infrastructure costs and reduced maintenance, making WiFi HaLow a more cost-effective option for expansive security installations.

### ***Less Congested Frequency Range***

The RF frequencies that conventional Wi-Fi operates at are typically very congested with high levels of interference. 2.4GHz is used by Wi-Fi, Bluetooth and microwave ovens resulting in high levels of interference for any cameras trying to use a 2.4GHz Wi-Fi link. The 5 and 6GHz Wi-Fi technologies suffer less congestion, but the range of 5 and 6GHz is less than that of 2.4GHz (due to their higher operating frequencies). The sub-GHz range of WiFi Halow is relatively less congested.

### ***Narrowband OFDM Channels***

Wi-Fi HaLow utilises narrower channel bandwidths than conventional Wi-Fi. The narrower the channel bandwidth the further RF signals can travel. Wi-Fi HaLow can use 1MHz channels whereas the lowest channel bandwidth that conventional Wi-Fi can use is 20MHz. Orthogonal Frequency-Division Multiplexing (OFDM) is a data transmission technique that's commonly used in wireless communication to increase efficiency and capacity. It splits a single information stream into multiple narrowband subchannels, or subcarriers, instead of using a single wideband channel. This allows multiple bits to be sent at the same time, or in parallel, instead of sequentially.

### ***Enhanced Security Protocols***

Given that WiFi HaLow is based on the IEEE 802.11 standard, it benefits from the latest advancements in WiFi security protocols, including WPA3 encryption. This ensures that the data being transmitted between cameras and central monitoring systems is secure and protected from unauthorised access or hacking attempts.

In addition, the ability to integrate with existing IP-based security systems allows security teams to deploy WiFi HaLow-enabled cameras alongside traditional cameras, creating a hybrid system that maximises coverage and flexibility without compromising on security.

As security systems shift toward smart, interconnected IoT networks, WiFi HaLow is set to transform wireless CCTV systems with its long range, low power use, strong signal penetration, and scalability. These features make it ideal for surveillance, whether in small residential areas or large commercial and industrial properties. WiFi HaLow will be crucial in providing efficient, reliable, and cost-effective solutions. Whether upgrading an existing CCTV setup or installing a new one, WiFi HaLow offers a forward-looking solution to modern security challenges.

With this technology, the future of CCTV is smarter, more connected, and more efficient than ever. ■

# Cybersecurity Should Be A Part Of A Business Strategy For You



Business strategy must include cybersecurity as part of an organization's business plan today. Cyber attacks and threats are becoming more sophisticated, so firms must prioritize cybersecurity measures to preserve their digital assets and maintain business continuity. A security breach may cost irreparable harm to an organization's finances and obstruct a company's ability to recover its public reputation, making a robust cybersecurity strategy essential.

To maintain a competitive edge, businesses must safeguard consumer data and other sensitive information from unauthorized individuals. Some ways to ensure cybersecurity's integration into corporate processes include multi-factor authentication, which allows a business to protect vital assets like customer data and impose access restrictions to safeguard sensitive information. Also, regular penetration testing manages security risks, and an incident response plan ensures company continuity.

Businesses must prioritize their cybersecurity posture in their plans and business strategies. To do so,

a business must safeguard its networks, ensuring that only authorized personnel have access and preventing unauthorized users from seeing proprietary information.

Good cybersecurity also involves:

Scanning for malware

Installing antivirus software to protect critical data

Establishing risk management techniques to address vulnerabilities

Preparing for data breaches if they occur

A good plan should also examine the risks provided by third-party vendors and ensure that vendors meet information security regulations. Attention to these vulnerabilities can help to prevent hackers from accessing confidential information as the result of a single data breach.

To achieve the best possible security, many businesses get assistance from cybersecurity

experts armed with modern technology and tools. These security professionals will ensure a company can maintain operations while providing services. They work to secure an organization's systems, detect potential breaches, harden systems against known threats, and mitigate other cyber risks.

A complete and proactive cybersecurity plan as part of a company's business strategy preserves the trust of customers and the company's reputation. By securing its operations and digital assets, this strategy shields the organization from risks.

To effectively integrate security measures, guard against cyber threats, and secure daily operations, organizations must prioritize data security. Also, they must identify risks and vulnerabilities to systems and networks and utilize access controls. When companies conduct regular audits and assessments and focus on identifying potential threats and risks, the company is more likely to reduce incidents and avoid financial losses.

Cyber security must be a company-wide priority, not simply an IT department mandate. Everyone should be trained to identify and report incidents like phishing scams, unauthorized access attempts, and unexpected network activity. Employees who are proactive and aware of risks may avert a data breach, retain customer trust, and safeguard customer information.

Data compromises may cost organizations money, reputation, and new customers. Advanced security technologies like encryption and malware prevention are highly effective in protecting sensitive data.

By integrating cybersecurity measures and a plan that goes beyond mere IT strategy, companies stand to protect themselves from the ever-changing cyber risk environment. Solid security measures involve a thorough examination of a business's cybersecurity procedures and educating staff about the dangers and responsibilities of safeguarding systems. This proactive cybersecurity strategy helps protect the company's sensitive information and systems and strengthens its commitment to customers, workers, and stakeholders.

Business managers who have delegated cybersecurity concerns to an understaffed IT department have learned this approach is beyond short-sighted and actively dangerous. They have also experienced the folly of ignoring critical risks.

The lack of foresight in planning, updating, training, and monitoring has led to costly data breaches that compromised critical assets, jeopardized customers, and caused reputational damage. Morgan Stanley®, Yahoo!®, Microsoft®, Equifax®, and MGM Resorts® are notable examples of disastrous

cybersecurity breaches.

Risk aversion is critical to business strategy, and a data breach could be caused for a number of reasons. Cyber attack methods include:

**Phishing:** Fake emails trick users into disclosing usernames, passwords, and financial details. According to StationX, phishing is the most common form of cybercrime and is on the rise.

**Malware:** Malicious software, such as viruses, ransomware, and spyware, can be slipped into a network from websites, emails, and downloaded email attachments. Ransomware involves malicious malware that locks up a system until money is paid by the victim. Countering ransomware is a priority of the U.S. government's Cybersecurity and Infrastructure Security Agency (CISA).

**Insider attacks:** Untrained employees and others who can access sensitive information might intentionally or unintentionally cause security breaches by disclosing information. Based on data collected in 2022, DTEX reports a "35% increase in data theft incidents caused by employees leaving companies."

Some security vulnerabilities within organizations include:

**Vulnerable passwords:** Short, easy-to-guess passwords and passwords that are not changed regularly are easy prey for cyber villains. According to Cybernews, weak passwords have been the root cause of significant breaches, such as the breach experienced by the North Ireland Parliament in 2018.

**Unpatched software:** Failing to update software, especially security provisions, enables instructors to gain access to networks. This failure to update software was a significant oversight in the Equifax

case and interfered with its business continuity.

**Insecure network configurations:** Misconfigured firewalls and unsecured Wi-Fi networks are open invitations to system attacks.

Countering these problems requires a multi-layered approach that begins with management's comprehensive understanding of the importance of being well-informed about cyber threats and dedicating resources to cybersecurity. Although the strategic priorities of a business will depend on its industry and existing vulnerabilities, here are some essential measures.

Leadership's commitment to cybersecurity is essential to the entire organization; otherwise, allocating resources and prioritizing security efforts is challenging. It will also be difficult to convince employees that protection measures are serious if there is no buy-in from their leaders.

