SECURITY

FOR TODAY'S SECURITY PROFESSIONAL

BUYER

Are we entering a new arms race?

Exploring the escalating situation between Russia and the US over the INF treaty
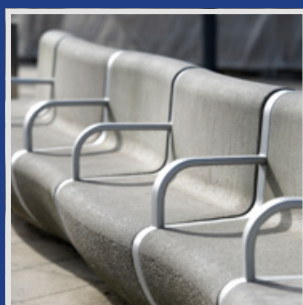
Surveillance

Fighting crime with a smart city mindset

THE GLOBAL SECURITY INDUSTRY'S LEADING SOURCE OF COMMENT, ANALYSIS AND OPINION

GOVERNMENT
E-SCAN RADAR ON
THE INDIAN BORDER

COUNTER TERROR
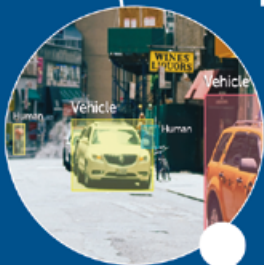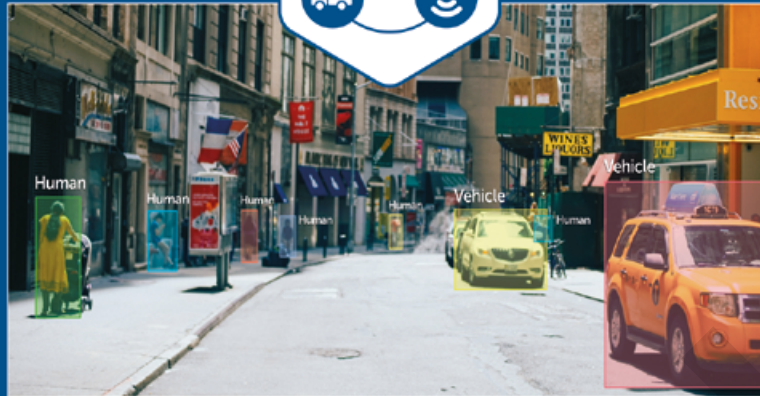MITIGATING VEHICLE-
BORN ATTACKS

EVENTS
SECURING THE
SUPER BOWL

SHOW PREVIEW
LOOKING AHEAD TO
THE SECURITY EVENT

Face recognition and search

Fire and smoke detection

NEURAL NETWORK ANALYTICS

Sharpen the vision of your VMS

Object classification

Human and vehicle detection

License Plate Recognition

AxxonSoft has developed a process for adapting neural network filters to the needs of a specific site. The neural network learns to perform customer-specific tasks from video material obtained at the site, which guarantees high-quality results.

To resolve issues of high resource consumption related to AI, AxxonSoft uses a blended approach with a neural network filter applied to an object tracker — the filter can identify a specific type of moving objects or abandoned items.

How it works:

1. The classic object tracker detects moving objects or abandoned items in the FoV.

2. It passes the section of the frame with the object to the neural network for analysis.

3. Any objects that don't match the defined type are ignored by video analytics (they don't trigger an alarm).

This technology is applied to video that captures high movement from interference (i.e. beyond the object of interest), such as trees blowing in the wind, light reflected off water, traffic, machinery, etc. Usage examples are alarms that are activated when people appear in hazardous areas of a facility, or applications that reduce the number of false alarms for abandoned objects in public spaces.

Learn more about AxxonSoft software

AxxonSoft products also use third-party tools for recognizing faces and the numbers on vehicle license plates, railcars, and shipping containers.

axxonSOFT

EXPERIENCE THE NEXT®

Welcome to the latest issue of Security Buyer

There is not a lot of security equipment that people form emotional attachments with. But military aircraft certainly fit into this category.

As such, it was not surprising that the news that the UK's Royal Air Force will officially retire its fleet of Tornado jets at the end of March managed to capture the imagination of the British public. And it is little wonder, with almost 40 years of active service under its belt, the aircraft has certainly achieved an iconic status.

First entering service in 1979, the aircraft has been used in operations across the world. It first saw active service during the first Gulf War in 1991 when 60 Tornado GR1s were deployed from bases in Saudi Arabia and Bahrain. Two years later the planes were upgraded to the GR4 model, which has been used ever since and seen action in the skies of Kosovo, Afghanistan, Iraq and Syria.

Most recently, the Tornado fleet was called upon for bombarding Daesh to push the terrorist group back through Syria and Iraq. Following four years as part of Operation Shader, on 5 February this year the aircraft finally returned home from operations for good. While retired from active service during February, the jet will still be taking to the sky for training missions above the UK until the end of March.

Of course, the end of service for one aircraft naturally leads to the start for another. In the immediate term, the RAF is replacing the Tornado fleet by upgrading the weapons capabilities for the Typhoon jet. Under 'Project Centurion', worth £425 million which has taken place over the past three years, the Typhoon now has deep strike cruise missile Storm Shadow, air-to-air missile Meteor and the precision attack missile Brimstone at their disposal.

Combined with this is the RAF's new fleet of F-35 Lightning jets. Alongside the Typhoon jets, these will be used to form the backbone of the UK's combat air fleet in the coming years.

It is easy to overlook the Tornado when discussing Britain's iconic military aircraft. But its key role in some of the country's recent military operations means it certainly deserves to be held up alongside some of the much-heralded aircraft of the past.

On a related note, I'm looking forward to attending SCTX in London this month. It would be lovely to see as many of you as possible at the show, so please do come along to booth I35 to say hello.

Enjoy the magazine!

If you'd like to submit relevant news stories for the next issue of Security Buyer please email **editor@securitybuyer.com**

James Ling,
Managing Editor

Twitter: @SecurityBuyer
LinkedIn: securitybuyeruae

SECURITY BUYER
FOR TODAY'S SECURITY PROFESSIONAL

MANAGING DIRECTOR
David Rossiter • + 44 (0) 1622 823 937
E-mail: david.rossiter@hand-media.com

MANAGING EDITOR
James Ling • +44 (0) 1622 823 922
E-mail: james.ling@hand-media.com

EDITOR
Christian Brown • +44 (0) 1622 823 922
E-mail: christian.brown@hand-media.com

DESIGNER
Emma Hampshire • +44 (0) 1622 823 922
E-mail: emma.hampshire@hand-media.com

DESIGNER
Rochelle Mills • +44 (0) 1622 823 922
E-mail: rochelle.mills@hand-media.com

PROJECT MANAGER
Ryan Graves • +44 (0) 1622 823 929
E-mail: ryan.graves@hand-media.com

OFFICE MANAGER
Lauren Mitten • + 44 (0) 1622 823 921
lauren.mitten@hand-media.com

HAND MEDIA
INTERNATIONAL
print | digital | video

HAND MEDIA U.S.A OFFICE
20F Street NW, Suite 700,
Washington D.C. 20001 U.S.A.
Tel : +(1) 202 507 6378

HAND MEDIA HONG KONG OFFICE
2/F, Shui On Centre, 6-8 Harbour Road
Wanchai, HONG KONG
Tel : +852 2824 8605

ANNUAL SUBSCRIPTION RATES:
UK and Europe £99 Rest of World: £149

SECURITY BUYER
is published by: Hand Media International

Goldings, Elphicks Farm, Water Lane, Hunton,
Kent, ME15 0SG, United Kingdom.
Tel: +44 (0) 1622 823 924
Fax: +44 (0) 1622 823 933
Email: info@securitybuyer.com
Website: www.securitybuyer.com

REPRINTS: For reprints of specific pages within this magazine please telephone Lauren Mitten on 01622 823 929 or e-mail lauren.mitten@hand-media.com

452/ISB/03/2019
The text paper in this publication is printed on PEFC paper

CONTENTS

030

HEALTHCARE

044

DATA STORAGE & SECURITY

032

RETAIL

050

CYBER
Huntsman Security provides cyber security scorecard, Sophos announced XG Firewall management platform

EDUCATION
Three Australian universities have rolled out SafeZone protection for students and staff using CriticalArc

060

EDITORIAL MISSION STATEMENT:
International Security Buyer Magazine is written for buyers and purchasers within the security industry. It also informs the security industry overall with the latest news, trends and innovative product releases. Readers are also given access to detailed features, interviews and case studies from some of the leading professionals within the global security industry.

SECURITY
FOR TODAY'S SECURITY PROFESSIONAL

SECURITY BUYER   @SECURITYBUYER   SECURITY BUYER

ON THE COVER THIS ISSUE

SECURITY
FOR TODAY'S SECURITY PROFESSIONAL
www.securitybuyer.com

Are we entering a new arms race?

Exploring the escalating situation between Russia and the US over the INF treaty

Surveillance

Fighting crime with a smart city mindset

THE GLOBAL SECURITY INDUSTRY'S LEADING SOURCE OF COMMENT, ANALYSIS AND OPINION

GOVERNMENT
E-SCAN RADAR ON THE INDIAN BORDER

COUNTER TERROR
MITIGATING VEHICLE-BORN ATTACKS

EVENTS
SECURING THE SUPER BOWL

SHOW PREVIEW
LOOKING AHEAD TO THE SECURITY EVENT

ON THE COVER OF THE MARCH 2019 ISSUE

TRADE WAR

SURVEILLANCE

@VERACITYGLOBAL

Don't miss out on visiting the Veracity booth at Security TWENTY19 in Birmingham on Thursday. Learn about VIEWSCAPE's extensive and successful history, with a large install base of long-term, high-profile customers. Register today http://bit.ly/ST19Birmingham

@AVIGILON

How to be an MVP in stadium security? Read our latest blog on the top 3 solutions to help stadiums meet their security needs: http://ow.ly/CoAD30nL5G7 #security #stadiumsecurity #publicsafety

@PULSESECURE

#PulseSecure #SDP is not about "rip and replace" but rather an evolutionary approach that's fully integrated within our #SecureAccess platform and your existing infrastructure. Check out Pulse Chief Marketing Officer, Scott Gordon's article on Pulse SDP™

@DALLMEIER_COM

Modern video surveillance in airports requires flexible solutions which fulfil stringent quality & security demands. Learn more about @Dallmeier_com Airport Solutions at 7th Annual Africa Airport Expansion Summit, Feb 25-26 2019 in Kigali, Rwanda http://africa.airportexpansionsummit.com/ @Lnoppen

HIKVISION EUROPE

Are previous employees still able to access your server? User management is an important part of maintaining cybersecurity. Check out how to configure this in our IP cameras

BAE SYSTEMS

Just as the smartphone has become indispensable in under a decade, so could cobotics become embedded in manufacturing and transform working practices of the future.

GET IN TOUCH
WITH SECURITY BUYER

Connect with us on Linked in, Twitter or Facebook, we look forward to hearing your thoughts and opinions on the latest topic in the industry.

veracity

COLDSTORE Colossus
Uniquely engineered for long retention of video storage

COLDSTORE'S patented sequential recording system greatly extends the lifetime of hard disk drives, offers high reliability with lower power and very low total cost of ownership.

LOW TCO

- Engineered specifically for IP video surveillance
- Optimised for long video retention periods
- 630TB Storage in COLDSTORE consumes < 80watts
- Low Total Cost of Ownership
- No data loss on disk failure and no rebuild required

GMB signs historic sole recognition agreement with ICTS at Heathrow Airport

GMB, the union for staff at Heathrow Airport, has recently signed a sole recognition agreement with aviation security company ICTS at Heathrow Airport following four months of negotiations. The agreement will cover all terminals and cargo at the Airport.

GMB has been recognised as the leading Union at Heathrow Airport representing the best interests of its members, especially following the success of its campaign to get the London Living Wage at Heathrow Airport, benefiting thousands of workers across the Airport. ICTS has many contracts across Heathrow including; aircraft guarding, hand baggage screening, aircraft crew screening and cargo security and has been successful in obtaining new contracts across all terminals where GMB have a large membership base.

GMB has worked with the company over many years at the Airport on the Virgin and Delta Airlines aircraft guarding contracts and now this will extend to all contracts across the Terminals at Heathrow.

"This is fantastic news for our members across Heathrow and the GMB London Region in securing this recognition agreement with ICTS," said Perry Philips, GMB Regional Organiser for Aviation at Heathrow. "This will give us the collective bargaining unit for all ICTS contracts for the purpose of pay and conditions negotiations and other business where the company will consult with the GMB on matters affecting our members.

"We have always held good working industrial relations with ICTS and this extension to our joint recognition agreement strengthens our partnership working together for the future and to the benefit of GMB members," he continued. "Both GMB and ICTS have worked together through good relations to achieve this agreement and credit should also go to our GMB Heathrow Aviation Branch and activists who have also worked hard with the company to secure this agreement."

British anti-terrorism security company claims Australian accolade

A British manufacturer of anti-terrorism security measures has been recognised by the Australian security industry for its latest innovative product. Coventry-based Safetyflex Barriers has received the 'Product of the Year' award at the Australian Security Industry Awards for its 9-40 Truckstopper Bollard.

Safetyflex teamed up with Australian distributors EZI Security Systems in 2018 after specifically testing the 9-40 for sale in the country, which has been on high alert since the January 2017 car attack in Melbourne which saw six people killed and 30 more injured.

The product is reportedly easy to assemble or take down as required and can stop a 7.5 tonne truck travelling at high speeds and is also described as the cheapest removable bollard system on the market today. It also has a foundation size of 20cm, meaning that it can be set up without the need to re-divert utilities.

"The team at EZI Security Systems are incredibly proud to have been honoured at the Australian Security Industry Awards, there is no higher accolade for their work over there," said Marcus Gerrard, Director at Safetyflex. "Our business in Australia is moving quickly, so to have made such an impact with our first design specifically made for that country is a testament to the quality of

our work. As Safetyflex Barriers is the fast-growing anti-terrorist barrier company in the world, we have some very innovative and niche products, that no other company can offer. "We have teamed up with EZI Security systems as they are the leaders in Australia for anti-terrorist bollards and barriers, as well as protecting key assets and public realm projects. We hope that our products and the confidence shown in them by such an important organisation gives people some piece of mind."

"We are proud to be working with Safetyflex to protect people and infrastructure in Australia," concluded Troy Donnelly, at EZI Security Systems. "The 9-40 Truckstopper Bollard is a great product and this award is recognition of the hard work that has gone into designing it."

Door Group signals doorset improvements for Network Rail

Door Group, a unit of ASSA ABLOY Opening Solutions UK & Ireland has supplied a number of high security steel doorsets to Network Rail for the upgrade of its remote signal rooms. The project was commissioned through Kent-based trade customer, Taylor Refit, which removed the existing doors and installed new high security steel doorsets certified to LPS 1175 security ratings from the Powershield range. The upgrade comes as part of Network Rail's plan to heighten the security level to its signal rooms following the recent vandalism.

Network Rail specified that the high security doors supplied to offer maximum protection to the remote rooms, whilst also providing a cost-effective solution. ABLOY Protec cylinders were also incorporated into the specialist locks throughout the sites. Taylor Refit was able to remove and install the security doors in one day, resulting in minimal disruption to services.

"We are delighted that Network Rail gave us

the opportunity to provide superior security doorsets to this project and we hope to build on our relationship in the future," said Chris Cole, Area Sales Manager (SE & London) for Door Group. "We pride ourselves on supplying high quality products and we work closely with our customers to understand their specific requirements and to provide specialist and tailored solutions. We had to ensure that the doorsets we were supplying offered maximum security, as per the customer's specifications."

Door Group's work with Network Rail follows several high-profile contracts with Transport for London and Crossrail Limited.

"We pride ourselves on our portfolio of well-respected clients that choose to work with us time and time again," concluded Brian Sofley, Managing Director for Door Group. "We attribute this to our comprehensive service offering and expert advice throughout each project."

Magenta Security Services' boss highlights need for security industry to support public services

A combination of uncertainty over Brexit negotiations and recent cut backs in other areas of police funding has highlighted an opportunity for the private security industry to support public services.

"Brexit is putting an incredible strain on resources of all types across the UK, including the police force, who are preparing contingencies for a host of challenges ahead of March 29," commented Abbey Petkar, managing Director of Magenta Security. "When combined with the selling off of police assets and the reduction in officers on the street it makes life very difficult when it comes to the prevention of criminal activity. I have incredible respect for the police. They are doing a tough job under difficult circumstances and deserve our support."

Petkar believes that via current contracts and private initiatives, security companies across the UK can deliver for clients whilst partnering the police to highlight and where possible stop criminal activity. "The security industry is incredibly diverse and already working across a host of services to prevent crime. We already support public services by filling gaps and spotting vulnerabilities that opportunists could exploit. A partnership-based relationship with the police will do nothing but improve this," continued Petkar. "For those of us carrying the proper certification there is even the opportunity to directly support public services, supplementing their workforce where needed."

Ultimately, Petkar believes there is a significant opportunity for the private sector to support public services and give back to the wider community. This is ever more true as the SIA works to professionalise and improve the quality of output from across the sector. Public safety should, in Petkar's opinion, be the responsibility of all, not just the few hardworking police officers.

Apprentices fired up by wireless alarm technology in Scotland

Apprentices in Electronic Fire and Security from New College Lanarkshire have learned about wireless technology from Kent-based company EMS. The company, which specialises in wireless and hybrid fire detection systems, gave a presentation to students at the Kirkintilloch Campus.

Mark Todd, the company's Regional Sales Director, enlightened trainees on the history of wireless systems and their growth to become a popular option in the industry. Around 30 second and third-year apprentices gained a greater appreciation of the differences between wired, wireless and hybrid systems and how the technology is applied.

Todd gave examples of when a wireless solution might be best used, including heritage buildings, time-critical installations, the expansion of existing wired systems, and situations where asbestos might be present.

"The students have gained an in-depth knowledge of EMS wireless fire alarm systems, how they operate through radio transmissions, and the massive benefits of wireless solutions for engineers, security companies and clients," said Douglas Couttie, Workbase Assessor in the Faculty of Engineering and Automotive Studies. "EMS' wireless system was used throughout the training session in order to demonstrate the system working in a live environment, programming devices on to the system and fault finding. It was interesting for our apprentices to see first-hand how the system is designed before installation, including conducting radio surveys."

