SECURITY update

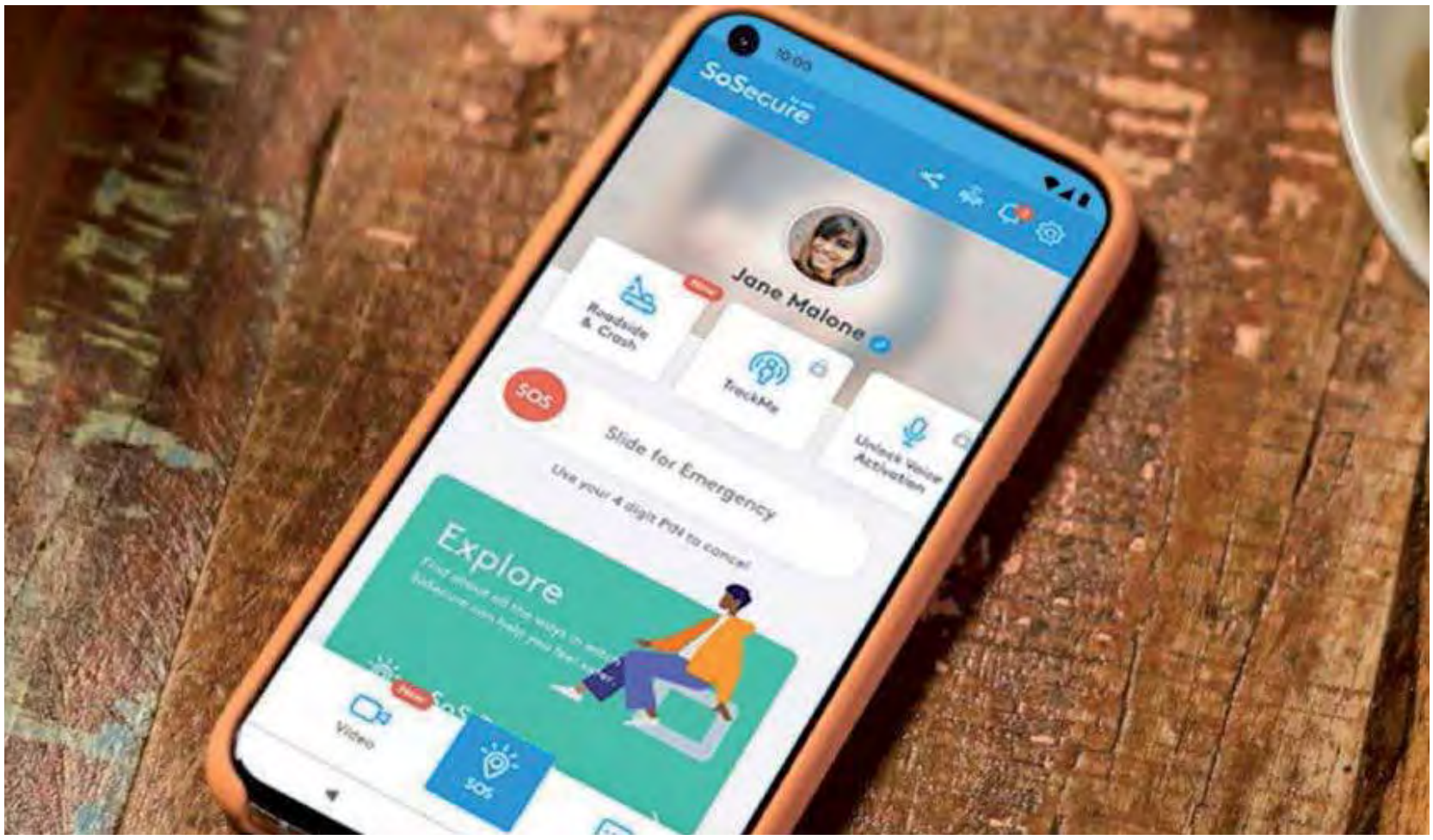
The Best Read Channel Tabloid

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

CREATING BUSINESS OPPORTUNITIES

Vol. 12 No. 03 | www.securityupdate.in | March 2022 | Pages 16 | Price ₹ 75

The Growing Popularity Of Personal Safety Apps



The past year has elevated consumer awareness about personal safety, from COVID-19 issues to social unrest, making safety top-of-mind and the need for personal safety solutions, even more prevalent. In addition, consumers spent more time at home, as schools closed, events were canceled and remote work increased.

This prompted two major shifts that, in my opinion, most significantly opened the need for and raised the popularity of mobile safety solutions.

Demand for grocery and food delivery apps surged

During the past 18 months, the use of app-based delivery services has skyrocketed. With more use comes more interactions among strangers in homes and businesses, and while the majority of these moments are completely safe and convenient, incidents are happening, ranging from uncomfortable situations to physical assaults.

And, with more delivery drivers on the road, there are going to be more accidents among gig-economy workers. Based on recent estimates, food and grocery delivery are expected to remain popular, even as we get back to normal life.

With more work shifting from stationary locations to working on-the-go, mobile security apps or wearables can be a lifeline in all sorts of situations. It's important for these mobile safety products to be comprehensive, dynamic and designed to address the full range of people's safety and security needs, from providing simple human reassurance to dispatching emergency help.

Domestic violence cases increased

According to the National Domestic Violence Hotline, due to COVID-19 lockdown restrictions, domestic violence rose as a result of many victims being stuck at home with their abusers, while working from home.

These situations necessitate the need for discreet ways for victims to call for help. U.S. Attorneys General and other state-elected officials have endorsed mobile safety apps, like SoSecure by ADT, as a tool to help victims of domestic abuse, safely call for help, without alerting their abuser.

Over the past year, the mobile safety app market has seen tremendous innovation, including more user-friendly ways to make SOS calls. Today, within a single app, a person can summon help hands-free, by saying a secret phrase, by text or by swiping a button.

Users can connect with people trained to help in unsettling situations over video, which can be an effective deterrent and provide video evidence. We've also seen the extension of mobile safety into wearable devices, in order to make these devices more discreet and usable.

There will always be some safety risks in our lives. However, the good news is there's no need to live in a constant state of fear. The easiest, most direct way to be prepared and ready to 'fight back' is by having a personal safety tool in your pocket, a mobile safety app that is there, when you need it most.

Dear Reader

The pandemic severely impacted the supply of electronic chips and components and disrupted the electronic manufacturing globally. However, as the pandemic waned, the encouraging recovery in world consumer markets, notably in the US, China, Western Europe and India, drove the growth in demand for electronics. This is resulting in buoyant growth in budgets for electronic goods, with electronic security systems being a subset.

The electronics sector rebound has made an important contribution to the recovery of manufacturing exports and industrial production in many East Asian industrial economies. The electronics manufacturing industry is an important part of the manufacturing export sector for many Asian economies, including China, South Korea, Taiwan and Japan.

The rapid rise in electronics production has also triggered a sharp upturn in raw materials input prices for electronics firms during the second and third quarters of 2021. According to the IHS Markit report, supply shortages of semiconductors and components are likely to continue to translate into price escalation. Printed circuit board assemblies are the most severely affected, but semiconductors, bare printed circuit boards, resistors, capacitors, and connectors are all expected to see price pressures.

Component, material and energy supply chains were already in a delicate phase of recovery following disruptions from the Covid-19 pandemic and subsequent semiconductor shortages. Now, the Ukraine crisis has severely compounded those difficulties.

The greatest risk facing global supply chains has shifted from the pandemic to the Russia-Ukraine military conflict and the geopolitical and economic uncertainties it has created.

The Russia-Ukraine crisis will only exacerbate the situation for companies in many industries, especially those reliant on energy resources.

According to a new report from Dun & Bradstreet, the international domino effect of global dependencies on businesses in the Ukraine region is already being felt. Why? Because 374,000 businesses worldwide rely on Russian suppliers—90% of these businesses are based in the U.S. About 241,000 businesses rely on Ukrainian suppliers and 93% are based in the U.S. Approximately 90% of neon, used for chip lithography in the manufacture of semiconductors, originates from Russia; alternative sources are not readily available!

Supply chain issues will continue to be a dominating security trend. Semiconductor shortages, global logistics bottlenecks, and corresponding cost increases will impact everything from cameras to readers and control panels to sensors and detectors. Disruption of trade routes, freight costs, inaccessibility of critical raw materials could derail economic growth and add to inflationary pressures.

Russia's ongoing war against Ukraine is first and foremost a human tragedy and has fast developed into a humanitarian crisis. But it is also apparent that in an increasingly globalised and interconnected supply chain, the conflict's ramifications will profoundly impact reshape geopolitics, economies, trade and the trajectory of the electronics manufacturing industry for years to come.

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

Alcatraz AI brings the Rock solution to promote touchless authentication at the office

Alcatraz AI, a pioneer in physical security technologies, announces an initiative to promote touchless authentication while returning to the office.

As companies decide how to safely return to work, Alcatraz AI is providing the opportunity to try its frictionless authentication solution, the Rock, which minimises touchpoints and provides facemask verification to ensure COVID safety.

Alcatraz AI is reimagining the way one enters secured spaces using the face as the credential. Alcatraz AI's state-of-the-art product, the Rock, transforms access control by leveraging artificial intelligence and analytics to make powerful decisions at the edge.

With features like touchless or multi-factor authentication, tailgating intelligence, and video at the door, the Rock makes companies' physical security strategies future-proof. One of the challenges with bringing workers back into workspaces is controlling access, including creating controlled or separate entrances and exits, monitoring who has access into facilities and when, and even dividing work areas into zones to limit large numbers of people congregating.

The Alcatraz AI Rock provides effective access control for the new normal world. The Rock can also function as an ONVIF camera, certified with Profile S and Profile T to provide IP-based video streaming. With an ever-increasing demand for new solutions in safety and security, companies like the Los Angeles Football Club and MLK Hospital are already using the Rock to secure their spaces.

The Rock is bringing these organisations into the future of smart buildings with its touchless building access while solving problems presented by the pandemic.

Anviz launches Secu365, a cloud-based intuitive physical security platform, specially built to protect businesses

For business owners, their business is more than just their livelihood, it's the culmination of years spent dreaming and planning. With that in mind, it only makes sense to protect the business with the smartest security system on the market.

A report by security market analysts, Omdia has highlighted the potential growth of an integrated physical security as a service (PsaaS) system. The market for integrated PSaaS solutions is estimated to grow at an impressive 24.6% CAGR, over the next five years.