Top leadership must be involved with oversight through a dedicated governance structure for a firm's security efforts, including:

Reporting risks and staying aware of regulatory requirements

Keeping current with the latest cyber threats

Issuing timely responses if breaches should occur

Committing resources toward data protection

Practical risk assessment and risk management optimizes the use of resources and ensures that cybersecurity measures align with overall business goals. Ideally, a business should conduct a thorough, ongoing risk assessment to identify critical cyber assets, threats, and vulnerabilities. These cybersecurity initiatives can be aligned with broader business objectives. ■

*Credits: Dr. Linda Ashar, Faculty Member, Business and Dr. Andre Slonopas, Faculty Member, Cybersecurity, American Public Security*

# Hanwha Head Of Product And Marketing On The Future of AI

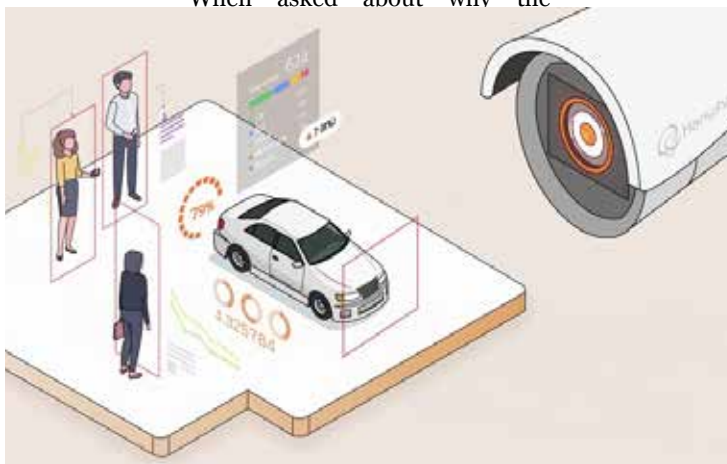
With more than 30 years of experience working across business development, sales, product and marketing for leading distribution and manufacturing companies, John Lutz Boorman, the recently appointed Head of Product and Marketing at Hanwha Vision Europe, has vast knowledge and expertise in the security industry. Here he talks about his view on innovations in video surveillance over the next few years.

The video surveillance market has rapidly evolved over the past few decades. Video cameras are no longer deployed solely to record images for security, but have become essential tools for organisations to refine operations, increase productivity, provide business intelligence and enhance safety. AI offers accurate detection of faces, people and vehicles (as well as their attributes) to reduce false alarms and deliver deeper operational insights.

In the opinion of John Lutz Boorman, over the next five years, AI will be increasingly deployed not only for “after the event” - but also to allow forensic search and analysis of hours of video in mere seconds. “Using AI, video systems trained on real-world scenarios defined by users will be able to predict behaviour and alert operators to the potential for incidents even before they happen. Predictive AI-

enabled video technology will, therefore, be called on to support business forecasting efforts, deploy corporate resources more effectively, and help users make better-informed decisions.”

When asked about why the



industry is so interested in AI ‘at the edge’, Lutz Boorman puts forward a compelling argument. “Putting AI to work used to involve vast amounts of computing power and infrastructure, which required a significant investment in energy and IT resources.

By including AI in the camera itself - or “at the edge” - significant efficiencies are now possible. Analysis of images using AI at the edge removes the need to stream raw data back to a server for analysis, freeing up bandwidth and reducing processing demands on centralised systems, as well as lowering data costs.”

He continues, “Cameras using AI at the edge can make a video installation more flexible and easy

to scale. This is particularly helpful for organisations that wish to scale a project in phases, as cameras can be added as and when required without the need to invest in additional server capacity. Furthermore, edge devices can be utilised for more bespoke end-user applications to meet the needs of varying customer requirements.”

Lutz Boorman further adds, “There are cyber security benefits, too, with AI at the edge. As video analytics occurs on the device, only metadata is sent across the network - no sensitive data is transmitted for hackers

to intercept. Additionally, running AI on a device can vastly improve the accuracy of event triggers and reduce false alarms. People counting, occupancy monitoring, queue management, and more can all be carried out with a high degree of accuracy thanks to edge AI utilising deep-learning technology.”

“Because AI offers such significant benefits, Hanwha Vision has led the adoption of AI at the edge for a number of years, having developed chipsets with improved processing power to allow data to be recorded and stored via SD card slots on its cameras. Edge-based AI also helps to ensure the widest possible adoption of this transformative technology, and for that reason, it should also be welcomed,” he concludes.

# Frost Predicts Rapid Growth In Corporate Cloud Protection Market

As businesses increasingly migrate to the cloud and adopt cloud-native technologies, the complexity and attack surface of their digital environments have expanded dramatically. Recognising the critical need to secure these environments, organisations are turning to Cloud Security Posture Management or CSPM solutions to address emerging challenges.

CSPM tools are rising in demand and are becoming increasingly crucial for organisations to maintain robust security postures as they need to deal with the complexities of multi-cloud and cloud-native technology management and meet stringent regulatory requirements, which is set to remain the driving force behind CSPM adoption.

According to research from Frost & Sullivan, the global CSPM market is projected to grow over three-fold by 2028, with revenues expected to reach \$5.58 billion.

North America is set to maintain its leadership in the field, growing from its 2023 revenue base of \$1.04 billion at a projected CAGR of 29.0% over the forecast period. Key drivers behind this buoyancy include the widespread and advanced adoption of public cloud and cloud-native technologies, necessitating more sophisticated and comprehensive security solutions.

With the increasing demand for unified security that provides granular visibility and robust protection across diverse cloud-native application environments, organisations are moving away from stand-alone cloud security tools. Previously relied-upon tools, such as CSPM, Cloud Workload Protection Platforms (CWPPs), vulnerability management, Infrastructure as Code (IaC), and container security, often result in manual risk correlation and operational complexities due to their

lack of unified coverage and context.

In response, businesses are increasingly adopting fully integrated Cloud-Native Application Protection Platforms (CNAPPs). These comprehensive platforms deliver end-to-end visibility, risk management, and security capabilities across all layers of modern cloud deployments, encompassing cloud infrastructure, workloads, applications, and data.

Frost & Sullivan's recent Voice of Enterprise Security Customer report highlights a significant increase in cloud security investments among global organisations. The report reveals that 31% of respondents are using cloud security to prevent breaches, while 30% are

leveraging these solutions to detect and respond to cloud threats. Additionally, 24% are investing in cloud security to prepare for unknown threats, and 12% are using cloud security technologies for regulatory compliance.

Anh Tien Vu, Growth Expert at Frost & Sullivan, explains: "This upward investment trend

underscores the growing awareness and prioritisation of cloud security among businesses worldwide. By 2025, it is estimated that 89% of organisations will employ Cloud Workload Protection Platforms (CWPPs), 91% will use Cloud Security Posture Management (CSPM), and 88% will implement Cloud Infrastructure Entitlement Management (CIEM)."

He adds that approximately 88% of organisations are expected to explore comprehensive cloud security platforms, including Cloud-Native Application Protection Platforms (CNAPPs). ■



# The Rising Importance Of Fire Safety And Protection Risks



In the realm of safety concerns, few carry the weight and urgency of fire prevention and protection. Fire, a force of nature both mesmerising and destructive, demands our constant vigilance and preparedness. As our environments evolve and our technologies advance, so too do the risks associated with fire.

Fire safety isn't merely a matter of compliance or regulatory adherence; it's a fundamental aspect of safeguarding lives, property, and communities. With urbanisation on the rise and buildings growing taller and more complex, the challenges of fire prevention and protection multiply, primarily due to increased building occupancy, vertical fire spread, firefighting accessibility limitations and water pressure / delivery of the suppression systems. The consequences of failure are severe, often resulting in devastating loss of life, economic hardship and environmental damage.

The landscape of fire protection risks is continually shifting, driven by factors such as urbanisation, climate change and technological advancements. Urban sprawl brings with it higher population densities and greater concentrations of infrastructure, amplifying the potential impact of fires. Climate change also exacerbates these risks, contributing to more frequent and intense wildfires as well as altering the dynamics of building materials and ignition sources.

As a result, building materials have significantly improved over the years to lower buildings' fuel load and reduce their vulnerability to fire. Fire-resistive materials, low combustibility and lower smoke development

features of building materials have also greatly reduced the challenges associated with fire in the buildings.