"EMS has been involved with young people for some time and we engage with many schools, colleges and learning establishments, as we believe that the future of our industry is in the hands of tomorrow's engineers and technicians," said Ray Puttock, Vertical Sales & Marketing Director for EMS. "We are a strong advocate of reaching students at an important time in their education path and informing them of options and career opportunities, in a technical manufacturing and service environment, which they may not know exist."

New College Lanarkshire has opened a specialist hub for Electronic Fire and Security courses at its Kirkintilloch Campus which allow apprentices to access state-of-the-art equipment for training or up-skilling.

Kryon achieves ISO/IEC 27001:2013 certification for information security

Kryon has announced that its information security management system has officially received ISO/IEC 27001 2013 certification. Kryon had already received certification for ISO/IEC 9001 for controlling quality procedures. In addition, it is compliant with the General Data Protection Regulation (GDPR).

"At Kryon, we are committed to maintaining the highest level of information security in order to offer a premium RPA solution," said Kryon's CEO, Harel Tayeb. "Meeting the standards laid out by the International Organisation for Standardisation and the International Electrotechnical Commission is an important achievement. It reflects the value we place on the security of our customers' sensitive data."

This certification is applicable to every level of Kryon's IT infrastructure, including research and development, marketing, sales, support, training and professional services. It covers all of Kryon's cloud-based and on-premises solutions: Kryon Attended Automation, Kryon Unattended Automation, Kryon Hybrid Automation and Kryon Process Discovery.

"We at Kryon believe that trust should not be given blindly to any technology, especially when woven throughout a business' processes," said Nathaniel Davidson, CTO of Kryon. "This ISO/IEC 27001:2013 accreditation is a reflection of our ongoing commitment to providing our customers with the level of security that they expect and deserve."

The requirements that companies must meet in order to receive ISO/IEC 27001 certification are laid out by ISO/IEC, a joint committee of the International Organisation for Standardisation and the International Electrotechnical Commission that sets international standards for information assets. Kryon's certification was granted by IQNet following preparation and submission by BDO, a global financial and auditing firm.

Non-profit organisation accelerates data classification to comply with GDPR and saves £80,000 per year

Horizon Leisure Centres has deployed Netwrix Auditor to ensure GDPR compliance and satisfy data subject requests in minutes. Horizon Leisure Centres is a not-for-profit organisation that operates leisure centres in the Havant and Waterlooville areas.

With limited financial and human resources, Horizon needed a cost-effective solution to secure personal information about its members to meet GDPR requirements. Specifically, it needed to streamline discovery and classification of regulated information and make sure it could quickly satisfy data subject requests.

Horizon reportedly chose Netwrix Auditor for its effective discovery and classification of data and real-time search functionality. With the software, Horizon achieved a number of improvements.

As the first step on Horizon's path to GDPR compliance, the IT team ran data discovery with Netwrix Auditor. With the accurate, detailed results, they were able to ensure that sensitive data is stored in secure locations where only management can access it.

Horizon is ready to address requests from data subjects in just a few minutes. Without Netwrix Auditor, even just a few requests per month would have required hiring four full-time employees and paying them £80,000 per year in total, a cost the non-profit's budget simply could not absorb.

The software enables the IT team to know what is happening across their file servers and detect improper or malicious activity around regulated information in a timely manner.

"Netwrix Auditor has enabled us to be proactive towards GDPR and classify all the data we have in over half a million folders. The software is a great time saver. To satisfy a data subject request, I will need only a few minutes to retrieve all necessary information," said Iain Sanders, IT Manager at Horizon Leisure Centres.

Rosehill Security partners with Damasec Global Group for Denmark and Sweden

Rosehill Security, a manufacturer of Perimeter Security Solutions, announced a product distribution agreement for Denmark and Sweden with Damasec Global Group for the company's range of hostile vehicle mitigation (HVM) barriers and perimeter security products.

Denmark-based Damasec wanted to add the line to address the growing need to protect crowded spaces and perimeters in light of recent vehicle borne attacks worldwide. Damasec's exclusive distribution rights will allow the company to sell Rosehill Security's products to clients with a wide range of HVM and perimeter security requirements throughout Denmark and Sweden.

"We are pleased to partner with Rosehill Security as an advocate and exclusive distributor of their products, as it will allow us to provide our clients with effective and inventive HVM and perimeter security systems while supplementing our existing product range," noted Henrik Færch, CEO at Damasec Global Group.

Made up of units weighing 49kg each, the Rapid Defender temporary VSB has been specifically designed to be manually installed in minutes to protect people at events from vehicle as a weapon attack. Requiring no special tools or lifting equipment, a four-man team can manually install a 15m barrier in under five minutes.

The much larger, IWA 14-rated Impakt Defender has been designed for temporary, semi-permanent and permanent applications to protect both entrance areas and site perimeters against hostile vehicle attack. Each 430kg solid rubber unit is connected by steel securing cables or rods to create a barrier capable of stopping heavy vehicles travelling at 48kph.

"Proactivity in providing protection against vehicle as a weapon attacks continues to be a high priority, so we are delighted to announce Damasec as our partner, ensuring access to a proven range of products for their clients," concluded Dalton Marshall, Sales Manager at Rosehill Security.

Dardan Security opens Cambridge Head Office to spearhead national growth

Dardan Security has opened a new three storey head office in Shelford, Cambridge to cater for its expanding client base and range of service provided for businesses and organisations throughout the UK.

"Continued growth and expansion, both geographically and in terms of the scope of the security services we offer, has seen the company become a major player on a national level," stated Philip Anthony, Dardan's Managing Director. "On the back of recent success and with clients located the length and breadth of the country, the requirement for a centrally located head office and control room has become increasingly evident."

The move has created eight new jobs in Cambridge. Dardan's new head office is at Grain House, Mill Court Great Shelford, Cambridge CB22 5LD.

LonTrend launches LTSX03 explosion-proof camera positioning system

LonTrend has launched LTSX03 explosion proof PTZ housing for monitoring harsh environment security.

Inheriting the attributes of its parent product LTEX17, LTSX03 comprises different variants like the flexibility for adding heater, blower, wiper and built-in IR 30/60/100m to fit a variety of installation environment. As for the pan and tilt function, LTSX03 standard product delivers 360° endless rotation and ±90° tilt which enables unlimited zero spot monitoring from limited installation sites.

Constructed by stainless steel 304/316L with CNEX certified Exd II CT6 explosion-proof marking, the LTSX03 is fully compatible with camera systems that support Pelco P/D protocol and RS485 standard. Therefore, the control of pan, tilt and wiper can be fully integrated with most of the IP camera systems.

Kinesis vehicle telematics helps Lincolnshire Security guard the guards

Kinesis vehicle telematics is giving Lincolnshire Security complete visibility of its mobile operation. The recently implemented tracking system gives the Boston-based company round the clock monitoring of mobile staff for resource planning, incident response, customer reporting and health and safety responsibilities.

Offering a wide range of guarding and mobile security, Lincolnshire Security service offering includes alarm response and key holding, mobile patrols, static guards and special event security.

Integration with fuel cards from UK Fuels means Kinesis also gives Lincolnshire Security additional intelligence including driver performance data and financial transactions with a single platform for all their fleet-related data. Other benefits of Kinesis include live traffic alerts and congestion reports, improved security and asset management and better financial management.

"We have used vehicle tracking for some time now," commented Lee Revell, Account Manager at Lincolnshire Security Ltd. "So, when the time came to review the in-situ system we looked around for alternatives. Kinesis was cost efficient, functionally rich and integrated with our existing fuel cards.

"Kinesis is easy to use with live location reports displayed against an easy to interpret map screen. It's also easy to access – available on any Internet connected device," continued Revell. "The peace of mind provided by Kinesis coupled with the additional evidence-based reporting is critical for staff safety and customer reporting and will help us control costs as we continue to grow the business."

Kinesis integrated fuel cards will reportedly help Lincolnshire Security reduce paperwork associated with credit card or expenses claims and improve the management of fuel consumption with accurate MPG calculations potentially assisting in decreasing costs and environmental emissions. Kinesis can also deliver driver performance data, including speeding, harsh braking and accelerating and idling, which can be used to monitor and improve driver behaviour for additional health and safety monitoring and cost control.

Two thirds of SMEs are more concerned about cyber-attacks now than they were 12 months ago

Businesses in the UK are more concerned about cyber-attacks now than they were a year ago, according to the latest Close Brothers Business Barometer research. Two thirds of SMEs (67%) said they were more worried about cyber security threats now, with around a third of these (31%) reporting that they were significantly so.

The figures were collected after several high-profile data breaches and other attacks were reported in 2018. Large and well-known enterprises were affected, including British Airways, Ticketmaster and Facebook.

Companies in London were most likely to be perturbed, with over 85% saying their concern had increased over the previous 12 months. In Yorkshire (75%), the North West (73%) and the North East (72%), business leaders were also more nervous about the issue now. Those in the South East were least likely, with just over half saying that they were more worried now than they were at the end of 2017.

Many businesses have met this challenge head on by investing in methods of protecting themselves against online crime. According to Close Brothers' research, 62% of companies are spending more on cyber security than they were a year ago. Just 25% of businesses said their spending had remained steady year-on-year.

Regional expenditure increases coincides with concern. London businesses were most likely to spend more, with 82% saying they devote a greater amount to cybersecurity now than they did a year ago. This was followed by increased outlay in Yorkshire (72%), the North East (67%) and the North West (65%).

"It is positive that businesses across the UK are taking online security seriously and are making every effort to ensure that they are not unnecessarily vulnerable to cyber-attacks," David Thomson, CEO of Close Brothers Invoice Finance. "SMEs can invest in cybersecurity prevention methods, such as anti-virus software, secure networks and staff training. However, even with these precautions in place, it is vital that businesses remain vigilant because online criminals are continually developing more sophisticated techniques and technology."

State of Utah projected to save millions of dollars with Forescout's integrated ServiceNow solution

Forescout Technologies has created an integrated solution with ServiceNow to deliver an asset intelligence solution for customers, such as the State of Utah. To protect approximately 60,000 network-connected devices across state agencies that serve 3.1 million inhabitants, the State of Utah relies on Forescout's integrated solution with ServiceNow's offerings for automated, agentless visibility and real-time asset management, resulting in projected compliance cost savings and a dramatic improvement in network visibility and control.

"The powerful Forescout solution that integrates ServiceNow's offerings helps the State of Utah eliminate network blind spots and maintain an accurate asset inventory at all times, which is critical to achieving regulatory compliance and minimising security risk," said Pedro Abreu, Chief Strategy Officer, Forescout. "We believe collaboration across the industry is key and this integrated solution brings together the right ingredients for Utah to orchestrate a successful security management system and as a result, improving its cybersecurity posture, IT efficiencies, and overall bottom line."

The State of Utah began looking for trusted security partners as manual compliance tasks on its large network were projected to cost more than US$1 million. With Forescout's ServiceNow integration, Utah is projected to save millions of dollars resulting from faster audits by automating real-time asset management, compliance remediation and incident response workflows.

"As a trusted and strategic digital transformation partner to more than 40% of the world's largest public companies, ServiceNow delivers digital workflows that create great experiences and unlock productivity," said Pablo Stern, Vice President and General Manager, IT operations management, ServiceNow. "The combination of our world-class security operations management and IT Operations management with Forescout increases operational efficiency, service reliability and cybersecurity effectiveness to transform how people work."

Color in Darkness

Full-color Camera for 24h Color Video Surveillance

Full-color

- Full HD STARVIS™ sensor & F1.0 aperture lens provide high color reproduction and excellent low light performance for a more vivid, brighter image.
- Advanced 3DNR & image processing technology delivers clearer images, super noise reduction and storage saving.
- 24/7 color monitoring significantly increases probability of collecting valid human, vehicle , and event evidence.
- Smart white light (HAC Models) serves as supplementary light source to guarantee image usability even in total darkness.
- Built-in mic and audio-in interface enable audio-over-coax collection as auxiliary for video surveillance (HAC Models).
- Great solution for applications in low-light environments, such as parking lots, urban streets, shops, schools, etc.

Recommended Models

IPC-HFW4239T-ASE	IPC-HDBW4239R-ASE	HAC-HFW2249E-A-LED	HAC-HDW2249T-A-LED
1080P Full-color Network Bullet Camera	1080P Full-color Network Dome Camera	1080P Full-color HDCVI Bullet Camera	1080P Full-color HDCVI Eyeball Camera

CE FC CCC UL RoHS ISO 9001:2000

DAHUA TECHNOLOGY

No.1199 Bin'an Road, Binjiang District, Hangzhou, China. 310053
Tel: +86-571-87688883   Fax: +86-571-87688815
Email: overseas@dahuatech.com
www.dahuasecurity.com

UK medical practices increase secure data protection measures

Shred-it has been helping GP practices, dental surgeries and other medical service providers in the UK ensure confidential paperwork, such as medical records, are securely destroyed when no longer needed. This is integral in the medical sector which holds an array of confidential data, from patient and medical records to staff data, all of which is of considerable value to malicious third-parties.

Data protection has become a top priority in the medical sector of late, especially since the implementation of the EU General Data Protection Regulation (GDPR). Through its partnership with the LMC Buying Group, a federation with over 6,500 members that negotiates discounts on a wide range of products and services for healthcare providers, Shred-it has helped the industry improve data protection measures and therefore their GDPR compliance plans.

"In the past, most medical practices would have destroyed their confidential information in the same way a household would," stated Helen Shuker, Head of Operations for the LMC Buying Group. "However, there's now been a push to ensure more secure processes are applied, so in 2010 we approached Shred-it to provide our members with an easy and reliable solution to document destruction."

As part of the partnership, practices utilise Shred-it's services on both an ad hoc basis, when they need to clear out an archive of papers that are no longer needed, as well as on a monthly subscription service basis. This involves practices receiving secure consoles that are regularly collected and shredded by Shred-it's team.

"Many medical businesses have had a wake-up call with the implementation of the GDPR," adds Ian Osborne, Vice President UK & Ireland for Shred-it. "There are so many other regulations that medical practices must comply with too. Utilising Shred-it's secure information security services offers them peace of mind."

Intelligent video surveillance from Bosch spots polar bears in Alaska

Oooguruk drill site (ODS), is an important location for Caelus Natural Resources Alaska, LLC. Over 30 million barrels of oil have already been produced from Oooguruk since 2008, but the drill site in Alaska's North Slope region is also frequented by polar bears. An intelligent security system from Bosch helps to spot them. The technology has to recognise the animals as early as possible and function reliably.

"Our ultimate goal is the protection of personnel and the polar bears, and we want to do that in the way that has the least impact on the polar bears," explains John Hellén, Health, Safety and Environmental Manager at Caelus Natural Resources Alaska, LLC.

Bosch's MIC IP fusion 9000i camera combines robust design with Intelligent Video Analytics and was developed specifically for use in extreme conditions. Eleven of the cameras have already been installed on ODS while five others are at the planning stage. The engineers performed the uncomplicated installation in the shortest possible time.

The intelligent camera is fitted with a solid metal casing and Bosch starlight technology. Even in the most difficult weather conditions and low light, the system reportedly produces high-quality images. "Within two weeks of installing the cameras, we recorded two events of polar bears on ODS. We even have one camera installed 100 feet (30m) from the ground, and the resolution is shockingly good," explained Dale Hoffmann, former Land Manager for Caelus Natural Resources Alaska, LLC.

The integrated function processes and interprets data directly at the source. Polar bears can be detected early by the cameras thanks to their thermal imaging technology – even when the animals are swimming or are far off in the distance.

As soon as a hazard is recognised, the Bosch cameras´ tracking function is automatically triggered and personnel are notified. The necessary safety measures can therefore be put in place quickly and efficiently. Bosch's solution has increased safety for humans and animals on ODS – regardless of the time, light or weather conditions.

Tavcom responds to airport Drone chaos with new detection course dates throughout 2019

Tavcom Training, part of the Linx International Group has responded to requests from the security industry, for expert training in order to be better prepared for and mitigate against the threat of Unmanned Aerial Systems (better known as drones). Dates for the two-day Drone Detection classroom-based course will take place throughout 2019 and early 2020.

As reported in the February 2019 edition of International Security Buyer, in late December, the UK was alerted to the impact of a drone attack, when suspected sightings resulted in 1,000 flights from Gatwick Airport being cancelled. Then, weeks later, Heathrow also suffered a minor drone-related disruption. The financial and logistical impact on the airport, airlines and travellers (approximately 140,000 in the case of the Gatwick incident) was immense, with current reports putting the cost to the aviation industry at between £50 - £70 million.

"The responses to the airport drone attacks were played out in the spotlight, with much public debate regarding the seeming lack of a pre-defined plan of action to prevent or contain such an incident," explained Sarah

Hayward-Turton, Sales and Marketing Director at Linx International Group. "Last year we introduced our Drone Detection course and this year we will run it three times to give security professionals expert advice from experts in drone technology, to help mitigate risk and implement countermeasures to thwart unauthorised drone activity.

The Drone Detection course covers understanding drone technology, CAA regulations, battery limits, drone threats, drone detection and counter measures, understanding radio frequency (RF), drone mitigation.

The course will take place in March, May and November 2019 as well as February 2020. The classroom course costs £375+VAT and results in a Tavcom Certificate.

Alerta and Hanwha Techwin agree distribution partnership

Alerta Electronics and Hanwha Techwin Europe have established a business partnership which will see the two companies work together closely to support installers and systems integrators in Turkey.

Alerta, one of Turkey's fastest growing distributors, has been active within the electronic security sector since 2005 and has built an enviable reputation for providing "best-in-class" video surveillance solutions, backed-up with high levels of pre and post-sales support.

"Alerta's extensive knowledge of network-based solutions makes them the ideal business partner to help us promote our Wisenet IP based security solutions to the Turkish market," said Yasin Altas, Country Manager for Turkey at Hanwha Techwin Europe. "The combined strength of our comprehensive range of products, many of which incorporate technologies unique to Hanwha Techwin, together with Alerta's local knowledge and sales and technical expertise, places us in an ideal position to successfully compete together for large-scale and mission

critical video surveillance projects throughout Turkey."

Istanbul-based Alerta will be offering all cameras manufactured by Hanwha Techwin. These include Wisenet X 2MP and 5MP models which are at the heart of the company's impressive range and premium Wisenet P cameras which deliver superb quality 4K (12MP) images. Alerta's customers will also have access to entry-level Wisenet Q network 2MP and 4MP cameras and Wisenet HD+ analogue camera which deliver Full HD images in 1080p without the need to upgrade cabling infrastructure, as well as Wisenet NVRs and WAVE Video Management Software (VMS).

