

# SECURITY Update

CREATING BUSINESS OPPORTUNITIES



For Manufacturers, Distributors, Dealers,  
System Integrators & Installers of Security,  
Fire & Safety Systems.

Vol. 13 No. 04

www.securityupdate.in

April 2023

Pages 16

Price ₹ 75

## DIY Vs Professional security: What is safer?



If you want to increase the security of your home or business facility, you've probably already identified the two installation methods typically used for new security devices — do-it-yourself (DIY) or having a professional install the system for you.

DIY security systems mean you install everything. You also need to determine where cameras and other components will fit and work best — which can be more challenging than it seems.

Alternatively, when you opt for professional installation from a security company, experienced technicians can help you design and install a security system that fulfills your specific needs. Professionally installed systems ensure correct equipment set up and offer helpful integration with other innovative technology. You also benefit from professional monitoring and maintenance after the installation is complete.

Tech-savvy home and business owners may feel comfortable in their knowledge level and decide to DIY. Meanwhile, homeowners with limited tech knowledge, buildings with multiple residents or larger, multilevel houses typically require expert installation to ensure safe and operational security.

Cost, monitoring style, overall protection

and other differences may motivate you toward one side of the DIY vs. professional home security debate. Most equipment used to protect your property will have similar capabilities and features, but your home's safety relies heavily on the devices and services you choose.

If you're researching DIY solutions to security, inexpensive security cameras may catch your eye. But are cheap security cameras safe? The short answer is no. Many models and brands that are available on the market can have critical security flaws. Even products with positive reviews can have underlying risks, making it challenging for homeowners to ensure a safe DIY security system.

When security products have critical security flaws — like weak default passwords and unencrypted data — they make it easy for hackers to breach the local internet network or even potentially gain control of the camera or other system components.

Even quality equipment with strong passwords and two-factor authentication can experience other safety issues during installation and monitoring. For example, DIY installation typically uses self-monitoring, which means a potential safety problem may go unnoticed for an extended length of time.

When an issue arises, you want a quick and effective response. DIY also cannot guarantee a working system or 24/7 security monitoring like many professional services.

Here are a few more reasons why you might reconsider your DIY home security plans:

- Security systems are more challenging to self-install in large, multilevel buildings: Most security equipment will operate on a wireless network separate from your home's Wi-Fi. You must ensure all components are working as they should be and are correctly connected to your monitoring system during installation. The larger the building, the more challenging it is to create an optimal and functioning system configuration.

- It is harder to maintain the system when you have no one to call if issues arise: If a problem occurs, you will be responsible for finding and fixing it. This process can require time that you aren't prepared to spend, leaving your home or business vulnerable for an extended period until you can correct the issue, putting your property at risk.

- All equipment may need to be purchased upfront without expert recommendation: Some security equipment, especially cameras, can be sold to consumers without proper security measures in place. This lack of quality control makes it challenging to know if you've purchased the best products for your needs. Even an abundance of positive reviews cannot guarantee a product's safety.

- Sufficient research is

needed to ensure the best quality equipment: Because numerous models and brands are available for each component, it can take some time and effort to gather everything you need. The most affordable may not be the most secure.

- DIY security systems are at greater risk of improper installation, leaving you vulnerable: The average person may not know how to locate and address all possible security threats. Any unprotected or non-functioning areas in the home security system can easily go unnoticed after the DIY installation is complete.

- The home or business owner is responsible for any repairs and replacements: DIY security lacks the same protection

and warranty offered by professional security alternatives. Equipment repairs and replacements occur more frequently with DIY security.

- Monitoring for prevention can be unreliable or come with an additional fee: Self-monitoring is less reliable than most professional monitoring alternatives. Many owners are unable to dedicate their time to monitoring security 24/7. While some DIY systems offer professional security monitoring for an added fee, it's often more beneficial to let professionals handle the entire job.

Professional security installation is a worthwhile investment, especially for businesses and multilevel homes. A technician will ensure correct installation

and quality equipment so that you have peace of mind knowing your family, employees, equipment, information and other valuables are safe. Consider hiring a professional who will provide customized security that protects all your home's vulnerabilities, avoiding security issues from DIY home security.

While home security DIY allows you to become accustomed to different electronic security devices at your pace, a professional company provides more immediate and expansive protection for residential properties. Keep your business and employees safe with full-time protection and comprehensive commercial security solutions.

Some of the benefits of having a professional

Contd on Page 3...

**PRAMA**  
MADE FOR INDIA - MADE BY INDIA - MADE IN INDIA

**ANALOG SURVEILLANCE SYSTEM GETS  
DIGITAL CLARITY**

Introducing the **HD camera** series from PRAMA

PRAMA HD cameras can be used for digital as well as analogue video surveillance systems. This is a perfect option for those who already have an analog security system, but want better resolution for their surveillance photos and videos. This is because of the camera's superior video quality and ability to use RG59 coax cable. Earlier, Analog cameras used to come in lower resolution i.e. TV lines but now higher resolutions HD cameras which support up to 2/5 MP resolutions are also available. Supports various focal length with fixed and Varifocal lenses. Also, different type of video signal output supported like TVI/AHD/CVI/CVBS.

/PramaIndiaOfficial **भारत में बना, भारत का अपना सर्वोत्कृष्ट 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, Maharashtra, India - 400 082.  
Tel : 022 6896 5500 Technical Support : 022 6896 5555 Customer Care : 022 6896 5566  
Email : sales@pramaindia.in / techsupport@pramaindia.in Website : www.pramaindia.in



Dear Reader

Speaking at a recent conference I recalled an incident a few years ago where a casino in the U.S. had got hacked through its internet-connected fish tank thermometer. The hackers exploited a vulnerability in the thermostat to get a foothold in the network. Once there, they managed to access the high-roller database of gamblers and "then pulled it back across the network, out the thermostat, and up to the cloud.



Internet-connected technology, also known as the Internet of Things (IoT), is now part of daily life, with smart assistants like Siri and Alexa to cars, watches, toasters, fridges, thermostats, lights, and the list goes on and on. This trend has revolutionised the way we live, work and communicate. From smart homes to connected vehicles, IoT devices have become an integral part of our daily lives. However, with this increased connectivity and convenience, comes an increased risk of security breaches.

IoT cameras have become increasingly popular over the years, from security applications to baby monitors, these devices are designed to make our lives easier and safer. However, these devices can also be a target for cyber criminals. Hackers can exploit vulnerabilities in IoT cameras to gain unauthorised access to sensitive information, spy on individuals, and even launch cyber attacks.

One of the biggest challenges with securing IoT devices is that they are often designed with minimal security features. In many cases, these devices are cheap and mass-produced, which means that manufacturers prioritise cost over security. As a result, many IoT devices have default usernames and passwords, which can easily be hacked. Furthermore, many IoT devices are not updated regularly, which means that vulnerabilities are not addressed, leaving them open to attack.

So, what can be done to secure IoT cameras and other devices? Firstly, it is important to choose reputable manufacturers when purchasing IoT devices. Look for companies that prioritise security and have a track record of producing secure devices. In addition, it is important to change the default usernames and passwords of IoT devices to a unique and complex one. This can significantly reduce the risk of unauthorised access.


Secondly, it is important to regularly update IoT devices. Manufacturers often release security updates and patches to address vulnerabilities in their devices. By regularly updating devices, users can ensure that their devices are protected against the latest threats.


Thirdly, users can enhance the security of IoT devices by segregating them from the main network. This can be achieved by creating a separate network for IoT devices, which is isolated from the main network. This can significantly reduce the risk of an attacker gaining access to sensitive information.


Finally, it is important to be aware of the risks associated with IoT devices. Users should be cautious about what information they share online and who they share it with. In addition, users should avoid connecting IoT devices to public Wi-Fi networks, as these networks are often unsecured and can be easily hacked.

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

G B Singh  
Group Editor

 gbsingh@1stasset.org

 @EditorGB

 linkedin.com/in/gbsingh9



SECURITY UPDATE is a focused educational publication on protection technology, products and solutions. It reaches the business community of manufacturers, distributors, dealers, installers, integrators and consultants of security, fire and safety systems. Printed monthly as a lightweight tabloid, it is easily carried and read on the move, reaching the remotest corner of India, even where the internet may not have reached!

**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. Deadlines are three weeks before this date.



©1st Academy of Security Science Education & Training Pvt. Ltd.  
ISO 9001:2008 Certified

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

# Effortless door control solves door access challenges



Assa Abloy's Free-Motion technology combines the safety and protection of door closing technology with the comfort of a door which opens naturally and resistance-free — and may be left open at any angle.

When a door is equipped with a high-quality door closer, building users can feel safer. They know that fire doors shut tight and sensitive openings are protected against unauthorised entry. But sometimes, according to Assa Abloy, door closer technology can also create barriers to genuine access-for-all. The problem is greater still for us-

ers who — for whatever reason — have restricted strength or mobility.

Why? Because door closer resistance may be too great. Or the time before closing begins may be too short. Every user is different, with individual access needs or challenges. So, as a result, in solving one problem, some door closers accidentally create another. A Free-Motion Door Closer from Assa Abloy Opening Solutions can solve these challenges.

When a user or building manager activates Free-Motion technology, automatic door closing is disabled. Doors may be left open, al-

lowing staff and visitors to circulate freely: The door opens weightlessly right up to its widest angle since Free-Motion activation.

Even heavy EN size 6 fire and smoke doors open easily. Everyone is able to move unhindered. At any time — in the event of a fire or other emergency, for example — Free-Motion operation may be stopped and doors once again close quickly after use. This can be done manually or, when integrated with a fire system, happens automatically when a threat is detected. As another layer of safety, every door fitted with Free-Motion technol-

ogy shuts automatically when power is cut.

A Free-Motion Door Closer can fit directly to the door leaf or to the frame. The range includes closers for double doors and the option of an integrated smoke detector.

Like every Assa Abloy Door Closer, Free-Motion technology is robust and durable by design. Assa Abloy has designed it to meet all critical safety and fire standards. Closing speeds, stronger latch speeds and closing force are all adjustable to meet the demands of the specific door or location.

And an Assa Abloy Free-Motion Door Closer is built for more than just fire or smoke doors: Free-Motion technology adds time- or event-based flexibility to every opening. For example, closers may be active during office hours to allow easy circulation of people, then deactivated overnight, so a door closes automatically after each user passes through it.

## Yale Home introduces Assure Lever Collection



Yale Home has announced an update for its Assure Lever Collection. The popular lock manufacturer states that its new update provides smart home Wi-Fi connectivity at new, lower price points for home-

owners. Yale Home explains the new Assure Lever Collection provides homeowners a choice of more affordable smart home lock solutions, and the company points out the products are available to purchase with a Wi-Fi Smart Module directly in the box.

According to Yale Home, previously its smart home security solutions required a Wi-Fi Connect Bridge, but now integrators can use a swappable module to

enable Wi-Fi connectivity to support smart home integration.