As society becomes increasingly reliant on technology, new fire hazards emerge. From lithium-ion batteries to electrical systems, modern innovations introduce novel risks that require specialised mitigation strategies, such as fires involving lithium-ion batteries, building integrated solar panels, electric vehicles and parking garages.

The proliferation of smart devices and interconnected systems also raises concerns about cybersecurity vulnerabilities, which could be exploited to compromise fire safety measures.

In the face of these evolving risks, the importance of proactive fire prevention and preparedness cannot be overstated.

Prevention begins with robust building design and construction practices, including the use of fire-resistant materials, adequate compartmentalization, and efficient egress systems. Furthermore, education and awareness campaigns play a crucial role in promoting fire safety practices among the public.

Preparedness, meanwhile, encompasses a range of measures aimed at minimising the impact of fires when they occur. This includes the installation of fire detection and suppression systems as well as the development of emergency response plans and evacuation procedures. Regular training exercises and drills are essential for ensuring that individuals know how to respond effectively in the event of a fire.

Advancements in technology offer promising avenues for enhancing fire safety and protection efforts. From advanced fire detection sensors to sophisticated modelling and simulation tools, innovative solutions are empowering stakeholders to better understand, predict and mitigate fire risks.

Fire and smoke modelling software provide quantification of the fire hazard, predictability of fire spread and escalation, and smoke movement inside the



buildings. Artificial intelligence and machine learning algorithms can analyse vast amounts of data to identify patterns and anomalies indicative of potential fire hazards. This is done by data collection and processing, model development and validation, which are in turn deployed to real world environments to continuously monitor fire hazards.

Similarly, the Internet of Things (IoT) enables the creation of interconnected systems that provide real-time monitoring and control of fire protection systems. Smart building technologies offer unprecedented levels of automation and responsiveness, allowing for swift detection and suppression of fires before they escalate.

However, as with any technology, ensuring cybersecurity and data privacy is paramount to prevent malicious exploitation.

The rising importance of fire safety and protection risks underscores the need for proactive and multifaceted approaches to address this critical challenge. As our environments and technologies continue to evolve, so too must our strategies for preventing, detecting and responding to fires. By leveraging innovation, fostering collaboration and prioritising safety, we can build more resilient communities and mitigate the devastating impacts of fire.

---

## Bull Products introduces new LFX Lithium-Ion Fire Extinguishers

Bull Products, the globally renowned provider of temporary fire protection solutions for a wide range of applications, has introduced its new Lithium-ion fire extinguishers, LFX, to its portfolio of life-saving fire solutions.

Designed to address the growing risks associated with lithium-ion battery fires, these water-based extinguishers offer protection against lithium-ion battery fires that is both highly effective and widely applicable across various sectors, from construction sites to offices and retail applications.

Lithium-ion batteries are now an integral part of everyday life, powering everything from smartphones and laptops to electric vehicles and industrial machinery. However, the rise in their usage has brought about a heightened risk of fire-related incidents. Bull Products' new LFX fire extinguishers are specifically engineered to help minimise these potential hazards.

The extinguishers utilise a water-based fire extinguishing agent with market-renowned heat-absorbing properties. This agent effectively breaks the chain reaction of thermal runaway, cooling cells that have already ignited and preventing adjacent cells from overheating. It not only extinguishes flames from failed batteries, but it also prevents the spread of fire to other cells, thereby containing the situation effectively.

“The safety of lithium-ion batteries is a growing concern, especially with their increasing use in everyday life,”

said Carl Leeson, Head of Sales at Bull Products, adding “Our new LFX fire extinguishers are designed to provide a robust and reliable solution that mitigates the risks associated with these power sources, ensuring that users, as well as property, are protected from potential fires.”

In addition to lithium-ion battery fires, the LFX extinguishers are also equipped to handle secondary A-class fires. This allows for the swift extinguishing of peripheral fires that may result from battery explosions, providing comprehensive protection in emergency situations.

Bull Products' LFX fire extinguishers come in 3, 6, and 9-litre options, making them suitable for a wide range of applications, from household use to industrial environments. They can be purchased individually, or as part of a First Responder Station, with or without protective wear, including a full-face respirator mask and heavy-duty Tegera gloves, offering flexibility to meet various safety needs.

As with all Bull Products' First Responder Stations, a fire alarm can also be added as an optional extra for enhanced security. The 6 and 9-litre extinguishers have successfully passed the NTA 8133 standard, the first publication for lithium-ion battery fires with medium capacities up to 600 Wh. This certification highlights the reliability and effectiveness of Bull Products' extinguishers.

# Minimising fire risks in recycling plants through video analytics and real-time verification systems



Sadly, we have seen too many times the devastation caused by fires in recycling and waste management plants across the country. Whether started by accident or through a deliberate act, the consequences are far reaching. The key to minimising the impact of these incidents is prompt fire detection, because once the fire becomes established, it may be too late, and the incident quickly gathers momentum.

Waste recycling facilities have become pivotal in environmental sustainability, processing, and repurposing of the materials that are generated and consigned to the rubbish bin.

It is well understood that these environments are susceptible to significant fire risks because of the highly combustible nature of the materials they handle day

in, day out, with the presence of machinery, electrical equipment, and other potential ignition sources adding to the risk.

This has been magnified in recent years by the increasing use of lithium batteries in so many consumer goods. Fires in waste management and recycling facilities can lead to substantial financial losses, cause environmental damage, and ultimately endanger lives.

Protecting against these risks is vital, and as a result, NetVu has developed FireVu, a video detection and visual verification solution designed to provide early warning and rapid response to fire incidents.

The system uses advanced video analytics to detect smoke, flames, and heat at inception.

Using FireVu's real-time verification, staff and emergency services can quickly assess an incident, make informed decisions, take appropriate action, and trigger suppression systems. Rapid identification and prompt action can drastically reduce the cost of damage and prevent small fires from escalating into a major incident.

It doesn't take long for a blaze to get out of control, and can take days to be extinguished, also putting substantial pressure on the resources of the emergency services. For example, an incident in 2013 at a facility in Bredbury in the north west of England, was reported to involve the combustion of large bales of recyclable materials. The fire took hold very quickly, and the emergency services were tackling the blaze for several days after it started.

The impact was far reaching, also causing major disruption to the local area including residents, and the ash and smoke from the fire was suspected to reach as far as Leeds, a city more than 50 miles away from the site. It is the seconds saved at the stage of verification that has the most impact, exponentially minimising the scale of an incident and the potential losses.

This is achieved through using a combination of Video Flame Detection (VFD) and Video Smoke Detection (VSD) technology, offering real-time alerts and delivering visual feedback to users. The system identifies the source of a fire on screen, allowing operators to verify the incident rapidly and take any necessary action.

The ability to remotely access and review incidents from any location is another feature of the functionality of FireVu, allowing operators to monitor and manage fire risks even when there are no personnel on-site.

Immediate reporting and user feedback are crucial for several reasons:

1. By pinpointing the exact location of a fire, FireVu's system enables operators to verify the incident quickly.
2. This rapid verification process is essential for distinguishing between real fires and false alarms, ensuring that resources are deployed efficiently.
3. With real-time alerts and visual feedback, operators can initiate a prompt response to the detected fire.
4. This timely action can prevent the fire from spreading and causing extensive damage, reducing the overall impact of the incident.
5. Immediate reporting enhances the safety of people

working in recycling facilities.

6. By providing real-time information about the location and severity of the fire, FireVu enables staff to take appropriate safety measures and evacuate if necessary.

One of the biggest challenges in fire detection is distinguishing a real incident from a false positive. False alarms can be costly and disruptive, leading to unnecessary shutdowns.

FireVu addresses this challenge with its unique flame, heat, and smoke detection system, which includes:

The measurement of Black Body Emitter signatures which arise from burning hydrocarbons – i.e. soot glowing creating the yellow and red flame characteristics.

Correlating these colours with absolute intensity, and applying physical laws, allows the system to make fast, reliable alerts.

Thermal sensors further reduce false alarms by verifying the heat source, and in addition detecting heat build-up before flames are visible, including identifying fires that are growing beneath the surface.