"We are very pleased to have the opportunity to offer the Wisenet range to our customers throughout Turkey," said Suphi Sözmen, Managing Director at Alerta Electronics. "Hanwha Techwin has already achieved a significant market share in Turkey with its Wisenet products and solutions which have a reputation for being ultra-reliable."

ROCKWOOL chooses Global Client Programme by Nedap for international security rollout

ROCKWOOL International A.S. has chosen Nedap's Global Client Programme to secure its offices and factories worldwide. AEOS, the physical security platform by Nedap installed during the programme, enables ROCKWOOL to establish a truly global security policy and unified work processes.

An advanced project rollout, the Global Client Programme is developed for large multinationals and reportedly offers several benefits, including standardisation across sites, shorter implementation times and cost efficiencies.

"The implementation of a standardised security solution across the world is a complex process," observed Fokko van der Zee, Managing Director at Nedap Security Management. "It involves a large project spanning many years and involving many stakeholders and demands a high level of project management. In the absence of a structured programme with defined guidelines, a global security rollout is likely to be a stressful execution. That's why we set up our carefully designed Global Client Programme."

ROCKWOOL Digital Service Lead, Matthew Thorne, agreed: "We've worked with

Nedap over the past few years and recently became a member of their Global Client Programme. Now we're equipped with the people and tools we needed to standardise our physical security solution. The Global Client Programme also minimises risk and guarantees compliance. It really meets our needs in every possible way."

The Global Client Programme is designed to ensure monitoring and control during every step of the rollout process. Timon Padberg, responsible for business development at Nedap Security Management, explained: "The repetitive nature of local site deployments allows us to work with models and templates, such as standard proposal and calculation documents. We can therefore produce a scalable process that ensures uniformity and a consistently high quality of implementation across each site."

News in Brief

Camden door control expands its lazerpoint RF product line

Camden Door Controls has announced the expansion of its Lazerpoint RF product line. New introductions are the CM-TXLF-1LP Lazerpoint RF recessed one-button key fob and the CM-TXLF-2LP Lazerpoint RF recessed two-button key fob. These new fobs are now also ideally suited for security/access applications.

In addition, they cannot be accidentally activated while in pocket. When used in conjunction with Camden's CM-TXLFB key fob base, they can be mounted on a wall or desk or on a belt or car visor.

Just some of the benefits of the Lazerpoint RF family of wireless products are transmission 'hops' over multiple bands to overcome interference; shorter wave length able to penetrate smaller gaps in building materials and longer battery life than any other system.

SAS 260 antennas from PPM Systems

Shrivenham-based PPM Systems has received a second order for SAS 260 antennas, for a European naval wideband electronic surveillance application.

Product features include dual low noise amplifiers, limiters and by-pass switches with antenna frequency ranges from 20MHz to 1GHz in the low the band with 20dB gain, and 1GHz to 6GHz for high band with 28dB gain. The SAS 218 version is also available with the same low band coverage and with an extended high band coverage from 1GHz to 18GHz.

These antennas are omni-directional in azimuth and vertical polarisation with an operating temperature range of 32°C to +55°C and are encased in a rugged radome. They are available in a wide range of radome colours.

Steel door and security solutions manufacturer invest in newl multi-million-pound production facility

Bradbury Group has moved into its new headquarters located on Foxhills Industrial Estate in Scunthorpe, North Lincolnshire, totalling an investment of around £8 million. The new 135,000 sq. ft production facility is an integral part of a mass expansion plan to be rolled out by the company, which is now in its 28th year of production. As part of the expansion, the company has invested several million pounds into new state-of-the-art machinery, including a new Salvagnini punch form line and a new fully-automated powder coating paint line.

This streamlined process reportedly achieves unrivalled production timescales and product quality and has significantly reduced any work in progress and the need for heavy manual handling by its employees. As a result of this investment, Bradbury Group has also announced its new three-day express steel door service, called M2MGO, for those customers that require an immediate, rapid solution or replacement security door.

The vast scale of the new premises means it can store up to 4,000 finished units, 10 times more than the previous facility, meaning that the Bradbury Group can accommodate and distribute larger orders more quickly and efficiently. Last year alone, the business produced around 17,000 door sets to clients throughout the UK, and with the capacity to produce circa 100 door sets on the new system in an average working day, higher levels of production can be achieved to satisfy increased demand.

"This investment marks the start of a new journey for Bradbury Group," said Managing Director, Tim Strawson. We are aiming high, with the aspiration to be the best and most trusted steel door manufacturer in the world. We've invested in infrastructure, machinery and our people, and we're very proud to continue the company's growth in our home town of Scunthorpe."

In the mountains of France, CLIQ key-based access control helps keep the clean water flowing

Critical infrastructure requires locks that are proven, tested and trusted. Sometimes electronic locking is the right choice; at other times, mechanical locking does the job. With CLIQ mechatronic locking technology, one water utility combined both in a single, secure system controlled by CLIQ software.

O des Aravis is responsible for water capture, storage quality, analysis and delivery of around 700,000m3 annually to homes and businesses in the Aravis Mountains region of France. PROTEC2 CLIQ key-based access control with programmable, battery-powered keys now secures 30 opening points across its premises. These locking devices are suited to protecting high-security openings, including a potentially dangerous room with high-tension electrical cabling and equipment. They are already deployed at critical infrastructure sites all over Europe.

The mechatronic CLIQ system enables the utility's facility managers to control, modify and trace every important access. They know who goes where, and when. They are aware of activity affecting all critical doors; it is even impossible to leave one unlocked. Because CLIQ is a flexible, key-based system, O des Aravis can also retain some mechanical locks at the site, operated by the same secure keys and with the same PROTEC2 high-security disc cylinders.

The CLIQ Web Manager software is built to help companies like O des Aravis manage complex workflows. System administrators can program, amend or delete keys remotely. It's straightforward to generate time-stamped audit trails for any lock or key, to track access in detail. The Web Manager can generate attendance reports for staff and contractors. Yet despite all these features, the CLIQ Web Manager requires minimal IT investment: it runs in the cloud and is accessed via an encrypted connection to a standard web browser.

At O des Aravis, comprehensive audit trails for any lock or key are available on demand. These also sync automatically when a user key is updated or revalidated. If a key is lost, a security manager can deactivate it instantly with a couple of clicks, ensuring buildings and clean water supplies are not put at risk.

New PTZ auto-tracking application with AXIS Perimeter Defender

Axis Communications' intrusion detection analytics, AXIS Perimeter Defender, now supports a pan-tilt-zoom (PTZ) auto tracking application, enabling a fixed camera and a PTZ camera to work seamlessly together to provide an enhanced solution for perimeter protection. The new application allows a fixed thermal or visual camera running AXIS Perimeter Defender to detect people and vehicles, and – when an alarm is triggered – take control of a PTZ camera to track and get closer views of alarm objects.

With AXIS Perimeter Defender PTZ auto tracking, the fixed camera sends the location data of the alarm objects to the PTZ camera, thereby controlling the direction and zoom level of the PTZ camera. The PTZ camera automatically adjusts the zoom level to keep in view all alarm objects, including new ones that appear in the fixed camera's detection zone. The application allows the fixed camera to maintain detection coverage over a large area while the PTZ camera can automatically zoom in to provide more details on the alarm objects.

AXIS Perimeter Defender PTZ auto tracking is compatible with specific Axis PTZ cameras and allows one fixed camera to be paired with one PTZ camera. The function requires a separate license from the AXIS Perimeter Defender analytics.

Defence News

DSEI launches area dedicated to manufacturers in defence

DSEI 2019 will for the first time host a Manufacturing Hub to highlight the vital contribution that tier 2, tier 3 and tier 4 manufacturers make to the UK defence industry.

DSEI 2019 will provide an opportunity for suppliers to penetrate the defence sector and strengthen their relationships within the industry, including with the prime contractors that rely on their skills and technology to deliver complex equipment programmes.

The Hub will be sponsored by the Manufacturing Technology Centre, a UK organisation established to bridge the gap between university-based research and the development of innovative manufacturing solutions, in line with the Government's manufacturing strategy.

"We are delighted to sponsor the Manufacturing Hub at DSEI 2019 and look forward to showcasing how we can help the defence sector and its supply chain modernise processes, generate efficiencies and improve productivity through new technology," said Andy Barnes, Associate Director for Defence and Security at the Manufacturing Technology Centre.

The manufacturing industry is a key part of the UK and world economy. UK manufacturing currently employs 2.6 million people, accounts for 44% of total exports and represents 70% of business research and development. Some of the most innovative technologies can be found within this space.

"We are really proud to be launching the Manufacturing Hub for DSEI 2019," noted Grant Burgham, DSEI Event Director. "We strongly believe the Manufacturing Hub will be the perfect platform to create opportunities and connections between different sectors of the manufacturing world and the defence industry. This new feature is testimony that the event is dedicated to the whole of the defence industry and to creating new opportunities for all tiers of the supply chain."

PARC and George Mason University selected for DARPA configuration security project

The Palo Alto Research Centre (PARC) and George Mason University (GMU) have been awarded a contract from the US Defence Advanced Research Project Agency (DARPA) Configuration Security programme (ConSec).

Researchers from PARC and GMU will collaborate on project SCIBORG: Secure Configurations for the Internet of Things (IoT) based on Optimisation and Reasoning on Graphs. The goal of SCIBORG is to devise fundamentally new approaches to determine security configurations that protect critical infrastructure and IoT-based systems.

"SCIBORG will measure its success in terms of the reduction of the impact of potential attacks. To reason about the security of an IoT configuration, it is important to evaluate the attack paths that are available to the adversary," said Hamed Soroush, Senior Researcher at PARC and the Principal Investigator. "Configuration settings that reduce the impact of these attack paths would, by this line of reasoning, be more secure."

The ConSec programme aims to develop new approaches to generate and deploy secure configurations of components that make up large cyber-physical and cyber-military systems. Particularly desired are configurations that will minimise the vulnerability to attacks while maintaining the expected functionality and performance. This is an intractable problem because the space of possible configuration settings is extremely large and because it is not clear how to reason about security and functionality in a system-of-systems scenario.

"SCIBORG's focus on attack paths has an interesting side benefit; it provides one way to generate evidence explaining why a chosen configuration is more secure," said Shantanu Rane, who manages the Cyber-Physical Systems Security research area at PARC and will be the co-principal investigator on this project.

To achieve SCIBORG's goals, PARC and GMU researchers will explore per-component configurations and construct graph-based models to capture within-component and between-component dependencies among configuration elements.

"SCIBORG's approach explicitly encodes constraints on the configuration parameters using graph-based models, allowing us to significantly reduce the actual number of configurations that need to be tested for security and functionality," said Ersin Uzun, Director of PARC's System Sciences Laboratory.

Royal Air Force selects SecureCloud+ for Team Tempest network collaboration

SecureCloud+, provider of next-generation secure information systems to government and defence, has been contracted by the Royal Air Force to deliver network collaboration services for Team Tempest.

The Tempest programme brings together the UK's industry and sovereign capabilities across four key technology areas for combat air systems. The four technology areas are advanced combat air systems and integration (BAE Systems); advanced power and propulsion systems (Rolls-Royce); advanced sensors, electronics and avionics (Leonardo) and advanced weapon systems (MBDA), all of which have joined with the RAF Rapid Capabilities Office to form Team Tempest.

"This is a critical programme that will deliver huge value for UK military defence capabilities," said Air Commodore Linc Taylor. "We have a long history of delivering world-class combat systems through collaboration with our best industries; this capability offers us the ability to fundamentally change the way we work and share information within and across our teams."

"We have a proven track record of delivering defence contracts on time and on budget using modern technologies to promote better communications," said Peter Williamson, Founder and CEO of SecureCloud+. "Our innovation and agility are critical components to rapidly build and develop greater collaboration. We are pleased to support Team Tempest and the vision for the Future Combat Air System Technology Initiative. This contract reinforces our commitment to innovation. And it is not just about secure collaboration – it is also about managing digital assets across industries to remove barriers to sharing and building trusted teamwork."

Boeing delivers KC-46A tanker to Altus Air Force Base

Boeing delivered its fifth KC-46A Pegasus tanker to the US Air Force, the first that will be based at Altus Air Force Base, Oklahoma. The KC-46 departed Seattle's Boeing Field for Altus, where the base's 56th Air Refuelling Squadron is responsible for Pegasus aircrew, maintenance and support training.

"We're excited to see the Pegasus arrive in Oklahoma, a strong partner to Boeing and America's military," said Boeing Defence, Space & Security President and CEO Leanne Caret. "We look forward to continuing to deliver KC-46 tankers to Altus, McConnell Air Force Base in Kansas, and New Hampshire's Pease Air National Guard Base, throughout this year."

The 56th ARS was activated August 2016 in preparation for the new tanker's arrival. Three additional KC-46A aircraft will be delivered to Altus in the coming weeks.

"The 'Mighty 97th' is looking forward to accepting and integrating the KC-46 into our mission," Colonel Eric Carney, Commander of the 97th Air Mobility Wing at Altus Air Force Base, said. "The 97th AMW has and will continue to produce combat-capable pilots, loadmasters, and boom operators for the KC-135, C-17, and KC-46 and we remain committed to innovating how we train them to be a part of a joint force to win our nation's wars."

During extensive flight testing to date, six KC-46 aircraft have completed more than 3,800 flight hours and offloaded more than four million pounds of fuel to A-10, AV-8B, B-52, C-17, KC-10, KC-135, KC-46, F-15E, F-16 and F/A-18 aircraft.

The first four multi-role KC-46 tankers were delivered in January to McConnell Air Force Base in Wichita, Kansas. The KC-46, derived from Boeing's commercial 767 airframe, is built in the company's Everett, Washington, facility. Boeing received its initial contract in 2011 to design and develop the Air Force's newest tanker aircraft.

L3 ASV delivers small long-endurance autonomous vessel to Royal Navy

L3 ASV, supplier of Unmanned and Autonomous Marine Systems, has announced the successful delivery of a long-endurance autonomous vessel known as the C-Enduro to the Royal Navy. According to the company, the C-Enduro will be used for military data gathering trials by the Mine countermeasures and Hydrographic Capability (MHC) programme as the Navy seeks to exploit autonomous technology.

"We are proud to support the Royal Navy in their plans to explore the uses of marine autonomy as they continue to invest in new and exciting technology," said Vince Dobbin, Sales and Marketing Director for L3 ASV. "This vessel is an evolution of our existing C-Enduro product range and provides the unique capability to collect a variety of data during any one mission over extended periods."

The 4.8m autonomous vessel is equipped with 10 sensors combining scientific and hydrographic survey equipment. The vessel operates using L3 ASV's proprietary control system, ASView, and is fitted with L3 ASV's autonomy package.

"The different ways in which the C-Enduro can be operated will allow the Navy to test and

develop the ability of an autonomous Unmanned Surface Vessel (USV) to effectively gather important hydrographic data and potentially form part of a future capability to be delivered by the MHC programme," said Alex du Pre, MHC Team Lead at Defence Equipment and Support.

The company say that this project marks the fourth delivery of a C-Enduro vessel, and previous successful missions include an 11-day over-the-horizon marine science mission north of Scotland for the National Oceanography Centre.

Airbus turns imagery into insight with The OneAtlas Platform

Airbus Defence and Space has released a brand-new version of The OneAtlas Platform, its unique collaborative environment to easily access premium imagery, perform large-scale image processing, extract industry-specific insights and benefit from Airbus assets for solution development.

"The OneAtlas Platform provides immediate access to data and analytics and gets it into the hands of many more users and partners to create new business opportunities," said Francois Lombard, Head of the Intelligence Business at Airbus Defence and Space.

The OneAtlas Platform provides access to data within the Living Library as well as value-added layers, Basemap and WorldDEM. The Living Library contains multi-resolution and premium optical satellite data, updated on a daily basis and immediately available via streaming, download and API.

F-35 Joint Program Office announces sustainment contracts with BAE Systems

BAE systems has announced its latest set of work which will carry out Maintenance, Repair, Overhaul & Upgrade (MRO&U) services for F-35 avionics and aircraft components for the European, Asia-Pacific and global fleet.

The Department of Defence has assigned repair components to Sealand Support Services Limited, BAE's joint venture with the UK Government and industry partner, Northrop Grumman for global repairs, and in the Asia-Pacific region, work will be carried out by BAE Systems Australia alongside a number of Australian defence companies.

"Within BAE Systems we have a strong track record of working alongside our national and international customers in delivering innovative support solutions and look forward to bringing this further in to the F-35 programme," noted Chris Boardman, Managing Director, BAE Systems – Air.

SPYNEL-X V-LRF Search & Track System with the highest definition in the World, showcased at IDEX

SPYNEL-X and its V-LRF option was showcased at the International Defence Exhibition and Conference, Abu Dhabi, for the first time. The recently-launched thermal sensor equipped with a visible channel and a laser range finder was presented to decision-makers from within the defence industry, alongside key representatives from governments, armed forces and the key military personnel.

Award-winner V-LRF option for SPYNEL was recognised as best anti-drone system at the Milipol international tradeshow and received the Innovative Product of the Year Award from SECONA Shield. With its HD visible camera equipped with a x30 optical zoom, the SPYNEL panoramic sensor reportedly ensures a better threat identification with no blind spot. The laser range finder provides the user with the exact distance of all detected threats on land, at sea or in the air.

The SPYNEL -X VLRF InfraRed Search & Track is used for varied military applications, providing 24/7 coverage of very wide areas on land and at sea, in harsh weather. Equipped with the advanced detection recognition and tracking software CYCLOPE, SPYNEL provides early target discrimination in total discretion, as the system is fully passive. The image quality provided by the panoramic IR sensor has a resolution of up to 120Mpixels.

Cyril Marchebout, Sales Representative of SPYNEL in Middle East, said: "We were proud to showcase our V-LRF innovation at IDEX 2019. SPYNEL 360° has become part of the must-have security and military equipment based on thermal imaging technology to detect asymmetric threats. We are committed to providing the best situational awareness adapted to our clients' needs, and to do so, our technologies must keep on evolving."