Anviz, the globally renowned smart security solutions provider, has launched Secu365 as an intuitive platform into a cloud-based physical security solution.

Regardless of what type of service a business provides, if it's a brick-and-mortar business, a well-rounded and easy-to-use security system is not just important, it's essential. Listed below are a few of the benefits that might be of concern for businesses and what they can get from the business security system:

- Monitor customers and employees with video surveillance, in case of any accidents that happen,
- Help prevent theft, vandalism, and other crimes,
- With a mobile device, remotely control the business from anywhere.

Furthermore, as businesses continue to maintain a mostly remote workforce, the drive towards adopting cloud-based and hybrid solutions has grown as well. Thus, with 24/7 video monitoring, indoor and outdoor cameras, integrated with biometric or mobile access, Secu365 system is the perfect way to protect any small business.

David Huang, Director of Secu365 in North America for Anviz Global, said "We've seen people that are more and more interested in moving to cloud services, specifically small business owners. They work

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-1, 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 01.03.2022

SECURITY TODAY®

SECURITY Update
CREATING BUSINESS OPPORTUNITIES

InfosecGirls

WISECRA
WOMEN IN SECURITY & RESILIENCE ALLIANCE

PRESENT

TOP INDIAN WOMEN INFLUENCERS IN SECURITY

27th April 2022

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

In order to recognise and honour the accomplishments, value and contributions of women in this vital sector of the economy, SECURITY TODAY & SECURITY UPDATE in association with InfosecGirls and WISECRA announce the "Top Indian Women Influencers in Security" recognition for the year 2021.

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

For further announcements please visit our website:

https://securitytoday.in & https://securityupdate.in

SUPPORTING PARTNERS

ASIS INTERNATIONAL
Stronger Together
Ahmedabad, Bangalore, Chennai, Hyderabad, Mumbai, New Delhi & Pune Chapters

PSP
PUNE SECURITY PROFESSIONALS

WiCyS
WOMEN IN CYBERSECURITY

very hard, arriving first and leaving last."

He adds, "They often take their work home with them to ensure their business is as successful as possible. Because of this, many business owners spend a lot of time worrying about how things are running in their absence, specifically when they're out-of-site or taking vacations."

A top concern for small businesses is theft, as it can have devastating effects. Therefore, first and foremost, there is a need to help SMB owners to be proactive instead of reactive, alerting them to issues, before they become problems.

An integrated security solution, which combines access control and video surveillance functions in a single platform, is a worthwhile investment for peace of mind and control.

Assa Abloy unveils new suite of Ecliq key options

Assa Abloy has released a powerful new suite of programmable Ecliq keys, designed to provide even more robust, longer-lasting performance. An IP67 rating against water and dust ensures new Ecliq Basic, Ecliq Professional and Ecliq Connect keys can handle any weather.

Connect keys can handle any weather. Durability is ensured with up to a 10-year lifetime from a single, standard battery for the Basic and Professional keys. All three new keys are compatible with new and existing Ecliq wireless access control systems — and can be used alongside existing Ecliq keys.

The core of the purely electronic eCLIQ locking system is the unique, innovative locking cylinder technology. With its setup and its structure, the eCLIQ locking cylinder offers a measure of compactness and security never achieved until now. The eCLIQ key is likewise a true innovation with considerable resilience in an exceptional, distinct design. Equipped with a chip of the latest generation, the entire eCLIQ system is faster, more powerful, more secure and more efficient than conventional locking systems.

By deploying new Ecliq keys, facility managers gain the flexibility to operate access control exactly how they choose. Both Ecliq Basic and Ecliq Professional keys can be updated at the desktop, via wall readers or with mobile programmers. The Professional key adds acoustic feedback to the Ecliq Basic's LED key feedback.

A third new member of the family, the new Ecliq Connect key will be released soon and may also be paired with a smartphone app to update access rights from anywhere. A security administrator simply updates the system; the keyholder transmits new access permissions from phone to key via an encrypted Bluetooth connection. A key battery typically lasts two years or up to 2,000 connections.

More than just simple and convenient, an Ecliq Connect Key also saves time, money and fuel wasted on unnecessary journeys to update a credential. In this way, issuing contractors and mobile workers with Ecliq Connect keys can help businesses to reduce their environmental footprint as part of an overall sustainability strategy.

A fully electronic extension of Assa Abloy's award-winning Cliq access control system, Ecliq is built around precision-engineered wireless locks and high-end microelectronics. A standard battery inside each programmable electronic key powers the Ecliq cylinder or padlock — and encrypts data transfer between lock, key and system.

The Ecliq cylinder range brings almost any opening into an access control system. Robust, durable Ecliq locks can secure lifts, machines, mailboxes, cabinets and more, with the same control as sensitive doors. Available in multiple sizes and formats — Ecliq cylinders help maintain security across an organisation.

Managing Ecliq is fast and flexible. Existing keys are programmed with the same easy-to-use software and hardware as the three new Ecliq keys. Security managers have a choice between a local software installation (Cliq Local Manager) or cloud-based Cliq Web Manager.

Because Ecliq keys are powered by standard batteries, they can extend powerful electronic access control anywhere — far beyond the reach of electric cabling. Cylinders and padlocks operate safely between –25°C and 85°C, indoors and outdoors, in almost any environment, however harsh.

CellGate's OmniPoint Access Control and QR Code Visitor Management Solutions

Cellular access control company, CellGate's technology development team has been hard at work over the last year creating multiple new products and access control functionality.

According to CellGate President, Noel Gouldin, they have the following new products:

• OmniPoint Wireless Point to Multi-Point Access Control. OmniPoint is a cost-effective access control solution for multi-tenant properties, that does not require expensive wiring infrastructure to install. One OmniPoint gateway device connected to CellGate's TrueCloud portal can control up to 100 doors on a property. One EPM (entry point module) must be installed per door, and is simply connected to either 12v DC or 24v AC power. An OmniPoint gateway can work up to a one mile range in unobstructed environments, and up to ½ mile range in more obstructed/urban applications.

• QR Code Visitor Management. QR codes are a visitor management feature that is available with all Watchman multi-tenant hardware models, including: the Watchman WXL, Watchman W480 and Watchman W461. QR code invites can be created and issued from the CellGate app, and once sent to a visitor, the recipient can quickly scan their QR code on the Watchman access control device and be allowed entry to the property during a specific date/time. QR codes provide a more secure and convenient way to manage visitor entry, with usage log tracking easily viewable in CellGate's TrueCloud™ portal.

• SmartScreen Call Management. With CellGate's new proprietary SmartScreen call management options, multi-tenant properties now have a variety of choices for how they may customize the home screens on their Watchman model access control units. First, there are now three standard/default icons to choose from on a Watchman multi-tenant system home screen: Directory, Access Code and Guest QR Code. A property can choose one, two or three of these icons to appear, based on their property's specific needs. Second, a single, custom call group can be added to the home screen, and be named whatever the property chooses. Examples might include "Receptionist," "Leasing Manager," or "Security." The property can also choose from one of four graphic icons to pair with the chosen name for their custom call group. A CellGate Gold Key Customer Service team member sets up the custom call group graphic choice, and the custom name designated, during new account onboarding.

Identiv's UHF RFID TOM

Identiv, Inc., a global leader in digital security and identification in the Internet of Things (IoT), has announced the launch of its UHF RFID TOM® (Tag On Metal) portfolio for flexible usage across adverse industrial environments with an unmatched performance and price point.

According to a report

by Global Market Studies, the demand for industrial labels is expected to reach 59.34 billion units by 2024, rising at an approximate compound annual growth rate (CAGR) of 4.86%. UHF RFID TOM® Labels are the most flexible solution available today. TOM labels provide the highest performing read range without interference on metal surfaces and other harsh industrial environments. The TOM portfolio is designed for scale at an attractive price point.

The portfolio features two product options, UHF TOM® Base and UHF TOM® Pro. UHF TOM® Base was designed for application on metal and nearly every other type of surface, providing a long read range at approximately 4.5 meters (longer range on non-metallic surfaces). UHF TOM® Pro is more resistant against surrounding interfering materials, provides a superior read range of up to 10 meters on metal, and can be applied on convex or concave arched metal surfaces. Additional metrics on performance and sensitivity are available.

UHF RFID TOM® Labels are designed for container tracking, metallic commodities and goods, bicycle tracking, and the automotive industry. The portfolio is available with customized artwork and is easily printable on transfer printers.

Identiv's RFID and NFC solutions verify identities and security in the IoT and are embedded in billions of everyday objects, including medical devices, books, toys, athletic apparel, perishable goods, and pharmaceuticals.

It is built with adaptive self-learning algorithms (patent protected) with what the company terms as an exceptionally high recognition level of diverse threats. It is also able to distinguish between various threats above or below ground – for example, footsteps, moving vehicles, digging and more.

SALTO introduces EAN Code standard into product packaging

SALTO Systems has introduced EAN13 standardised barcodes into its product packaging, answering partners and channel needs. The EAN code is a 13-digit bar code used internationally to identify each product.

The International Article Number (also known as European Article Number or EAN) is a standard describing a barcode symbology and numbering system used in global trade to identify a specific SALTO product model, in a specific packaging configuration, with a unique identification number.

The use of EAN codes across SALTO products will allow partners and installers in the identification and distribution of SALTO products and reduce the margin of error within their channels. One of the major benefits of standardisation through product codes is having better warehousing processes and product tracking.

The EAN code will allow SALTO and its partners to obtain valuable information about SALTO products and optimise stock management, product information, operations, or even improve competitiveness.

The introduction of EAN13 codes will facilitate the selling and distribution of SALTO products across the channel. EAN codes help in distinguishing one SALTO product model from others easily and fast. These numbers are unique and describe the attributes of the products via identification marks.

They can represent details like:

- The type of lock, cylinder, or reader model
- Technology compatibility
- Price, weight, or colour
- Manufacturer
- Country code
- Other product-related data

The EAN13 code standardised barcodes will be adopted gradually into the complete product range from SALTO.

SATO partners with Xerafy to offer cost effective RFID labels and inventory management to global markets

Internationally renowned company in next-generation auto-ID and labelling solutions, SATO (SATO Europe) has partnered with Xerafy, to bring pioneering metal skin radio frequency identification (RFID) labels to the automotive, manufacturing and healthcare global markets, through its range of RFID-enabled printers.

The Xerafy Metal Skin RFID labels, which provide real-time traceability and asset management visibility, are easy to print from a SATO RFID-enabled printer, such as the CT4-LX and CLNX Plus series, and flexible due to their ability to be used both on- and off-metal.