Yale Home emphasizes that not only are its smart home technologies more installer friendly, but they are now more homeowner friendly because they are available at lower price points. Through the improvement in technologies and lower price points, the company continues, integrators can offer their clients smart home security lock locations in the

home that range from garage doors to side entry ways.

Beyond the applicability to single-family homes, the newly announced Yale Home Assure Lever Collection can also be used for situations such as shared housing environments like roommates or multi-generational homes to enable property owners to easily manage multiple users.

### FORM IV

Statement about ownership and other particulars about newspaper (SECURITY UPDATE) to be published in the first issue every year after the last day of February

1. Place of publication: Gurugram

2. Periodicity of its publication: Monthly

3. Printer's Name: Ask Advertising Aids Pvt Ltd. Nationality: Indian

Address: 88, DSIDC Complex, Okhla Industrial Area, Phase-I, New Delhi-110020

4. Publisher's Name: GB Singh on behalf of 1st Academy of Security Science Education & Training Pvt Ltd.

Nationality: Indian

Address: 24-B Udyog Vihar-V, Gurugram 122016, Haryana

5. Editor's Name: GB Singh Nationality: Indian Address: G-19/11 DLF City-1, Gurugram-122002, Haryana

6. Names and addresses of individuals who own the newspaper and partners or shareholders holding More than one per cent of the total capital:

GB Singh, G-19/11 DLF City-1, Gurugram-122002, Haryana

Amandeep Singh, G-19/11 DLF City-1, Gurugram-122002, Haryana

I, GB Singh, hereby declare that the particulars given above are true to the best of my knowledge and belief.

Date 01.03.2023



# Motorola unveils new Avigilon security suite

Motorola Solutions has released the new Avigilon physical security suite, designed to provide secure, scalable and flexible video security and access control to organisations of all sizes around the world. The Avigilon security suite includes the cloud-native Avigilon Alta and on-premise Avigilon Unity solutions, each powered by advanced analytics and designed to provide an effortless user experience.



Avigilon has been the capstone of Motorola Solutions' Video Security & Access Control business, which has grown through strategic acquisitions over the past five years to achieve over \$1.5 billion in annual sales (2022). The launch of the new Avigilon security suite marks the combination of technologies from three acquisitions – Avigilon (2018), Openpath (2021) and Ava Security (2022) – to create one of the most extensive physical security platforms on the market today, all under a modernised Avigilon brand.

The new Avigilon security suite makes enterprise-grade physical security accessible to businesses of any size, with modular layers of security that can be tailored to protect them from the increasing number and complex nature of threats around the world. It fills a critical void in the market today, bringing together the necessary capabilities to help keep people, property and assets safe.

Motorola Solutions' video cameras allow customers to comply with the National Defense Authorization Act (NDAA) Sec. 889 and highlights Motorola Solutions' continued commitment to advancing

technologies that protect the nation's networks and supply chains from equipment that threatens national security.

Avigilon Alta is an entirely cloud-native security suite that brings together Ava Security's video portfolio and Openpath's access control solutions. It requires no infrastructure beyond cameras, controllers and access control readers utilising cloud infrastructure managed by Motorola Solutions. Avigilon

Unity is an on-premise security suite that has all the hallmarks of the original Avigilon portfolio, including Avigilon Control Center, Avigilon Cloud Services and Access Control Manager. It is designed for enterprises that want to manage their own systems.

Avigilon Alta and Avigilon Unity features:

- Scalable, flexible design for today and the future. The Avigilon security suite can scale as businesses grow, enabling organisations to include multiple sites, cameras and locations that can be operated from anywhere via a browser or mobile device.
- End-to-end security technology for complete situational awareness. The Avigilon security suite centralises video security, access control, analytics and decision management into one easy-to-use platform.
- Advanced artificial intelligence (AI) for proactive security alerts in real-time. The Avigilon security suite helps to make watching live video obsolete with AI-enabled analytics. Automatic alerts are sent to security operators who can securely access the platform from anywhere on any device to gain immediate visibility and insight into a threat.

## NOW CONTROL YOUR SECURITY FROM WHEREVER YOU ARE

Addressable Intrusion Alarms with Easy BUS (Single Cable) Wiring



### JABLOTRON

CREATING ALARMS

#### JA-100+

- Emergency alarm alerts to the user & authorities
- 24/7 burglary, fire, flood, & CO protection
- Notifications with 3 layers of backup via integrated GSM/GPRS/LAN
- SMS & voice reports from the system to up to 15 users
- Panic & duress modes
- Integrate with CCTV cameras
- Programmable outputs for lights & other automation
- 20 independent calendars to schedule automatic events
- Remote control the system via web/mobile app/call/sms
- Detailed reports pinpointing the individual device
- Door lock control with RFID card
- User friendly keypads with control segments





Technology on Guard

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

**APPLICATIONS:**  
HOMES, OFFICES,  
BANKS, FACTORIES,  
BOARD ROOMS,  
LABS, R&D CENTRES,  
SHOPS...

Contd... from page 1

# DIY Vs Professional security....

vs. DIY security system include:

- Increased safety: You gain greater assurance that the system is installed correctly and receive alerts about property breaches right to your phone, keeping any residents and valuable assets safe.
- Reliable monitoring: Professional security has more reliable monitoring for prevention — some services even offer 24/7 protection and guard response. They can immediately notify authorities of unauthorized behaviors and emergencies.

- Higher quality: With a professional system, you can effectively combine all of your security alarm, surveillance and monitoring needs. You receive professional monitoring services and the ability to view any of your cameras anytime, anywhere from any mobile device.
- More experience: Technicians have the experience and knowledge necessary to make helpful recommendations and answer any questions. Ensure that safe, well-known brands are installed correctly and that all of your property's

vulnerabilities are secure.

- Customized design: Your system is customized to your specific circumstances and requirements, providing more effective protection. Add security alarms, surveillance, artificial intelligence video analytics and more.
- Integration options: It's easier to integrate your security system with sensors, smoke detectors, fire systems, access control and other add-on equipment.
- Easier maintenance: Your system provider typically covers routine maintenance, ensuring

your equipment remains operational and that any issues are addressed before more significant damage occurs. If something does go awry, they can also troubleshoot the issue for you and fix the problem as quickly as possible.

So take your decision judiciously when you are trying to make either your home, business or any other premise safe. It's fine to self install a lone security camera outside your door, but when it comes to assessing where your camera needs to be set up, get a professional!

[www.securityupdate.in](http://www.securityupdate.in)



# SAFR™ SCAN highlights new integrations, features and mobile app in secure, seamless facial authentication platform

SAFR™ SCAN from RealNetworks, the AI-powered face authentication solution designed for mainstream commercial applications, revealed its latest computer vision access control solution recently.

With a focus on security, convenience, and affordability, SAFR SCAN is a frictionless solution that's environmentally sound and avoids adding to the approximately 300 million plastic proximity cards disposed of or lost each year.

SAFR SCAN integrates with AMAG Symmetry, Avigilon ACM, Feenics, Genetec Synergis, Johnson Controls C•CURE 9000, PCSC LINC-NXG, and Schneider Electric Access Expert software platforms at the API level. SAFR SCAN interfaces to any access control system via Wiegand or an integral, fully encrypted Open Supervised Device Protocol (OSDP) connection.

SAFR's computer vision code is among the smallest footprints and most efficient offerings in the facial recognition marketplace, making it easy to deploy in edge devices. SAFR SCAN authenticates up to 30 individuals per minute and functions as a 3-in-1 device for access control, video surveillance, and video intercom capabilities.

Since its initial introduction in 2022, SAFR SCAN continues to evolve, adding a powerful feature to help detect and prevent tailgating as well as full-person record export and import capabilities.

Certification & Expansion with AMAG

## Technology

SAFR SCAN biometric access readers provide direct interface capabilities with Symmetry Access Control from AMAG Technology. The symmetry mobile enrollment application seamlessly enables enrollment to SAFR SCAN for face authentication.

The SAFR solution allows easy management of credentials, enabling administrators to add or remove users, modify user access levels, and restrict access based on permissions.

This integration provides full record export and import of physical identity credentials as well as batching; mask detection to ensure policy compliance; live detection and real-time spoofing alerts with 98.5% accurate recognition of masked faces; and real-time alerts of unauthorised entry attempts.

Feenics Bi-Directional Integration

SAFR SCAN connects directly to the Feenics cloud, allowing for complete system management of transactions, credentials, enrollments, and system configuration. This integration simplifies access control specifications by utilising the door controller features of SAFR SCAN.

It allows for enrollment, deactivation of credentials, and setting access levels and permissions directly from the

SAFR SCAN reader, meaning no panel is required.

Certification of Genetec Integration

SAFR for Access Control and SAFR for Surveillance is officially certified by the Genetec Development Acceleration Program to run with the Genetec Synergis™ access control system and Security Center video management system (VMS).

The SAFR platform provides best-in-class access control with the SAFR SCAN frictionless door station integrated with Synergis and SAFR video surveillance software integrated with Security Center, which yields actionable data from the live video feeds like surveillance watchlist, occupancy, demographic composition, dwell times, and more. All data passed through SAFR is protected with AES-256 encryption in transmission and at rest.

SAFR Key Mobile Credentials

With mobile credentials continuing to gain popularity, SAFR Key mobile credentials provide an affordable and convenient physical identity solution, enabling users to leverage their smartphones to access secured areas.

SAFR Key uses Bluetooth Low Energy (BLE) to enable communication between the mobile device and SAFR

SCAN. The user's mobile device acts as a virtual key and transmits an encrypted code to the access control system to unlock the door.

SAFR Key can be used as the only credential read by SAFR SCAN for those who wish to opt out of face authentication or used with face authentication for dual-factor credentialing at high-security doors.

SAFR Key is extremely secure and compatible with the Public Key Open Credential (PKOC) standard, an open specification written and supported by the Physical Security Interoperability Alliance (PSIA). It is available for both iOS and Android devices and supports a wide range of mobile devices, including smartphones and tablets.

Ideal for both indoor and outdoor environments with changing lighting conditions, SAFR SCAN's facial recognition technology is 99.9% accurate and uses anti-spoofing technology to ensure the liveness of the individual being authenticated.

All SAFR SCAN data is secured and encrypted with no facial images being recorded or stored anywhere within the system for further personal privacy protections. SAFR SCAN incorporates two types of liveness technologies to combat presentation attacks: structured 3D liveness and RGB liveness. The SAFR algorithms were developed to minimise bias; SAFR performed best for low bias of all algorithms tested by the National Institute of Standards and Technology (NIST).



This means that it can detect at various heights, with a 15m and 90° adjustable detection area, more precisely identifying what is actually triggering the alarm.

Patented Independent Floating Threshold (IFT) technology allows the detectors to adjust their thresholds based on the environment's infrared and background noise automatically and dynamically. This essentially reduces false alarms caused by background noise interference.

The detector uses digital temperature compensation to automatically adjust the alarm threshold according to the environment. This also means it is much more resilient in bad weather conditions, and enables consistent detection throughout.