Orbex unveils new rocket design for UK spaceport in Scotland

Orbex has publicly unveiled its Prime rocket for the first time at the opening of its new headquarters and rocket design facility in Forres in the Scottish Highlands. Designed to deliver small satellites into Earth's orbit, the rocket was unveiled at an opening ceremony attended by VIPs from the UK and European space community as well as local community stakeholders.

The completed engineering prototype of the Stage 2 rocket (the stage that will transit into orbital flight after launch) is made from a specially-formulated lightweight carbon fibre and aluminium composite and includes the world's largest 3-D printed rocket engine.

Orbex Prime is a completely re-thought and re-engineered two-stage rocket, designed by Orbex aerospace engineers with professional experience from organisations including NASA, ESA and Ariane, as well as other commercial spaceflight companies. Prime launchers are up to 30% lighter and 20% more efficient than any other vehicle in the small launcher category, packing more power per cubic litre than many heavy launchers.

Seen for the first time, the 3-D printed rocket engine was uniquely manufactured in a single piece without joins in partnership with additive manufacturer SLM Solutions. Given the extreme temperature and pressure fluctuations involved in space flight, this gives the engine an advantage over other rocket engines, which can suffer from weaknesses associated with joining and welding.

It is also the first commercial rocket engine designed to work with bio propane, a clean-burning, renewable fuel source that cuts carbon emissions by 90% compared to fossil hydrocarbon fuels, supplied by Orbex's new exclusive BioLPG fuel partner Calor.

Graham Turnock, Chief Executive, UK Space Agency said: "Orbex's new rocket design facility brings Britain one step closer to having its own domestic commercial launch capability and firmly positions the UK as Europe's frontrunner for those looking to Earth's orbit and beyond for new opportunities. The new facility and future spaceport operations will help unlock vast economic and societal benefits not just in Scotland but right across the UK."

MBDA and Milrem Robotics unveil world's first anti-tank UGV

MBDA has presented the Atlas-RC/ LIC2ORNE combination which, together with the Mistral missile, provides protection to light, mobile units. The company has stated that Mistral is an extremely reliable fire-and-forget air defence missile, with a success rate of nearly 95%.

"Equipped with an infrared imaging seeker and advanced image processing capabilities, the Mistral offers excellent countermeasure resistance and can engage low thermal signature targets such as UAVs and turbojet-powered missiles at long range, in addition to the usual combat aircraft and helicopter targets," stated Francis Bordachar, MBDA's Military Advisor Land Systems.

The Atlas-RC is an automated turret, carrying two ready-to-fire Mistrals and controlled from the cabin of the vehicle. It is equipped with day/night sensors for fire control and tracking. LIC²ORNE is a command and control unit, developed from a set of software components that have already been trialled on MBDA's Mistral and VL MICA air defence systems.

"It can coordinate up to eight Atlas-RC systems and connect them to higher-level command systems, including via advanced links such as Link 16 or satellite links. With its ability to use radar or electro-optic sensors, LIC²ORNE ensures that the Atlas-RC turret has sufficient early warning to make full use of the Mistral's firing envelope," explained Bordachar.

The company states that thanks to LIC2ORNE's open architecture, MBDA has been able, "in just a few months", to build in defences against mini and micro UAVs.

"Drawing on the lessons of recent conflicts in Europe or the Middle East, the Atlas-RC/ LIC²ORNE combination is designed to provide a real air defence and engagement capability in the lower layer while ensuring very high mobility to accompany and protect mobile detachments and front-line units," concluded Bordachar. "The deployment of an air defence system as close as possible to ground units is once again becoming a necessity, and a key survivability factor for ground forces."

University of St Andrews | FOUNDED **1413**

HANDA **CSTPV**
The Handa Centre for the Study of Terrorism and Political Violence
1994-2019
25th Anniversary

Terrorism Studies
Leading online course

Individual Modules | 4 Weeks
Certificate | 16 Weeks
Advanced Certificate | 32 Weeks

Start dates: February, June, October

Learn online with expert tutor support and connect with a global network of like-minded professionals.

www.terrorismstudies.com/sbm19
Tel: +44 (0)20 7017 4483 | Email: security@knect365.com | Quote VIP code: sbm19

IN PARTNERSHIP WITH
KNect365 Learning
an Informa business

UNLOCK NEW CAREER OPPORTUNITIES IN SECURITY

STUDY SECURITY, COUNTER-TERRORISM, DIPLOMACY AND MORE BY TUTORED DISTANCE LEARNING

Starts: 16th September 2019

Courses include:
- Security Studies
- Counter-terrorism
- Security and Terrorism Law
- Security Management
- Terrorism, Policing and Security
- Intelligence and Security
- Diplomacy and Security

Available as Postgraduate Certificate / Postgraduate Diploma / Master

LIVERPOOL JOHN MOORES UNIVERSITY

www.security-studies.com/sb19
+44 (0)20 7017 4483 | security@knect365.com
Quote VIP code: sb19

IN PARTNERSHIP WITH
KNect365 Learning
an Informa business

Pelco by Schneider Electric launches new Spectra Professional 4K for high-resolution fixed and PTZ surveillance cameras

The new Spectra Professional 4K camera from Pelco was designed to produce high resolution surveillance in rugged and outdoor settings. With state-of-the-art features that clarifies details of interest in crowded or poorly lit areas

Pelco by Schneider Electric has announced the launch of its latest edition to the 4K surveillance camera range. The Spectra Professional 4K camera resolution and compression standards reportedly provides pinpoint accuracy in surveillance solutions. It enhances the ability to recognise and identify objects at greater distances, provides infrared illumination up to 150m, streams video in H.265, H.264 or MJPEG formats, and can see 15° above the horizon.

Areas such as seaports and waterways are particularly in need for better surveillance technology, with an estimated US$50 billion in loss annually according to the National Cargo Security Council. The Spectra Professional 4K provides a solution for organisations who are frustrated with the inability to zoom into crowded, outdoor areas with low levels of light.

"Traditionally, when operators zoom in on 1080p video, the details can become indistinct because there are only so many pixels," explains Rob Yockey, Senior Product Manager at Pelco. "With 4K resolution, one camera can cover a large area and offer the ability to zoom with greater detail. This technology greatly improves security operations in both live monitoring as well as in forensic analysis.

"Pelco continues to better and expand its 4K resolution camera range with the Spectra Professional 4K line of PTZ cameras by providing detailed images more clearly than ever before at greater distances," Yockey continues. "Spectra Professional 4K's innovative features capture outstanding detail in low-light conditions and is ideal for tracking people and vehicles across wide spaces."

In addition to the described benefits of the Spectra Professional 4K, the camera also includes improved infrared illumination detection that has up to 4K resolution at 30ips, which can cover a large area, up to 150m, with clarity of detail to record information such as license plate number recognition or faces of people.

The new camera is equipped with integrated IR, primarily for outdoor applications with poor lighting conditions, similar to the capabilities of Esprit Enhances IR models. In response to some cities passing laws that restrict white light pollution near apartments or in empty parking lots, the camera provides IR illumination that enables operation in the absence of visible light.

> "WITH 4K RESOLUTION, ONE CAMERA CAN COVER A LARGE AREA AND OFFER THE ABILITY TO ZOOM WITH GREATER DETAIL. THIS TECHNOLOGY GREATLY IMPROVES SECURITY OPERATIONS IN BOTH LIVE MONITORING AS WELL AS IN FORENSIC ANALYSIS."

Spectra Professional 4K surveillance offers improved operational efficiency. It features H.265 video encoding operators and Pelco Smart Compression that the manufacturer states reduces the storage required, while preserving image quality. With what is described as "excellent PTZ responsiveness" and features such as patterns and frame scan, the camera enables close manual tracking of people or vehicles and the ability to cover spaces in an automated fashion.

Lastly, the surveillance solution allows for innovative extended viewing where it can tilt to 15° above the horizon look-up. It is also equipped with Electronic image stabilisation (EIS), which reduces blurring associated with camera motion in environments subject to vibration.

www.pelco.com

Idax Software puts the user experience first with launch of version 3 of its identity analytics platform

With insider threat now reaching epidemic proportions, Idax Software has launched Version 3 of its identity analytics platform which the developer believes puts user experience first and gives staff the information they need to make the right decisions

Idax Software has launched Version 3 (V3) of its identity analytics platform. Idax's platform analyses what data and files that staff have access to and tells users which access rights they shouldn't have.

Insider threat is now reaching epidemic proportions, with an estimated 90% of tech crimes being committed by employees. Whether they are the result of bad actors, collusion or unwitting accomplices, most data breaches are simply about access and opportunity. A reported 75% of employees say that they have access to data they shouldn't, and 25% of employees are willing to sell data to a competitor for less than US$8,000.

Many organisations are still reliant on outdated methods to counteract this ever-growing threat. Traditionally, line managers are required to review a list of applications and systems that their staff have access to, and approve or deny all of this, with no context, explanations or ability to question individual items.

It would seem that both modern tools and a large-scale culture shift are needed to tackle this threat. Everyone in the organisation needs to be made to feel that cybersecurity is their own responsibility – from the CEO to the worker on the shop floor. But to achieve that, they need better tools and more useful information.

With the launch of V3, Idax provides insights for the whole organisation, not just the IT or security team – increasing cyber effectiveness, mobilising the organisation and reducing insider threat.

Idax' technology is the first identity and access management system that puts user experience first, giving staff the information they need to make the right decisions. This is a critical step in changing the culture around protecting assets; in order to engage everyone, you need an identity management solution that puts everyone at the front of the fight. A positive user experience is not just a "nice to have", but a critical step in making a company's cyber defence strategy work.

Idax finds employees with access to data they shouldn't have, within minutes, and without any prior knowledge about your day-to-day business. Idax implements preventative controls that it states eliminate risk right at the source. Critically, it lightens the load on managers currently faced with managing permissions for their team, giving those managers more context

and information with which to make better decisions and establish least privilege.

"You can throw as much analytics at identity and access management as you like, but it will all be futile if the technology is not easy to use and to engage with – if the user experience is not positive," commented Mark Rodbert, CEO of Idax Software. "With the launch of Idax V3, we have put the users at the heart of Idax analytics."

V3 of Idax's technology brings a modern, interactive user interface to the identity analytics platform. This new UI is browser-based, and can be accessed from anywhere, making it more easily accessible for users. The latest version also makes Idax' insights actionable, giving managers the power to approve or make changes to employees' access within the platform.

"This new user interface is about much more than just making it more aesthetically pleasing," continued Rodbert. "Putting the user first and empowering them to make informed decisions about access management is critical to changing attitudes towards securing data and to protecting the organisation from data breaches."

"With the launch of V3, Idax has completely reinvented the look and feel of its platform, transforming the way users interact with it," commented the head of security architecture at a major international bank. "We are rolling out V3 of Idax across our organisation and are delighted with the results. Staff members across the company are able to take responsibility for their teams' access rights, and we are already seeing a clear improvement in risk scores."

www.idaxsoftware.com

Acronis extends cyber protection capabilities for partners and customers with its new Acronis SDI appliance

Acronis is delivering an SDI Appliance universal infrastructure solution which has been designed to deliver cyber protection to the manufacturer's partners and customers with the objective of assuring them peace of mind that all of their data is secure

Acronis has announced the availability of Acronis SDI Appliance, a universal infrastructure solution based on a significantly updated, pre-configured Acronis Software-Defined Infrastructure software. Acronis Software-Defined Infrastructure (formerly Acronis Storage, a software-defined storage solution) reportedly transforms standard customers' hardware into a protected, enterprise-grade hyper-converged system, and has been designed specifically for cyber protection for all data, applications and systems.

The appliance has been created to simplify the complex tasks of cyber protection, users an easy way to store and manage the data protected by the company's Acronis Backup and Acronis Backup Cloud solutions. Acronis SDI Appliance reinforces the manufacturer's ability to deliver complete cyber protection to customers and partners, addressing all five vectors of cyber protection — safety, accessibility, privacy, authenticity and security. The result is described as a comprehensive approach that ensures easy, efficient, and secure protection for all data, applications and systems.

With Acronis SDI Appliance customers can reportedly experience up to five times faster storage than the Ceph on the same hardware and can benefit from turned hardware with integrated SSD for caching. The cyber protection platform can access data across multiple data centres via object storage geo-replication and can guarantee data authenticity with Acronis Notary's blockchain-based certification.

"We help our customers and partners integrate the best cyber protection approach into their infrastructures," said Serguei Beloussov, CEO of Acronis. "Our

software-defined infrastructure – which is integrated, preinstalled and extensively tested on reliable hardware – is the solid foundation for Acronis' data protection services. It is fundamental to our vision of delivering complete end-to-end cyber protection. The new solution brings the ultimate level of reliability, cost-efficiency and universality, simplifying the data protection processes of customers so they can focus on their core business."

"The new Acronis SDI appliance is a pretty robust in terms of data storage and data management," said Phil Goodwin, research director, IDC. "The plug-in-play hardware has virtualisation and software-defined storage for cyber protection in private or public clouds. We believe it's the optimal backup destination for Acronis Backup and Acronis Backup Cloud users. Acronis is leveraging its partners' ecosystem, having served the market for over 15 years and is taking a natural next step by introducing a purpose-built backup appliance."

Working closely with manufacturing and logistics partner, RNT RAUSCH GmbH, Acronis designed and developed a hardware solution that complements its software solutions to ensure Acronis SDI Appliance meets the data centre needs of customers looking to optimise their use of Acronis software.

Acronis Software-Defined Infrastructure, which powers Acronis SDI Appliance, offers what the manufacturer describes as reliable, cost-efficient, scalable and universal solutions that combine compute, networking, block, file and object storage workloads using industry-standard hardware. The seamless integration with Acronis products via Acronis Backup Gateway means it is universally accepted. It also delivers cyber protection by incorporating Acronis CloudRAID and Acronis Notary with blockchain, ensuring data immutability and preserving the authenticity of essential data and sensitive documents.

Other features include virtualisation for high-performance and high-availability hyper-converged computing, AWS S3 compatibility, software-defined networking, and monitoring.

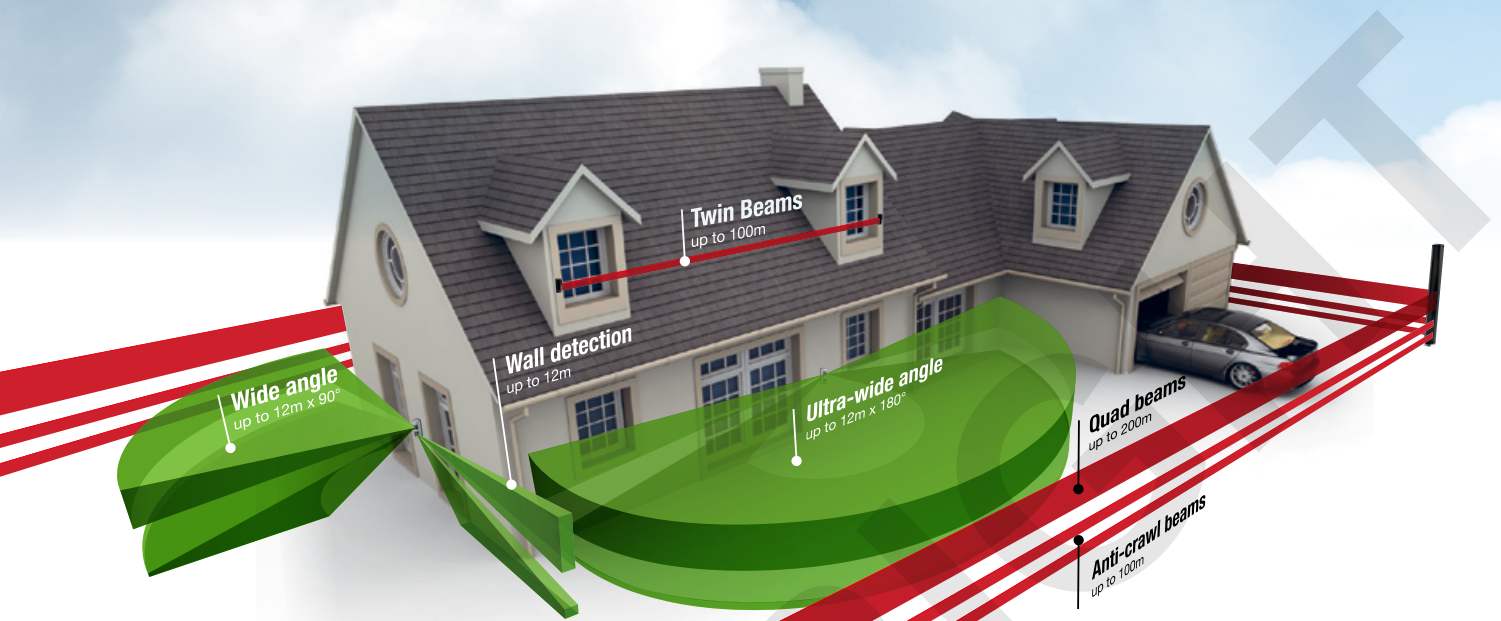Acronis SDI Appliance will be shipped in 3U rack mount form-factor, carrying five nodes, each equipped with an Intel 16-core processor, 32GB RAM (up to 25 GB) and three Seagate 4/8/10/12TB enterprise SATA HDD. Acronis SDI Appliance can store up to 180TB of raw data. Acronis SDI Appliance is currently available in the US, Canada, UK, Germany, Switzerland, Austria and North European countries.

www.acronis.com

TAKEX

Twin Beams
up to 100m

Wall detection
up to 12m

Wide angle
up to 12m x 90°

Ultra-wide angle
up to 12m x 180°

Quad beams
up to 200m

Anti-crawl beams
up to 100m

PERIMETER
INTRUDER
DETECTION

Whether you need wide angle, ultra-wide, window, wall, or perimeter protection, we have you covered. Our versatile range of wired and battery-powered security sensors offer flexible, reliable intruder detection like no other.

With Dual-zone outdoor PIR sensors combining horizontal and downward zones to prevent unwanted activations from animals, and Twin, Quad and Anti-Crawl photoelectric sensors synchronising up to 16 beam paths for maximum stability across open territory, TAKEX sensors are designed with the most demanding of intruder applications in mind.