This early detection capability is particularly valuable in recycling facilities, where fires can smoulder for extended periods before any flames are visible.

These sensors also help to distinguish false positives such as sunlight bouncing off a puddle, or a wet plastic bag blowing in the wind.

We have also introduced powerful thermal profile algorithms to measure small changes or differences in specific circumstances.

Finally, FireVu also uses a visual smoke detection algorithm, providing advanced early warning, even if a fire has started outside of the field of view and the smoke may be spreading to other areas.

Waste management and recycling facilities must prioritise fire safety to protect their operations, personnel, their local communities, and the environment. Implementing advanced fire detection systems is essential for achieving this goal.

By addressing the unique risks and challenges associated with fire detection in these types of environments, FireVu's technology ensures that these facilities can continue to operate safely and efficiently, contributing to a more sustainable future. ■

## Hanwha launches explosion proof AI camera



The TNO-C8083E is the first explosion-proof camera with artificial intelligence from Hanwha Vision. The compact 5MP explosion-proof AI model features AI object detection and classification alongside intelligent video analytics. It has a wide range of explosion-proof certifications, including IECEx, ATEX, KCs and JPEX, making the camera ideal for environments at a higher risk of an explosive atmosphere due to gas or dust - such as oil refineries, gas storage, and grain mills.

Accurate AI object detection and classification of people and vehicles vastly improves operator situational awareness. AI algorithms can discern people as distinct objects separate from irrelevant motion, for example shadows or animals, thus reducing false alarms and improving operator efficiency. Meanwhile object-type metadata created by the camera enables rapid and efficient forensic search for investigations when

necessary.

Intelligent video analytics, such as loitering and line-crossing detection, alert operators to abnormal activities in real-time to keep areas safe and secure.

The TNO-C8083E is compact and at just 4.78kg, according to Hanwha, it is 57% smaller and 32% lighter than its closest comparative model. This makes it easier to install in more challenging environments than other more bulky explosion-proof cameras on the market. In addition, a 1/2" explosion proof cable gland means the camera can be installed without any sealing compound.

The TNO-C8083E supports enhanced video quality through wide dynamic range (WDR) technology, Wise NRII and low-light noise suppression. WDR enables operators to monitor objects easily in backlit scenes, while Wise NRII leverages AI object detection to reduce motion blur and improve image noise. In low light environments, AI works to refine image clarity by suppressing noise.

The camera also comes with WisestreamIII, a cutting-edge video compression technology that reduces bandwidth by up to 80% without compromising video quality.

Cyber security measures in the TNO-C8083E are referred to by Hanwha Vision as being "next-level" with user and network authentication, and unauthorised access blocking. It validates the boot process, has signed firmware and firmware encryption, and authentication information encryption, to securely store information.

---

## VOSKER unveils new VKX surveillance camera with solar power

VOSKER has unveiled its latest surveillance camera, the VKX, featuring improved image quality, a 2X larger solar panel, and a new front-access design for easy battery swaps. Operating autonomously for up to six months without external power, the VKX requires only LTE connectivity—no wires or wifi. Designed for remote, off-grid security, this compact camera



allows quick installation and upgrades without compromising security.

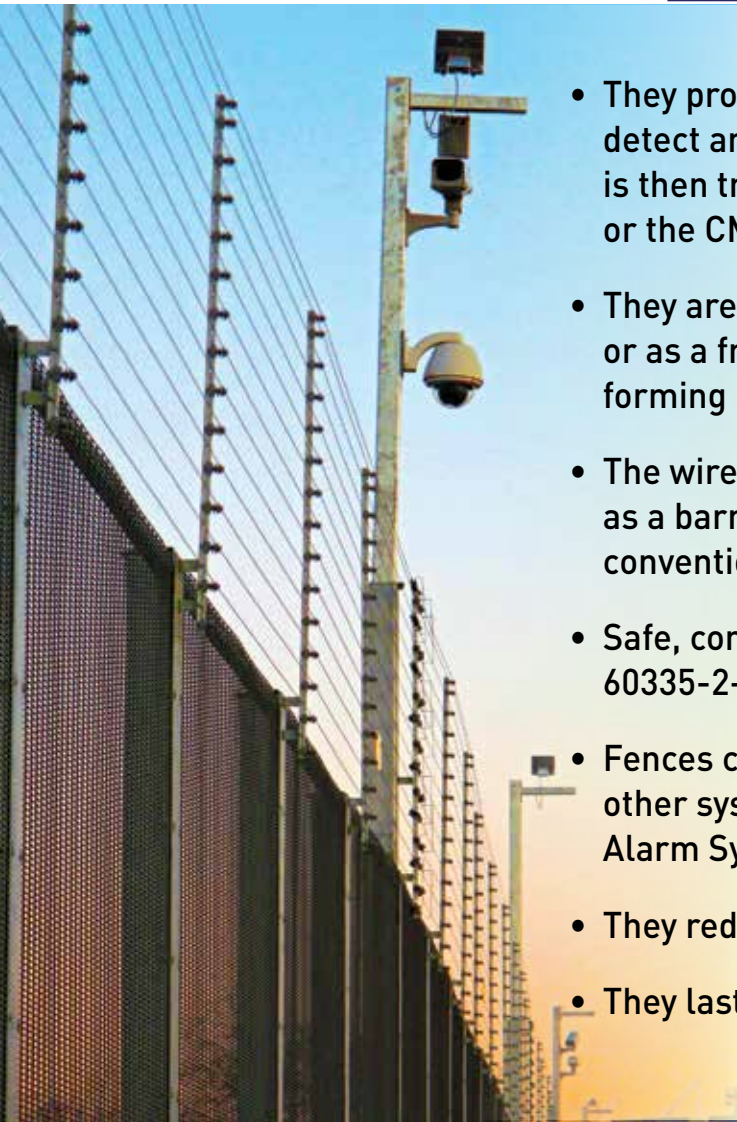
The launch follows a \$125M funding round to accelerate VOSKER's growth and innovation. The VKX is also supported by an enhanced VOSKER app with better search, filters, and notifications, pushing the limits of modern surveillance technology.

# YOUR SECURITY BEGINS WITH YOUR PERIMETER



DETER, DETECT & DELAY INTRUDERS.  
BEING FOREWARNED IS BEING FOREARMED!

ECONOMICAL. RELIABLE. EFFECTIVE.



- They provide a higher level of detection capability to detect an intrusion attempt and set off the alarm which is then transmitted to the security personnel, police or the CMS.
- They are installed easily on existing walls or fences, or as a free standing secure energy perimeter fence, forming your first line of defence.
- The wires of a free standing secure energy fence serve as a barrier, alleviating the need to erect another conventional fence or wall, reducing cost.
- Safe, complies with International IEC Standard 60335-2-76
- Fences can be remote controlled and integrated with other systems such as, Perimeter Lighting, CCTV, and Alarm Systems.
- They reduce cost of security personnel.
- They last for years and have low maintenance cost.

APPLICATIONS:  
BUNGALOWS, FARM HOUSES, CAMPUSES, PRISONS,  
GOVERNMENT & MILITARY SITES, CRITICAL INFRASTRUCTURE FACILITIES...



Email us today  
for more information:  
[info@kawach.com](mailto:info@kawach.com)

## Defend Outdoor Camera from Tactacam



Defend is Tactacam's new cellular camera designed to provide security and monitoring without the need for Wi-Fi to provide a more advanced surveillance solution for owners of large properties, homesteads, off-grid cabins, agricultural lands, construction sites and more.

Engineered to meet the unique needs of property and equipment owners, Defend offers a list of features that ensure comprehensive surveillance and peace of mind.

Key product features include:

- **Advanced Cellular Connectivity:** No need for Wi-Fi! Stay connected with real-time updates and phone alerts through a reliable cellular network.

- **High-Resolution Imaging:** Capture detailed property visuals and any potential threats.