Any successful security system is subject to attempts to overcome it. One of these is 'masking', where a potential criminal 'covers' the sensor(s), for example with a spray. The AX PRO device uses active IR anti-masking - the detector can initiate

a mask-processing sequence to check whether it has been masked or not. The 'operator' receives an alarm and can act accordingly.

The optional camera module provides GIF verification, allowing the 'operator' to see an image of an 'incident' for visual verification. The module has a 2.0mm lens with adjustable angle and can provide up to 20 images with VGA/QVGA/QQVGA formats.

Other features include:

- Pet immunity up to 40 kg
- Waterproof to IP65 standard
- Automatic sensitivity
- Easy to install and cost-effective, with no power/network cables needed.

In a market where accurate intruder alerting is exploding and verification is becoming more important, the Wireless Triple Signal Detector can provide an innovative solution in a wide range of scenarios.

## Telaeris deploys new facial recognition technology

Telaeris, Inc., a handheld solution provider for physical access control systems (PACS) announces its new facial recognition verification system on its XPID200 series handheld, mobile readers running XPRESSEntry software. This new technology comes at a great time when facial recognition accuracy is hitting new highs.

Handheld facial verification provides security and safety professionals more options for employee identification as well as accelerates the mustering of employees in an emergency evacuation. Workplace environments are dynamic and range in a wide variety of different shapes and sizes. Security and safety professionals are present-

ed with unique and challenging scenarios every day making it difficult to maintain workplace compliance.

Security professionals patrolling and monitoring activities need more than just radio or cell phone communications to perform their job and keep the workplace secure. Safety professionals need more than paper rosters for OSHA-compliant emergency evacuations when mustering workers and visitors at assembly areas. XPRESSEntry directly helps close these gaps.

XPRESSEntry readers enhance access control systems by verifying permissions and authenticating credentials or biometrics against the iden-

## New innovative Hikvision AX PRO Wireless Triple Signal Detector takes false alarm reduction to a new level

The newly introduced AX PRO alarm product line has the Wireless External Wireless Triple Signal Detector and (optional) dedicated camera module. This powerful intruder detection system provides a better image, more precise detection, and a handy modu-

lar design – all working to enhance alarm system capabilities for both homeowners and small businesses.

Tapping into the industry trend of using external passive infrared (PIR) detectors for video verification, the detector protects a property with

innovative technology for precise detection and video verification.

In these scenarios, false alarms are often triggered by anything from bad weather to leaves or branches to pets. The answer to deal-

ing with these is to be able to identify them and ignore them as 'non-threats'. As its name suggests, a Wireless Triple Signal Detector uses three sensors: a PIR sensor at the top, a microwave sensor, and another PIR sensor at the bottom.





tity information on record in the access control system database from anywhere, record entries and exits where door readers are not practical or available, challenge credentials from within secured spaces, spot check permissions to deter tailgating/piggybacking, quickly muster employees during an emergency evacuation, maintain facility occupancy information, and much more.

XPressEntry is a powerful tool that provides information stored in companies' access control databases on a handheld, mobile device that may be used anywhere. XPressEntry is already a

proven, fast, and reliable emergency mustering solution that integrates with 30+ access control systems. Each XPressEntry reader can scan 200-250 security badges and complete a mustering event in 10 minutes or less.

Now with facial recognition, XPressEntry even further accelerates mustering in an emergency evacuation by being able to scan a group of faces at an assembly area all at once and accounting for them as safely evacuated. In addition, XPressEntry supports entry/exit tracking, time and attendance, managing confined spaces, events and train-

ing, bus entry validation, guest/visitor tracking, remote parking, mobile enrollment, and more.

Founded in 2005, Telaeris, Inc. is a US-based software company, specializing in handheld and hands-free safety and physical security solutions to enhance access control and occupancy tracking systems. Telaeris' XPressEntry is a hardware and software solution that seamlessly integrates with any industry-leading access control system, providing fixed, kiosk, and handheld devices capable of reading any badge technology, biometrics, and facial recognition.

## Rapid Gunshot Response in Campus Security

Law enforcement professionals rely on gunshot and weapon detection technology in many municipal and public settings in the United States. In many ways, the university and college campuses are not unlike other public locations when considering security.

Four new technologies are in use:

1. Audio Detection and Triangulation of Sound Matching a Gunshot Profile
2. Computer Vision That Identifies a Firearm from Video Images
3. Advanced Sensor Technology and Artificial Intelligence Weapons Screening

location of the weapon when fired. Responding security teams need to know where to start looking for a potential shooter. They also need to know what they might be walking into upon arrival. Knowing where the shooter might be is critical information for first responders.

### Weapons Detection

Milestone Systems partners with technology companies to leverage their artificial intelligence (AI) to work with XProtect. Weapons detection technology is relatively new, using computer vision to identify a weapon from a camera. The software confirms the presence of a gun. Furthermore, it works along

works quickly to verify and provide for an accurate assessment.

### Muzzle Flash Detection

Muzzle flash detection applications analyze live video feeds for visible or infrared light signatures generated from weapons fire. The software confirms the muzzle flash is from a gun and triggers a security response.

### Adding Value for Campuses

Colleges and universities find that detection systems can be surprisingly affordable and add value to existing security and surveillance infrastructure. Campuses are rapidly adopting this technology to provide ad-



## New Id-Gate boxed solution to upgrade ACS

RecFaces, an international developer of smart biometric security, has recently presented Id-Gate – software that significantly expands the functionality of Access Control Systems, improving security by verifying visitors in under a second.

Designed to verify access rights of a company's employees and visitors, Id-Gate uses biometric face identification instead of unreliable key- and RFID-cards. Upon entering the facility, each person's face is compared with a profile database. If it complies with the company's profile database, the person is allowed in; otherwise, the system immediately denies access.



Id-Gate has solved access control tasks at a manufacturing plant in Guatemala. Not only does the system provide quick access opportunities, but it also records the arrival/departure time and the total time spent on the premises, which was also one of the most important requests. These features make Id-Gate highly in demand among construction companies that implement biometrics in their smart offices and buildings. This solution allows them to make modern offices even more comfortable, innovative and safe.

Id-Gate has ready-made integrations with the world's security manufacturer of ACS's. They are included in the total price of the Id-Gate's licenses without extra fees. Thanks to seamless integrations, security operators work in the familiar interface of ACS with new full-featured biometric capabilities. Moreover, RecFaces's team can provide an open API for integration with third-party systems.

RecFaces is a software developer of facial recognition solutions that are simple, applicable and easily integrated into existing VMS, ACS, CRM, etc. Their quality has been proven by numerous installations around the world, including the MENA, APAC, and LATAM regions. With its global partners, RecFaces

delivers solutions to security, transport, retail and financial industries, as well as other areas, providing free training and demos on the company's products.

You can try a demo of the high-end facial recognition solutions for free!

For more details scan the QR



4. Video Analytics That Detect a Muzzle Flash from a Firearm

### Gunshot detection

Gunshot detection technologies depend upon an array of microphones to detect sounds that match the sound profile of weapons fire and measure the differences of the same event recorded on different microphones to hear the gunshots using frequency sound patterns and percussion.

XProtect® open platform by Milestone Systems, works with technology partners to provide alerts to your security team via the video management software (VMS). The VMS sends notifications to smart devices via text messages or email notifications, providing rapid response when the event detection occurs. Remote operators can also access XProtect on phones, tablets, or laptops to improve real-time situational awareness while in the field.

With the use of multiple audio sensors, advanced systems can triangulate the approximate

with XProtect VMS to alert appropriate personnel. The applications analyze live video and monitor for the appearance of a weapon so that they can use caution, keep the public safe, and respond appropriately.

Some of today's technology relies on sending alerts after seeing or hearing the weapon. But what about early detection and screening in areas where traditional metal detectors and property searches don't make sense?

Unlike traditional metal detectors, some companies use advanced sensor technology and artificial intelligence to screen guests without stopping or handing over their belongings as they walk past sensors. When a weapon is detected, XProtect alerts security officers who can initiate contact with people to search for firearms and take necessary precautions.

Companies using artificial intelligence for object detection rely on advanced analytic algorithms to detect specified objects in video, including guns or knives. AI

ditional protection in the public gathering areas, such as sporting venues on their campuses. Additionally, some schools offer alert notification and system access to local police precincts to speed response and remediation in an active shooter event on their campuses.

Milestone works alongside partners and system integrators to provide high-quality and scalable solutions on school campuses around the world. The safety of the faculty, students, and guests on your college or university campus is worth the investment to give them the peace of mind they deserve when they visit your campus. Milestone XProtect VMS can make your campus a safer and more secure environment, providing your security team with speedy detection of incidents and the opportunity to provide for rapid remediation of any threats or incidents that happen in your space.

*Credits: Milestone Systems, a leading provider of open platform video management software.*



# Ambarella launches 4K, 5nm edge AI SoC for mainstream security cameras



Ambarella, Inc., an edge AI semiconductor company, has announced the CV72S 4K, 5nm AI vision system-on-chip (SoC) for mainstream professional security cameras, built on its latest CVflow® 3.0 AI architecture.

That architecture allowed Ambarella to create this new CV72S SoC with the security industry's highest AI performance per watt and fusion of radar and camera data, for better nighttime and all-weather AI perception. Its dedicated AI hardware efficiently runs the latest transformer neural networks (NNs), which now outperform convolutional NNs for many vision tasks.

Additionally, the CV72S offers 6x greater AI performance than its predecessor, enabling it to also run Ambarella's groundbreaking AISP for neural network-enhanced 4K, long-range colour night vision and HDR at very low lux levels with minimal noise and no external illumination, while leaving plenty of headroom for additional, concurrent NNs (e.g., person tracking and mask detection).

As a result of the CV-flow architecture's efficiencies, combined with 5nm process technology, the CV72S consumes less than 3W of power, offering the mainstream security market's highest

AI performance per watt.

The growth of infrastructure cameras powered by a processor with advanced AI acceleration is expected to increase significantly in the coming years, with a CAGR22-27 of 23%.

Through its deep understanding and experience in the security market, Ambarella designed the CV72S to also enable higher-end cameras with advanced 16MP30 fish-eye dewarping and 4x 5MP30 multi-imager AI capabilities.

For single-imager cameras, the CV72S supports 4KP60 encoding for AVC and HEVC—a 2x performance increase over its predecessor. These features are ideal for a broad range of mainstream security cameras, including smart city and traffic applications, as well as monitoring crowded areas (e.g., retail stores, malls and stadiums).

Additionally, the CV72S provides rich details for human viewing while enabling advanced

video analytics such as long-distance object detection and licence plate recognition.

Ambarella's in-house Oculii™ virtual aperture imaging (VAI) AI radar technology equipped the company with the know-how to integrate hardware acceleration into the

CV72S for fusion with camera data, as well as dynamic load switching between radar and cameras.

Ambarella's Oculii technology features 10-100x better radar resolution than any other radar solution on the market today. These radar capabilities are particularly important for applications such as perimeter security and nighttime monitoring, as well as any system that needs to operate in rain, snow or fog.