In addition, the RAIN UHF RFID labels are ultra-thin, due to their unique design and can be read up to five metres on metal and up to four metres off metal. "Our Metal Skin series offers customers in manufacturing, automotive and healthcare, with a cost-effective way to track stock in and out of operations," said Michel Gillmann, Director of Product & Marketing at Xerafy.

Michel Gillman adds, "Since the labels operate with global RAIN RFID frequencies, they provide the best fit for international supply chains, as they work with a wide range of applications, from IT assets to product authentication and medical supplies."

The innovative product has already been successfully used by Sichuan Airlines, the largest airline in western China, to reduce inventory time of its 60,000 maintenance, repair and operating parts by 80%. Daily inventory counts, which used to take two weeks, instead of 80 days.

"Our RFID system has made it possible for Sichuan to not only identify the exact location of missing parts and consumables, but it has completely eliminated manual data entry associated with the inventory process, reducing human error," added Michel Gillmann.

As a SATO Partner for over five years, Xerafy has worked closely with the auto-ID and labelling expert, in order to enable large-scale industrial RFID projects on customer sites. The Metal Skin series is now the latest range of RFID labels that can be used with SATO industrial printers.

Available in four different sizes to incorporate human-readable printing, barcodes and graphics, the product's flexibility makes it ideal for tracking small parts and medical devices.

New generation of buried perimeter security released

Sensoguard, an Israeli based manufacturer of intrusion detection systems, has released a new generation of the company's buried perimeter security system.

The company has just been recognised by Frost & Sullivan as the product leader in the underground defence sensors market for 2021, and has now taken another step that it believes sets a new standard for the buried sensors market.

The Invisifence Plus is a smart buried sensor cable for perimeter intrusion detection. The InvisiFence Plus system has been designed to eliminate the need for local processing units along the perimeter line, and is thought to be the first and only fully digital buried seismic system for perimeter security.

The Invisifence Plus buried sensor cable creates an invisible perimeter security system around the secured area – one that, according to Sensoguard, is impossible to dig under or jump over.

Ava Security announces the release of Ava Quad, the first cloud-native multi sensor security camera

Ava Security has announced plans to release Ava Quad, the first cloud-native multisensor security camera on the market, further expanding the suite of cloud-connected video monitoring tools available on the Ava Aware platform.

Multisensor security cameras are designed to provide 360° visibility through multiple sensors, which is advantageous for customers looking for multi-angle coverage over wide outdoor or indoor areas, such as large crossroads, parking lots, campuses, and stadiums.

With more area covered by a single device, multisensor cameras are also more cost and time-effective when it comes to installation and maintenance. However, until now, multisensor cameras have only been available for on-premise instalments, which has meant a lack of flexibility and remote access and left cameras vulnerable to out-of-date software.

The launch of Ava Quad, expected in Q2 of 2022, will bring the first multi sensor security camera in the cloud to market. Customers will benefit from easier access to security data and in-built video and audio analytics, which further reduce costs for organisations by cutting the time and staff needed to analyse the footage.

It also improves response to incidents with machine learning algorithms that can identify critical events before they escalate. It also brings the ability to store forensic details that customers might need to detect threats without the additional burden of storing large volumes of footage. Ava Quad is the latest in the suite of intelligent cloud security cameras added to the Ava Aware video security data platform.

Clare Controls announces the launch of Color At Night high-performance IP surveillance cameras

Clare Controls, the maker of the powerful ClareVision Surveillance line and the ClareOne wireless security and home automation system distributed exclusively by Snap One, has announced the immediate availability of a new series of Color At Night high-performance IP surveillance cameras that leverage wider apertures, Sony® Starvis™ sensors and integrated

LED lighting to deliver improved nighttime performance and visibility.

Featuring image sensors specifically designed for low-light, wider apertures that capture up to four times more light, and warm-toned LED lights that ensure accurate color and wide visibility in even the darkest areas, Clare Controls' new Color At Night Series cameras provide clients with a nighttime surveillance solution that rivals daytime recordings.

Where infrared cameras provide black-and-white nighttime imaging, the new Color At Night series captures full-color images in low-light environments, and even in complete darkness with the help of the integrated warm LED light. This leap in capability offers homeowners and businesses greater nighttime security and peace of mind, providing much clearer videos with greater detail that can help identify bad actors after a security incident.

By replacing IR illuminators with newer technologies, the Color At Night series eliminates IR reflections from rain or snow while the use of PoE (power over ethernet) and the integrated light enable installation in unlit, unpowered locations without the need for new high-voltage wiring. This can greatly reduce the cost of surveillance installations across full properties, as both the camera and LED light operate on low voltage wiring that doesn't require a licensed electrician or conduit.

It's an ideal solution for properties with little or no exterior lighting, or dark spots such as alleys or landscaping. Users can even adjust the LED lighting intensity, so no location is off-limits.

"For instance, the warm-toned LED light is designed specifically to produce accurate colors in nighttime recordings without the harshness of a bright white light, while also acting as an active deterrent simply by lighting up more space." The Color At Night series includes 4MP (megapixel) and 8MP models with a fixed 2.8mm lens in either bullet or turret style, plus 8MP models in bullet or turret style with a motorised 2.7mm-13.5mm varifocal lens.

The 8MP models can record up to 4K resolution at 25 frames per second. The 4MP models come with a 32GB micro SD memory card and both the 4MP and 8MP models support micro SD cards up to 512GB. As part of Clare's Performance Series, all six Color At Night models feature power over ethernet capability and Smart AI events including people, intrusion, line crossing, loitering, and people gathering detection.

Teledyne FLIR introduces two-year warranty for Neutrino SWaP and IS Series cooled MWIR camera modules

Teledyne FLIR, part of Teledyne Technologies Incorporated doubled its standard warranty to two years for Neutrino SWaP and Neutrino IS series designed for commercial, industrial, and defence Original Equipment Manufacturers (OEM) and system integrators. With an industry-pioneering cryocooler Mean Time To Failure (MTTF), Neutrino provides a cooled Mid-Wavelength Infrared (MWIR) solution for imaging systems with size, weight, power, and cost (SWaP+C) constraints.

Cooled MWIR camera modules must be designed, tested, and manufactured to meet rigorous environment and reliability requirements. Recognising that reliability and operational lifetime are predominantly determined by the lifetime of the cryocooler, Teledyne FLIR developed, tested, and manufactures the ruggedised, long-life, FL-100 linear cryocooler for its SWaP-optimised Neutrino MWIR camera modules.

Based on lifetime tests and Weibull analysis, the MTTF of the Teledyne FLIR FL-100 cryocooler has increased to approximately 27,000 hours, significantly reducing the cost of ownership for systems using Neutrino.

"Teledyne FLIR understands the criticality of mission readiness and the importance of long, low-maintenance infrared system operation," said Dan Walker, vice president, product management OEM, Teledyne FLIR. "An MTTF of 27,000 hours and a two-year warranty on Neutrino offers a low risk and high-performance MWIR imaging solution for integrators."

The Neutrino MWIR camera portfolio continues to provide shortened time-to-market and reduced project risk with off-the-shelf design and delivery of High Operating Temperature (HOT) Focal Plane Array (FPA) technology in 640x512 or 1280x1024 resolution.

Teledyne FLIR can deliver high volumes of Neutrino, reducing the supply chain risk of typically the most critical component in a high-level imaging system.

The purpose-designed, factory-integrated Continuous Zoom (CZ) lenses and MWIR camera modules provide performance, cost, and schedule risk benefits unmatchable by other camera or lens suppliers.

Teledyne FLIR also provides highly-qualified technical services teams for integration support and expertise throughout the development and design cycle. Neutrino series are classified under US Department of Commerce jurisdiction as EAR 6A003.b.4.a and are not subject to International Traffic in Arms Regulations (ITAR).

GeoVision brings GV-AI Guard Basic AI video analytics software to enhance monitoring solution

Surveillance products are widely deployed in modern society to give protection. Facing hundreds of video feeds at a time can be challenging to catch the most vital information.

False alarms such as waving branches of a tree on a windy day or movement of small animals have always troubled control room operators. When searching for a security event, watching hours of video footage can be very exhausting.

What if one has a security guard who never takes a break and is never distracted? GeoVision Deep Learning AI video analytics software can help control room operators focus on responding to real incidents and not waste effort on false alarms. In addition, deep learning software also allows operators to search for specific objects by attributes.

GV-AI Guard Basic is deep learning AI video analytics software. It is an open platform to support ONVIF compliant cameras. Push notification on mobile apps and SDK for 3rd party software integration are available.

Key features include, Smart Search in Playback - search events by vehicle type & vehicle colour, and search events by clothing colour; Vehicle detection - Colour, vehicle type and illegal parking;Human detection - colour of clothes, face mask detection, social distance detection, and hard hat detection.

GV-AI Guard Basic software can be practical for city surveillance, industry, commercial building, security company, etc. Contact GeoVision to get more information and customised design as per the project requirements.

Hanwha adds 3 intrinsically safe cameras to line-up

Hanwha Techwin, a global supplier of security solutions, has announced the launch of three NDAA compliant explosion-proof camera models (TNU-6322E, 6322ER, TNO-6322ER) designed to operate safely even in industrial locations with highly volatile atmospheres.

The intrinsically safe cameras are contained within IECEx and ATEX certified stainless steel housings, which have the ability to prevent any sparks generated by the camera escaping the device and igniting gases or other ignition sources in the environment.

TNU-6322E/6322ER models feature 360° endless panning and 180° tilting, and, combined with powerful 32x (4.44 ~ 142.6mm) optical zoom lenses, these cameras will reach into every corner of a large industrial site.

2MP high-quality resolution guarantees sharp and clear image capture and Hanwha's wide dynamic range (WDR) technology improves the accuracy of images in scenes containing a challenging mix of dark and bright areas by compensating differences in brightness.

For external installations an onboard defog function ensures clear images can be achieved in all weathers, whilst the long-range IR illuminator built into the TNO-6322ER and TNU-6322ER models allows night-time surveillance at a distance of up to 200m. There is also a gyro sensor, which drastically reduces motion blur caused by vibration, and therefore ensures stable images even in the most challenging environments.

Embedded WisestreamII compression technology effectively reduces data size, whilst still maintaining optimum image quality, thereby minimising bandwidth requirements. In addition, the cameras are IP67 certified water and dust resistant and IK10 certified vandal-proof.