- **Rugged and Durable Design:** Waterproof and resilient, Defend is built to withstand the harshest outdoor conditions.

- **Enhanced Night Vision:** State-of-the-art night vision capabilities provide imagery even in complete darkness for 24-hour all-season monitoring.

- **Long Battery Life:** An extended battery life reduces the need for frequent visits to change batteries, benefiting those with properties that are not close in proximity. For the greatest reliability and fewest trips, consider the optional Defend Cam Solar Panel.

- **Easy Installation and Setup:** User-friendly setup process, no matter the conditions.

“We recognize the unique challenges our customers face in securing assets in remote areas or places without Wi-Fi access,” said Kelly Hover, Chief Experience and Marketing Officer. “With Defend, they can have peace of mind knowing that their property is protected with the most advanced cellular camera technology available.”

---

## Alvarado Argus V60 Optical Turnstile from dormakaba

The new compact Argus V60 optical turnstile offers security, elegance and efficiency all in one, and in the smallest of spaces. Thanks to modern sensor technology, this compact optical turnstile gives architects and users more freedom without compromising on personal protection and separation detection.

With a housing footprint of 9.5” x 7”, the Argus V60 proves to be the smallest optical turnstile on the market, especially in areas such as foyers or inside office buildings. The new Argus V60 optical turnstile provides reliable people flow control and integrates elegantly into any building.

With its compact dimensions and a wide range of finish options, the optical turnstile adapts to modern interior design. The Argus V60 optical turnstile also offers a choice between uni- and bidirectional separation. It enables the passages to be monitored using the new dormakaba sensor technology in both the entry and exit

directions.

For an additional increase in the security level, the door leaves can be raised to a top edge of 47.25” and are thus visually compatible with the top edge of the Argus V60's side cabinets. The integration of the respective card readers for electronic access control can be surface-mounted or as a concealed installation under glass cover with illuminated RFID icon. Options such as illuminated door leaves, additional integration of a bar code reader or system status indicator lights round off the Argus V60.

The Argus V60 optical turnstile is user-friendly, convenient and safe for those with restricted mobility. As with all Alvarado optical turnstiles, 36” ADA compliant passage widths are available. The Argus V60 can also be easily integrated into a building's fire and life safety systems to automatically open all turnstile lanes in the event of an emergency—allowing for easy evacuation.

## Teledyne Flir launches new Forge SWIR camera

Teledyne Flir IIS, a Teledyne Technologies company, has introduced the Forge 1GigE SWIR (Short Wave Infrared) 1.3 MP camera. The first camera in the Forge 1GigE SWIR series is equipped with a wide-band and high-sensitivity Sony Sen SWIR 1.3 MP IMX990 InGaAs sensor. The advanced sensor captures images across both visible light and SWIR light spectrums (VisSWIR) with 5µm pixels, providing an extended spectral range from 400nm to 1700nm.



This capability enhances anomaly detection and material analysis, making it ideal for applications such as industrial semiconductor inspection, food and beverage quality control, recycling, security surveillance, environmental monitoring, precision farming, and more.

“We’re excited to introduce the Forge SWIR camera series to grow our imaging portfolio from the visible spectrum to SWIR wavelengths,” said Sadiq Panjwani, General Manager at Teledyne IIS. “The series expands on Teledyne’s SWIR line scan expertise to boost a range of 2D area scan applications such as industrial inspection, environmental monitoring, and recycling.”

The new camera features a design measuring 40mm x 40mm x 43mm that balances a compact size with superior image quality. Forge 1GigE SWIR includes advanced camera features such as Pixel Correction, Sequencer with ROI (Region of Interest), Logic Block, and Counter which provide reliable and precise control for a variety of complex applications.

## IPVideo HALO Amplify Connected Sensor Suite

HALO Amplify – The Connected Sensor Suite – extends security, health, and situational awareness for the HALO 3C family of products, offering more sensors for safer schools, businesses, hospitals, retail stores, hotels, and more. Designed to help protect people and property, current options include panic button, people counting, open door/window, temperature/humidity, and water leak sensors.

Up to 30 Bluetooth-enabled sensors can wirelessly connect to your HALO Smart Sensor 3C or 3C-PC on a network. Sensor and event data is accessible in real-time via the HALO Cloud dashboard, HALO

Cloud App, HALO device web interface, and third-party integrations.

Users can have peace of mind knowing HALO Amplify provides the same level of privacy protection that all HALO products do. Ideal for use in isolated areas like restrooms, executive board rooms, hotel rooms, healthcare facilities, and more, the device operates without the use of video or audio recording and never captures any personally identifiable information (PII).



## Renesas RRH62000 All-In-One Sensor Module

Renesas Electronics Corporation, a supplier of advanced semiconductor solutions, has introduced an advanced all-in-one sensor module designed for indoor air quality monitoring.

The RRH62000, the first multi-sensor air quality module from Renesas, integrates multiple sensor parameters in a compact design and accurately detects different particle sizes, volatile organic compounds and gases harmful to human health.

With a Renesas microcontroller (MCU) on board, the module offers an intelligent sensor management solution for a growing market of air monitoring applications, including air purifiers, smoke detectors, HVAC systems, weather stations and smart home systems. Its robust firmware also enables customer products to comply with various air quality standards around the world.

The RRH62000 features one of the smallest footprints in its class of sensor modules, measuring only 46.6 x 34.8 x 12 mm. It packs Renesas' RA Family MCU and seven sensor signals: the laser-based PM1/2.5/10 sensor, ZMOD4410 gas sensor, and the HS4003 humidity and temperature sensor. Together, these sensors can detect particulate matter, total volatile organic compounds (TVOC), estimated CO<sub>2</sub>, temperature and humidity all in one system. All key components have been pre-integrated and fully calibrated at the factory, allowing developers to start their sensor system designs

right out of the box.

“Our RRH62000 module represents the next step in sensor fusion technology, which combines data from multiple sensors and turns it into comprehensive and actionable insights for environmental monitoring,” said Uwe Guenther, Sr. Director, Modules and Solutions Product Line at Renesas. “We are



dedicated to providing integrated sensing solutions that simplify development for customers and will continue to drive innovation in sustainable products that reduce environmental impact and enhance safety and comfort in our lives.”

Public interest in air quality and its effects on health has increased significantly since the COVID-19 pandemic. People are now more aware of how air pollutants can affect respiratory health and overall well-being. Less known is that pollutants are typically six to ten times more concentrated indoors than outdoors. These include dust, paint fumes, smoke from cooking, pollen and particulates from HVAC filters, which can enter the respiratory system and cause lung damage,

cancer and other health problems.

In order to meet these new challenges, Renesas' new sensor module is equipped to monitor a broad range of air quality conditions. Using laser-based technology, which offers higher precision compared to conventional LED methods, it can monitor concentrations of PM<sub>1</sub>, PM<sub>2.5</sub>, PM<sub>10</sub> particulates -- particles with diameters of 0.3- to 10µm -- as well as absolute or relative TVOC measurements in different power mode settings, providing the highest level of accuracy for these pollutants. The RRH62000 delivers seven sensor outputs simultaneously, and its on-board MCU allows the system to detect surrounding air quality data in real time.

The RRH62000 combo module comes with building standard firmware plus artificial intelligence (AI) algorithms, which lets engineers configure the sensors to conform to the requirements of various green air quality standards in public buildings, such as The Well Building Standard (WELL), Home Ventilating Institute (HVI) and RESET. With these features, for example, a school in China can use the same hardware as one in the U.S. or other location and simply update the AI-enabled firmware for its needs.

Intelligent sensor devices, such as the Renesas RRH62000 and recently announced RRH46410 gas sensor module, can support demand-controlled ventilation, allowing HVAC systems to adjust



air flow based on carbon dioxide levels and occupancy information to maintain optimal air quality and energy efficiency. Similarly, these modules use AI algorithms to predict when HVAC filters must be replaced or detect an anomaly before system failure occurs, significantly saving cost and time for system maintenance.