TWIN BEAMS	QUAD BEAMS	DUAL-ZONE PIR	ANTI-CRAWL	BEAM TOWERS
Protect windows, doors, fence lines, entrances, & driveways up to 100m.	Trouble-free perimeter detection for distances up to 200m.	Hard-wired or battery operated outdoor PIR up to 180° x 12m.	Ideal for high-security applications to detect crawling attempts.	Rugged floor and wall mounted enclosures in 1/1.5/2/3m heights.
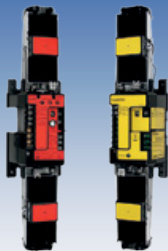
📞 **+44 (0)1256 475555**
email : sales@takex.com

TAKEX EUROPE
www.takex.com

Spectral Edge Fusion set to deliver higher resolution, more colour accurate images in low light than competitors

Spectral Edge is set to launch its RGB+IR Fusion technology to the professional security market at ISC West. The technology has been created to provide surveillance cameras with high resolution, colour accurate images, even in very low or mixed lighting conditions

Spectral Edge RGB+IR Fusion technology (or Spectral Edge Fusion), which will be formally launched into the professional security market at ISC West this year, can reportedly provide surveillance cameras with high resolution, colour accurate images, even in very low or mixed lighting con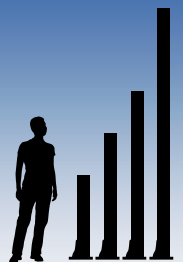ditions. Spectral Edge Fusion (Fusion) also assists in providing detailed images even in foggy, misty or hazy conditions when normal RGB sensors would be unable to pick out.

Spectral Edge Fusion achieves this by intelligently-balancing Red Green Blue (RGB) and Near-Infrared (NIR) light in real-time. The manufacturer states that it is the only technology on the market today that can engineer RGB and NIR light fusion without introducing pixilation, artefacts or additional noise.

Fusion works by taking four channels – Red, Green, Blue and NIR light – and reducing these to three by fusing the NIR light into the RGB, creating smooth transitions as natural light levels reduce below levels where fine detail would ordinarily be lost. The technology optimises the illumination that is present, even in the lowest light levels well below one lux.

The power of Spectral Edge Fusion is in the way it fuses and tunes RGB and NIR data, processing these light sources together within the same image. It ensures minimal loss of resolution, while delivering improved contrast, dynamic range and signal-to-noise ratio. As a result, what's lost in colour as daylight fades, is made up for in additional texture and depth of the image which NIR lighting provides.

Camera build saving

Fusion also generates a build saving for camera manufacturers because only one sensor is needed for day/night cameras and no mechanical switching between sensors is required. It removes the need for an IR-cut filter, for example, further helping minimise moving parts which wear out over time and extending surveillance cameras' Mean Time to Failure.

An additional cost advantage flows from using NIR because it can be included on the same semiconductor process as an RGB sensor. Thus, NIR can be combined on the same sensor chip as RGB with no extra cost at all if some of the pixels which sense visible light are replaced with pixels sensitive to NIR.

Sensors which support both RGB and NIR wavelengths exist already, including On Semiconductor's AR0237.

Supports accuracy of a wide range of person, event and action recognition applications

Fusion optimises existing video content analytics applications such as motion detection, object detection, tripwire and facial recognition. It is being integrated into a number of surveillance-ready chipsets compatible with both 2x2 and 4x4 Bayer Pattern RGB+IR CMOS sensors, to improve image accuracy and performance for facial recognition and other security applications. In tests, Fusion proved highly effective in identifying objects such as vehicles' license plates and colours, and more easily spotting and flagging "security incidents" such as a pedestrian crossing a railway track or motorway.

Improved facial recognition

Fusion can not only generate high quality images capable of reliable identification of an individual in low light conditions but also when there is "mixed lighting". Many images taken from a bus camera would not be high enough quality to enable automated positive identification using facial recognition software.

However, by combining RGB and NIR light to additional detail and depth it would be possible to get a reliable, consistent image capable of identifying an individual accurately in more than 90% of these cases.

Where next?

Now that Fusion software can be integrated into existing chipsets without increasing the silicon area significantly, Spectral Edge has turned its attention to developing chip vendor partnerships. It is developing a prototype camera reference design with RGB+IR fusion capability built into it and is already talking to camera vendors about conducting field trials using this prototype in challenging, real-world conditions.

www.spectraledge.co.uk

A NEW ERA IN PERIMETER SECURITY

PROTECT YOUR BUSINESS WITH THE FLIR SAROS PERIMETER SECURITY CAMERA

The FLIR Saros™ Dome camera is a detection solution for small-to-medium size businesses that watches over an entire perimeter. Saros combines an optical camera with thermal sensors enabling analytics to limit false alarms. From the industry leader in thermal imaging, FLIR Saros provides an effective, efficient, and economical security solution.

◆FLIR

FLIR.com/saros

Access control, rights management and **staying on the right side of GDPR**

Nick Smith, Regional Sales Manager at Genetec discusses why privilege management becomes increasingly complicated when it comes to the way that companies manage their data

Privilege management has never been a simple task. It is a minefield of ensuring that the right people have the correct level of access to certain physical and digital infrastructure. This can be simple enough for a small business with few staff and access points, but at scale, it is incredibly difficult to manage. This responsibility has historically been for the security of the organisation. However, with GDPR it is now more important than ever that businesses are fully aware of their data and how they manage access.

The reality of rights management in 2019

An increase in stringent regulations has impacted the way that the industry works. In Europe, the General Data Protection Regulation (GDPR) has forced businesses to look for efficient ways to be compliant, enforce policies and standardise practices across sites. Failing to comply can see companies handed steep fines should they fail to remove access rights from identities that are no longer associated with the company. Previously, a company could get away with forgetting about a former employee with little recourse, this lack of oversight now has the potential for serious consequences. Similarly, it makes keeping on top of the access rights of any guests a much greater priority.

This difficulty is further complicated by the growing trend of insider threats. The bigger security risks come from within an organisation. In the 2016 Cyber Security Intelligence Index, IBM found that 60% of all attacks were carried out by insiders. Of these attacks, three-quarters involved malicious intent, and one-quarter involved inadvertent actors. IBM Security research also found that healthcare, manufacturing

and financial services are the top three industries under attack due to their personal data, intellectual property, physical inventory and massive financial assets, respectively. Whether unintentional or malicious, internal cardholders have the advantage of knowing the internal security vulnerabilities, putting them in a unique advantage to cause harm to the organisation.

We are also seeing within and outside our industry a surge in mergers and acquisitions that has led to a growing interconnectivity. As organisations expand and merge their access control systems (or add new ones), access rights management becomes increasingly complex. Especially when these organisations are driven to move their cardholders onto a one card solution, to consolidate systems and find new efficiencies to improve their day-to-day operations. Businesses are looking for efficiencies because of the overwhelming piecemeal approach to security.

With the described current state of affairs, one might assume that a proactive manager would be able to address these issues over time, but there are a variety of reasons why privilege management becomes increasingly complicated.

How rights management becomes more complex over time

As is the case with any deployment of technology, when most businesses first installed their access control system (ACS), the chances are that they did this in reaction to the needs they had at the time. They chose and deployed a new ACS based on traditional needs to secure doors, the emergent threats at that present moment and on the budget they had allocated. An intelligent buyer would ensure that they had the best solution available for the foreseeable future, but organisations and threats can

grow in an unpredictable manner, making purchasing decisions more complicated.

Additionally, many corporations often acquire smaller companies to grow or expand into a new market or geographic region. However, one consequence of this is that they inherit the company's pre-existing access control infrastructure. In many cases it is simpler and more cost-effective to continue using the pre-existing system rather than replace it with an upgraded one. More cardholders, new access rights and ever-changing security policies emerge making it challenging to remain consistent and compliant. As a result, workarounds begin to emerge, and cardholders are now expected to carry multiple cards to get from one site to the other.

Inconsistent and unmanageable policies begin to emerge as policies evolve. They run across unused cards, too many rules, outdated rights and security gaps. Access control databases become polluted overtime, especially when disparate systems can't talk to each other duplicating efforts and data.

With compliance as the focus, organisations will then likely begin assessing a variety of options but usually focus on existing ACS technology suppliers. They invest in new security systems or hire more staff, but the root cause goes unnoticed. And it goes unnoticed because access control alone is only half of the equation. Access control is about managing doors, cardholders and credentials. You run reports, manage alarms and control access. Access control systems were never designed to automate access rights management or help ensure compliance. This creates a gap in the market as companies evolve.

Striking a balance between lowering risk, restricting access and ensuring convenience is difficult because there isn't an efficient and consistent way to manage access rights and automate the process. At the extreme, everyone has access everywhere. Imagine if a contractor required

access to the HVAC closet after hours. For many organisations, they'll give that contractor 24-hour access to that area just in case it's needed because they don't have an office or reception that is open after hours to process the contractor's access request. As a result, the organisation is increasing its risk.

A new approach to managing access

Every day, employees, contractors and visitors rely on an access control system to allow them entry to the areas they need. Limiting the ability to make access rights changes to security operators or IT staff might have worked at one time, but in 2019 it is an impractical approach. In most cases, when an identity needs to request a change, they must visit their badge office or receptionist, further delaying the process. Operators don't know who should be accessing which areas, so they must ask, or they guess.

A manual approach to managing access policies can put a strain on an operations team and draw focus from their core responsibility of protecting people and assets. This can compromise efficiency, lead to human error and increase the chance of security breaches. As such, organisations, should look for a solution that manages the identities of people across all their locations.

By standardising and automating their security policies and ensuring authorised employees approve access requests, it heightens security without a compromise to operations and everyday activities within their facilities. Through increased operational efficiency, they not only proactively protect their employees, buildings and assets but they're better equipped to comply with internal and external regulations. This can be achieved by employing a cloud-based architecture that allows users to centralise their policies, while simultaneously facilitating the distribution of identities across sites. A unified solution such as this lowers operational risk by moving away from the manual and error prone method of making access requests and managing access rights and it removes the friction employees face when requesting and receiving access to secure areas.

Only by reinterpreting and reconsidering the approach to modern times can organisations deliver on a promise of a sophisticated and unified access management system.

www.genetec.com

"A MANUAL APPROACH TO MANAGING ACCESS POLICIES CAN PUT A STRAIN ON AN OPERATIONS TEAM AND DRAW FOCUS FROM THEIR CORE RESPONSIBILITY OF PROTECTING PEOPLE AND ASSETS."

Nick Smith, Regional Sales Manager, Genetec

Meesons Security Portal achieves
fire rating certification

The FPJ140 2SF from Meesons had joined the manufacturer's FPJ140 1AF Security Portal in providing fire protection and smoke control on both sides of the flat side doors

The FPJ140 2SF from Meesons has now achieved an EI60 Fire Rating from both directions. The FPJ140 2SF now joins FPJ140 1AF Security Portal in providing fire protection and smoke control on both sides of the flat side doors as per the European Fire Resistance norm: EN 13501-2 and EN 1634-1: 2014.

Achieving the fire rating on both directions of the flat side of the portal means that architects and specifiers have reassurance that the Meesons FPJ140 2SF and FPJ140 1AF Security Portal will provide the required levels of resistance to fire. The certification means the portals will retain their structure and integrity in the event of a fire and prevent the passage of flames of hot gases as well as limiting the temperature on the unexposed face of the unit.

The FPJ140 1AF can be supplied with a fire rating to meet either EI60 and EI120, providing 60- or 120-minutes protection respectively. FPJ140 1AF EI60 provides a more cost-effective solution and with an option to increase the resistance to fire up to 120 minutes.

Meesons FPJ140 2SF and FPJ140 1AF are the only Security Portals that have been specifically designed as fully integrated stand-alone units, which have been independently tested by an accredited third-party laboratory, to meet the fire rating requirements set out in EN 13501-2 and EN 1634-1: 2014. Both Security Portals prevent tailgating and are reportedly suitable for new buildings and retrofitted into existing openings to create a safe, secure fire line.

Achieving the fire rating on both sides' means that architects and specifiers can specify Meesons FPJ140 2SF and

"THE CUSTOMER IS DELIGHTED WITH MEESONS FPJ140 2SF SECURITY PORTAL, WHICH HAS OPERATED CONTINUOUSLY SINCE INSTALLATION AND COMPLEMENTS THE OVERALL LOOK AND FEEL OF THE DATA HALL WHICH IS A KEY HUB IN THEIR WORLDWIDE IT OPERATION"

FPJ140 1AF Security Portals as part of a wider fire safety strategy ensuring the containment or prevention of fire spreading.

As well as maintaining a secure fire line, Meesons fire rated Security Portals prevent tailgating by only allowing the transit of one person at a time, ensuring only authorised users can gain access to a secure area.

"Our FPJ140 2SF and FPJ140 1AF are he only Security Portals that have been

specifically designed to meet fire rating requirements as a single, fully integrated unit," says Jeremy Terry, CEO at Meesons A.I. Ltd. "Gaining fire rating on both sides of the flat side doors provides specifiers with the assurance that the portals will perform exactly as tested and from both directions."

The FPJ140 2SF and FPJ140 1AF Security Portals are available with Attack Resistant Class 3 and 4, EN1627-30:2000 or Bullet resistant glazing up to BR4–EN 1063 on the external curved side. This makes them an ideal entrance control solution for highly secure areas that also require the fire line to be maintained.

Meesons' FPJ140 1AF Fire Rated Security Portal features a manual swing door with automatic sliding curved doors. The FPJ140 2SF features automatic sliding curved doors and flat doors. The manufacturer states that both Security Portals can be customised to suit individual client requirements with different types of finish options available as well as the integration of third-party devices. Battery backup is also provided, so in the event of power loss the units will remain operational for up to six to eight hours.

One company to have seen the benefit of the FPJ140 2SF is VITRUS, the UK's fastest growing data centre operator.

It's flagship data centre in London, LONDON2, has the portal as an integral part of its security system.

The customer wanted to preserve operational space and maintain the integrity of the fire wall. Meesons proposed the FPJ140 2SF due to its compact design and fire-rated approval.

"At VIRTUS we take great pride in delivering flexible solutions to meet the exacting demands of our customers," states David Watkins, Service Deliery

Director. "The security of our facilities was a key factor in securing the contract initially, and the ability to enhance further to meet all of the customer requirements was very well received. The customer is delighted with Meesons FPJ140 2SF Security Portal, which has operated continuously since installation and complements the overall look and feel of the data hall which is a key hub in their worldwide IT operation."
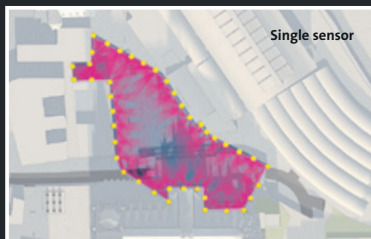
www.meesons.com

"OUR FPJ140 2SF AND FPJ140 1AF ARE THE ONLY SECURITY PORTALS THAT HAVE BEEN SPECIFICALLY DESIGNED TO MEET FIRE RATING REQUIREMENTS AS A SINGLE, FULLY INTEGRATED UNIT"
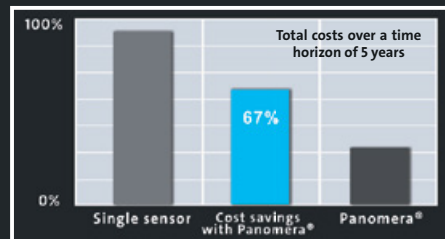
IDIS boosts safeguarding for Southern **Health NHS Foundation Trust**

The latest HD video technology from IDIS has been chosen by Southern Health NHS Foundation Trust for a comprehensive upgrade across its facilities in Hampshire.

In one of the largest projects of its kind, the new system has been installed to improve safeguarding at a number of sites for patients requiring specialised mental health care in a secure setting. DIS's Korean technology is described by the manufacturer as fully network-tested and approved, which means it is secure enough to be linked to the wider NHS network, at any point in the future, giving further options for centralised monitoring and control.

Because of the sensitive nature of the care being provided, the vulnerability of patients and the risks to staff, it was essential that the video solution was not only network-secure but could be relied on to capture scenes in close detail in all lighting conditions. Southern Health wanted a fully managed system, linking all of its sites onto the local LAN without the risk of the system being hacked. This element is described as a key NHS consideration in selecting any IP CCTV solution.

The IDIS equipment was reportedly identified as the best for the project following a full proof-of-concept comparison, with equipment set up on site to demonstrate both picture quality and ease of use. It replaces a previously installed IP video system, comprising a mix of equipment from different manufacturers, and in comparison, it offers the benefits of lower cost of ownership due to ease of use, simple installation and maintenance combined with the industry-leading warranty.

The first phase of the upgrade was recently completed by local fire and security integrator ISD Tech, with an installation at Ravenswood House, Fareham. This phase comprises almost one hundred 12MP vandal-resistant IR Fisheye cameras as well as full HD IR domes, DirectIP H.265 4K recorders, PoE switches and full-HD monitors.

The older system at Ravenswood House had been proving to be difficult to use. Recordings could not be easily archived, and image quality was inconsistent, explains Tracey Edwards, Security Manager of Southern Health NHS Foundation Trust.

"We had identified gaps in coverage and our efforts to provide a safe environment were being hampered by footage that was often unclear," says Edwards. "The old system was proving too complex to use and it was taking too long for operators to identify and retrieve recordings."

This was a major issue because staff at the site are caring for vulnerable people and, if an incident occurs, it's vital that they can quickly access recordings that show exactly what happened. Delays in investigations can result in interrupted care delivery and costly disruption, so need to be minimised as much as possible.

The advantage of the IDIS 12MP fisheye cameras is that they allow all events to be captured automatically without the need for operators to focus in on an incident.

Recordings from the new cameras always provide a complete 360° view of any given area without any blind spots. Just as importantly, the system is easy to use, and the footage can be accessed quickly. The fisheye units offer a choice of six de-warping view modes and ensurenight-time IR viewing at up to 15m.

The new system has also helped to overcome a particular loophole at Ravenswood House. In some areas, motion-sensor activated lighting was not sensitive to very slow movement, meaning the previous system could not capture images because it had no IR capability. This increased the vulnerability of both patients and staff.