NOW CONTROL YOUR SECURITY FROM WHEREVER YOU ARE

Addressable Intrusion Alarms with Easy BUS (Single Cable) Wiring

- 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

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

KAWACH PROTECTION SYSTEMS Technology on Guard

Email us today for more information: info@kawach.com

Imou launches new outdoor smart home security cameras

Pioneers in video-centric smart IoT solutions & services, Imou has launched two new outdoor, smart home security cameras, the Bullet 2 and Cruiser. Imou's newly launched cameras aim to give consumers the ability to confidently protect their homes and loved ones, through smart connections and high-definition surveillance.

A highly beneficial human detection has the capability of identifying human targets outside the home and distinguishing them from pets or other moving objects, to avoid false alerts. The Cruiser pan and tilt camera feature Imou's Smart Tracking algorithm which quickly follows and focuses on moving targets, ensuring complete protection of your home.

Available in both 2MP (1080P) and 4MP (2K), the newly launched cameras also have built-in spotlights which not only offer a practical lighting solution to dark areas outside the home but when triggered by an event, act as a deterrent to warn off potential intruders. This spotlight ensures full colour, smart night vision to enable users to capture footage with clear-as-day clarity, even in the dark.

The new outdoor cameras both benefit from alarm notifications, which are sent to any connected smart device such as a PC or mobile phone when the cameras sense movement, and a two-way talk feature, so users can either scare strangers or welcome guests.

The robust Bullet 2 is Imou's base model outdoor camera and is ideal for anyone looking for an excellent value smart AI home security camera that is simple to use, with all of the latest features available, but without a hefty price tag.

The Cruiser is a motorised outdoor camera for consumers wanting complete coverage, with full HD or super HD live monitoring & recording and 0~355° pan & 0~90° tilt features, to ensure every corner of the home is completely covered. It's sleek in design and features programmable favourite locations for fast navigation, human detection, and smart auto tracking to follow subjects. Both models have IP67 certified housing meaning the cameras can be used outdoors under any weather conditions, perfect for use in multiple scenarios.

Imou cameras are compatible with virtual home assistants such as Alexa and Google Assistant, allowing users to get stuff done without having to do more than speak. With the Imou Cloud service, users will have access to camera footage, as long as an Internet connection is available.

However, if there is no network users can still connect the camera locally to view live footage or check recordings via an SD card. Imou Cloud connects and integrates all Imou smart devices and provides value-added and bank-level encryption services to users, which makes life smarter and easier.

Additionally, the user-friendly Imou Life App and Imou PC Client allow you to stream live video, play recorded clips, easily arm and disarm the system, and stay aware of what's happening in the home at any time, anywhere. With just one touch, the app pairing enables firmware updates to activate, keeping the cameras "watch, listen, speak, analyse and act" capabilities advanced and issue-free.

Imou's new outdoor, smart security cameras, both the Bullet and the Cruiser are available from Currys. Imou is offering a family of smart home security camera options so consumers get affordable, customisable, and connected peace of mind, protecting what's inside their home, whether they are at home or out.

Newly opened stadium ensures security with contactless access

A fully-integrated access management solution from Abloy will ensure smooth, secure and safe access for customers and staff at the newly-opened Nokia Arena in Tampere, Finland. With a capacity of 15,000 people, the visually-striking Nokia Arena also includes a restaurant, hotel and casino. To ensure the easy passage of its anticipated 1 million customers per year, plus 600 permanent staff and numerous temporary workers during events, it is essential to separate public areas from premises accessible only to employees or hotel guests.

The carefully-tailored solution implemented by Abloy combines the assets of Abloy OS access control, including overall management and access rights to smart devices, electromechanical Protec2 Cliq locking products and keys, wireless Aperio door handles and Abloy Exit push bars.

In the arena, the doors are opened with access rights stored on mobile devices and wristbands. "For example, an ice hockey team training in the rink does not have to worry about losing or returning keys to the right place when their access rights expire at the end of the session," says Jani Helenius, Property and Security Manager at Nokia Arena. When granting access, it is also possible to determine which premises can be accessed and at what times.

"The locks are integrated into the work shift system of the arena's restaurants," says Mikael Ermala, Key Account Manager, Abloy. "For example, when a waiter arrives at the beginning of his or her shift, the access rights granted to the person immediately take effect in the necessary premises."

Directing an audience of 15,000 to safety in case of emergencies is essential. That's why the locks on the arena doors are integrated with the fire safety system. Smooth evacuation is ensured by Abloy push bars, so that the doors open quickly and easily when needed.

Nokia Arena is a striking example of security trends, where access rights are becoming digital and door environments are touchless. second counts. Plus it's easy for things to get lost. To lose a key is particularly irritating: 50 colleagues, which means 50 keys. In the past, losing a key was a major problem. We can't allow just anyone to have access."

A Cliq Go electromechanical system from Assa Abloy now provides a 21st-century access control solution. The station has been fitted with 15 Cliq mechatronic locking cylinders, which are installed and operate wire-free. Fifty programmable, battery powered Cliq keys have been distributed among authorised keyholders. A standard battery inside every Cliq key powers the microelectronics inside the locking cylinder.

Cliq Go's app-based system management makes access control easy for Mistelbach's fire brigade. They can run all their locks from a standard smartphone. From the Cliq Go app, any non-specialist can issue new keys or cancel any that are lost.

"The major advantage of the Cliq system is the easy key management," says Alexander Kopp, a security specialist at Alexander Kopp Schlosserei & Sicherheitstechnik in Parndorf. "One key for all cylinders. Programming is easy and there are no additional software costs. Access can be defined individually for every key and blocked again easily if a key is lost."

The Cliq principle has also made retrofitting much easier, as no cables need to be routed for the installation. The power supply is provided via batteries in the key — which are easy to replace — and not via the cylinder.

In awarding Cliq Go a GIT Security Award in the "Access Control, Intruder Alarm & Perimeter Protection" category, one awards jury highlighted its ability to help users "carry out day-to-day access control management from anywhere. For locksmiths, just one mechanical coding for all systems enables them to keep keys and cylinders on stock, and to programme and configure on demand using the software."

Fire service finds solution with electronic locking upgrade

In the town of Mistelbach, close to Austria's borders with Czechia and Slovakia, a voluntary fire service has been in operation for 140 years. In that time, they have not only fought the dangers posed by fire, but also provided first aid in special operations such as vehicle recovery and rescues. Recently they sought an upgrade to their locking system to avoid problems with lost keys and improve efficiency.

A disaster assistance service is also in place to provide regional aid in the event of a disaster and to support or relieve fire brigades on major assignments, such as large-scale fires, natural disasters, supplying emergency provisions to the population or clearing roads.

Michael Holzschuh, assistant commander of the voluntary fire brigade, outlined the requirements for a new locking system: "Quick response is essential if we are called out and every

G4S combines people & technology to secure Danish bridge

The Storebælt Link in Denmark straddles the Storebælt strait - or Great Belt in English- a stretch of water which divides Denmark into two. Danes are extremely proud of their bridges, which are some of the greatest civil engineering wonders of the modern world.

G4S has worked with bridge owner and operator A/S Storebælt, a subsidiary of the Danish state-owned Sund & Bælt Holding A/S, since 2016, managing and securing the toll operation. G4S had its contract renewed for a further three years in 2020, the first existing supplier to have done so on the project.

When it first opened on 14 June 1998, the Storebælt link, which consists of a rail tunnel and road bridge, was the longest in the world at 18 kms, and today the bridge and the toll operation ensures the smooth and efficient movement of up to 56,000 vehicles a day.

G4S manages the toll operation of the bridge which connects Zealand to Funen. The toll plaza has 12 lanes on the westbound side and 10 lanes on the eastbound. These are all located in Zealand. Drivers from Zealand go through the plaza before crossing and those driving from Funen make their payment once across.

"When a driver has difficulty making a payment or if there is a technical issue, G4S team members led by our traffic manager, are on hand to talk remotely to the driver using a voice link," said Brian Zimmerman, the department manager at the Great Belt Bridge for G4S.

"We can also turn on the video monitoring in any particular lane so we can see the payment machine and help the person remotely, so there is no need to go to the lane in person."

The operation has changed substantially over the last three years, with the implementation of a new technology system, which G4S has worked with A/S Storebælt to ensure it works accurately. This is part of A/S Storebælt's digitalisation strategy to improve the safety and security of drivers and employees alike. It has transformed the safety and physicality of the working conditions for G4S professionals, who prior to this system's operation, could walk up to 12 kms in an 8-hour shift, helping drivers with their payments.

The combination of skilled G4S employees and the technology provided by A/S Storebælt, means that up to 6,000 vehicles per hour can pass through the toll plaza. The record for a single hour is 5,600 vehicles.

Hochiki fire system installed in Norfolk Sixth Form site

Following a recommendation from Norwich Education Services, Paston College, Norfolk, has upgraded its fire system to one provided by life safety specialist, Hochiki. Norwich to become Paston College. This marked a significant milestone in the history of both colleges and saw the expansion of education and training opportunities for learners and employers in North Norfolk.

Following a recommendation from Norwich Education Services, a completely new fire system was required which would need to meet BS5839 Part 1 2017 for an L2 category. The life safety system installation project required networking across multiple sites and buildings as well as ensuring the protection of the historic Nelson Museum. And with a main road acting as a physical divide through the middle of the campus this was a complex project to undertake. TP Fire & Security were commissioned to install the new system who selected Hochiki's ESP intelligent range of addressable fire detection and alarm equipment.

Ramtech's wireless security and monitoring system helps secure Scampston Park Lodges in the United Kingdom

Part of the tranquility that comes with holiday parks is the stunning, natural surroundings, attractive on-site accommodation, and plentiful resources. To maintain this, parks must rely on robust security and safety systems, which play a huge role in safeguarding beauty spots from harm, protecting people and property.

The United Kingdom is home to roughly 6,000 holiday parks, according to Savills, generating about £9.3 billion in visitor spending, before the COVID-19 pandemic. When protecting such valuable assets, holiday and leisure park owners are challenged by the risk of break-ins and other security, or safety threats.

To better protect sites, there is a rise in parks seeking connected systems that can work together to provide the best protection combined with other useful park management tools.

Holiday parks can have multiple security and site management systems in place. Popular forms of protection include physical teams of security staff patrolling parks, CCTV cameras, intruder alarms and more. It isn't uncommon for parks to utilise a combination of tools, however, managing multiple systems often leads to increased cost and more time spent by staff managing the park security.

On top of this, park owners also have an obligation to ensure that the site is well run and safely managed. This means being able to raise alerts to hazards such as fire, medical emergencies, SOS and more.