Renesas has combined the RRH62000 with numerous compatible devices from its portfolio to offer a wide array of Winning Combinations. This includes the In-home Air Quality Monitoring System and Air Quality Monitor (PM2.5) with Secure Cloud Connection, which combine

the RRH62000 with the RA6M3 and RL78/G14 MCUs, and various power devices to enable cost-efficient, compact, modular solutions for modern appliances.

These Winning Combinations are technically vetted system architectures designed from mutually compatible devices that work together seamlessly to bring an optimised, low-risk design for faster time to market. Renesas offers more than 400 Winning Combinations with a wide range of products from the Renesas portfolio to enable customers to speed up the design process and bring their products to market more quickly.

## SECO-LARM E-941SA-80Q Mini-Maglock

SECO-LARM has announced that the E-941SA-80Q 80-lb Mini-Maglock is now ETL certified to conform to UL Std. 294.

The E-941SA-80Q Mini-Maglock, with its compact size and 80-lb holding force, is ideal for small, minimum-security doors, including cabinets and drawers. Despite its small size, it boasts many of the advanced features found in the company's larger, more powerful locks.

### Key Features:

- ETL Certified to UL Std. 294: Ensures high safety and performance standards.
- Compact Design: Perfect for small, minimum-security doors, cabinets, and drawers.



- Built-in MOV Surge Protection: Protects the lock from voltage spikes.
- No Residual Magnetism: Ensures reliable and consistent operation.
- Low Current Draw: Minimises energy consumption.
- Versatile Operation: Supports 12~24 VDC operation.
- Easy Installation: Comes with a detachable mounting bracket.
- Durable and Waterproof: IP67 rating for use in various environments.
- Complete Installation Hardware: Includes all necessary hardware for almost any typical installation with additional brackets available for special situations.

### We'd Love to Hear From You!

Share your 'Security' insights with us! Email your articles, case studies, or press releases in an MS Word file, along with images. We look forward to featuring your work!

Submit your work at: [info@1stasset.org](mailto:info@1stasset.org)



## RelayX Connectivity Platform

Relay's RelayX features redundant connectivity, designed to provide teams across manufacturing, warehousing, hospitality, and healthcare with a simple and powerful platform to manage the unplanned complexities of frontline work. RelayX is powered by a revolutionary array of 5G/4G LTE cellular, Private LTE, LoRa, and Wi-Fi connectivity. RelayX's patented software platform seamlessly weaves these connections together to create an ultra-redundant, turnkey network that results in reliability that frontline teams can leverage for communication, worker safety, and operational insights.

RelayX's advancements in connectivity, durability, and audio quality were developed for the most challenging frontline environments, particularly manufacturing plants and distribution centres, where productivity is impacted when associates and leaders can't effectively coordinate exceptions to scheduled work.



clear audio, and incredible durability. Now, more than ever, frontline businesses need an edge - something that will help them improve both their team's performance and safety - we think RelayX can be that edge."

RelayX combines multiple 4G/5G networks, Private LTE, LoRa, and Wi-Fi into one resilient connection - creating an ultra-redundant, turnkey network that drives unprecedented reliability.

RelayX was designed to meet the demands of even the harshest working environments. RelayX has industrial-grade durability, having received IP68 and MIL-

STD-810H certifications, meaning it is drop-tolerant, submersible, and dust-resistant. RelayX's audio system allows it to deliver audio that is loud and clear in very loud environments, using its high-output dual speakers, three digital microphones, and enhanced background noise

cancellation. RelayX features a high-contrast OLED screen, which is clearly visible even in bright sun making it usable inside and out.

"The new digital display screen makes it easier for all users wherever they are located. The other feature that we use...is the translation feature. This is beneficial for multiple languages, making it easier to communicate with new hires. The Relay device has significantly improved our safety and security by introducing a panic alert feature. Panic alerts have taken safety and security to the next level with a press of a button. Relay has simplified our company's communication, making a significant difference in a fast-paced environment where employees are constantly in motion," added Gary Peloso, Food Safety Manager at Ace Endico.

## Securing sensitive spaces in healthcare applications

In hospitals, health centres, clinics and other medical buildings, the small spaces often need as much care as large areas. Yet while traditional mechanical keys can cure the problem of medicine and equipment security, this may come at the cost of time- or operational

efficiency.

In a busy hospital ward, keys are easy to misplace. Mechanical locking cannot log who accesses each opening, and when. Nurses either take on this laborious

task for themselves or medicine managers surrender some control over access. Auditing drug discrepancies or investigating incidents becomes more difficult. Just like any sensitive opening, in any building, the risks and costs of a security breach or unauthorised access can be great.

“Managing the security of additional access points mechanically, outside the scope of a digital access system, increases risk, complexity and workload,” says Lars Angelin, Business Development Manager at Assa Abloy Opening Solutions EMEA.

The drawbacks of many mechanical solutions can get in the way of medical care. Often multiple staff need access at different times in a setting where 24/7 operation is standard practice. Searching for the right key or keyholder causes delays, wasting nursing staff time.

All keys in circulation must be logged and monitored, for medicine safety or to ensure patient belongings are safe in bedside cabinets. If keys go missing, locks must be changed, which costs time and money. Hassles and headaches multiply if a master-key is lost.

Digital access seems an obvious solution. Yet such settings often have many points where typical wired access cannot reach. These may be mobile, like Electronic Prescribing and Medicines Administration (EPMA) carts. Cylinder sizes may be small with non-standard cam-



types, as on bedside cabinets or medicine storage.

“Instead, choosing digital access – traceable, flexible, convenient – with the Aperio KL100 Wireless Cabinet Lock brings many more access points under the control of the digital system,” explains Angelin. “These important openings are managed from one integrated software interface and offer the same level of control as any other digital access device.”

The robust, road-tested, battery powered Aperio KL100 makes cabinets, EPMA carts, medicine drawers and almost any other small opening an integral part of a digital access system. An adjustable cam makes it a straightforward retrofit solution for patient-accessed medication or “POD” lockers and bedside cupboards. This digital device also consumes very little

energy: Powered by one battery, it only “wakes up” when a credential is presented and needs no specialist maintenance.

In line with the rest of the Aperio range, the KL100 brings added flexibility over physical keys. It is compatible with smartcards and fobs using all major RFID technologies, as well as smartphone unlocking via Bluetooth LE and NFC. The device can accept multiple credential technologies simultaneously, in parallel, so security managers can roll out mobile keys at their own pace, or to appropriate employees only. ■

# Serving The Mission Critical Requirements Of The EdTech Market With A Broad Range Of Smart Technologies, Including Security

*With inputs from Hikvision*

***The rapid growth of EdTech is transforming education, offering new ways for students to learn remotely and making classrooms more interactive and engaging. Alongside these advancements, the integration of security technologies is enhancing campus safety, ensuring a secure environment both online and on-site. As educational institutions embrace these innovations, they are creating smarter, more flexible learning spaces that protect and empower students.***



EdTech is a developing field, and people are discovering new uses for it every day. A survey of students enrolled in online courses found that 78 percent of them thought the online experience was equal to or better than their experiences with in-person courses.

Studies like these suggest that innovations in EdTech will play a significant role in the future of education. As it develops it also takes into account ways to secure a campus and ensure that students are kept safe and secure. Not just physically but even as they delve deeper into the internet.

Some educators, like those who started their careers well before the internet emerged, may have issues with EdTech. Some fear that increased use of technology in the classroom could potentially eliminate the need for teachers.

But the burden the pandemic has put on parents to assist in their children's education only proves that technology can't replace teachers entirely. Relieving educators of some responsibilities, however, allows them to focus on their primary role and dedicate more of their time to individual students and their needs.

Here are some other benefits of EdTech, and later, we look at its convergence with SecuTech.

### **1. Provides opportunities for remote learning**

One of the most crucial benefits is that EdTech allows students to learn from virtually anywhere. There are no longer restrictions keeping students and teachers in the classroom or even in the same geographic location as their instructors. When a student has the freedom to learn from anywhere, it can make learning more convenient and may make students feel more comfortable.