Additionally, radar can accurately measure the distance, speed and direction of separate objects over a long range, for applications such as traffic cameras. Other features of the new CV72S SoC include a 2x increase in CPU performance over the prior generation, via dual Arm® Cortex-A76 1.6GHz cores. It also features 2x the DRAM bandwidth, with support for 32-bit LPDDR4x/LPDDR5/LPDDR5x DRAM.

Additionally, this SoC integrates hardware security to prevent hacking, including secure boot, OTP and Arm TrustZone technology. The CV72S also has new high-speed PCIe and USB 3.2 interfaces, enabling more complex, multi-chip security system designs.

Ambarella's CVflow AI development platform provides a full set of tools for easy porting, and supports all common CV frameworks. With its rich set of features, as well as Ambarella's tools that are compatible across its entire AI security portfolio, the CV72S lowers design costs and maximises software reuse.

delays inherent in some other PTZ solutions, delivering unmatched situational awareness for outdoor sites.

Powered by AI-based classification analytics, IR illumination, 33x optical zoom, 360-degree pan, and a 5MP imager with excellent low-light performance, Sighttracker

PTZ is ideal for the outdoor PTZ market.

Sighttracker PTZ is available right away and

suggested application uses are for protecting utilities and substations, data centres,

transportation assets, or any commercial site vulnerable to outdoor theft and vandalism.

## BriefCam releases 2023 M1 version of its video analytics platform



BriefCam has announced the release of version 2023 M1 of its video analytics platform. With this version, BriefCam debuts its Custom 'ClassifID' solution, and also introduces optimizations to the platform's infrastructure, real-time performance and accuracy, as well as new features to enhance usability and investigation efficiency.

With Custom ClassifID, organizations can define additional object classes for video search, alerting, and intelligence, on top of the set of detected classes available in the BriefCam Video Analytics Platform. With environment-specific classifications – such as unique vehicle types or uniformed employees – users can independently tailor the video analytics technology to meet their specific and evolving

needs at scale without sending data off-site or outsourcing classifier network training.

BriefCam has also improved usability for the existing and ever-expanding set of metadata classes and attributes that can be searched, alerted on, or visualized for analysis and decision-making, the company reports. The enhanced UI includes new customer-driven capabilities designed to accelerate video investigations and drive efficiency across the platform.

The strength of BriefCam's solution is in the extensibility of its analytics capabilities across the platform for accelerated video search, real-time alerting, and data visualization and analysis. Beyond the user experience, BriefCam notes

that it has bolstered its technology with a significant infrastructure improvement to drive increased performance, accuracy, and speed for real-time channels.

The company reports that users upgrading to 23 M1 leveraging the existing Windows-based infrastructure and hardware can expect an optimized throughput of up to 25% for real-time and on-demand channels; those upgrading to the Linux-based infrastructure will realize 100% increased throughput for real-time channels: This means that users can confidently and accurately analyze more video data in real-time, including leveraging real-time channels for instant video review and investigation, with less hardware and a lower total cost of system ownership.

## Broaden surveillance horizons with Geovision

Has the user ever installed cameras to monitor a parking lot or any other large indoor space? Can a single camera cover a wide angle and maintain surveillance over a large area?

GeoVision would like to present Panoramic IP Cameras which are equipped with a single 8MP lens providing a 180 Degree Panoramic View giving an increased coverage area. No dewarping or stitching of multiple lenses is required, as the camera's native view is

already a 180-degree panoramic view.

Furthermore, when connected to the GeoVision VMS V18 software platform, these cameras can perform AI Perimeter Protection & Classification (Human, Vehicle), real-time alerts, events playback, and more. Additionally, these cameras can be used with third-party VMS platforms to provide 180-degree coverage.

With the help of a single camera, it is possible to cover a large area which reduces

hardware and installation costs. This is an ideal solution for monitoring warehouses, loading bays, or any open area that requires wide-angle coverage.

Features include: 8MP H.265 (Up to 25 fps at 3840 x 2160), 180° panoramic view, Built-in microphone, IP67 & IK10 protection rating, IR distance up to 15 m (50 ft), AI deep learning - AI Perimeter Protection and Classification (Human, Vehicle).

# Sightlogix launches smart edge AI camera with automatic zoom

The new Sighttracker PTZ from Sightlogix is designed as a smart camera with Edge AI that automatically zooms and follows outdoor intruders with fast, on-target responsiveness.

By embedding Sighttracker software and AI classification analytics inside high-perfor-



mance PTZ, the camera offers automatic tracking of targets without latency or the network





# Security And Fire Expo

West  
India

18 - 20 MAY 2023  
Hall 2, BEC-Mumbai



**BEYOND THE TRADITIONAL  
APPROACH WE ADDRESS  
ALL YOUR SECURITY CONCERNS**

## KEY PRODUCTS



Surveillance Cameras  
with Night Vision



Digital  
Video Recorders



Encoders &  
Decoders



Security Alarm  
Systems



Audio Video  
Door Phones



RFID  
Systems



Baggage  
Scanners



Biometric  
System



Access  
Control



Electronic  
Locks



Entrance  
Management  
Solutions



IOT &  
Home Automation



GPS  
Tracking



Parking  
Automation



Anti- Theft  
EAS Systems



Security  
Gates



Peripheral  
Accessories



Storage  
Devices



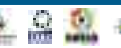
Perimeter Intrusion  
Detection Systems



Artificial  
Intelligence



UAV  
and Drones



**CONTACTS:-** **BENGALURU:** Sanjeev Rao, Project Director | M: +91 98452 93126 | E: sanjeev.rao@informa.com  
**NEW DELHI:** Sanjay Khandelwal, Assistant Project Director | M: +91 98117 64515 | E: sanjay.khandelwal@informa.com  
**MUMBAI:** Rajeev Jain, Sr Project Manager | M: +91 99877 90776 | E: rajeev.jain@informa.com

[www.safeindiaexpo.com/west](http://www.safeindiaexpo.com/west)

Media Partner





# Cozaint BOBBY kiosk implemented as safe zone security tower at Arizona Tribal Police Station



Cozaint Corp, the developers of intelligent surveillance solutions, has been selected by the Pascua Yaqui Tribe Police Department in Tucson, AZ, to deliver the BOBBY physical security tower to provide a “safe zone” location for local citizens to conduct sales transactions, custody transfers, or other dealing where a security monitored area would provide a safe setting.

Cozaint’s BOBBY platform of physical security kiosk tower provides 24/7 situational awareness for organisations of all sizes with various IoT security sensors, constant video surveillance, and tied to a remote monitoring centre.

The Cozaint BOBBY kiosk tower also has a 27” interactive display that displays information about local tribal

activities as well as allowing for visitors to activate a “panic button” if they feel threatened. The BOBBY “safe zone” tower is connected to the tribal police department where officers can see and speak with the user to determine if an emergency exists and how best to respond.

“With certain transactions occurring between complete strangers — such as online sales— sometimes our community may wish to meet at a more secure location where video surveillance and the ability to reach one of our officers in an emergency is all in one safe zone,” said LT. Elizabeth Esparza of the Pascua Yaqui Police Department.

With 360-degree video surveillance coverage and 24/7 video recording, the BOBBY safe zone tower delivers the peace of mind that the Pascua Yaqui Police Department and its citizens are looking for to safely meet others with eBay or other sales transactions, when custody transfer events occur, or other

interactions where a safe and monitored location is preferred.

“Our BOBBY tower unit is an ideal community safe zone security platform, where users can rest assured that they are being monitored for safety and security reasons when dealing with various transactions with others in the community,” stated Jay Jason Bartlett, CEO, Cozaint, adding “Interacting with the Pascua Yaqui Police team in the event of an emergency provides an additional level of security for the local community.”

The BOBBY tower unit also displays local community information as well as current events, helping to keep the community up to date on what is happening throughout the tribe.

This particular BOBBY tower unit is located on tribal land in the desert of Tucson, AZ, where the summer rains and high temperatures create harsh operational conditions for an outside device such as this.

and to keep the old system working at the same time as the new installation was taking place. This was to ensure the security and safety of our residents at all times.”

“We worked with IDS right from the initial design stages to identify a solution. Comelit-PAC was recommended not only to accommodate the installation process but also to ensure a high-quality finish, with door entry panels and monitors that could blend with the aesthetics of the development. The system is also flexible enough to accommodate the integration requirements to ensure a seamless security experience for our residents and guests.”

Comelit-PAC specified its Simplebus 2 wire system, allowing the installer to utilise the existing cabling so the site could have the old and system working at the same time to maintain the security for the site. The solution was completed with Comelit-PAC’s ultra-digital entrance panels.

Each apartment now features a Comelit-PAC mini hands-free monitor with a custom adapter plate, allowing homeowners to benefit from instant intercom control and video door entry capability.

## IDIS enables hybrid surveillance upgrade for hypermarket chain



IDIS was chosen by Prisma’s chain of hypermarkets in Finland to implement a video surveillance upgrade to tackle shrink and improve system usability at four of its hypermarkets. The huge retail chain opted for a hybrid solution integrating many third-party products to improve their centralised view of operations and cut shrink.

Prisma’s existing surveillance system had been expanded and added over the years and encompassed more than 150 third-party analogue cameras to provide coverage in four malls – the Prisma Vaasa, Prisma Kouvola, Prisma Tripla and Prisma Kristiine.

Operating the system had become very challenging, with significant latency impacting

camera control and no complete, “single pane of glass” overview of the system or sites.

Image quality and speed of the third-party video wall in the central control room were also issues that hampered their security team’s ability to track suspected thieves.

Working with systems integrator, Safe IT, Prisma opted for IDIS Solution Suite (ISS) VMS to facilitate a simple integration and deliver comprehensive coverage. ISS comes with easy-to-use live video streaming, management, and administration tools and the ability to seamlessly integrate third-party cameras from a single user interface.

The flexibility of IDIS Solution Suite was

# Comelit-PAC’s latest integrated video door entry systems deployed at Cardiff's Landmark Place



Comelit-PAC’s latest integrated video door entry systems have been installed at premium development, Landmark Place, a 16-storey building that comprises predominantly residential dwellings, with retail at the ground and first floors.

Located in the heart of Cardiff city centre, Landmark Place was the city’s first skyscraper development, which features 280 high-end apartments, mixed-use luxury facilities and a 24-hour concierge service.

Comelit-PAC was specified via main fire

and security specialists - IDS Fire and Security, to integrate necessary door entry systems across the development, incorporating main site access and car park entrance systems, together with video calling capability for all apartments and fully shared network fa-

cilities.

Says a Director, who represents the Section 20 Committee for Landmark Place: “There was a definite need to upgrade our legacy door entry system, but what was critical was the requirement to use our existing cabling infrastructure



in evidence as Safe IT used an analogue and IP mix-and-match approach of new IDIS cameras while retaining existing third-party NVRs and legacy models. The cameras were rapidly and easily connected using a third-party encoder

while improving system performance.

An IDIS video wall was deployed to provide live and centralised monitoring capabilities, enabling rapid identification, tracking, and rapid response to potential

threats with operators benefitting from IDIS Smart UX Controls.