Furthermore, practical considerations like invoicing occupants based on their cabin's energy usage and keeping track of when shared utilities need cleaning or servicing, can continue to add up to the extra time and resources spent on monitoring a park.

Realising that the number of security, maintenance and alert systems needed by holiday parks is vast, has resulted in the advancement of technology to create 'connected parks'.

Connected parks link together security and other monitoring requirements of the park, in order to keep it safer than ever before, while also providing crucial insight to help streamline park operation.

An example of this technology in action is at Scampston Park Lodges, which has used Ramtech's wireless WISE security and monitoring system to cover the 35-acres site, since 2011. Choosing to have 27 alarms, once an alarm is activated inside a lodge due to a break-in, this then works in harmony with the Ramtech REACT cloud-based system to deliver a notification, which is instantly sent to park staff, pinpointing the exact lodge for a response.

For lodge owners, the peace of mind this offers is priceless, particularly given the system's wireless capability, ensuring it can be installed in even the remotest of locations, as well as being completely scalable should they need more alarms in future.

By using smart wireless technology, systems like the WISE security alarm that Scampston Park Lodges has in place, are then straightforward to combine with other useful security and safety systems, including Ramtech's WES emergency wireless fire safety alarms.

The WES system for instance can combine both fire monitoring and emergency call point features, that once activated will inform the park operators and the emergency services if programmed to do so.

While sites must ensure that safety and security is robust, often supporting insurance claims and marketing the site to prospective holidaymakers, other park management features, which support the efficient and daily running of the park, are also welcome. This is where technology has evolved to help answer these added value requirements at the same time as emergency response needs.

As an answer to this, WISE has integrated smart metering services, communicating in real time accurate energy use data and consumption patterns. Benefiting the guest and staff, employees can be connected from a park management perspective, receiving reports on any cleaning and maintenance activities that are required to be undertaken.

The potential to transform holiday park security, safety and general management, through integrated and connected solutions is within grasp. By combining monitoring and alert systems, this not only saves valuable management time, but also allows for easier gathering of data and ultimately helps to increase the speed of responses. For busy holiday park site owners and their teams, the value of connected parks therefore cannot be underestimated.

Raytheon selects viisights Wise Behavioral Analytics for TSA Evaluation Initiative

viisights, the developer of innovative behavioural recognition systems for real-time video intelligence, has been selected for airport cargo security evaluation by global defence contractor, Raytheon Security (RTX).

The Transportation Security Administration (TSA) contracted Raytheon Technologies to select and evaluate next-generation security solutions for airports. To conduct the test, Raytheon deployed viisights' advanced video and behavioural analytics solution for cargo security at various airports across the U.S. for evaluation over twelve months.

Powered by neural networks and advanced deep learning algorithms, viisights' unique behavioural analytics technology can identify suspicious behaviour, vehicle traffic congestion, crowd density and human proximity, perimeter protection, and people or parcels in restricted areas with outstanding accuracy.

To help ensure compliance with new health safety-mandates, viisights advanced analytics can also detect and notify security personnel if individuals are not wearing protective face masks in areas where masks are mandated.

Optimised to minimise false alerts and their related costs while maximising safety and security, viisights video and behavioural analytics solutions provide new levels of predictive and proactive video intelligence for myriad applications including violence and suspicious activity detection, incident prevention, response management, and risk mitigation.

To maintain personal privacy protection, viisights advanced technology analyzes general behaviour patterns of individuals, groups, vehicles, and traffic-flows without identifying faces or licence plates.

Raytheon plans to keep the viisights behavioural analytics solution in place at the airport installation test sites after the initial evaluation period has been successfully completed to help better secure airports moving forward.

Vimpex's ClamBell helps protect remote modular data centres

Vimpex's innovative new ClamBell fire alarm bell has been chosen by a global supplier of Modular and Skid-mounted solutions to be fitted to the outside of the company's modular to sound a loud, audible warning in case of fire.

Central Engineering manufactures a range of Electrical, Mechanical, Process, and Communications Modules, each uniquely designed to securely house equipment and plant for the data centre, oil & gas, utility, mining, and marine markets. Modules are installed indoors, outdoors, onshore, or offshore often in remote locations, with deployments in Ireland, the UK, Europe, Russia, the Middle East, Africa, and South America.

Jack MacNelis of local installers JMN Fire Alarms Ltd. Says, "As these modules are often sited in hostile, remote, mountainous areas, Central's requirement was for an extremely reliable and weather-proof external fire bell for its modular that, in case of a fire, would be loud enough to warn anyone in the vicinity. ClamBell's 'two minutes to fit' and rugged durability has proved to be the perfect solution."

Vimpex's ClamBell is an innovative, UK manufactured, fire alarm bell with a unique hinged design that swings shut after installation, which means it's quick to install, aesthetically pleasing, and reassuringly reliable - setting it apart from other fire alarm bells on the market.

The ClamBell's permanently fitted gong and unique hinged design do away with the long, complicated installation process of other bells. With no central bolt, the ClamBell® can be fitted in a matter of minutes. All installers need to do is fit the ClamBell to the wall, wire it to the circuit and then click it shut. It is that easy.

With three different base types, shallow, deep, and waterproof, as well as multiple voltage variations, the ClamBell® meets the needs of the international market and has every installation method covered.

ClamBell is designed and manufactured in Britain by Vimpex, Europe's independent manufacturer and distributor of fire alarm system components. Due to careful design and manufacturing, a single model has simultaneously been approved to EN54 Part 3 by LPCB and is pending UL 464 for the U.S. market. The ClamBell has also been independently IP tested to IP56 by Intertek, meaning true weatherproof performance.

Hikvision secures one of the busiest shopping malls in Turkey's capital

Keeping a watchful eye over the thousands of visitors that flock to Ankara's vast Metro Mall every day is no easy job. To achieve real peace of mind, the security team chose a video security solution from Hikvision and received reliable, innovative, and cost-effective technology to protect shoppers and staff 24/7.

The Metro Mall in Ankara, Turkey, is one of the busiest entertainment and business centers in the capital. Combining more than 200 stores with offices, a cinema, cafes, restaurants, and a gym, the site covers nearly 220,000 square metres, while the nearby metro station sees a footfall of more than 300,000 commuters every day. Given the busy nature and complexity of the location, the security of shoppers and workers is a top priority – but it's also a challenge.

"We knew well before it opened that the Metro Mall was bound to become a hotspot for shoppers and commuters and that security would be a challenge," says Bahri BERÇİN, the Metro Mall Manager. "We needed a solution that could cope with this complexity, and which we could rely on."

"We had several proposals of CCTV solutions, but the proposal from Hikvision Turkey stood out by far," said Bahri BERÇİN. "The full solution was very thorough and the technology appeared to be of extremely high quality."

Hikvision began the project by working with Meriç Technology ltd. to carry out a site survey. "Being such a complex and busy site, we needed to ensure we had enough cameras to offer comprehensive security," says Yunus Bölükbaş, the Presales Engineer at Hikvision Turkey.

Following the survey, Hikvision and its partner designed a CCTV solution comprising more than 500 cameras to be located both inside the mall, the parking lots, and around the perimeter.

For security inside the mall, Hikvision recommended its 2MP Varifocal IR Bullet Cameras mounted to the walls, and Vandal-proof Network Dome Cameras mounted on the ceiling, assisting the security team with situational awareness at all times.

For reliable outdoor security – day, night, and in all weathers – Hikvision Network IR PTZ Dome Cameras were installed around the perimeter of the mall, for a comprehensive view of the mall's exterior, while their 20x optical zoom enables the security team to inspect potential threats in very close detail.

Hikvision also installed Access Control panels and Mifare Card Readers, to enable security personnel and other authorized mall staff to gain secure card-based access to restricted areas. The whole solution was connected to Hikvision Network Video Recorders, to support all processing and analysis of the recordings at the mall's security control center.

"It's making a real difference," says Hüseyin GENÇER, the Metro Mall technical manager of the project. "The solution is helping us protect the mall's customers much more effectively, and providing reliable evidence for the investigation of security incidents, which is exactly what we had hoped for."

The access control panels are also helping to secure the restricted areas of the mall. "We can give each member of staff access to the parts of the mall that are relevant for their work. We are also able to see where everyone is at all times," adds Hüseyin GENÇER. "Also, integration between the Hikvision CCTV and Mavili fire Alarm systems has helped us improve our low voltage system management operations".

The security team is planning to expand its system to the nearby residential area, which comprises five buildings, each 30 stories high. Hikvision also plans to install the iVMS-5200E Centralised Management System and integrate it with the mall's third-party alarm system, so that the Metro Mall team can manage video streams, access control devices, and fire alarms from a single place.

Hüseyin GENCER is very happy with the technology and how the project was run.

Fire alarm & detection market rises with Covid impact

The global fire alarm and detection market size is expected to reach USD 56.06 billion by 2030, registering a CAGR of 7.2% from 2022 to 2030, according to a study conducted by Grand View Research, Inc. The market is gaining prominence, more so amidst the Covid-19 pandemic that hit the world economy in 2020, with businesses shifting to remote working models.

The demand for residential fire safety witnessed a rise, with people spending extended hours working from home. The global demand continues to witness growth over the next seven years. While the pandemic created a few lucrative opportunities for the Original Equipment Manufacturers (OEMs). Awareness about the safety and security of assets in the commercial sector also increased.

As businesses resume operations, the need to safeguard facilities with guidelines and installations promoting fire safety will encourage building owners to either replace old equipment or install new safety devices. In addition, the advancements in fire safety products by leveraging the latest wireless technologies will help OEMs keep up with the competitive rivalry in the industry. Advancements followed by cost-effective products and service & maintenance post installations will go a long way in favouring sales. Vendors aim to launch new products and leverage opportunities in emerging markets by developing a local sales network and closing new business deals.

All such efforts by OEMs will drive the growth of this market over the next few years. Apart from new equipment sales, the demand for the replacement market is also on the rise. Ageing infrastructure with outdated fire safety devices will pave the way for new business opportunities over the next seven years. The replacement scenario is likely to create several growth opportunities particularly in the North American and European regional markets, where the market has hit the ceiling, in terms of growth.

A summary of other findings from the report include the point that mandates and guidelines promoting fire safety in residential, commercial, and industrial settings will upkeep the product demand over the forecast period; smoke detectors witnessed a significant demand in 2021; however, heat detectors will register a significant CAGR from 2022 to 2030; regulations governing the commercial sector resulted in the segment dominating the market in 2021; and the market in North America has reached maturity, in terms of demand; however, ageing infrastructure will drive replacement sales over the forecast period.