Overcoming this, the built-in IR capability in the IDIS fisheyes enables the capture of crisp, clear images even in darkness. Crucially, the new solution also features IDIS's Smart Failover technology which protects against loss of footage due to a wide range of potential fault conditions, including network instability, network failure, storage failure, recorder hardware failureand power supply failure.

IDIS and ISD Tech worked particularly closely to ensure the phase oneinstallation went smoothly, says Nicky Stokes, ISD Tech's Managing Director. "Our engineers had to be very sensitive and careful working on this project because of the nature of the site and the needs of the patients. Everything went smoothly – IDIS equipment really is 'plug and play', which makes our job much faster, and we appreciate the high-level support wthat IDIS always gives."

With phase one completed, full roll-out of the IDIS technology through Southern Health NHS Foundation Trust sites will continue throughout 2019.

"We are delighted that IDIS technology has been chosen for this important NHS project," says Jamie Barnfield, Sales Director, IDIS Europe. "We know that our technology will provide outstanding service for years to come. Not only is it backed by our IDIS Ultimate seven-year warranty, our commitment to leading the way in new product development means that it will be forward-flexible and meet all the customer's future needs."

www.idisglobal.com

> "OUR ENGINEERS HAD TO BE VERY SENSITIVE AND CAREFUL WORKING ON THIS PROJECT BECAUSE OF THE NATURE OF THE SITE AND THE NEEDS OF THE PATIENTS"

Nicky Stokes , MD, ISD Tech

Jumbo Ten Brink Food named
safest store in the Netherlands

Facial recognition technology from Panasonic has proved critical for Jumbo Ten Brink Food as it was named the safest store in the Netherlands

Panasonic's FacePRO facial recognition technology has helped supermarket chain, Jumbo Ten Brink Food, to win an award or the 'safest store in the Netherlands'. The solution deployed by the retailer includes the manufacturer's face server and cameras.

Jumbo Ten Brink Food introduced Panasonic's face server into its store environment in March 2017. This came as a result of the discovery that almost 80% of shoplifting took place via large shopping bags. Since this initial part of the project, Jumbo has installed 80 Panasonic cameras in-store. These combined with he server helped the supermarket chain to win the award.

This is the latest accolade to be associated with the Panasonic technology. Previously it has been recognised by the National Institute of Standards Technology (NIST) which described it as "the most accurate on the market". Panasonic's face server uses deep learning technology which the manufacturer states maximises the performance of the core engine to achieve accurate and reliable recognition. The technology has been created to identify faces that are ordinarily difficult to recognise with conventional techniques. These include coping with challenging images such as those taken from an angle of up to 45° to the left or right as well as 30° up or down. It also reportedly maintains a 90% accuracy rate when detecting faces that are partially hidden by sunglasses or face masks.

Panasonic created the FacePRO facial recognition technology as a way to reduce loss from shoplifting in your stores. The technology works to allow users to match the faces of the people in the store with a known person database. The system will generate alerts in real-time to let a retail store's security team know when a known person enters the shop. This allows the user to allocate staff to take proactive action. As a result, the FacePRO solution is described as a tool to help prevent shoplifting and reduce loss in your stores.

If people are caught stealing, their image remains on the known person database. The face server provides a real-time processing capacity of up to 20 cameras per server and can has the ability to execute high-speed searches of up to 30,000 registered reference faces. With his improved accuracy, the manufacturer
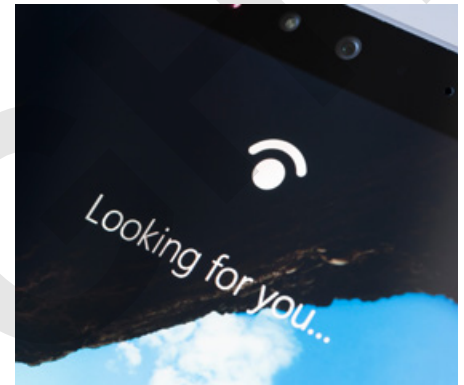
matching server, Jumbo has been proclaimed the safest store in the Netherlands."

states that security protection is enhanced and the system allows matches even when images are 10 years old.

"The moment that a known shoplifter attempts to re-enter the store, an internal alarm is triggered, and we can take the best suitable action," explains Edwin ten Brink, founder of Jumbo Ten Brink Food stores. "Thanks to the Panasonic face

"We are pleased to see that our customers are winning awards as a result of implementing our technology," adds Karen Sangha, Panasonic's Security Solutions Regional Marketing Manager. "We firmly believe that our face server is industry-leading and Jumbo Ten Brink Food's success is testament to that."

www.panasonic.com
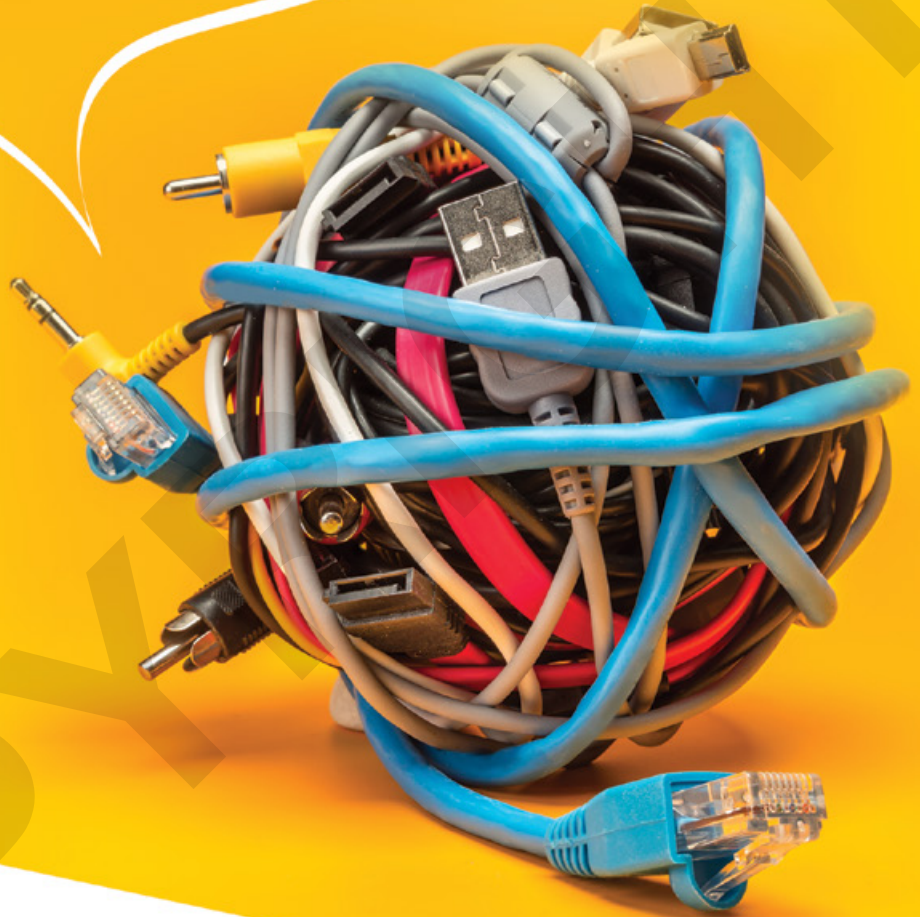
Using intelligent video
for retail experiences

Can the security technology installed into the retail environment form the basis of a larger solution that can provide more advantages for store-holders?

The retail sector has felt the disruptive impact of e-commerce more than most. The inevitable costs of staffing, rent, maintenance and daily operations has left traditional stores struggling to compete with more agile online counterparts.

In addition to this, the one competitive advantage of physical retail outlets – being able to provide a more personal customer experience – has also taken a hit, thanks to a lack of in-store and operational efficiency. Customers find it hard to locate the products they're shopping for, are faced with longer queues for payment, and the most valuable 'VIP' customers are often overlooked.

The question, therefore, is how can stores optimise operations and improve the customer experience at this critical time?

Technology: at the heart of a better customer experience

One challenge that retailers often face is not having a way to collect accurate data and visualise it intelligently in order to make smarter business decisions about the shop floor. For many, reorganising store layout and installing additional equipment is not a realistic option – either because there is not the available space, or because of budgetary constraints.

In these circumstances, an effective solution could be artificial intelligence (AI) and deep learning. Together, these technologies create a video surveillance offering that can give retailers valuable insight into real-time operating conditions, to boost customer service and in-store competitive advantage.

Intelligent video technologies can be applied to retail in a multitude of ways.

This includes people-counting, to track customer flow and numbers; VIP recognition, so retailers can tailor service to key individuals; heat mapping, to reveal the popularity of specific goods in the store; queue detection, to monitor the queuing situation in real-time; and Point of Sale (POS) integration, to retrieve precisely when dispute occurs.

People counting

Understanding the flow of customers is the key to optimising a store's sales performance. By using an accurate people-counting camera, stores can understand daily/weekly/monthly peak times, so that store managers can arrange staffing accordingly. What's more, by layering this data over days, weeks and months, retailers can start to see customer flow trends. The data can be benchmarked against the store's sales figures and its overheads, to inform future operational strategy, and help managers to optimise store profitability.

Furthermore, people counting can also help retail managers gain insights into the customer experience. One example would be to evaluate the conversion rate, which depends on the actual number of purchases divided by the number of people entering the store. Retailers can calculate this rate easily using people counting technology. Even better, people counting can also help stores determine the results of their marketing activities. Each marketing campaign can be quantified by people counting to measure return on investment. This is just one of several technologies that provide insight into consumer behaviour and optimal marketing practices.

VIP recognition

Loyal high-end or VIP customers are enormously valuable to retailers, but service staff cannot always identify them immediately. This means that business operators miss valuable opportunities to extend a special service.

Intelligent facial recognition cameras, however, can provide unique opportunities that were previously unavailable. When customers opt to participate in VIP marketing promotions or other incentives, facial recognition technology will give retailers accurate tools to identify VIPs so staff can provide the right kind of service at the right time. There would be no more need for customers to show membership cards to receive special offers. The whole shopping experience becomes more convenient and efficient.

Heat mapping

Retailers usually want to know which products customers are most interested in, and which promotional products can attract customers to stop. With heat-mapping technology, retailers can see a colour-coded map of how much time shoppers spend in specific store areas. This can reveal hot spots and dead zones, as well as how many people actually shop for a specific product, versus those who just decide to pick it up as they casually walk by.

By layering this data over time, retailers can get insight into how o best place items in store, and how best to design the overall store layout.

One of the most useful heat-mapping tools available to the retail market is the fisheye camera. A single, compact camera can capture a panoramic high-definition image over an impressively wide area, while its heat-mapping function provides the colour-coded map. Because fewer cameras are needed than with most heat-mapping solutions, installation is cost-effective, making this the ideal solution for a location such as an independent shopping mall.

Queue detection

Waiting time can have a devastating effect on the in-store customer experience. If a customer sees a long queue in a store, they may stop shopping and go elsewhere. Worse still, if there is always a long queue every time they visit the store, they may avoid that store completely in future.

Queue detection solutions can help retailers manage their checkout lines, and the queue detection cameras are designed to monitor queues in real-time. The cameras count the number of people in each queue, and if there are too many people in each checkout line and customers still continue to flock to the checkout area it triggers an alarm to store management, who can open a new checkout.

Point of Sale integration

Transaction records and surveillance videos can provide valuable information to reduce disputes at checkout. In the past, these are two completely independent data systems. In order to find the right video footage, the surveillance video must be retrieved manually. Therefore, collecting evidence around a transaction normally can take several hours, which is costly for the business.

Point of Sale (POS) integration, also known as POS Text Overlay, is uploading of transaction data to the video management system through the POS and encoding it with the video stream. This combination of retail transaction data with surveillance videos makes it easy to identify certain transactions to be reviewed for customer complaints, mainly used for post-retrieval when a transaction disputes occurs.

Smart retail solution gives Dutch shopping centres a business edge

People-counting is very important to shopping centres. Retailers always want to know what footfall they are likely to expect, and larger chains use this information to decide whether or not to move in to the shopping centre at all.

At the Schalwijk Shopping Centre in Haarlem, The Netherlands, centre management was counting footfall by using the number of connections to the centre's Wi-Fi. But this was delivering inaccurate and limited data. People were still using the centre Wi-Fi from outside the mall, while many shoppers inside the mall were not using it at all.

To address this, the shopping centre decided to work with Hikvision. The centre management team installed Hikvision Dual-lens DeepinView People Counting cameras (iDS-2CD6820F/C) at all the entrances to the shopping centre. The cameras feature deep learning technology, binocular stereo vision, 3D people detection and height filtering – all contributing to their 97% accuracy rate.

As a result, the Schalwijk Shopping Centre now has highly accurate visitor numbers and flow information, which can maximise both customer experience and layout effectiveness.

Intelligent video: transforming the in-store shopping experience

The intelligent, self-learning video solutions outlined above are designed to empower retailers with much of the insight they need to bring brick-and-mortar stores right up to date. Those that are willing to adopt these solutions will very rapidly see their value, and be able to reap the rewards of increased competitive edge.

Through accurate people-counting, quick identification of VIPs, optimal layout of goods and reduced waiting times, retailers can transform the shopping experience and enhance their sales strategy very quickly. And thanks to the valuable customer insight that is generated on an ongoing basis, they will have the tools to create an in-store shopping experience that should only get better and better.

A three-tiered approach to
mitigating vehicle-borne attacks

Lara Valdur Eha, product manager at Marshalls Landscape Protection, argues that considering protective measures for three different uses offers a more holistic approach to protection

The threat of vehicle terrorist attacks on pedestrians has presented a new challenge to those responsible for planning, specifying and designing our towns and cities. Considering protective measures for three different uses offers security professionals a more holistic approach to protecting busy, urban spaces than traditional methods used in the UK.

The terror threat posed to the public has evolved dramatically in recent years, with vehicle assaults targeting pedestrians becoming more common. High profile attacks, such as those in London, Stockholm, Nice, Berlin, Barcelona and New York, have regularly hit the headlines as part of a grim global trend.

This unpredictable threat poses a dynamic challenge to the security services, but also those in charge of planning, designing and specifying urban areas which feature high footfall such as town squares and high streets.

The stock response has been to install concrete blocks or steel barricades to defend those specific spaces which appear the most vulnerable to attack, such as the entrances to sports stadia and shopping centres where large groups of people congregate. Together with neglecting how the protection can blend in with the rest of the surrounding environment, this approach often overlooks the different types of measures which can be used to secure a public space against this type of threat.

Instead, security professionals need to tackle this challenge more holistically and consider a number of different types of protection that can be used to deter, deflect and defend against vehicle attacks.

An aesthetically appealing defence

The first step to securing a public space is identifying the areas that have a significant footfall and a high risk of being accessed by a vehicle travelling at speed.

Rather than using utilitarian measures such as concrete blocks and long lines of bollards that can make a place feel fortified, security advisors should consider protective landscape furniture that can act as a far subtler and more visually appealing line of defence.

These measures, which range from planters, seating and litter bins to lighting columns, cycle stands and even signage, are built to stop cars, vans and lorries in their tracks and are crash-tested to the Publicly Available Specification (PAS) 68/IWA 14.1 certification. This is the latest accreditation for barriers and bollards to assist in terrorism prevention and specifies a classification for

> "...SECURITY ADVISORS SHOULD CONSIDER PROTECTIVE LANDSCAPE FURNITURE THAT CAN ACT AS A FAR SUBTLE AND VISUALLY APPEALING LINE OF DEFENCE."

vehicle security barriers and their foundations when subjected to impact. The products are available in a range of specifications to mitigate against different levels of risk. Using the strongest classification, for example, a single piece of street furniture can stop a 7.5-tonne articulated lorry travelling at 50mph. They're also built with foundations of varying depths, meaning they can be installed across town and city centres where space for excavation is often limited due to the presence of underground infrastructure.

> "THE INCREASING NUMBER OF PROTECTIVE MEASURES INSTALLED ACROSS THE UK SHOW THAT BOTH LOCAL AUTHORITIES AND SECURITY PROFESSIONALS ARE TAKING SIGNIFICANT STEPS FORWARD IN MITIGATING AGAINST POTENTIAL VEHICLE ATTACKS."

Marking a shift from the status quo

The increasing number of protective measures installed across the UK show that both local authorities and security professionals are taking significant steps forward in mitigating against potential vehicle attacks.

Yet, while it's clear that concrete blocks and long lines of bollards provide invaluable protection, the majority are utilitarian in design, which has a detrimental impact on how attractive the streetscape looks and reminds the public of the threat that exists. This can unnerve and potentially deter people from visiting high streets, attending sporting events or taking trips to historic city sites. There are numerous examples of this occurring across the UK, with installations at Windsor Castle and in Manchester and Westminster attracting negative headlines for their obtrusive and intimidating appearance, which in turn affect the aesthetics and general feel of an area.

The continued threat from this type of attack means we can expect those in charge of securing and protecting public places and people to place greater focus on using methods which can keep them safe while integrating well with the surrounding environment. By considering the protective measures they use on the three levels outlined here, they can help deliver more secure spaces for the people using them.

www.marshalls.co.uk

Specifying protection for lower-risk areas

In addition to this, consideration should be given to more sheltered areas where vehicles will only be able to access at lower speeds. Rather than using products that are crash-tested to PAS 68, security professionals now have the ability to procure measures which meet lower specifications and can be used to deflect a car or van from its target. Products crash-tested to the new PAS 170 accreditation, which provides the proof of performance that the anti-ram solutions previously specified were unable to deliver, can stop vehicles of up to 2.5 tonnes travelling up to 20mph.

Deter the danger

The third strand consists of a range of protective measures that can simply act as a visual deterrent to would-be attackers. Located on the outer perimeter of a public space where the risk to the public is low, these products can be installed to show that a "buffer-zone" has been created and build the perception that the area within is well protected.

Products that can serve this purpose include telescopic bollards, where vehicle and pedestrian access needs to be controlled, together with post and railing systems. Larger planters, strategically-placed to restrict access to vehicles and guide pedestrian flow, can also offer an important addition to a scheme.

IFSEC International and SCTX to **co-locate from May 2020**

Show organisers Clarion and UBM have announced the co-location of two important events to the UK security industry in a ground-breaking strategic alliance, from May 2020 onwards

Next year will see IFSEC move to a brand-new date of 19 - 21 May and welcome three prestigious events alongside it at ExCeL London; Security & Counter Terror Expo (SCTX), Ambition and Forensics Europe Expo.