IDIS tech is providing Prisma with an improved user experience and enhanced security. In addition, IDIS technology gives Prisma the

best total cost of ownership (TCO) with single one-off, upfront licensing and has allowed the hypermarket chain to extend the life cycle of existing equipment to improve sustainability and realise a rapid return on investment.

## Dahua Technology provides video-based security system to enhance security for an injection moulding production facility in Mexico



A site-wide and extensive video-based security system from Dahua Technology has been installed at an injection moulding production facility in Mexico. The 40,000 m2 Haitian International site in Jalisco needed perimeter protection, access control and site video monitoring to provide security and the efficient management of the site.

The remote location and sheer size of the site and its perimeter provided managers at Haitian International with security and infrastructure challenges. Installation challenges included the remote location of the site with its lack of infrastructure, the size and complexity of the installation – including the provision of a wireless

network – and the sheer range of Dahua products and systems, including a range of internal and external cameras, perimeter protection sensors, access control hardware and software, and time and attendance systems.

A whole host of security, surveillance monitoring and access control systems were installed by installation company Aldo. This includes: pole-mounted IR dome, speed dome and other network cameras for intrusion detection; wall-mounted IR speed domes, and eyeball cameras for external video surveillance; and quad beam fence-mounted detectors (and network cameras) for long distance perimeter protection.

One notable solution

implemented in the production site is the access control comprising several integrated Dahua products. Two ANPR cameras (DHI-ITC215-PW6M-IRLZF) were installed at the parking entrance to manage incoming/outgoing authorised vehicles.

Dahua also provided a personnel access control system that includes turnstiles at the main entrance gate that can be activated by security cards. Swing barriers (ASGB510J-L, ASGB520J-D, ASGB510J-R) were also installed at the administrative building entrance to facilitate the access of employees, guests and other visitors in the building.

There's also an attendance terminal (ASA2212A) with a fin-

gerprint identification module at the lobby for quick and easy clock in/out, which is managed by an interface that is completely made by Dahua.

The installation also included: a video entry system for the administrative building; individual door entry access points at certain doors; a video wall consisting of four 55-inch screens; and a PTZ keyboard with joystick.

Internally there are 106 cameras – a mix of IR dome, eyeball, panoramic, mini PTZs and other network cameras – to monitor the production line, public area and administrative building.

Managers at Haitian International now have the assurance of a highly secure site, thanks to a comprehensive and integrated security system from Dahua Technology. In addition, they are now running an efficient and safe operation using state-of-the-art technology in a seamless fashion. This delivers high levels of security and efficient access control and vehicle management solutions to help with the smooth running of the facility.



all aspects of the access control and biometric systems are fit for purpose and will respond quickly as and when re-

quired. This is all without disturbing the care home facilities or the essential services they offer.”

## Improved fire safety at Middle Eastern oil and gas company



The critical national infrastructure of a Middle Eastern oil and gas company is being protected by new systems. More than 40, 4- and 16-loop Taktis fire detection panels have been put in place by Khayber Fire and Security Systems WLL, a turnkey contractor of fire and security systems based in the Kingdom of Bahrain.

The Taktis panels are manufactured by life safety systems company Kentec Electronics.

The Khayber Fire and Security Systems WLL Team working on the project noted it was one of many projects completed in the region using Kentec panels.

Kevin Swann, MD of Kentec, says this project is one of Taktis' most globally significant installations. He said: “With more than 60 buildings, linked to sev-

eral thousand devices, the fire protection system is one of the world's largest and most complex.

The ongoing installation project features 41 panels, of which 32 are a part of one ring network. In the next stage of the project, Khayber is working with Kentec to utilise Vizulinx, a fire alarm management solution that facilitates the integration of the Taktis system with the plant DCS via Modbus signals.

This enables site managers to monitor and control fire detection systems remotely, in real time through the DCS graphic. The Taktis 16L provides up to 144 zone indications, supports more than 2,000 detection devices and can network up to 127 panels.

## Integrated Protection Maintenance Services (IPL) announces partnership with WCS Care

Integrated Protection Maintenance Services (IPL), an Amthal Group company, is pleased to work with WCS Care, for the ongoing safety of staff, residents, and visitors. WCS is a registered charity and runs 13 care homes across Warwickshire, UK, eleven offering residential and short-term respite care and a further two for younger adults with physical disabilities or long-term conditions.

IPL currently provides maintenance to three of WCS's homes for their biometric access solution, Castle Brook, Woodside Care Village, and Fairfield.

On three sites, IPL has installed and now maintains an integrated Paxton access control solution to operate through its dedicated building management system. The system is simple to operate and seamlessly blends with

its surroundings to ensure staff and residents can operate everyday routines.

Ally Keating, IPL Senior Technical Engineer, said “Care homes have unique requirements when it comes to security. By their very nature, they want to create a welcoming environment, yet at the same time, it is where dependent and often very frail individuals live.”

She adds, “Keeping them safe, without impacting their everyday requirements, or their carers and visitors, is paramount.” Ally Keating continues, “For us, as part of our commitment to customer excellence, we create a scheduled maintenance programme with charities such as WCS, who provide exemplary good care.”

She adds, “We work in partnership to ensure



# viisights proactive behavioural recognition video analytics deployed at the headquarters of the Tata Group



viisights, Inc., a global pioneer in behavioural recognition video analytics, announced the deployment of viisights Wise™ and related software products at the headquarters of the Tata Group in Mumbai, India.

This security system upgrade involves dozens of cameras and will enhance perimeter protection, support occupancy analysis, and improve the early detection of suspicious activity and safety-related events such as outdoor fire and smoke. Tailgating detection, for alerting on unauthorised access, will be deployed later this year.

These improvements demonstrate the value

that Tata management places on the safety and security of staff and visitors, as well as on the preservation of the historic Bombay House that serves as their corporate headquarters.

Tata Group is a global leader in many industries, from steel to power to airlines, and they understand the value of proactively ensuring safety and security.

The Associated Building Co. is the Tata division that owns Bombay House. In the 2010s, Tata upgraded Bombay House to become the first heritage structure in the country to achieve a Gold rating from the Indian Green Building

Council. Implementing viisights Wise to help protect Bombay House is the essential step to continue moving forward.

Designed for fast and cost-efficient deployment, viisights behavioural recognition video analytics leverage investments in existing video systems to autonomously detect and issue real-time alerts on unsafe conditions and security incidents so they can be addressed before they cause injuries or losses.

viisights' unique video understanding technology utilises deep neural networks to analyse video streams from existing video camera systems to automatically detect

developing security and safety risks, and real-time issue alarms to authorised personnel to take remedial action.

The early notification of upcoming and real-time events of interest enables responders to take faster action, effectively reducing or eliminating negative outcomes from potentially threatening or harmful events.

viisights intelligent behavioural recognition video understanding technology is currently deployed in critical applications around the world, helping create safer and more secure facilities and workplaces.

# Johnson Controls' video solution ensures safer school environment

It may sound like a small change, but installing security cameras on a property can significantly impact occupant and visitor behaviour by enabling more accountability.

This is notable for environments such as K-12 schools where occupants are younger and more impulsive.

A public school system on the East Coast of the USA faced frequent incidents of bullying, vandalism and theft among students as well as the harassment of faculty and staff and was struggling to keep its occupants accountable.

The lack of visibility in back parking lots or school pick-up areas prevented administrators from monitoring student whereabouts and activity on school grounds both during and outside of learning hours.



In addition, members of the general public were often walking through school property when students were outside, making it more difficult for staff to control and oversee these high traffic areas to ensure students are safe from strangers and not misbehaving.

The school leadership brought in Johnson Controls (JC) to install solutions to mitigate these problems.

The JC team conducted a careful audit of the situation, meeting with principals from each school in the district, who walked them through the campus to identify problem areas. The team also brought the customer to their Customer Experience centre in Austin, TX to discuss all the possible solutions available that would meet their needs.

The school and Johnson Controls determined that the way to address the issue at hand was

through heightened video surveillance.

They installed several cameras of various styles – fish-eye, 4-way and PTZ – to monitor the environment and reduce potential blind spots in problem areas. By maintaining open communication with school district officials, security service professionals for the school district and county commissioners, JC was able to ensure that the project stayed on track with its timeline throughout its duration.

Although their No. 1 priority was security, school district leaders sought to add thermal cameras, portable air filters and access control solutions as well to create healthier and more productive learning environments for students, teachers and staff. As anticipated, the school

district was able to reduce vandalism, harassment, bullying and loitering by increasing visibility and accountability.

With the new video system, there are minimal blind spots, allowing school administrators to identify the perpetrators creating issues on campus. In addition, theft of school property has reduced to almost nothing and the few incidents that did occur post-installation were easily identified on the cameras.

All occupants, including students and faculty, are safer on campus and have peace of mind knowing their belongings can be kept safely on school property. As a result, the school district was able to create a more productive and welcoming environment to teach and learn and leaders within the district can focus on their primary mission of educating and empowering.

# Homelessness charity enjoys safety and security improvements at community home



A building which hosts a homeless charity in Bolton has had an intruder system updated by Texcom. The community home run by Emmaus Bolton now has repaired personal call-out buttons for each of the bedrooms, new keypads, panel, external

detection and bell boxes.

The new system means residents are designed to have access to support by use of a call-out button, alerting a central control system and members of staff at the homelessness charity.

Emmaus Bolton provides up to 22 people with a home, support, training and the focus of supported work each day in different shops and services within its grounds in the town, according to the vendor.

As well as private

bedrooms and bathrooms, the residential part of the building contains community kitchens, a dining area, lounge and games room, gym, computer suite and meeting rooms.

The installation and setup of Texcom Connect 4G and end-user mobile app is designed so that multiple staff can be notified of alerts and respond, providing more protection for the site and its residents.

The site is now said to be self-maintained and remotely monitored by the installation company using Texcom Cloud services without the 'necessity' to visit the site.



# Aviotec video-based fire detection wins another award



At the Finest Skills & Talents (FIST) Awards 2022 in the Indian capital Mumbai, the Aviotec innovative video-based fire detection technology from Bosch was recently named Product of the Year in the Fire Detection category and presented with the renowned FIST Award – India’s number one fire safety and security accolade.

“Bosch Aviotec is the latest and fastest way of detecting fire as compared to any traditional fire detection system. The AI-based algorithms enable detection of flames and smoke in no time, resulting in the saving of lives and assets,” says Pankaj Dharkar, who is on the panel of judges and a member of the Advisory Council of the Fire and Security Association of India (FSAI). This organisation

presents the awards annually, together with the PwC auditing and consulting firm.

The FIST Award 2022 takes the number of prestigious awards Aviotec has received to seven. The highlight to date in terms of international accolades, it has given the team responsible a particular boost. Its speed and accuracy make Aviotec a particularly reliable and innovative smoke and flame detection solution, even in difficult conditions such as industrial environments with high fire loads, vast buildings with high ceilings, and protected outdoor areas. This is possible thanks to video analysis controlled by AI algorithms that visually detects smoke and flames directly at their source.