### **2. Potentially alleviates sources of stress for teachers**

While remote learning isn't easier for everyone right off the bat, once teachers develop a good process, EdTech can relieve them of some of the traditional duties of an instructor.

They can build lesson plans right into their online courses, cutting down on the time they spend preparing each day's work. Online teaching platforms can also make grading and data collection much quicker, as online tests can often be graded and

recorded automatically.

### **3. Provides the ability to create individualized lesson plans**

Often, certain students in a classroom will have different educational needs than the rest of the class. EdTech gives teachers the flexibility to create different learning plans for each student if the course is asynchronous (self-paced) rather than synchronous (taught in real time). This can ensure each student gets what they need, whether it's additional help with the basic curriculum or the chance to explore advanced topics.

### **4. Encourages more engagement from students**

If you give a student a choice between a 500-page textbook and an interactive app on a tablet, you can probably guess which tool they'll pick. EdTech resources expand instructors' options for engaging students. They might give students the ability to visit new locations through videos or play educational games, or they could even use augmented reality (AR) or virtual reality (VR) to enhance a lesson.

### **5. Makes collaboration easier**

When teaching resources are exclusively online, students and instructors can easily collaborate on assignments during class and after school. Platforms like social media, collaborative wiki pages, and interactive whiteboards also allow students to work together easily and virtually.

Before EdTech changed how students learn, getting in touch with a teacher outside of school was difficult. Now, with messaging apps and virtual meetings, a student may be able to get real-time help when they need it — if the instructor is available, of course. Before allowing students to begin living, studying, and enriching themselves on campus, universities have a duty to provide safeguarding.

New and emerging technologies could spark the end for campus crimes.



## Safe Digital Learning Platforms

As online learning grows, cybersecurity becomes critical in protecting sensitive student data, maintaining privacy, and securing access to educational content. Firewalls, encryption, and secure login systems help protect EdTech platforms from cyberattacks.

## Remote Monitoring

Security technologies like CCTV cameras and access control systems can be integrated with EdTech platforms, allowing administrators to remotely monitor classrooms or campus spaces, whether in traditional settings or in hybrid/remote learning environments.

## Data Security and Privacy

With EdTech platforms storing massive amounts of student and school data, security technologies such as encryption, two-factor authentication, and secure cloud services are essential for protecting this information from breaches.

## Cloud-Based Access Control

Cloud-based access control is the future of campus



security systems. It provides the same security measures as traditional access control while offering a wide variety of additional benefits:

- Easy installation: since cloud-based access control

communicates using remote methods, installing and planning complex wiring systems is unnecessary. Instead, companies can simply install the device and connect it to the cloud-based router.

- Remote management: System administrators can access and manage door locks from anywhere, viewing access logs using a mobile application for more responsive security procedures.
- Integration potential: with cloud-based security tools comes the potential for integration, allowing campus security to unify all security data on a single platform, eliminating data silos that could hinder security investigations.

In addition to these benefits, cloud-based access control supports using mobile access credentials instead of keycards and fobs. This presents the potential for cost savings, as keycard and fob replacement can incur significant costs throughout the academic year.

Mobile access control also supports a more convenient and hygienic strategy for entry - touchless entry. Students and faculty can enter the building simply by waving their hands over the access reader to trigger remote communication with their devices. The reader detects their credentials, and the door unlocks.

When onboarding new students, the university simply sends them an activation code allowing them to download their access credentials. There is no need to create thousands of fobs and keycards each academic season. Using this self-serve security onboarding method allows campus security to focus on more important tasks at the beginning of the year, such as establishing strong security presence across campus.

One of the most popular integrations for cloud-based access control in education is visitor management software. Educational institutions have a duty to provide safeguarding and ensure only students and faculty are allowed on the premises unescorted.

To make this possible, many campuses are integrating visitor management software with access control. The software allows guests to digitally register when entering the campus, gaining temporary access control permissions to enter.

Once they leave, they won't be able to enter again. Providing this security measure allows people to enter the premises for appointments and meetings while reducing the burden on staff.

## Emergency Response Systems

Both physical and digital security technologies can be integrated with EdTech to trigger automatic alerts during emergencies, whether it's a physical threat on campus or a cybersecurity breach affecting the learning environment.

## Cloud-based video surveillance

Cloud-based security cameras provide benefits similar to those of a cloud-based access control system. Security staff can easily deploy surveillance without planning complex wiring infrastructure. They simply connect the camera to the server, which allows them to view security camera footage from anywhere using a mobile application or browser.

Cloud-based security cameras have integration potential that enables AI integration, making campuses much safer. AI-enabled security cameras can perform automated threat detection, providing campus security with alerts based on triggers. For instance, it could detect a weapon on campus using object recognition or physical threats with behavior recognition.

Since campus security won't be able to monitor video feeds and detect potential security incidents consistently, this solution is essential for responsive and proactive security. Without it, many threats would go unnoticed, leading to crimes on campus.

Many campuses use reporting platforms, allowing students to contact security when they feel unsafe or report suspicious activity. Providing these platforms to students allows for instant security response, allowing their voices to be heard when they feel unsafe.

## Integration of Alarm Systems

Modern alarm systems, both fire and security, are allowing for more crisis aversion on campus adding to the life safety of students. Advanced fire detection and prevention systems can be linked to digital platforms that provide real-time alerts to students, staff, and even parents in case of emergencies, facilitating rapid

evacuations and incident reporting. Glass Break sensors allow security staff to respond instantly to property damage and intrusion, while gunshot detectors can provide life-saving agility. Gunshot detectors sound an alarm that allows students and faculty to immediately take action, evacuate, or take cover.

## Emergency Response Systems

Both physical and digital security technologies can be integrated with EdTech to trigger automatic alerts during emergencies, whether it's a physical threat on campus or a cybersecurity breach affecting the learning environment.

## Real-Time Communication and Alerts

Security systems can provide real-time alerts through EdTech platforms, ensuring students and teachers receive immediate information about potential dangers or emergency situations, both online and on-campus.

The tech innovations listed above are becoming staples for effective, responsive, and agile security strategies on college campuses. It's worthwhile to consider investing in these technologies as they storm the security landscape. Cloud-based technologies are the future of security, and more commercial industries are taking note.

“According to Research and Markets, the global EdTech market grew from USD 149.79 billion in 2023 to USD 182.26 billion in 2024. It is expected to grow at a CAGR of 22.62%, reaching USD 624.36 billion by 2030.”

The education technology (EdTech) market presents a challenge for vendors since it ranges broadly, covering areas as diverse as interactive learning, content sharing, campus security, and management software. The good news is that Hikvision's smart technologies provide solutions for all of these, making it a valuable partner in this growing sector.

According to Research and Markets, the global EdTech market grew from USD 149.79 billion in 2023 to USD 182.26 billion in 2024. It is expected to grow at a CAGR

of 22.62%, reaching USD 624.36 billion by 2030. This robust growth is drawing technology vendors eager to capture a part of that market share.

However, as the market develops and the range of technologies expands, the challenge for those selling to educational institutions is becoming harder. Universities, in particular, are seeking a streamlined solution to multiple EdTech technologies rather than engaging with multiple vendors.

For example, as digital learning tools rapidly advance, traditional methods such as whiteboards are becoming insufficient for presenting complex scientific concepts. There is an increasing demand for more dynamic and interactive teaching aids.

At the same time, the shift towards flexible and hybrid learning environments isn't just a response to unforeseen events like the pandemic, but also aims to enhance accessibility for educational institutions. Moreover, there is a growing need for advanced security systems to ensure a safe environment for both students and staff.

By integrating advanced audio-visual technology, artificial intelligence, and data analytics, Hikvision's smart solutions for EdTech offer a comprehensive approach to addressing these challenges. They help transform ordinary classrooms into interactive, collaborative spaces that enhance both teaching and learning experiences. What's more, its security systems deliver thorough protection across entire campuses.