Building on a rich history of the two exhibitions - IFSEC steeped in the trade and commercial security world and SCTX immersed in national security – the collaboration of these key events has been designed to meet the strength of demand for a central focal point for the security industry.

IFSEC will feature The Keynote Arena, a high impact, stylish area forming the centrepiece of the show. This will feature inspirational and transformational presentations from leading security influencers. At The Converged Security Centre hosted by Vidsys visitors will see converged security information management (CSIM) in real time. The LPCB Attack Testing Zone returns to showcase physical and perimeter security solutions as demonstrated through live tests by our partners from BRE Global/LPCB. Finally, The Future of Security Theatre hosted by education partner, Tavcom, will offer insights about future security solutions.

The additional synergies between the first responder focused, Ambition and Forensics Europe Expo, which currently run alongside SCTX, and FIREX International, as well as the wider security community, also lend additional diversity and strength to this new alliance.

ExCeL London will host 38,000 trade, commercial, public and policing security professionals at one venue. In doing so, the industry will see a single marketplace for the security ecosystem made up of installers, government end users, corporate end users, integrators, manufacturers and distributors.

The announcement of the move to stage IFSEC and SCTX together is already being warmly welcomed. "This has come at the perfect time for the security industry," said Mike Reddington, CEO, BSIA. "The BSIA are excited to be supporting this major new partnership between the UK's two leading security exhibitions. We have a long-standing partnership with IFSEC, and we look forward to extending our welcome to SCTX."

"Dahua is excited to see this partnership between IFSEC and SCTX in 2020," notes Steve Norman, Sales Director, Dahua Technology UK & Ireland. "It will provide a rewarding balance of end-users, consultants, installers and integrators. This presents a fantastic opportunity for

likeminded end-users and integrators to exchange ideas with manufacturing security professionals."

Discussing this move for the market, the organisers of IFSEC and SCTX share their thoughts as they announce the culmination of these 18 month-long discussions to co-locate these events. "SCTX is by far the most prestigious and market leading event in the counter terror arena, with a proven track record in drawing a high calibre audience of government specifiers, law enforcement and related crime intelligence agencies," said Gerry Dunphy of IFSEC. "This is a great fit for IFSEC as it strengthens our message of the critical nature of security as a major global issue. IFSEC will also highly complement this offering by continuing to champion integrated security for the trade and commercial markets. The prospect of these events, working in harmony, promoting expertise and guidance for the broader security environment has already been met with immense anticipation by the security community."

Bringing the events together will offer exhibiting manufacturers and distributors an opportunity to access the entire end-to-end security audience. Over 600 exhibiting companies will join to represent all aspects of the security sector, ranging from the latest developments in commercial and corporate security through to critical national infrastructure and policing.

For 2019, Clarion's Security & Counter Terror Expo, Ambition and Forensics Europe Expo will take place at Olympia from the 5-6 March and IFSEC International will bring expert security products to ExCeL, from 18-20 June.

www.dallmeier.com
www.panomera.com

ATG Access cements international
success with Greater China Awards win

ATG Access has been awarded the Rising Star accolade at the Greater China Awards as it continues its global reach, delivering state-of-the-art, intelligent barrier systems worldwide

The threat of terrorism continues to increase across all continents – individual country risk varies but critical infrastructure must be protected in all countries, as well as temporary events such as major sports tournaments, international conferences or summits or a high-profile visit of overseas dignitaries.

More than ever, there is a need to keep both people and property safe from extreme threats both in the public realm and on private land. Many deterrents and preventative measures are taken to combat such threats, one such option being the use of barrier systems.

ATG Access is a designer and manufacturer of medium and high security vehicle barrier systems including bollards, rising arm barriers and road blockers and has secured its international credentials by winning the Rising Star accolade at the Greater China Awards.

A UK-based competition for the North West of England, The Greater China Awards recognise organisations that have made a significant contribution to developing business or innovative partnerships within mainland China, Hong Kong, Macau or Taiwan. The Rising Star Award is specifically awarded to businesses which have had innovative and successful partnerships with

Greater China for fewer than three years. ATG Access fought off an eight-strong shortlist to win the much-acclaimed accolade, with judges praising the team's willingness and eagerness to forge strong business relationships and fully submerse itself in the territory. As well as its high-profile work in Shanghai.

To overcome cultural and linguistic barriers, ATG spent many years making regular trips to the region, before taking the decision to hire a native Chinese speaking professional to fill the role of South East Asia Export Manager. Appointing someone who has a deep-rooted understanding of this region has enabled ATG to create stronger communication networks and relationships with its exporting partners.

As such, ATG Access has had a long-standing relationship with both Northern and Southern China with its first project – securing the National Exhibition Centre in Beijing with non-impact tested, automatic bollards – taking place in 2010.

ATG Access was also called upon to better protect The Bund, one of Shanghai's busiest tourist attractions, after the tragic event on New Year's Eve 2014, where 36 people sadly lost their lives. The high-profile security project involved ATG deploying 86 of its SPTT automatic crash test bollards at seven different road junctions.

ATG was presented with the prize at an awards ceremony that took place at the Department for International Trade North West in Manchester.

"We are delighted to have won the Rising Star Award," said Gavin Hepburn, Director at ATG Access. "What really sets us apart is that we pride ourselves on doing business face-to-face. We don't just want to arrive in a new market, we want to fully understand it from a cultural, linguistic and business perspective, which for us means getting out there and putting people on the ground.

"Obtaining the contract in Shanghai did not come easily – it required a considerable amount of groundwork from our Asian manager, as well as our UK sales team who ventured out to the city to meet with stakeholders and build up the essential relationships needed to win the project," he continued. "As part of our continued international growth strategy, we aim to build on our relationships with countries across the globe, so to have an award tied to such an important market for us gives ATG Access the sort of recognition we need to take the business to the next level."

ATG Access has been protecting many major international critical infrastructure projects across the world for over a decade and is now supplying its products to 42 counties. In the last financial year (2017/18), the company's turnover increased by 12%, taking it from £15.6 million to £17.5 million, partly owed to its growing international footprint

360 Vision Invictus cameras deployed
across seven Greater London towns

360 Vision Technology's Invictus cameras are being used in a number of areas in a North London borough in order to provide effective night-time quality with the latest compact modules

Following the recent successful installation of 360 Vision Technology's Invictus ruggedised PTZ camera by a North London borough, the same borough has now rolled-out over 100 Invictus cameras across seven Greater London towns in a project with DSSL Group.

With an early success in prosecuting serious crime following the deployment of Invictus, its highly effective night-time HD quality colour video footage proved to be just one of the useful attributes of the UK manufactured camera. This was added to when a recent significant impact by a vehicle to a camera column tested its suitability for roadside deployment. The Invictus camera took the high-speed impact in its stride and showcased its 'Attack Detect' feature, automatically resetting to the last viewing position prior to being forcibly moved from its previous viewing direction, and with no damage to the camera or its direct drive PTZ mechanism.

Commenting on the broader roll-out of Invictus cameras, DSSL Group's Works Director, Aaron Stephens, who specified the 360 Vision Technology cameras confirms: "The importance of selecting a product that is 'fit for purpose' when being deployed roadside in a town centre is often overlooked by some companies, who deploy non-ruggedised cameras purely on the basis of cost.

"If a PTZ camera were to fall from height following an impact, which is a real risk, there would be a substantial public health and safety incident. At DSSL, we take a holistic view to consider the surveillance needs at each individual location, to ensure that all aspects of camera deployment are taken in to consideration. Based on our experience, 360 Vision's Invictus camera was the obvious choice for us to recommend to this important Local Authority customer."

The expanded installation takes the total number of Invictus cameras to over 100 and allied to wireless links forming a major part of the system's infrastructure, comment has been made regarding the quality of the Invictus camera video over wireless infrastructure. Theproject also saw the integration of Genetec Security Centre with the Invictus PTZ cameras.

Commenting on the camera/control technology collaboration, Genetec Country Manager, Paul Dodds notes: "Our close technical partnership with 360 Vision Technology has enabled deep systems integration and control of the Invictus cameras. Genetec Security Centre unified platform and Omnicast video surveillance has been used to seamlessly blend full Invictus camera menu control, within a single intuitive interface. 360 Vision cameras are a Genetec certified product on our supported device list. This successful deep integration has simplified the London borough's surveillance operation and effective management. We value all of our technology partnerships, and especially with manufacturers such as 360 Vision Technology, who offer reliability with their Invictus PTZ cameras, as illustrated here across seven north London towns."

Adrian Kirk, Strategic Account Director at 360 Vision commented on the green credentials of Invictus, which was a factor in the overall decision by DSSL to specify the camera: "With a focus on reducing carbon footprint, we are continually working towards reductions in camera power consumption. On larger projects like this, the savings on energy and reduction in associated pollution offers significant advantages over Far East camera alternatives, helping Local Authority end-user system operators to meet their carbon footprint reduction goals. With a host of performance and user centric operational benefits, Invictus is well placed to feature extensively in future Local Authority upgrades, as customers look at total cost of ownership and the need to ensure CCTV equipment deployed road side is fit for purpose."

www.360visiontechnology.com

Rajant delivers CCTV network solution
for recent high-profile public safety events

Rajant Corporation has delivered surveillance solutions in the last year to major events such as the Royal Wedding – as it disussed at the Police National Technical Surveillance Conference

Kinetic Mesh networks manufacturer, Rajant Corporation, has provided a detailed technology briefing to the Police community on the success of recent high-profile public safety projects for the British monarchy.

Rajant worked alongside Thames Valley Police to boost the already significant public safety and security arrangements at the weddings of Prince Harry to Meghan Markle and Princess Eugenie to Jack Brooksbank in Windsor last year. Together, the entities were responsible for providing additional video surveillance coverage, which included deploying the Rajant wireless infrastructure, for secure and stable CCTV.

The briefings at the conference described how the additional surveillance was required to cover the hundreds of thousands of visitors and guests in Windsor during both weddings to catch a glimpse of the royal couples. The whole area was securely monitored with footage made available at multiple surveillance points and delivered in real-time in high-definition. This comprehensive security was deployed with maximum efficiency thanks to Rajant's Kinetic Mesh network in key points where network fibre infrastructure, for the essential additional cameras, was unavailable.

"Our brief was to provide supplementary CCTV coverage for the Royal Weddings," recalls a member of the Thames Valley Police team. "It became quite apparent during the design process that using conventional point to point/multipoint would not suffice in the urban environment of Windsor. A true mesh network would better provide the resilience and coverage we required. Rajant was identified as a supplier of mesh networking equipment, available in both the police and licence-exempt frequencies, with ease of deployment making Rajant's mesh network a superior solution."

"For both high-profile events, Windsor saw a significant increase of well-wishers coming into the town to watch the carriage rides," adds said Chris Mason, Director of Sales for EMEA at Rajant. "Delivering additional CCTV systems, which could then be monitored by police and security services, was a top priority. Given the route for the post-wedding processions by the royal couples was through the winding streets of Windsor and up through Windsor Castle's Long Walk, Thames Valley Police decided to enhance the existing extensive CCTV coverage with dynamically deployed supplementary cameras. The operational team put a project in place to rapidly deploy a solution which, when combined with the existing capabilities, could comprehensively monitor each day's oute to ensure public safety."

The Kinetic Mesh technology integrated with existing communications infrastructure at key locations. This enabled large amounts of mission-critical video data to be delivered with high throughput and low latency across the network, giving the police the visibility, they needed. According to Thames Police:

"The imagery provided over the Rajant network was several seconds ahead of the television broadcasters covering the event and met the expectations of our users."

Rajant worked alongside the Thames Valley Police to deliver the project in just three days. Deploying 11 cameras with 13 of Rajant's BreadCrumb nodes, delivery of fast, stable and high-definition CCTV was achieved. The network utilised multiple high-bandwidth frequencies, ensuring that the massive amount of wireless output from broadcasters, other security organisations and the general public did not prevent transmission of the key imagery.

"Rajant's focus is to ensure public safety requirements are provided quickly and securely for authorities, and these two projects were no different," adds Mason. "Rajant is developing its portfolio of Kinetic Mesh technologies to address the requirements for enhanced public safety and security by enabling organisations such as Thames Valley Police, to deploy networks extremely quickly in response to planned or unplanned events. Showcasing these deployments for the first time at the Police Conference was a great privilege. We highlighted the key capabilities of our technology as well as illustrating how events of this scale can have rapidly deployed, secure, reliable communications. We are pleased to have played a part in making both wedding days enjoyable, but most importantly safe for all involved."

www.rajant.com

Fight crime more efficiently
with a smart city mindset

New technologies have arisen to make the job of Law enforcement teams more efficient. However, only a few have offered such advances in efficiency as smart, connected video solutions

If you look at Maslow's Hierarchy of Needs, you'll find the need for safety and security ranking second after the basic needs like food and water. Already today, technology plays a central role when people look to increase safety and security. Many companies, and a constantly growing number of home owners, use security cameras connected to an alarm system to protect their premises and prevent criminal activity. For law enforcement agencies – those at the sharp end of public safety and security – technology is becoming an increasingly important tool to improve every-day efficiency. By adopting a smart-city mindset, where devices, data and stakeholders are connected to better manage assets and resources, law enforcers benefit from new, innovative ways to prevent, deter and solve crime.

Real-life success in increasing public safety

Law enforcement teams around the world share fundamental objectives, but also key obstacles. Their long-term mission is to keep citizens safe and secure. At the same time, they are challenged by limited budget and resources. Throughout history, there have been many new technologies that have made their job more efficient. Examples would be police radio, fingerprint databases and DNA forensics. Besides the listed technologies, today's smart, connected video solutions rank also very high on the list of game-changing improvements in terms of crimefighting efficiency. Their success can be seen in many cities.

Let's take Kolhapur in India for example. A city known for its magnificent palaces and beautiful gardens. It's vicinity to Mumbai makes it a growing tourist attraction. Therefore, local authorities had to take care of crime management as

well as traffic control and disaster management. The requirement of an efficient and integrated security surveillance solution was the need of the hour.

The city implemented a smart solution in the form of 165 network cameras at 65 locations to reduce the possibility of a security threat. This has enabled the Kolhapur Police to reduce response times and get faster access to evidence in case of law violations. Round-the-clock observation of entry/exit points, junctions and tourist attractions help authorities to better manage traffic and improve the overall operational efficiency.

Combining public and private resources

Another example of how connected video solutions can help law enforcement to combat crime and improve emergency preparedness comes from the City of Atlanta. As the city's population grew, it became apparent that the Atlanta Police Department (APD) needed a force multiplier to assist its citywide surveillance efforts to better protect its citizens. The APD launched Operation Shield, a video integration

> "WHAT STARTED WITH 17 DOWNTOWN SURVEILLANCE CAMERAS HAS SINCE BEEN GROWING TO A NETWORK OF OVER 400 CAMERAS."

initiative that pulls video resources from private and public entities into a single command centre. This way the law enforcement is provided with a more holistic view of prioritised areas across the city.

What started with 17 downtown surveillance cameras has since been growing to a network of over 400 cameras. Furthermore, the APD has partnered with city organisations, such as Atlanta's Public School System and the rapid transit authority, which all together contribute another 4,000 cameras. But the biggest part of this camera network is taken up by cameras of private entities such as multi-

incidents such as gunshots, trespassing, burglary, robbery or suspect vehicles.

Operations centre: Sometimes referred to as a real-time crime centre, the operations centre is a hub for incident management. This is where information from the cameras and all the other connected devices comes together. Once there is an alert – from an emergency call, a sensor, or a camera – operators can use their access to the cameras to examine the situation and react accordingly. Being able to make informed decisions, helps to have faster responses and decreases the risk of an unnecessary deployment of resources.

Connected field resources: For law enforcement officers who are in the field, it is important to be continuously updated with the latest information in order to be able to respond in the best possible way. The data processed by the operations centre is forwarded to mobile devices used in the field. Important information, such as license plate numbers, images of suspects or vehicles and other details can be sent to officers on their way to the scene, so they know what and whom to look for. Not only does this improve the response success but also keeps officers safe as they know what to expect (and how to prepare in an effective manner).

A path to safer and smarter cities

Many cities and law enforcement agencies have already discovered how a strategic network of cameras and other connected devices offers invaluable support in their everyday battle against crime. Real-time access to visual data helps to ensure quick and appropriate incident response, and high-quality video footage serves as valid proof in court. Besides providing a higher level of public safety and security, these connected surveillance solutions serve as an enabler for new, innovative forms of collaboration. The total cost of a citywide security network can be shared between multiple public and private stakeholders, while creating value for all parties involved. And in a smart city fashion, it enables more efficient use of public resources with the long-term ambition to create safer and more liveable cities.

www.axis.com

family housing properties and local businesses. The video is streamed to a secure cloud storage, where it can be disseminated when required by the law enforcement team.

The result is that Atlanta Police Department has access to 24/7 surveillance throughout the city, giving it a real-time view of situations that take place in the monitored areas. Should anything happen at a public school, in the public transit system or at any of the other connected public or private entities, the APD has an instant view of the incident, helping it to react and respond more efficiently.

It also means that the private businesses and housing complexes that share their surveillance video with the APD, benefit from quicker and better-prepared response from the emergency responders.

Additionally, this public-private collaboration has saved the city a considerable investment in equipment and maintenance, as many of the surveillance resources are owned by private stakeholders.

Three cornerstones of crimefighting with video surveillance

If we examine these real-world examples, it becomes obvious that they share three key attributes that are crucial in the fight against crime.

Networks of cameras and sensors: A network of cameras observes key locations where crime is frequent, or where citizens have a particular need to feel safe. In many cases, additional sensors and video analytics solutions, can be added to automatically detect potential dangers and

How secure is **your data?**

GDPR has been one of the major concerns with data storage recently. However, there are solutions that can help as Graham Hutchins from Simms International explains

When GDPR was announced back in 2016 there was a lot of scaremongering with the threat of large fines if you lost data. To a certain extent this is true if you really are that negligent and buried your head in the sand hoping a breach would go away, as can be seen from Google's €50 million in France.