Key Players operating within the fire alarm and detection market and cited by the analysts in the report include: Johnson Controls, Honeywell, Napco, Nittan, Siemens, Halma, UTC, Bosch and Eaton.

What to know about data centre fire protection

Despite the rarity of data centre fires, they can devastate your organisation when they occur. Good fire protection provides insurance you hope you don't have to use. Good data center fire protection requires four elements: mitigation, detection, suppression and recovery. This means you have facility elements in place to prevent fires from occurring, alert staff when a fire does happen, put out or control a fire and repair facilities after fire damage.

Fire mitigation

Mitigation is the easiest and least costly part of fire safety, but also the most often ignored. Never store flammable materials, particularly cardboard boxes and plastic packaging, in the data center. These also contain major particulate contaminants you shouldn't bring inside.

Infrared (IR) scan your main electrical connections at least yearly. Varying IT loads can cause wires to expand and contract. IR thermal imaging detects loose connections before they become dangerous, which eliminates one of the major causes of electrical fires.

Fire detection

Smoke detection is a code requirement. To avoid shutting down your data center, you can use dual-interlocked systems with ionisation- and infrared-type heads, both of which must activate before alarming.

Even better are early detection aspirating systems that sense smoke earlier than standard heads. The Xtralis VESDA, which stands for very early smoke detection apparatus, and Honeywell FAAST, for fire alarm aspirating sensing technology, are the most common systems used in data centres. These smoke detectors suck air samples through small pipes and can distinguish between smoke and dust.

Early smoke identification enables you to identify and respond to fire threats with portable extinguishers well before standard heads would detect it. Aspirating systems are the least expensive part of any fire control system.

Fire Suppression With Water

You can suppress fires through a variety of means, although gas and sprinklers are the most common forms in data centres. Most codes require sprinklers, which activate when fire gets hot enough to melt fusible links in the heads and send a deluge of water into the space.

This can greatly damage your data centre and present issues related to leaks and malfunctions, so many data centres use dry-pipe, preaction, dual-interlocked designs. In these designs, pipes are charged with compressed air or nitrogen to keep them rust-free, and the system can alert you to leaks before water escapes. Water only enters the system when two detectors alarm, but it doesn't discharge until fire melts the fusible links in the heads. However, the drawback to such systems versus traditional wet-pipe sprinkler systems is that you often accumulate a more significant amount of smoke and fire damage before the room floods with water.

A fog mist system disperses water in tiny droplets that remove heat from fire by evaporation but don't get equipment wet enough to cause harm. Mist also enters cabinets where standard sprinkler water might not and suppresses smoke, which is often as harmful as the actual fire. Local codes determine whether fog mist works as a substitute for sprinklers.

Fire Suppression With Gas

Gas-based systems come in two types: clean agent and inert gas. Clean agent systems contain chemicals that break the fire triangle by removing heat. Inert gas systems reduce the oxygen level such that fire can no longer burn but people can still breathe.

FE-24 is a halocarbon related to FE-36 that requires no piping change and causes zero ozone depletion. FE-36 is the clean agent used in handheld fire extinguishers. The most recent clean agent is 3M Novec, which is stored as a liquid and dispersed as a gas. Novec is a non-halocarbon with zero ozone depletion, zero global warming potential and only a five-day atmospheric lifetime. Total immersion liquid cooling systems also use this agent.

Inert gas systems combine atmospheric gases that, when discharged in a closed space, reduce the oxygen percentage to below 15% so fire can't burn but people can still breathe. The most widely known are Inergen -- composed of 52% nitrogen, 40% argon and 8% carbon dioxide -- and Argonite -- 50% each nitrogen and argon. Being atmospheric gases, they cause no global warming and no ozone depletion, but they require a large amount of gas. This necessitates significant storage space for very-high-pressure tanks. Additionally, when suppressed with just inert gas, fires can still smoulder and emit smoke.

All gas-based systems can produce noise levels on discharge that can damage high-density disk drives. Most manufacturers can supply lower-velocity heads to help mitigate this damage. All gas-based fire suppression systems also require rooms to be sealed and ceiling tiles to be clipped into place, which means additional construction expense -- a requirement water-based systems do not have. A hybrid system, such as Victaulic's Vortex system, can combine water suppression with reduced oxygen fire suppression.

Recovery from a data centre fire

Data centre recovery time is costly. Hard shutdowns of IT hardware mean a full recovery could take up to several days. Damage sometimes requires obtaining and configuring replacement equipment.

Water might be more messy than harmful, provided it doesn't actually enter your hardware, but smoke can be highly difficult to clean up. The best course of action is to minimise your chances of a fire from the outset, have an early warning system in place, and ensure that someone can respond quickly if an alert occurs in the middle of the night.

As more electric cars take to UK roads, attention is turning to their safety, in particular fire safety

No matter that petrol and diesel cars can catch fire and many of them do, an electric vehicle fire (there were 54 in London in 2019) commands a lot more attention.

A few reasons: the technology is new, so newsworthy; EV fires are complex and often heralded by a highly toxic vapour cloud accompanied by a hissing noise and highly directional jets, followed, possibly, by an explosion; they can occur spontaneously; and putting out an EV fire is virtually impossible. You think it's out and then it erupts again hours, days or even weeks later.

All this considered, it's no wonder people are becoming concerned about electric car fires, not least those who have to put them out. Thankfully, fire services are developing strategies to deal with them. Bedfordshire Fire and Rescue Service, for example, has announced that in the aftermath of any incident, road traffic collision or fire involving an EV, "one of our attending fire engines will follow the recovery vehicle back to the unloading point at their yard to assist with any fires". It also said it has developed a system that enables fire crews to identify what model of EV is involved in an incident and where its battery and isolation switches are.

Experts are divided on how best to tackle an EV fire but, gener-

ally, immense quantities of water to cool the battery pack (although this won't prevent fire erupting again), a fire blanket to suppress the flames and breathing equipment for the firefighters to protect them from the toxic vapour cloud is the standard approach. Either that or simply let the blaze burn itself out.

Attempting to suffocate the fire with inert gases is ineffective because, being a chemical blaze, it does not require oxygen. Meanwhile, the surrounding area must be checked for discarded battery cells that could have been propelled from the battery pack by an explosion and might spontaneously ignite later. Following containment, the burnt-out EV must be removed and deposited in a compound away from buildings and other vehicles. (Some 25% of scrapyard fires are caused by spent lithium ion batteries.) More radical steps include immersing the car in water, although not sea water because chlorine gas can be released.

It all sounds quite alarming and a good reason not to buy an electric car, but Paul Christensen, professor of pure and applied electrochemistry at Newcastle University and senior advisor to the National Fire Chiefs Council, is keen to quell fears about EV fire safety, especially given the benefits the technology offers.

"As someone who assisted Nissan during the creation of its battery plant, I would, if I could afford one, have a Nissan Leaf tomorrow," he says. "We don't need to be worried about the small incidence of fires involving electric vehicles but we do need to be aware. A lithium ion battery stores a huge amount of energy in a very small space. Since 2008, the adoption of such batteries has outstripped our appreciation of their risks. We're running to catch up but we will do eventually."

As part of his campaign to improve EV fire risk awareness among first responders, Christensen has, so far, presented to 30 of the UK's 50 fire services, as well as to fire services in Europe, Australia and New Zealand. He begins each talk by describing the structure of a lithium ion battery cell. A sliver of aluminium, called the cathode, is coated with a mixed-metal oxide ink. It's partnered by a slice of copper coated with graphite called the anode. In between them is a fragile, perforated plastic separator soaked in an organic solvent that contains a small quantity of additives whose identity is, troublingly, known only to the cell manufacturer. Depending on whether the battery is being charged or discharged, the lithium ions move either from, or to, the cathode and anode.

Then the professor gives his audience of firefighters their first shock. Full, a cell contains 4.2V of charge, but even when empty, it still holds 2.5V. A Nissan Leaf has from around 192 cells in 24 modules and a Tesla Model S over 7000 in 16 modules. That's a lot of energy when the car's power indicator says it has none. Full or 'empty', the risk of this energy escaping in an uncontrolled fashion is what some scientists believe leads to 'thermal runaway', when heat and gases fuel even higher temperatures and still more gases, including hydrogen and oxygen, in a self-fulfilling loop until the cells begin to burn and burst. A toxic vapour cloud develops, bringing with it the risk of deflagration. Once thermal runaway has started, no battery management system or circuit breaker can stop it. "A battery fire can be controlled but it cannot be extinguished," says Christensen.

He has demonstrated in tests how perforating or otherwise damaging a battery pack, as in a crash, can cause it to catch fire. "If an EV's battery case is dented, you have to assume it's dangerous," he says. Battery packs have been known to catch fire through overheating and while being charged. More worrying, a battery fire can erupt spontaneously, contamination of even just a single cell during its manufacture being one possible explanation. "Even the most experienced and careful manufacturers have defective electric cells passing through their very careful quality control systems," says Christensen.

A battery flame is like a blowtorch that will quickly ignite anything in its path, which is why Christensen wants councils and other organisations to consider EV safety risks in underground car parks, as well as bus depots where vehicles are parked side by side. "In Germany, three bus depots have gone up in flames in the past six or so months," he says. "Tunnels, ferries, car parks, cargo ships transporting EVs – all the places you find electric vehicles should be considered a safety risk and the appropriate steps taken."

He's worried about classic cars being converted to run on used lithium ion batteries, too. "Nobody really knows how safe used lithium ion batteries are and no standard test has yet been devised to tell us," he says. "Some batteries re-enter the market having been removed in illegal chop shops. How safe are they? There's a lot of research into lithium ion battery safety but everyone needs to link up because, right now, we're at the bottom of a very steep learning curve."

Tackling supply issues in the security & fire safety market

The fire safety and security markets are highly dependent on electronics and with that they are also affected by the supply chain crisis, caused by a combination of the pandemic and the rapid global acceleration and demand for digitalisation. Here, Euralarm looks at the impacts of the supply chain crisis, including compliance issues and the "green deal" and what may lay ahead for the security and fire industries.

Several industries had problems even before Covid-19. Producers of chips, computer parts and other components needed for the digitalisation of our society were already under great pressure. The production capacity of these goods is limited worldwide and the slightest change in demand can cause supply problems. This was already the case with smartphones, (game) computers or televisions. Chips had already entered the automotive industry on a large scale, and with the electrification of this industry, the demand for chips soared. We see a similar development in industries and parts of society where the (Industrial) Internet of Things is becoming commonplace.