As a result, Aviotec

reacts much faster than conventional ceiling-mounted fire detectors where the smoke has to rise far enough before the alarm is triggered. This speed is a vital advantage when every second counts. Safety and security personnel can verify the alarm in the video image and pinpoint the exact location of the fire.

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

ignated smoke areas still the risk may arise if rules are not followed

- Poor housekeeping. The clutter or waste material lying around, and hazardous chemicals not stored properly can lead to an untidy workspace which in turn can cause fire hazards

## Fire Safety Checklist

Below are some recommended steps to follow the appropriate fire safety checklist:

### 1. Cleanliness

Proper housekeeping of the workplace is one of the most important and recommended steps to control and minimize fire hazards. Employers must encourage their staff members to tidy up their work areas. They are also required to store the waste and combustible material properly and follow proper cleaning practices, and safety guidelines to minimize fire risks.

### 2. Electrical Safety

Taking measures to prevent electrical hazards leading to fire risks is also crucial to maintain workplace safety. Never leave electrical appliances unattended and don’t forget to turn off the switch when the equipment is not in use. Employers are also required to conduct regular tests for electrical devices and equipment to ensure their proper use.

### 3. Storage

It is a significant step to follow when it comes to fire safety at work. The responsible persons must check the fire door exists,

fire equipment, and fire notices to ensure they are unobstructed. Storage areas must be accessible to firefighters and inspected regularly to ensure safety.

### 4. Flames & Fires

Keeping a check on flames and the sources of ignition in the workplace is also important when it comes to minimizing fire risks at work. Employers must provide designated smoke areas for their workers to smoke outdoors, and the cigarette buds are properly extinguished to mitigate any kind of danger.

### 5. Flammable Liquids

Keeping flammable liquids and chemicals safe is also an effective fire prevention approach. They must be stored in secure and dry places with appropriate labels to make employees and workers aware of the severity of the hazard. They are also required to be kept away from the potential sources of ignition.

### 6. Fire Protection Equipment

The responsible persons or employers are also required to inspect and maintain their fire safety equipment regularly this includes fire hydrants, fire alarms, fire extinguishers, and sprinklers system. Employers are also required to undertake routine checkups to minimize any obstruction in emergency exit routes or fire doors.

### 7. Staff Training

Along with the above-mentioned steps, adequate

staff training is also very important to raise fire safety awareness among staff members. There are numerous training options that employers can offer their employees and work online and on-site depending on their requirements.

The popular courses in this regard are fire awareness training, fire safety training, fire risk assessment training, fire door inspection, fire warden training, or other relevant training sessions. These training courses teach employees the basics of fire safety in the workplace and help them take reasonable actions in an emergency.

Fire hazards can occur at any time and in any work environment that leads to a catastrophic impact on businesses and their employees causing severe injuries or even deaths. What needs to be done is to have proper fire safety arrangements with appropriate control measures to identify potential sources of ignition in the workplace and implement vital controls to minimize the risk of fire hazards.

Employers are also required to take account of their staff training needs and arrange proper training sessions to create fire safety awareness among them and teach them how to keep themselves and others around them safe. This piece of content has covered some of the basic yet important steps to implement to ensure a safe and secure work environment for everyone.

## What should a fire prevention checklist include?



Well-organized and carefully maintained work premises are safer from any type of major workplace hazards, fire hazards are no exception. Having adequate fire prevention approaches and safety checklists helps lessen the likelihood of fire breaking out in the workplace. This blog post, therefore, will explore potential fire hazards at work and what a fire safety checklist must

include in reducing fire risks.

### Common Fire Hazards at Work

Whether we realize it or not, every workplace has potential fire hazards that need timely protective measures before the situation gets worse.

Below are some common hazards to occur:

- Faulty electrical equipment. Faulty electri-

cal equipment is one of the major causes of severe fire hazards at work that requires regular testing to identify and mitigate any such risks

- Flammable liquids. Flammable liquids like cleaning products in work environments like warehouses, industries, or offices also have the potential to cause fire hazards that must be kept and stored correctly to minimize the health hazards

- Waste or combustible material. Waste materials like cardboard or paper in the workplace can also build up leading to dangerous fire hazards even from smaller sparks

- Smoking. Smoking on the work premises is also a potential source of workplace fires. Although most workplaces have des-

## Ministry Of Heavy Industries launches first-of-its-kind training programme on e-bus fire safety with GIZ, CFSL and ASDC

John Davidson, the National Security Inspectorate’s Approval Schemes Manager, provides practical help to those responsible for fire safety in flats and their residents on how to avoid hazards and implement important ‘housekeeping’ measures.

Multi-occupied residential buildings, namely those containing flats, are subject to increasingly stringent fire safety measures. The 2017 Grenfell tragedy has been a catalyst for the introduction of positive and important measures to better protect tenants from potential hazards. But what are the main risks involved, and how can they be minimised?

One of the biggest dangers in any purpose-built block of flats, or a building that’s subsequently been sub-divided into flats with communal areas including hallways and staircases, lies in the risk of fire breaking out within one of the flats. Containment of any such fire is essential, to ensure it doesn’t spread into communal areas and impede the safe exit of tenants, residents and visitors.

### Fire doors

Recognising the importance of such measures, the Fire Safety Act 2021 (applicable in England and Wales) requires mandatory fire risk assessments for buildings containing two or more flats to include any entrance doors to flats

opening onto communal areas. In practical terms, this means specifying, installing and maintaining an FD30 (30-minute fire resistance) front door. Depending on the circumstances, an FD60-rated (60-minute) front door may be required instead.

Fire-rated doors comprise elements including a self-closing mechanism, three hinges, and intumescent seals that expand when exposed to heat – thus closing any gaps between the door and the frame to protect those evacuating a building. Fireproof letter boxes are also required, using similar intumescent seal flaps. All fire doors fitted must have the appropriate proof of performance for the rat-





ings they carry, tested by a UKAS approved certification body to either BS 476 Part 22 or BS EN1634-1.

On 23 January 2023 the Fire Safety (England) Regulations 2022 legislation took effect in England, which includes a requirement affecting those responsible for fire safety of residential buildings over 11m in height to carry out annual checks of flat entrance doors and quarterly checks of all fire doors in the common parts.

Communal areas' 'housekeeping'

Good practice practical fire safety 'housekeeping' measures adopted within any building containing flats will help ensure that hazards are avoided. These actions should be combined with effective maintenance regimes, including regular testing of emergency lighting.

To optimise safe and speedy evacuation of residents and visitors from a building, there should not be any obstructions and/or trip hazards within communal areas. These can include the accumulation of potentially combustible uncleared rubbish and inappropriately stored items, as well as unsafe storage of material within cupboards. These areas must therefore be regularly monitored and any items removed when required.

Depending on the building's height, automatically opening smoke vents may be installed and their operation should also be regularly tested in accordance with any manufacturers' recommendations.

Equally, an appropriate inspection and maintenance regime for dry and wet risers should be overseen by a competent service provider, given the vital role these systems of valves and pipework play in providing a readily available means of delivering considerable quantities of water to extinguish or prevent the spread of fire.

Firefighting lifts may also be installed in larger or complex buildings, as a dedicated means of assisting firefighters. Specific regulations apply to equipment including an independent power supply and smoke extraction capability. In such circumstances, it's important to ensure that specialist lift maintenance schedules are in place covering their operational capability in the event of an emergency. Monthly checks are now required by law, in England, for firefighters' lifts within high-rise residential buildings.

Mobility and other e-scooters/bikes represent a potential fire safety issue, since they require regular electrical charging. Charging of this type of equipment should only take place in dedicated charging areas or within the tenant's flat.

By contrast, the inappropriate use of extension leads trailing through front doors and charging of mobility scooters and e-scooters/bikes cannot be allowed in communal areas, given the fire safety implications – particularly from potentially combustible lithium-ion batteries.

According to the London Fire Brigade, the majority of fires related to e-bikes and e-scooters have happened in homes and are often caused when charging batteries, due to factors including overcharging and use of batteries and chargers not compatible with the equipment in question.

Fire risk assessments for flats

Where 'life safety fire risk assessment' (LSFRA) for flats, or communal areas in blocks of flats is required by national legislation it underpins fire safety arrangements across the board.

These assessment findings are implemented by a 'legally identified 'Duty Holder' (sometimes called 'Responsible Person'), who may be one of a num-

ber of possible persons, e.g. the contracted residential managing agent, to help ensure people and premises are kept safe. In reality, any freeholders' company director(s) will also ultimately be responsible in law.

In practice this means fire safety shortcomings identified by a LSFRA must be carried out in full, as specified, with their recommendations being completed within the stipulated time frame. The results of an LSFRA may require, for example, the implementation of fire safety protections including fire detection, extinguishing and alarm systems, and emergency evacuation procedures – depending on the size and height of the residential building involved.

Competent service provision

Fire safety requirements, and the need for providers to demonstrate their competence, are becoming more stringent every year as post-Grenfell weaknesses and loopholes in previous measures are addressed.

Third-party certificate providers, who are independently approved/assessed, can provide significant reassurance for flat owners, tenants and landlords, as well as those tasked with managing buildings containing flats. Holding approval from a UKAS (United Kingdom Accreditation Service)-accredited independent certification body such as NSI demonstrates fire safety providers' competence, clearly verifying their services are compliant with current appropriate industry standards and best practice.

Choosing independently approved service providers who meet required ongoing legislation and insurance stipulations safeguards all those involved in protecting flats and those who live in them.

# RIBA forms coalition to urge government fire safety action

Since the devastating fire at Grenfell Tower in 2017, the Royal Institute of British Architects has been advocating for stronger regulation to make the built environment as safe as it can be. We have been clear that consistency and clarity are needed on a height threshold at which two or more staircases are necessary to provide adequate access for firefighters and evacuation of residents from their homes.

In December 2022, the Department for Levelling Up, Housing and Communities (DLUHC) launched a consultation which sought views on the maximum height threshold for the provision of a single staircase in new residential buildings – the consultation proposed a 30 metre height threshold.



RIBA responded to the consultation outlining that, from the best available evidence and guidance from our Expert Advisory Group on Fire Safety, we believe that the appropriate threshold for a second staircase in new residential buildings is 18 metres.

An 18 metre height threshold would harmonise with the wider regulatory environment and aligns with requirements in Scotland, which have been in place for four years.

"We have written a letter to Levelling Up, Housing and Communities Secretary of State, Rt Hon Michael Gove MP, outlining the reasons for our 18 metre position, and why we believe the government must adopt this. The letter is also signed by organisations representing multiple sectors - the built environment, fire safety and disability rights groups, including:

- Royal Institute of Chartered Surveyors (RICS)
- Chartered Institute of Building (CIOB)
- National Fire Chiefs Council (NFCC)
- Housing Learning and Improvement Network (Housing LIN)
- Disability Rights UK
- Inclusion London
- Claddag (Leaseholder Disability Action Group)

While arguments exist for a range of thresholds, both higher and lower, an 18 metre threshold would bring the greatest harmonisation with the wider regulatory environment, and therefore the greatest simplicity and certainty for industry at this time.

a minimum of six storeys in London.