Together, they help higher education institutions bridge the gap between traditional education methods and

cutting-edge digital technology.

Hikvision's Interactive Flat Panels bring interactive learning to life in classrooms and labs. These smart panels are particularly useful during laboratory sessions, where observing experiment details can be challenging. Teachers can use their smartphones to project content onto large interactive displays by scanning a QR code, ensuring all students can clearly view essential details.

The HikCentral ClassIn, integrated with existing educational applications, enhances remote teaching and collaborative learning. It supports real-time screen sharing and is compatible with popular video conferencing tools such as Zoom.

The ClassIn software platform allows remote students to participate in lectures and discussions as if they were in the classroom. It also simplifies the distribution of digital content such as lecture recordings. Meanwhile, educators can use the Education Sharing Device to record lessons with a single click and retain necessary resources, facilitating real-time interaction between multiple classrooms.

Hikvision's safe campus solution leverages advanced technologies to create a secure environment for students and teachers. This usually includes TandemVu PTZ Cameras that provide wide-area coverage and detailed close-ups with high image quality, 24/7. The advanced video security system has significantly improved campus safety and operational efficiency, allowing students and faculty to focus on their academic pursuits with confidence in their safety. ■



YOUR **O** **INION**  
MATTERS

At SECURITY UPDATE, we are dedicated to ensuring our content is consistently **Informative**, **Engaging**, and **Captivating**.

We welcome your thoughts, feedback and suggestions.  
Write to us at: [info@1stasset.org](mailto:info@1stasset.org)



# DOES SECURITY REALLY MATTER?

OUR PAN-INDIA SUBSCRIBERS SAY

**YES IT DOES!**

**INDIA'S #1 SECURITY MAGAZINE**

For Subscriptions, Advertising and other Brand Building opportunities email us at: [info@1stasset.org](mailto:info@1stasset.org)



<https://www.securitytoday.in>


CITIES/TOWNS LISTED ARE ACTUAL SUBSCRIBER LOCATIONS



# EVENTS CALENDAR

 **BANGLADESH**  
**12-14 September 2024**  
IFSEC Bangladesh  
Hall 4 (Naboratri), ICCB  
Dhaka  
<https://ifsecindia.com/bangladesh/>

 **INDIA**  
**05-07 October 2024**  
India International Security Expo  
(IISE)  
Pragati Maidan,  
New Delhi  
<https://www.indiatrading.com/>

 **INDIA**  
**14 November 2024**  
SECURITY TODAY Knowledge  
Summit  
Grand Hyatt- Gurgaon  
Delhi NCR  
<https://knowledgesummit.securitytoday.in/>

 **GERMANY**  
**17-20 September 2024**  
Security Essen 2024  
Messe Essen, Norbertstrasse 2  
Essen  
[www.security-essen.de/impetus\\_provider/](http://www.security-essen.de/impetus_provider/)

 **Bosnia & Herzegovina**  
**09-10 October 2024**  
ADRIA Security Summit  
Convention Centre Hills  
Sarajevo  
[www.adriasecuritysummit.com](http://www.adriasecuritysummit.com)


 **USA**  
**19-21 November 2024**  
ISC East  
Javits Center  
New York City  
<https://www.discoverisc.com/east/en-us.html>

 **USA**  
**23-25 September 2024**  
Global Security Exchange (GSX)  
Orange County Convention Center  
Orlando  
Florida  
[www.gsx.org](http://www.gsx.org)

 **Turkey**  
**9-12 October 2024**  
ISAF 2024  
Istanbul Expo Centre  
Istanbul  
[www.isaffuari.com/en/](http://www.isaffuari.com/en/)

 **Egypt**  
**26-28 November 2024**  
Egypt Energy 2024  
Egypt International Exhibition  
Centre  
Nasr City, Cairo  
<https://www.egypt-energy.com/en/home.html>

 **UK**  
**24-25 September 2024**  
International Security Expo  
2024  
Olympia  
London  
[www.internationalsecurityexpo.com](http://www.internationalsecurityexpo.com)

 **UK**  
**17 October 2024**  
Consec 2024  
Hilton Hotel, Terminal 5  
Heathrow  
[www.securityconsultants.org.uk/events/consec](http://www.securityconsultants.org.uk/events/consec)


 **UK**  
**2-4 December 2024**  
IFSEC International  
ExCeL London  
<https://www.ifsecglobal.com/ifsec-international-security-event/>

 **Philippines**  
**25-27 September 2024**  
ADAS 2024  
World Trade Center Metro  
Manila  
[www.adas.ph](http://www.adas.ph)

 **CANADA**  
**23-24 October 2024**  
Security Canada Central  
Toronto Congress Centre  
Toronto  
<https://securitycanada.com/attend/central>

 **INDIA**  
**12-14 December 2024**  
IFSEC India  
Pragati Maidan  
Delhi NCR  
<https://ifsecindia.com/>

 **Saudi Arabia**  
**01-03 October 2024**  
Intersec Saudi Arabia  
Jeddah Center for Forums & Events  
Riyadh  
[intersec-ksa.ae.messefrankfurt.com/ksa/en.html](http://intersec-ksa.ae.messefrankfurt.com/ksa/en.html)

 **Singapore**  
**4-5 November 2024**  
ASIS Asia Pacific Conference  
Singapore Marriott Tang Plaza  
Hotel  
<https://asis-singapore.org.sg/asis-asia-pacific-conference-2024/>

 **INDIA**  
**30 January 2025**  
Top Indian Women Influencers  
In Security  
Bangalore  
<https://intersec.ae.messefrankfurt.com/dubai/en.html>

PRESENT

**TOP INDIAN WOMEN INFLUENCERS IN SECURITY****30<sup>th</sup> January 2025, Bengaluru**

*Globally women are playing a key role in the advancement of the profession of security in all sectors, verticals and levels of the industry.*

*In order to recognise and honour the accomplishments, value and contributions of women in this vital sector of the economy, SECURITY TODAY & SECURITY UPDATE in association with Infosec Girls and WISECRA announce the "Top Indian Women Influencers in Security" recognition for the year 2024.*

*In 2020, this accolade was developed to help recognise women in security in India who made significant contributions in shaping the industry and shaped the path for future generations of professionals. 20 torch bearers were recognised from 272 nominations received in a virtual ceremony by the nation's 1st, most famous & iconic lady IPS officer, Her Excellency, Dr. Kiran Bedi, the then Hon'ble Lieutenant Governor of Puducherry. Distinguished senior people from different sectors were carefully chosen as 'members of the jury' for this event.*

*Till date 41 women influencers from globally established companies have gained this recognition.*

**Visit: <https://tiwiis.securitytoday.in>**

PAST SPONSORS



PAST SUPPORTING PARTNERS

**PRAMA**<sup>®</sup>  
MADE FOR INDIA - MADE BY INDIA - MADE IN INDIA



SECURING PEOPLE,  
**ENRICHING LIVES**



**WE AT PRAMA BELIEVE IN ENRICHING LIVES.**

The cutting-edge technology in our security products assures every life is protected.

 /PramaIndiaOfficial

**भारत में बना, भारत का अपना सर्वोत्तम ब्रांड**

 /PramaIndiaOfficial

**PRAMA INDIA PRIVATE LIMITED**

Office No. 103, F. P. No. 765, Fly Edge,  
TPS III Junction of S. V. Road,  
Near Kora Kendra, Borivali West,  
Mumbai - 400 092, Maharashtra, India.  
**Board No.:** +91-22-6896 5500  
**Web:** www.pramaindia.in



**Sales:** +91 22-6896 5533 | **E mail:** sales@pramaindia.in



**Toll Free:** 18002091234



**Tech Support:** +91 22-6896 5555 | **Whatsapp:** +91 9076305555 | **E mail:** techsupport@pramaindia.in



**Repair Service:** +91 22-6896 5544 | **Whatsapp:** +91 9076005544 | **E mail:** service@pramaindia.in