The consequences of the corona crisis have led many governments to recognise that the high dependence on producers out of one region poses a great risk to certain sectors. The challenge is to reduce the risks by the creation of more and better distributed production facilities. In the pursuit of lean manufacturing, production has been outsourced to Asia which means that a shutdown of factories in one country can have a global impact. According to Euralarm, the EU also recognised this even before the pandemic. Accelerated by the corona crisis, the EU is focusing its policy, among other things, on increasing domestic capacity and diversifying the number of suppliers.

For many companies that were caught off guard by global lockdowns, the speed of recovery is almost as insidious and led to another supply chain crisis during the pandemic. Increased consumer spending and thus demand for products, combined with delayed transportation by sea and air caused major shortages and record backlogs. The tightness on container capacity is expected to continue for some time. This will not help to clear shortages of electronic components, which is expected to continue for some time.

In the fire safety and security industries, the effects not only concern the manufacturers of equipment but also companies in the field of service and maintenance of systems. Outside this there are other areas that can impact building safety. The chain reaction initially caused by the shutdown of factories in countries affected not only the supply chains but also the workflows within and between companies.

Paul van der Zanden, General Director of Euralarm adds: "Another relevant topic that affects our industry is the compliance of the products that the industry delivers. With electronic components not being available due to the supply chain problems, manufacturers need to reconsider replacement of parts that aren't available. However, with the replacement of certain components, the conformity of the final product may also be at stake." This could make it necessary to have the product retested and re-certified. High (and unnecessary) costs could result from this.

Securing a sustainable supply of metals and minerals used for components in fire safety and security equipment is also key to meeting the energy and climate targets for 2030 and beyond. The European Green Deal aims to make the EU's economy sustainable. However, the transition towards green technologies, like renewable energy, e-mobility and stationary energy storage relies heavily on critical raw materials, such as cobalt, neodymium, tungsten, etc. and on new products and services. Both globally and in Europe it is expected that the demand for these materials will continue to increase. This can create challenges for the Green Deal. The impact of extracting and processing these resources is high while the supply chains are often not transparent and may lack traceability. Another challenge is the recycling of the materials. For most critical raw materials, the recycling efficiencies are low while the dependency on non-EU countries is high and still increasing.

The green ambitions of the EU could therefore also lead to certain activities being brought back to the West either to reduce the dependency of non-EU countries or to avoid CO_2 emission as a result of transporting goods from other parts of the world to Europe. This could lead to shorter logistics chains and more sustainability in several sectors. In that sense, Euralarm suggests that the current crisis in the high-tech supply chains contributes to a greener world and a stronger Europe.

Alcatraz AI discusses about top 7 data security breaches and ways to prevent them

Tech talk

No one is immune to a data breach. From universities and hospitals to corporate giants and government agencies, almost every organisation has encountered a security incident. Data security breaches not only expose sensitive information but can also cripple businesses. Users need the right physical and digital security measures to safeguard critical information.

If users want to protect the data, they should know what to look out for. Learning about the top security breaches can help better prepare against attacks.

So, how do security breaches commonly occur? Alcatraz AI discusses the most common ways intruders infiltrate an organisation and provide solutions to help users reduce the risk of a data breach.

A data breach is a security incident in which confidential information has been accessed without authorisation. The information can be financial data, medical records, or trade secrets. Data security breaches can be physical or electronic whilst most data leaks are attributed to hacking, theft of hard drives and physical files also compromise sensitive information.

Breaches typically occur when an unauthorised individual can bypass digital or physical security controls. Despite employing modern security systems, many institutions are still vulnerable to infiltration by hackers and intruders.

Whether it's customers' personally identifiable information (PII) or commercial secrets, safeguarding sensitive data is crucial to running a successful business. For many organisations, a security breach can be a disaster. In addition to the immediate financial impact, a data security breach can undermine trust in the brand and make companies lose competitive advantage.

From class-action lawsuits to lost customers, failing to protect data inflicts significant costs and consequences on businesses. In 2021, the average cost of a data breach was $4.24 million. Leaks and attacks are even costlier in heavily regulated industries. The cost of a data breach is $6.45 million for healthcare organisations and $5.86 million for financial service institutions.

Now that users know why information security is so important, how can users keep the data safe? Although users can't completely avoid data security breaches, they can mitigate the risk of it happening. With the right security measures in place, users can shield confidential data from digital and physical compromise. Following are the top security breaches and how to prevent them:

1) Distributed Denial-of-Service

Distributed denial-of-service (DDoS) is a cyberattack that shuts down a network by flooding it with traffic from multiple sources. This overwhelms the system and makes it unavailable to its intended users whilst a DDoS attack doesn't constitute a data security breach, the tactic is often used as a smokescreen to distract the IT department from network infiltration attempts.

DDoS attacks are tricky to identify because they can be indistinguishable from legitimate traffic spikes. Although they can't be prevented, users can employ rate limiting, network diffusion, and web application firewalls to mitigate the impact of the attack. Pay careful attention to network intrusion attempts that might be running in parallel to the attack to prevent a security breach.

2) Password hacking

Many employees create simple passwords that are easy to remember. In addition to weak passwords, one in three employees shares their credentials with co-workers. These poor password practices are behind many data security breaches. According to a Verizon Data Breach Investigations Report, 81% of hacking-related breaches used weak or stolen passwords.

Despite being one of the top security breaches, password hacking is quite easy to prevent. Setting up two-factor authentication (2FA) can help users deter unauthorised access. 2FA employs a two-step verification process to authenticate the user. After entering their password, a security code is sent to the user's mobile phone to verify their identity and grant them access.

3) Physical data theft

When talking about averting data security breaches, most people automatically think of antivirus software. But cyberattacks are not the only way data is stolen. Almost 10% of malicious breaches are caused by a physical security compromise. Lax physical security in the server room or other privileged areas of the facility can lead to the theft of data and hard drives.

Adopting biometric access control systems like the Alcatraz AI can help prevent physical data theft by intruders. Its facial authentication solution employs artificial intelligence and tailgating detection technology to bar unauthorised entry into secured spaces. By providing access only to approved individuals, Alcatraz AI keeps sensitive assets in trusted hands.

4) Phishing scams

Users probably know about or have been a victim of a phishing scam. Phishing is a form of cybercrime in which hackers attempt to steal information from users by tricking them into revealing sensitive data or downloading malicious software like ransomware. Because the emails and websites mirror those of reputable companies, many people fall for this scam.

In 2020, phishing scams were the most common cause of data security breaches globally. How can users avoid falling prey to this top security breach? The best way to protect an organisation from phishing attacks is to teach the employees how to identify suspicious emails. Implement an ongoing cybersecurity training programme to keep the staff educated on the latest threats.

5) Information misuse

Security breaches don't always result from malicious intent. Accidents and negligence can also lead to compromised data. Sometimes an employee stumbles into confidential information they should not have seen. Or a member of the staff handles a document without following the correct procedures. These instances can lead to information leaks and data loss.

Improper use of information is responsible for more than one in twelve data security breaches. These incidents often occur because the organisation doesn't have appropriate access controls in place. Alcatraz AI will help users set different access privileges for every employee. This will prevent low- and mid-level staff members from seeing or using sensitive information.

6) Malware attacks

Malware short for malicious software is a blanket term for harmful programmes that are designed to control, spy on, or damage computer systems. There are many different types of malware. These include viruses, worms, trojans, spyware, and ransomware. Malware can be used to steal data, disrupt operations, or extort money from the victim.

Malware attacks are among the top security breaches. More than 17% of data security breaches are attributed to malware infections. Users need a multi-pronged strategy to keep this ever-growing threat at bay. Installing anti-virus software, using non-administrator accounts, and updating the operating system regularly can decrease the risk of a malware breach.

7) Insider threats

Many organisations are so preoccupied with neutralizing external attacks that they overlook insider threats. Employees know the ins and outs of how an organisation operates. A malicious insider can inflict significant damage on the establishment. The Sony Pictures data breach known as the hack of the century was allegedly conducted by disgruntled employees.

Unauthorised personnel are involved in 30% of data security breaches. Creating zero-trust security architecture is essential to protect high-value information from disloyal employees. By requiring all employees to be authenticated, authorised, and continuously validated before granting access, Alcatraz AI fosters a zero-trust environment to help reduce insider security threats.

Despite using the latest cybersecurity tools, data breaches are on the rise. That's because, in addition to digital security, users must also protect the data physically. Restricting physical access to sensitive hardware can shield sensitive data from unauthorised personnel. Users need a modern physical security system alongside cybersecurity solutions to thwart data breaches.

With real-time verification, multi-factor authentication (MFA), and tailgating detection, Alcatraz AI is the best physical security solution users can find. Its cutting-edge technology is easy to set up and provides a seamless user experience. Sign up for a free demo now to see firsthand how Alcatraz Rock can improve a facility's data security.

How public passport systems benefit from digitalisation

Thanks to digital systems for the application and issuance of identity documents, countries around the world are modernising and optimising their processes. Veridos, a leading global provider of integrated identity solutions, explains why these systems are an important tool to increase efficiency and transparency.

Today, digital systems ensure fast and secure processes for the application and issuance of ID documents in many countries. "These solutions provide significantly more efficiency and transparency in the passport system," says Marc-Julian Siewert, CEO at Veridos.

Non-transparent analogue processes in public administration can be a source of widespread problems. This also affects the ID and passport system. Too much paperwork instead of a central digital platform can lead to applications not being processed in chronological order or containing errors. Due to this lack of transparency, citizens may even receive documents to which they have no entitlement. This applies, for example, to diplomatic and consular passports. Furthermore, citizens cannot trace how long the issuance of documents takes, which complicates further public registrations or travelling.

"Digitalisation allows a high level of process transparency which guarantees both the citizens and the respective state more security and predictability. Both benefit from this development," explains Siewert. "The example of the People's Republic of Bangladesh is an impressive example of this."

In Bangladesh, for example, workflow systems automatically send alerts when applications

remain unprocessed or work steps are not carried out, so that clerks can intervene immediately. Automatic text messages inform citizens that their documents are ready for the pick-up, providing them with official proof. Through online payment, the systems keep cash out of the processes and thus provide payment transparency.

To ensure that as many citizens as possible can benefit from these efficient processes, the systems are inclusive. For example, micro-payments via SMS also integrate people without smartphones or credit cards.