This amounted to nearly 8,500 people choosing to evacuate buildings rather than 'stay put' before the arrival of the London Fire Brigade during an incident.

This demonstrates the importance of occupants having access to a safe, smoke-free evacuation route in buildings over 18 metres, helping to remove the risk of a single point of failure.

In England, there is currently no maximum height for residential buildings with a single staircase. In contrast 'Buildings other than dwellings' are only permitted a single stair up to 11 metres, under Approved Document B, Volume 2.

Following the COVID-19 pandemic, increased hybrid working patterns mean that occupants are spending more time in their homes. Therefore, an 18 metre height threshold for requiring a second staircase in residential buildings would better align with non-residential requirements.

While we believe 18 metres is the correct height for a second staircase for new residential buildings, it is not a panacea for fire safety. We also urge the government to undertake a full review of Approved Document B. We must ensure that regulations and guidance are consistent, clear, unambiguous and actually deliver safe buildings.

Critically, it is important to note that there is an extensive existing single staircase housing stock. An 18 metre height threshold for a second staircase in new residential buildings does not make existing single staircase residential buildings inherently unsafe.

However, to ensure existing buildings are as safe as possible, we recommend that the government require existing single staircase residential buildings over 18 metres be refurbished with evacuation lifts, sprinklers and centrally addressable fire alarm systems as 'consequential improvements' where a building is subject to 'material alterations'.

Research has found that post-Grenfell, more people are choosing to evacuate their building when there is a fire. Between 1 April 2019 and 31 March 2022, there were 154 cases where 10 or more people evacuated from a block of flats of



# How organizations can optimize existing cybersecurity investments



Between inflation and a potential economic downturn, there's plenty of uncertainty going into 2023—including security. Rather than looking for the next “hot tool” that will solve all potential business problems, why not optimize existing investments? Not only will this save your organization time and money, but it can also help you focus on amplifying the value of existing investments.

First, look at your



security tool portfolio. If you're like most organizations, there's likely some capability overlap in tools—many tools today have multiple functions as they try to displace other vendors that are competing for that limited security budget. While most tool vendors have robust functionality in one or two functions (usually the ones they started with), many have additional functionality that is less mature as they look to compete in adjacent functions.

This is happening a lot right now in code security technologies. For example, only a few years ago you needed a single tool for Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), Software Composition Analysis (SCA), and Interactive Application Security Testing (IAST). Now you can get many of these in one or two tools. The same dynamic is happening in the Third-Party Risk Management (TPRM), Attack Surface Management (ASM), and Digital Risk Protection Management (DPRM) space. Analyze these tools. Based on your specific risk appetite, decide what functions must be best

of breed, and what other functions just need to be “good enough.” Then consolidate. It will save you budget and reduce the burden on your vendor management, procurement, training, and sustainment responsibilities.

Once you've done some consolidation, audit the policy configuration of the tools that remain. In the hustle and bustle of current operations, it's likely your teams have not reviewed the current policies that are implemented, and further, it's likely these tools have evolved with additional features since you last configured them. What you're likely

to find is that many policies are overdue for some refinement based on both business changes and tool advancements. More specifically, look for the opportunity to apply more granular policies that facilitate more prevention (blocking) without impacting the business.

Policy Tuning to perfection doesn't end there. In addition to blocking, most of our tools throw out a lot of alerts, and honestly, a lot of them are noisy. Too many alerts are unimpactful or of low severity. It's important for the SOC to determine which alerts are high fidelity—with a high probability of malicious activity, and which ones generate a lot of “low severity noise.” Once qualified, if the noisy alerts cannot be turned into higher fidelity, consider consolidating them into a report, or turning them off altogether. Make sure that you're getting to the signal—the things that matter and trimming the noise. And be sure to lean on your SOC partners to help you.

This philosophy can also be applied to labor, which continues to be a challenge in the cybersecurity industry. Today's CISOs should prioritize

retaining and upskilling their existing security teams by identifying how they can best support them with the right tools, training, and benefits. Particularly in security operations, but in all technical support, we struggle with how to take the “low-brain, high carb” activity off their plate. In the SOC analyst role, responding to high volumes of meaningless alerts or continuing to answer every phishing email is mind-numbing. How do you reduce that burden, so that your teams can focus on more proactive business needs? One word—automation.

Automate everything from provisioning and deprovisioning credentials to the investigation of malware or virus alerts. It's an area we focus on heavily because roughly 70-80% of an analyst's time is spent investigating alerts. If you can automate the context required for, to accurately adjudicate an investigation, you can free up the analyst for more proactive and business-impacting work.

Here are three proactive activities worth considering should you unburden your analysts using automation. These happen to be the areas I try to focus my teams on when they are not chasing alerts.

The first one is “credible threat mitigation.” It's a fancy term for keeping up with the threats that matter most to your business by ensuring you have controls aligned with their techniques. And further, instead of focusing on every MITRE technique in the model, why not focus maniacally on those techniques that your most credible threats are using?

Credible threats are those that are specifically targeting you, targeting your sector, or those that use techniques for which you are particularly vulnerable. In other words, you are focusing on those threats you're most likely to come up against and validating the alignment of your controls. This is a focus area that keeps businesses better protected and helps manage risk.

The second proactive activity is threat hunting which aggressively looks for anomalous activity.

The primary goal of proactive hunting is to confirm or deny a hypothesis—typically centered around the existence of a threat (or not). Equally important, however, is the second-order benefit of getting to know the traffic patterns in your environment so you can very quickly see when something is anomalous. Most of the time, the discovered anomalous activity is safe—the result of misconfigurations or undisciplined human activity (often unknown), which are equally valuable. Many of these hunts should be run automatically on a recurring basis. Hunts like anomalous firewall traf-

fic, anomalous authentications, and anomalous DNS traffic, should be scheduled to automatically run on a recurring basis with pre-configured filters that highlight traffic outside of what is expected.

The third proactive activity is control testing. In breach postmortems, how often do we hear about a control that was missing (not installed), not properly configured, or incorrectly logging? In other words, how do you know what you own is working? One word: Testing. And better yet, recurring, and automated testing. There are lots of automated testing tools

businesses can use.

In summation, in the face of an uncertain resource environment, embrace the concept of a “waste not, want not” mentality of “less is more”. With a little focus, leaders can optimize existing tooling and human resources to save money, reduce attack surface and tune away noise. While those are valuable just standing on their own, you can also further improve your team's morale and security posture by transitioning to some higher value proactive work like credible threat mitigation, hunting and controls testing.

*Credits: ReliaQuest*

## Does voice recognition have a place in modern banking?

Fraudsters are financially motivated, adaptable, and are increasingly becoming more adept at using the latest technologies to execute account takeover fraud, so it's no wonder that, as biometric authentication becomes ubiquitous in the financial services sector, bad actors are finding opportunities to exploit these systems—but does this mean that technologies like voice recognition have no place in modern banking?

A recent article from VICE exposed how a

produce realistic results, as reported by both MIT and Google respectively. With the advancement of such technologies, spoofing voice recognition systems when you have access to the victim's voice data is entirely possible.

Voice recognition systems, like the one used in the VICE exposé, rely on the victim saying something aloud, either a unique passphrase (similar to a password), or a generic statement such as “my voice is my password.” Both are vulnerable to exploitation,

making critical changes, such as updating the contact details, resetting passwords, adding new beneficiaries, or ordering a replacement card, to someone's account over the phone.

Normally, the customer would be asked specific security questions about their transactional and account data to verify their identities—this kind of data is hard to obtain without direct access to the account. That being said, it is possible that a threat actor would be able to dig out more obscure data like transactional history from their victims, especially if the person is known to them.

There are heightened concerns for public figures, as fraudsters can harvest their voice data from interviews and social media—with platforms like Instagram, TikTok and YouTube opening up the floodgates for these kinds of attacks. However, obtaining sensitive account data would be much more difficult, making this kind of attack relatively unscalable for threat actors, who today have access to more efficient means of account takeover fraud.

When it comes to fraud prevention in financial services, mitigating threats based on their financial impact or their ability to be executed at scale is key to reducing the threat surface.

Voice recognition spoofing today poses less of a threat to the general public as it's difficult to



journalist proved, by hacking into their own account, how easy it is to bypass telephone banking security steps using synthetic voice technologies generated by AI. Sometimes referred to as voice cloning or voice spoofing, these attacks have sparked an outpouring of privacy concerns about our voices being harvested and used against us.

Since the launch of Lyrebird and WellSaid Labs, synthetic voices generated by AI have evolved to the point where they are indistinguishable compared to real voices, and need only a minute of voice data to

with the latter being particularly weak in terms of security.

While this is alarming, it's neither unexpected nor is it a cause to boycott the technology altogether. Generally speaking, banks will not rely on a single form of authentication, so the debate around the effectiveness and security of voice recognition therefore depends on the mitigating factors put in place to stop spoofing threats from escalating into full blown fraud.

Fraud prevention processes typically require banks to practice a higher degree of diligence when



execute at scale. To be successful, threat actors would need to have substantial personal information about a customer in order to successfully evade the bank's layered security defenses. However, that does not mean that such attacks don't have a high impact when successful.

High-net-worth customers are a particular risk, as their transactional data may be managed by trusted associates like employees, making them more vulnerable to such attacks. Plus, they're more likely to have given interviews or spoken online – making it possible for fraudsters to illegally harvest their voice data.

However when it comes to protecting against voice spoofing threats, the answer is not replacing biometric technologies altogether, but complementing biometric solutions with additional security measurements.

To avoid spoofing threats, all biometric authentication solutions – whether voice, face or fingerprint – need to have robust fallback methods and be used together with fraud detection engines. When high-risk activity is detected, it's important that banks re-authenticate their customers, regardless of the amount of friction this would cause for the cus-

tomers.

Fraud detection systems typically provide banks with:

- Behavioral analysis: This involves analyzing patterns in the user's behavior during the authentication process. For example, the system may look for unusual typing patterns or mouse movements that suggest the user is not who they claim to be.

- Device identification: The system may also analyze the device being used to authenticate the user. This can include checking the device's IP address, location, and other characteristics to ensure it is a legitimate device.

- Geolocation: The system may also analyze the user's geolocation data to ensure that they are in a location that is consistent with their usual patterns of behavior.

- Time-based analysis: The system may also analyze the time of day and day of the week that the authentication attempt is made. This can help to identify patterns of behavior that are unusual or suspicious.

- Fraudulent pattern analysis: Machine learning algorithms can be used to analyze large amounts of data and identify patterns that are

associated with fraudulent behavior. These algorithms can learn from past patterns of fraudulent behavior and use this knowledge to identify new instances of fraud.

If and when high-risk activity is detected, it's important banks use step-up authentication to ensure that it's the real person authenticating – not a fraudster using deepfake technology. Step-up authentication is when customers are asked to re-authenticate themselves. This could be when adding a new beneficiary, ordering a new card, or making a transfer to an unknown or new account.

When compared to passwords and PINs, which can be easily compromised, biometric authentication solutions provide a much higher level of security – but this does not mean they should be used in isolation. By combining biometric solutions, such as voice and facial recognition with other authentication challenges and fraud detection systems, banks can help protect their customers from the financial impact of identity fraud and account takeover threats.

*The author, Fabian Eberle, is co-founder and COO at Keyless Technologies.*



rent smart home ecosystem demands.

WPA2 is also known to be vulnerable to exploitation and can be bypassed or manipulated easier than the newer WPA3 counterpart. The idea is to ensure your wireless router and future devices support WPA3 when building your smart home ecosystem. This is especially crucial regarding security cameras since they can record audio and video of your personal space. These devices should be protected from potential external threats or hacks to keep your private data safe and sound. The faster we move past the old WPA2 era, the better it'll be for everyone.

What are the signs your smart home security cameras have been hacked?

Before discussing methods to prevent your smart home and security cameras from getting hacked, we need to mention the ways to notice it before it's too late. How can you tell if your cameras have been or are currently being hacked? You'll see odd behaviors from your cameras, including the LED light randomly going off, the cameras panning or moving by themselves, camera data usage activity spiking high when you're not using it, and your security settings have changed. Another telltale sign is that you see an unknown device accessing your Wi-Fi network.

How do you prevent your smart home security cameras from being hacked?

Now that you're aware of the common signs your smart home security cameras are being hacked, it's crucial to learn how to prevent it from happening. Whether you've been hacked before or not, it's a good practice to ensure maximum safety for your personal data and privacy. Nothing is guaranteed, but you can reduce your chances of getting hacked by following the methods be-

low. you don't want a stranger accessing your smart home security cameras. To do this, you'll have to log in to the web settings for your router.

Use the firewall feature on your wireless router

You should consider using the built-in firewall from your wireless router to enhance the security of your home Wi-Fi network. Turning it on if the firewall isn't enabled can help monitor your incoming and outgoing web traffic. This allows you to keep an eye on the devices that access your network anytime during the day or night. If you notice an activity you don't recognize, you can immediately prevent it from accessing your network. This is an excellent defense for stopping the outside threat that may be trying to control your network.

Upgrade your wireless router with Wi-Fi 6 capabilities at the minimum

We talked about Wi-Fi 5 earlier. It wasn't built with modern smart home devices in mind, such as security cameras. If you have an older Wi-Fi 5 wireless router and are looking for a new one, a Wi-Fi 6 router for your home is a leap forward. It has WPA3 security features, allowing better protection over your compatible wireless devices. It also pushes faster network speeds, which is excellent as gigabit (1000+ Mbps) home networks become popular. Wi-Fi 6 also supports more device requests simultaneously, which means better overall responsiveness from your smart home ecosystem.

Smart home security cameras can be beneficial if you take the proper safety precautions

We use smart home security cameras to help us feel safe during all hours of the day or night, but they also come with a few asterisks. Using the factory default settings is typically never a good idea. You'll need to do some extra legwork to ensure a safe and secure experience. At the same time, you put yourself at risk by using older wireless routers and camera systems that don't support modern features. If you follow the tips mentioned in this guide, you can put your mind at ease.

## How to keep your home security cameras from being hacked

Smart home security cameras are great tools that many of us use daily to keep an eye on the surrounding goings-on in the world. They offer motion detection capabilities and can alert us when a package has been delivered. Their benefits are worth the effort. Many of the best security camera systems have features and a price that should fit the needs of everyone. However, hackers trying to snoop on your private video feeds can exploit those benefits.

A hacker can access your smart home and security cameras in one of two ways: remotely or locally. The most common of these is through a remote hack, which allows an outside threat to invade your network from anywhere in the world. For example, a

bad actor might send you a spam email or text message with a bogus link to click, and visiting the website instantly records your unique IP address. Using various open network ports, they can leverage that new information and attempt to brute force their way into your private home network.

In comparison, a local-based hacker must physically be in or near your home to hijack your network. Crafty bad actors might set up a fake hotspot outside the house with a similar name to your Wi-Fi network. This is an attempt to fool you or others into connecting to the spy device instead of your own. They can then see your IP address and try to get into your network from there. Both remote and local

hacks have the same end goal: Access your private network and locate any personal information they can use.

Why are older smart home devices more at risk of being hacked?

It all starts with the wireless router – the method used by your smart home devices to connect to your local private network. The common generation of Wi-Fi routers still used in many homes today, Wi-Fi 5, uses an older Wi-Fi Protected Access (WPA) security protocol by default. Known as WPA2, this dated form of wireless protection was introduced in 2004, making it not ideal for modern smart homes. It takes time for the overall consumer adoption rate to catch up to the new standards that the cur-



Partnering with **Kawach**  
will always be a **BRIGHT** idea



SECURITY SOLUTIONS FOR HOMES & BUSINESSES

Established in 1983, Kawach has been the most trusted source of highly efficient and dependable electronic protection solutions for thousands of end users across India. As a Master Distributor of Jablotron, the world's leading European manufacturer of high quality intruder alarm systems, Kawach has access to the latest technological innovations. We provide a full range of wired and wireless alarms with GSM/LAN communicators, central monitoring stations, comprehensive training and support to our business partners.

JABLOTRON  
CREATING ALARMS



JA-100. The addressable 4 wire alarm system range

Complete solutions for Intrusion Detection & Alarm Systems

When it comes to making a choice of technologies and devices to protect life and assets, we uncompromisingly leverage our 33 years of hands-on experience to suggest the best technology, field proven devices that fit within the assigned budget. Our arsenal comprises of military grade systems to simple home and personal security systems.

Call today to schedule  
a training, see a live demo or  
to place an order...

"Security House"  
24-B Udyog Vihar - V, Gurgaon-122016, India  
Tel: +91 - 124 - 4001111 | E-mail: info@kawach.com  
Web: www.kawach.com

INDUSTRY  
EVENTS



RUSSIA

11-14 April 2023  
Securika Moscow 2023  
Crocus Expo International  
Exhibition Centre  
Moscow Russia  
<https://securika-moscow.ru/Home?culture=en-GB>



UK

25-27 April 2023  
The Security Event  
N.E.C.  
Birmingham  
U.K.  
<https://www.thesecurityevent.co.uk/>



UK

25-27 April 2023  
The Fire Safety Event 2023  
N.E.C.  
Birmingham  
U.K.  
<https://www.firesafet-yevent.com/exhibitors/fireco>



INDIA

27-29 April 2023  
Secutech 2023  
Hall No. 1, BEC  
Mumbai  
India  
<https://secutechindia.in.messe-frankfurt.com/mumbai/en.html#>



NIGERIA

09-11 May 2023  
Securex West Africa 2023  
THE LANDMARK CENTRE,  
LAGOS  
Nigeria  
<https://www.securexwestafrica.com>



UK

16-18 May 2023  
IFSEC International  
ExCeL London,  
London  
United Kingdom  
<https://www.ifsecglobal.com/ifsec-international-security-event/>



UK

16-18 May 2023  
International Firex  
ExCeL London,  
London  
United Kingdom  
<http://www.firex.co.uk/>



UK

17-18 May 2023  
ISecurity & Counter Terror  
Expo – SCTX 2023  
Excel London  
United Kingdom  
<https://ctexpo.co.uk/>



INDIA

18-20 May 2023  
SAFE West India Expo  
Bombay Exhibition Centre  
Mumbai, India  
<https://www.safeindiaexpo.com/eng/main.asp>



NETHERLANDS

21-23 May 2023  
ASIS Europe 2023  
Rotterdam  
NL  
<http://www.asiseurope.org>



USA

05-08 June 2023  
ESX Electronic Security Expo  
Kentucky International  
Convention Center  
Louisville, KY  
USA  
<https://www.esxweb.com/>



SOUTH AFRICA

06-08 June 2023  
Securex South Africa 2023  
Gallagher Convention Centre  
South Africa  
<http://www.ifsecca.com/>



UK

20-22 June 2023  
Infosecurity Europe  
Excel  
London  
United Kingdom  
<http://www.infosec.co.uk/>



INDIA

06-07 July 2023  
Chennai Trade Centre  
Chennai  
India  
<https://www.safeindiaexpo.com>



INDIA

26-27 July 2023  
International Police Expo 2023  
Pragati Maidan  
New Delhi  
India  
[www.internationalpoliceexpo.com/](http://www.internationalpoliceexpo.com/)



INDIA

24-26 August 2023  
FSIE 2023  
Jio World Convention Centre  
Mumbai  
India  
[www.fsie.in](http://www.fsie.in)



USA

11-13 September 2023  
Global Security Exchange (GSX)  
Kay Bailey Hutchison  
Convention Center in Dallas  
Texas USA  
<https://www.gsx.org/>



SAUDI ARABIA

03-05 October 2023  
Intersec Saudi Arabia  
Jeddah Center for Forums &  
Events  
Riyadh, Saudi Arabia  
<https://intersec-ksa.ae.messe-frankfurt.com/ksa/en.html>



UK

12 October 2023  
Consec 2023  
Twickenham Stadium  
Twickenham  
United Kingdom  
<https://www.securityconsultants.org.uk/events/consec>



INDIA

07-09 December 2023  
IFSEC India  
Pragati Maidan,  
New Delhi,  
India  
<https://ifsecindia.com>



BANGLADESH

07-09 December 2023  
16th International Safety &  
Security Expo Bangladesh 2023  
International Convention City  
Bashundhara Dhaka Bangladesh  
<https://www.cems-safetysecurity.com/>



**HIKVISION**<sup>®</sup>  
See Far, Go Further

**ColorVu**  
Turbo HD Camera

**24/7**

**Colorful Imaging**  
View in Color, Even in Darkness



**F1.0 Super Aperture**

Collects more light to produce brighter image.

**Friendly Lighting**

Soft and warm supplemental light works to guarantee colorful images when in zero-light environments.

**Advanced Sensor**


Vastly improves the utilization of available light.


 /HikvisionIndiaOfficial

 /HikvisionIndiaOfficial



Corporate Office:  
PRAMA HIKVISION INDIA PVT. LTD.  
Oberoi Commerz 2, International Business Park,  
18th Floor, Near Oberoi Mall, Off W.E. Highway,  
Goregaon (East), Mumbai - 400 063.  
Tel: +91-22-4041 9900, 2846 9900  
Web: [www.hikvisionindia.com](http://www.hikvisionindia.com)

 Sales:  
+91-22-4041 9944, 2846 9944  
[sales@pramahikvision.com](mailto:sales@pramahikvision.com)  
  
 RMA Support:  
+91-22-6822 9977, 3322 6070, 2846 9977, 0250 663 6677  
[rma@pramahikvision.com](mailto:rma@pramahikvision.com)

 Technical Support:  
+91-22-6822 9999, 3322 6060, 2846 9999  
[support@pramahikvision.com](mailto:support@pramahikvision.com)  
Toll Free: 1800 222 699