"In order to have the processes completely under control, Bangladesh has also brought the entire value chain into its own country, including production and personalization centres," adds Siewert. "Comprehensive know-how transfer has also proved to be a decisive factor. Local employees have been trained in the technologies and procedures and are consistently putting them into practice."

Veridos is a world-leading provider of integrated identity solutions. According to the company, governments and public authorities in more than 100 countries use the company's uniquely comprehensive product portfolio. The company creates end-to-end tailored solutions and services to meet every government identity needs.

AI and ethics rank high in 2022 surveillance trends

The new landscape brought on by the global upheaval and change over the last two years, has also created new types of security challenges. Employees, customers and partners increasingly are working from remote locations, sharing and collaborating through disparate online networks, which may leave data vulnerable to theft. And, as sites are monitored remotely, new public health and safety guidelines are governing how businesses operate. Here is a preview of some of the new trends as seen by Hanwha Techwin's Head of Product & Marketing, Uri Guterman, and his assessment of how they will impact our industry in 2022.

1. AI edge computing / analytics: the proliferation of data and analytics is driving business decisions

Surveillance and security solutions are increasingly incorporating on-board analytics to deliver data that can drive intelligent protection and monitoring. The role of on-board analytics will continue to expand significantly in 2022 and beyond, as customers combine edge computing and AI to achieve enhanced monitoring and search efficiency.

One industry report predicts that the total global edge computing infrastructure will be worth more than $800 billion by 2028. The use of AI at the edge, especially with analytics based on deep learning algorithms, will form a key element in a range of "smart surveillance" applications. These include object detection and classification as well as the collection of attributes in the form of metadata – all while reducing latency and system bandwidth requirements and enabling real-time data gathering and situational monitoring.

AI and edge computing will continue to improve the efficiency and effectiveness of network video surveillance systems, applying analytics (object, loitering, virtual line and area crossing, detection to name a few) to monitor every type of area or situation. With AI and edge computing enabled by cameras being used across vertical sectors, users can conduct 'pre-emptive detection' and rely less on reactive monitoring - increasing safety and efficiency.

2. Vision-based surveillance systems are being integrated with AI

Network video surveillance systems are advancing from being simple monitoring devices to form comprehensive solutions that can be applied in every vertical industry and market sector. The driving force behind this is AI technology integrated with systems at every level, a trend that is expected to see unparalleled growth. Indeed, industry analysts estimate the global AI-based surveillance and security market will reach $4.46 billion as soon as 2023.

The data generated by AI vision solutions using AI cameras as vision sensors creates meaningful business intelligence to help organisations gain a better understanding of their customers and their operations. Thermal imaging and body temperature detection cameras at public space entrances and lobby areas use edge-based AI algorithms to bypass non-human heat sources and reduce the frequency of false alarms. Cloud-based solutions use people-counting algorithms to help store owners evaluate sales or floor design strategies, or heat-mapping to measure and avoid long checkout lines to increase customer satisfaction. Similar applications and benefits can apply to traffic management or smart parking systems, logistics and distribution, or healthcare for critical area monitoring. Businesses can automate their security tactics, with the appropriate response already planned and ready to deploy.

3. The rise of the 'as a service' business model

'Video Surveillance as a Service', 'Access Control as a Service' – these are all terms being heard more commonly across the security industry. But what do they really mean, and what are the benefits of an 'as a service' business model?

With the evolution and increasing maturity of cloud-based services, video surveillance manufacturers can now transform into 'Solution as a Service' providers. Video surveillance system installers and integrators can now provide solutions to their customers through cloud-based platforms, and then extend this model to every area of their business.

The global market for public cloud application services is set to be a multi-billion-dollar industry in 2022. Companies can realise many benefits by packaging applications, infrastructure and business processes into a combined 'as a service, or 'aaS' offering. They can react quickly to rapidly changing market conditions, go to market faster with new products and services and maximise the benefits of advanced analytics to enhance operations through meaningful insights – all helping to create a unique competitive advantage.

Using these models, organisations can tailor solutions more closely to their needs, instead of relying on off-the-shelf offerings. An aaS approach can deliver scalability and cost-effectiveness, reducing capital expenditure by providing services under an operating expenditure framework, with services provided on a subscription basis.

Applying aaS principles to video surveillance – resulting in so-called 'VSaaS' – can allow users to adopt cloud-based recording. This removes the need for on-site servers and allows organisations to rapidly deploy systems without the need for complex and time-consuming network configurations. Cameras and all devices can be centrally monitored and many network and system processes can be automated.

4. There is an increased focus on the responsible and ethical use of technology

As organisations have embraced digitisation, the ability to manage operations remotely and gain better insight through the data that systems generate has delivered greater value. For many businesses, it has been nothing less than transformational.

Yet as more of their operations move online, are managed remotely and rely on the cloud, organisations must put robust cyber security strategies into place to protect the data that is proved so valuable to them. For, according to Interpol, instances of cyber-attacks have increased dramatically during the pandemic, whether through phishing, online scams and malware such as distributed denials of service (DDoS).

As a result, organisations are increasingly aware of their data protection responsibilities under measures such as the General Data Protection Regulation (GDPR), and are looking for suppliers and partners that not only understand surveillance-related data privacy rules, but can help ensure their data is kept safe at all times.

While it is a US-based initiative, the National Defence Authorization Act (NDAA) is still of importance to many European businesses. National security concerns are spreading beyond the US, and governments around Europe are showing clear signs of hardening their stance.

On this basis, manufacturers vying for certain types of contracts, especially in the government sector or related to international trade, will need to enforce compliance across their operations and product lines if they expect to win new business opportunities.

5. The integration of technology is set to continue

Network technology and the Internet of Things (IoT) are already widely embraced but they will continue to disrupt the security camera market, enabling new advances in HD video streaming, even on mobile devices. These technologies will expand the potential applications for audio and video analytics and AI in an increasingly connected world. On a broader level, there's a massive upsurge in widespread digital transformation, with the key technologies driving this change including IoT and network as well as cloud computing, intelligent data and AI.

The IoT is expected to be positively impacted by developments in network technology, especially in terms of bandwidth and latency. Adding advanced network technology to cameras supports remote real-time video surveillance, the expanded use of mobile applications and legacy network management.

Artificial Intelligence Internet of Things (AIoT) can enable an almost unlimited array of potential opportunities, from open and integrated system/platforms to expanded device connectivity.

In short, 2022 will see the continued development of technologies such as AI to provide greater value to users, which in turn will create new business opportunities for installers and integrators. And, as AI is increasingly adopted at the edge – on camera – its benefits will reach a far wider audience and are set to transform the security market.

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

KAWACH PROTECTION SYSTEMS
Excellence on Guard

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
01-04 March 2022
SecureExpo 2022
Ekspograd-Yug
Krasnodar
Russia
http://www.securexpo.ru/en-GB/

INDIA
03-06 March 2022
PACC 2022
Goa,
India
https://fsai.in/

NORWAY
09-10 March 2022
Sectech
Norges Varemesse
Lillestrøm
Norway
http://www.securityworldmarket.com/sectech/no/index.asp

UK
15-17 March 2022
Security & Policing 2022
Farnborough International Exhibition and Conference Centre,
Farnborough,United Kingdom
https://www.securityandpolicing.co.uk/

INDIA
23-25 March 2022
7th Smart Cities India 2021 Expo
Pragati Maidan
New Delhi India
http://www.smartcitiesindia.com/

UK
05-07 April 2022
The Security Event
N.E.C. Birmingham
U.K.
https://www.thesecurityevent.co.uk/

RUSSIA
12-15 April 2022
Securika Moscow 2022
Crocus Expo International Exhibition Centre Moscow
Russia
https://securika-moscow.ru/Home?culture=en-GB

CANADA
20 April 2022
Security Canada East
Sheraton Laval, Laval,
Quebec
Canada
http://securitycanadaexpo.com/

KOREA
20-22 April 2022
Secon 2022
Korea International Exhibition Centre - Kintex Seoul
Korea
http://www.seconexpo.com/2020/eng/main.asp

INDIA
27 April 2022
Top Indian Women Influencers In Security
Delhi/NCR
India
https://www.securitytoday.in/

NIGERIA
10-12 May 2022
Securex West Africa 2022
Lagos,
Nigeria
https://www.securexwestafrica.com

UK
17-19 May 2022
International Firex
ExCeL London,
London
United Kingdom
http://www.firex.co.uk/

INDIA
19-21 May 2022
Secutech India
Bombay Exhibition Center,
Mumbai
India
https://secutechindia.tw.messefrankfurt.com/mumbai/en.html

CZECH REPUBLIC
22-24 May 2022
ASIS Europe 2022
Prague Congress Centre,
Nusle Prague
Czech Republic
http://www.asiseurope.org

USA
14-17June 2022
ESX Electronic Security Expo
Music City Centre
Nashville, TN
USA
https://www.esxweb.com/

INDIA
17-18 June 2022
Security & Fire Expo-South India
Chennai Trade Center
Tamil Nadu
India
http://www.safeindiaexpo.com/

UK
21-23 June 2022
Infosecurity Europe
Excel
London
United Kingdom
http://www.infosec.co.uk/

INDIA
06-07 July 2022
International Police Expo 2022
New Pragati Maidan
Delhi
India
www.internationalpoliceexpo.com/

USA
24-26 August 2022
IAFC Fire-Rescue International
Phoenix Arizona
USA
http://www.iafc.org/fri

SAUDI ARABIA
13-15 September 2022
Intersec Saudi Arabia
Riyadh Exhibition Center
Riyadh,
Saudi Arabia
https://intersec-ksa.ae.messefrankfurt.com/ksa/en.html

GERMANY
20-23 September 2022
Security Essen 2022
Messe Essen, Norbertstrasse 2, Essen,
Germany
https://www.security-essen.de/impetus_provider/

SECURITY UPDATE Postal Registration No. GRG/32/2022-23
Published on 28th day of every month

SECURITY UPDATE is registered with
The Registrar of Newspapers for India, No. HARENG/2011/39714

HIKVISION®

See Far, Go Further

WEB CAMERA

REMOTE CONFERENCE

BRIDGE ANY DISTANCE

FOCUS ON THE MOMENT

HD 1080p

Wide-angle Lens

Hi-Def Sound

Plug & Play

USB

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

Sales:
+91-22-4041 9944, 2846 9944
sales@pramahikvision.com

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

RMA Support:
+91-22-6822 9977, 3322 6070, 2846 9977, 0250 663 6677
rma@pramahikvision.com