For many, GDPR was a necessary evil but also a timely update to company policies on the way data is handled, stored and secured. Yet we still hear stories on the news about large organisations losing data which has been downloaded onto a humble non-encrypted USB drive. As these stories illustrate, unfortunately, the biggest cause of a data breach is employee negligence.

Keeping data secure is changing and fast. Five years ago, AES 256-bit encryption was mainly considered for use in the military. However, fast forward to 2019 and it is now becoming the standard across flash storage devices.

But this does raise the question, how good is 256-bit encryption? The best supercomputers have not even come close to cracking 128-bit let alone 256-bit encryption so to answer this point, it's safe to say it's good.

There are many kinds of encrypted data storage devices available, suitable for all manner of applications; from servers to surveillance systems, laptops to USBs there is a solution for most things.

Taking one of the four areas mentioned, server SSDs have come a long way now that 3D NAND flash is firmly established as the storage chip of choice. For example, Intel offer 2.5-inch SSDs with up to 8TB capacity and 256-bit encryption as standard across its entire range.

With the biggest data breach being employee negligence there are many solutions in place to keep data secure on the go such as encrypted USBs. Kingston and Apricorn lead the way with their pocket size solutions for all kinds of budgets, all with 256-bit encryption as standard. More companies are turning to encrypted USBs as a way of keeping data secure outside of their network as part of their wider IT policy.

While some may believe this could raise GDPR issues, this is not the case. Most people do not know that Article 34 of GDPR states that if data is lost and is encrypted you do not have to contact the affected parties. In addition, Article 32 states that "appropriate levels of security to the risk are in place" such as encryption of personal data.

As a result of this portion of the law, using encrypted USBs can tick a small but important box to assist companies with their GDPR compliance.

www.simms.co.uk

UDT
Undersea Defence Technology

13-15 May 2019

Stockholmsmässan, Sweden

1,100+ attendees expected

80+ exhibiting companies

3 days of high-level briefings

40+ countries represented

30+ VIPs attending

THE GLOBAL EVENT FOR UNDERSEA DEFENCE AND SECURITY

EARLY BIRD DEADLINE: 15 MARCH 2019

REGISTRATION NOW OPEN

🌐 www.udt-global.com   🐦 @UDT_Event   in www.linkedin.com/groups/1882279

UK MOD © Crown copyright 2018

Headline partner	Lead diving sponsor	Featuring	Organisers of	Organised by
SAAB	JFD	MILITARY DIVER CAPABILITIES	ADECS ASIA DEFENCE EXPO & CONFERENCE SERIES 2020	CLARION EVENTS

Oversharers and underspenders: An **international tour of security habits**

Phil Allen, VP EMEA at Ping Identity explains what the company's 2018 Ping Identity Consumer Privacy Report tells us about attitudes to data security in different markets around the world

Once, and not too long ago, people might have said "who would want to hack me?"; they might laugh at the possibility of Facebook feeds helping to elect presidents; they might balk at the idea that liberal democracies are snatching as much personal data as they can get their hands on. Still, things change.

Few can now deny what was so easily ignored only a few years ago: That their data matters.

That's partly why we commissioned the 2018 Ping Identity Consumer Privacy Report. We surveyed over 3,000

consumers across the US, UK, France and Germany to examine evolving consumer attitudes towards privacy and data.

The results are encouraging. After a data breach, 78% of our respondents would stop using a brand's online presence. Another 49% would not engage with that brand in the first place. Overall, 54% of people are more concerned with protecting their personal information than they were a year ago.

Although everyone had responded to this new landscape, they all did so in their own idiosyncratic ways. The advent of the internet has connected the world, but

the recognition of that fact seems highly subjective.

The ever-optimistic US, for example, continues to have faith in online services. US citizens reported more breaches than anyone else – 27% of them said as much – but they largely maintained their trust of online services. They were the most ready to share their credit card details (40%) and even their social security numbers (16%). Furthermore, at 62%, they're the most willing to spend money on online services and nearly half of them (48%) said that they were confident in the ability of those services to protect their personal data.

This stands out in stark contrast to the French, who are naturally more suspicious of online services. Only 38% of our French respondents were confident in the ability of those services to keep their data private and safe.

French society has often registered a profound suspicion of social platforms and foreign tech companies in general. Still, their distrust reaches further than Silicon Valley to the US itself. Edward Snowden's allegations that the National Security Agency was collecting private information of foreign citizens, and were doing so with the cooperation of US tech giants, did not sit well in France, nor the rest of Europe.

That could be the reason why they're taking up the concept of "digital sovereignty" with such enthusiasm. In late 2018, parts of the French state – including the military – owed that they would no longer use foreign alternatives and only use Qwant, a European search engine which claims to not track ts users.

"NOW THAT THE SMOKE HAS CLEARED, 42% OF US RESPONDENTS – STIRRED BY THE NEWS – CLAIM THAT THEY WILL NOT BE USING FACEBOOK LOGIN ANYMORE."

It's a concept which has resounded with Germany too. In 2015, both countries committed themselves to developing European tech industries which would privilege privacy and the protection of European data. Furthermore, they stated, they wanted "the ability for Europeans to decide in an autonomous way the level of security for their data, in particular in the context of negotiations of trade agreements."

With part of the country spending much of the twentieth century under the thumb of a despotic Soviet regime and their all-seeing secret police, The Stasi, it's understandable that Germans place a singular premium on their privacy.

Our survey bore that out. Only 13% of Germans will share their credit card details, 6% are willing to share their government credentials with online services.

They trust social platforms almost as little as the French with 42% saying that they are not confident that social platforms can protect their data. They've also taken the Cambridge Analytica revelations much harder than the US and even their European neighbours. Half of our German respondents declared that they would not be using Facebook social login to connect to other apps and services.

This point is important, because it sits at the very centre of not just the Cambridge Analytica incident but Facebook's use of data globally.

When Cambridge Analytica worked on he 2016 US elections, it did so in a very particular way. Using data scraped from social media, the political consultancy could create individual psychological profiles of voters and target them on a level of granularity that was largely unheard of. Much of that data was gathered through Facebook social login, wherein users could use their Facebook credentials to access other apps and services. According to a user's settings, developers of those apps could then use that data (including the data in their friend lists) for their own purposes. One app called This is Your Digital Life was used by 270,000 Facebook users. Those downloads effectively turned into profile data for nine million people. By 2017, the company was claiming that it had profiles on 220 million US citizens.

Now that the smoke has cleared, 42% of US respondents – stirred by the news – claim that they will not be using Facebook login anymore.

The smallest response seems to come from the UK, where only 39% of UK citizens will stop using Facebook login on the back of the news.

The British don't seem particularly fazed by the threat of a cyberattack at all, being the least willing to shell out any more money for added security. The survey found that 64% of our British respondents told us so, compared with Americans of which 52% were happy to pay more.

Then again, that laid back demeanour may be down to the fact that they generally have less to worry about. UK citizens were the least likely to have experienced a breach, at an impressive 15% compared to a high of 27% in the US.

That difference between the two shores of the Atlantic is crucial. It's those differences that have defined much of the titanic political conflicts between Brussels and Silicon Valley. EU-US Privacy Shield had to be hastily pieced together to govern transatlantic data flows after the Snowden Revelations. Even more significant for enterprises is the arrival of the General Data Protection Regulation (GDPR), a piece of law which aims to protect the data of all European citizens from hackers and data hungry businesses alike. It sets out very clear rules for the handling, securing and disposal of data and threatens large fines for those who infringe them.

These results are understandable. Foreign tech companies that share personal data with opaque intelligence services and political consultancies will be viewed with suspicion in countries with cultures that privilege privacy. The fact of the internet creates problems for national sovereignty, and it's not surprising that European governments (and by extension, their citizens) would judge foreign tech companies with hostility. What's more surprising is that these results haven't come sooner.

www.pingidentity.com

Are we at the start of a new
global arms race?

Russian President Vladimir Putin uses state-of-the-nation address to promise Russian retaliation
if US deploys new missiles in Europe, pushing the two countries closer to a new arms race

Russia's President Vladimir Putin warned the United States against deploying new land-based missiles in Europe, threatening to retaliate in kind by targeting Western capitals with his own new weaponry.

On 20 October 2018, citing Russian non-compliance with its deployment of its 9M729 missile, US President Donald Trump announced the withdrawal of the US from the 1987 Intermediate Range Nuclear Forces treaty (INF). This treaty, originally signed by President Ronald Reagan and Soviet leader Mikhail Gorbachev, intended to eliminate nuclear and conventional ground-launched ballistic and cruise missiles with intermediate ranges of 500 to 5,500km. The treaty came into force on 01 June 1988.

Political unrest between the US and Russia has heightened due to this treaty since 2012, when the United States complained about treaty violations with Russia's deployment of the cruise missile 9K720 Iskander launcher. Similarly, the US has now claimed Russia's continued violation with its new 9M729 missile, leading to the country formally suspending the treaty.

President Putin has now stated his belief that the US is purposefully abandoning the integral arms control pact to free its hands in order to build new missiles in Europe. The disbanding of the Cold War-era treaty has effectively signalled the start of a new arms race beginning 1 February 2019 with the official withdrawal of both parties unless Russia returns to compliance within six months.

President Trump's statement asserted the US "will not remain constrained by its terms while Russia misrepresents its actions… We will move forward with developing our own military response options and will work with NATO and our other allies and partners to deny Russia any military advantage from its unlawful conduct".

The warning came during this year's state-of-the-nation address to parliament, in which President Putin focused primarily on social spending and growth rate,

primarily for poor living standards. The address centred around providing the people of Russia with what they wanted and needed to hear.

However, his response to the accusations from the US regarding Russian missiles and in turn the deployment of US missiles around Europe, was not so softening, but instead promised an "asymmetric" response from Russia if the US stationed such missiles in Europe.

He stated that, due to not hearing statements of the opposite, the deployment of missiles would "sharply aggravate the situation in the sphere of international security", as it will be viewed as a direct threat to Moscow.

During the address, President Putin stated: "I'll say today and openly, so that no one will reproach us later, so that it will be clear to everyone what we are talking about here: Russia will be forced to create and deploy types of weapons that can target not only those territories from which a direct threat emanates, but also those territories where there are decision-making centres for the use of missile systems that threaten us."

President Putin warned the US that Moscow would match any move made by President Trump. He detailed the potential implementation of nuclear weaponry that Russia had already been working on in 2018. His descriptive warning told of the ability to station the new Zircon and Poseidon hypersonic missiles on ships and submarines for the Russian navy. The ships would be outside of the US territorial waters and constantly moving so that they were virtually undetectable.

He described the speed and ability of the Zircon and Poseidon missiles as

"invulnerable", as they have the capability to travel at nine times the speed of sound, with a travel distance of up to 1,000km. The remaining time and cost of the programme would not be too excessive as it is designed to be equipped to Russia's existing surface ships and submarines.

Russian Defence Minister General of the Army, Sergei Shoigu, released in an interview with reporters after President Putin's address to the Federal Assembly, that, "the new Russian weapons will guarantee security without increasing costs and without joining an arms race."

President Putin's warning echoed that of The Cuban Missile Crisis that erupted in 1962, when Moscow responded to a US missile deployment in Turkey by sending ballistic missiles to Cuba, sparking a standoff that brought the world to the brink of nuclear war.

As tensions rise again, Russia, the US and NATO, have all made assurances in their statements of being open to arms control talks and the desire to maintain a friendly political relationship.

President Putin continued by adding: "Russia is not interested in confrontation" and that it is open to arms control talks with the US. Despite this, it is clear by his address, that Russia will not be backing down to Washington.

Piers Cazalet, NATO Deputy spokesperson,

released a statement in response to the threats from Russia. Cazalet stated that NATO's missile defence system, including the Aegis Ashore facilities in Romania and Poland, are purely defensive and compliant with the INF treaty.

Cazalet acknowledged the Russian leader's address and considered his threat against allies unacceptable. "We have noted President Vladimir Putin's address of 20 February. Russian statements threatening to target allies is unacceptable. We call on Russia to focus on returning to compliance with the Intermediate Range Nuclear Forces Treaty. NATO is a defensive alliance, which stands ready to defend all members against any threat. We do not want a new arms race, and allies have repeatedly called on Russia to verifiably destroy its intermediate-range missiles."

NATO Chief, Jena Stoltenberg has reiterated in a statement to reporters that the alliance would not deploy any new land-based nuclear weapons in response to the Russian missiles. "We urge Russia to take this opportunity [to fix alleged compliance breaches]," stated Stoltenberg. "At the same time, we are planning for a world without the INF treaty. At this meeting of defence ministers, we will discuss what steps NATO should take to adapt to a world with more Russian missiles and maintain effective deterrence and defence. I will not speculate on what those steps will be… Any steps we take will be coordinated, measured and defensive. We do not

intend to deploy new ground-based nuclear missiles in Europe."

The US State Department has also responded to President Putin's threats, claiming that Washington was not developing "exotic new nuclear weapon delivery systems" and maintained its claim that Russia violates the INF treaty, while the US does not.

A State Department spokeswoman, on condition of anonymity, said, "President Putin's remarks are a continuation of Russia's propaganda effort to avoid responsibility for Russia's actions in violation of the INF treaty".

If both parties deny responsibility and continue to provoke responses from one another, a new arms race is soon to come to fruition.

Vladimir Putin
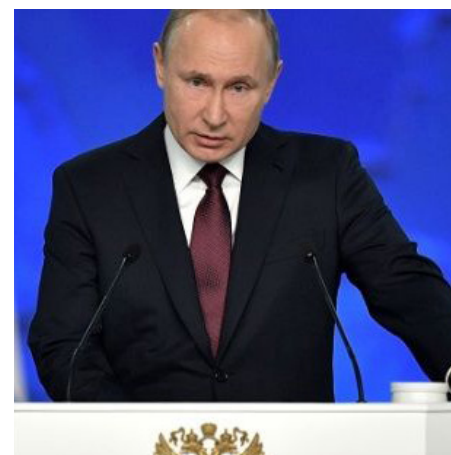
Cyber security scorecard gives business real-time
understanding of security risks

Cyber-risk is becoming a very prominent issue in recent years and businesses are relying on software
companies like Huntsman Security to provide a clear outlook and give simple solutions

As executives struggle to understand their organisations' exposure to cyber-risk, Huntsman Security has launched The Security Scorecard – the first tool of its kind to give instant visibility of an organisation's Cyber Security Posture. The Scorecard is a standalone product that gives non-IT people such as auditors, risk managers and senior executives an understanding of an entity's cyber security exposure.

The Scorecard technology automatically measures eight key security controls whose effectiveness determines just how secure an organisation is from a cyber-attack. Based on findings by the Australian Signals Directorate (ASD), these best practice controls can reduce the likelihood of a cyber-attack by more than 85%. Measuring against these, the Scorecard gives an immediate and automated understanding of risk and exposure, allowing the business to tune the effectiveness of the controls in line with its risk appetite.

"One of the biggest issues security teams face is presenting a convincing argument to the board about what measures need to be taken to reduce risk, and why," said Jon Collins, industry analyst at Gigaom. "In this situation, the security team doesn't want to present a list of thousands of outstanding actions, but a shortlist of the highest priorities. A simple scorecard acts as a paring knife, allowing organisations to act more quickly to reduce risk.

"Ultimately, any organisation suffering a breach wants it to be because they fell victim to a complex, never-before-seen attack; not because they failed to follow basic precautions," he continues. "Huntsman's scorecard is a great starting point for security teams and executives who want to ensure they have taken essential precautions, based on clear criteria."

Utilising the "essential eight" controls, the solution consists of eight processes that, together prevent initial attacks, limit the extent of incidents, recover data and restore systems availability. The processes are split into a "top four" – application whitelisting, patching applications, patching operating systems and restricting admin privileges – that are critical to achieving security. Plus, a further four – disabling untrusted Microsoft office macros, user application hardening, multi-factor authentication and daily backup of important data. The "top four" controls are mandatory for Australian federal government departments, and the eight controls collectively complement the best practices put in place by other

governments, such as the UK or USA.

The Security Scorecard continuously measures the performance of the controls, reporting clear metrics and red, amber, green colour-coded status that the manufacturer states is understood by any audience. Armed with this information, stakeholders have an immediate overview of their exposure and security teams know whether to focus on these essential processes or examine other ways to reduce risk further.

A standalone product, the Scorecard has a small proactive footprint that sits alongside other security technologies. Security teams can continue with their primary operations without any distraction and without significant investment in new security systems. Because of this, the Scorecard is easy to implement for any organisation. The Scorecard can be used by organisations in a supply chain to give visibility of their security posture to partners up and down the chain.

"No matter how good or detailed your criteria for effective security, if you only measure it once a year; it won't give auditors a representative view of operations and it certainly won't enable the proactive management of risk that security teams and executives aspire to," said Peter Woollacott, CEO and founder of Huntsman Security.

As a Computer Aided Audit Tool (CAAT), rather than providing a "snapshot in time" it delivers a continuous view of cyber posture for auditors. It also serves to support security specialists in their pursuit of plugging any security gaps.

www.huntsmansecurity.com

Sophos Central Management platform offers
next-gen cybersecurity protection

With the addition of Sophos XG Firewall, this will provide advanced Synchronised Security capabilities for accelerated response to cyberattacks from a single cloud-based management console

---

Sophos has announced that the next-gen Sophos XG Firewall is now available through Sophos Central, bringing its complete portfolio of cybersecurity solutions into a single, cloud-based management platform.

In addition to the efficiency of managing multiple products through a single, cloud management platform, threat detection and response times are improved by the Security Heartbeat in the manufacturer's Synchronised Security technology. This approach shares security incident alerts directly between Sophos network and endpoint protection products.

The XG Firewall will automatically communicate with Sophos' endpoint products to proactively protect against threats, interrupt the attack chain by isolating machines, and take steps to remediate the attack. Sophos Central effectively creates a system of security that can leverage the artificial intelligence in Intercept X with EDR to reportedly respond faster and more effectively than individual products alone.

"IT organisations do not have the resources to respond to the volume of constant and constantly shifting cyberattacks," states Dan Schiappa, senior vice president and general manager, Products, Sophos. "Sophisticated threats require intelligent security solutions that are predictive, multi-layered, and can work together as a system. With Sophos Central, partners and their customers have access to all Sophos next-generation security technologies and can benefit from the advances in Synchronised Security from one single location.

"The threat landscape has evolved and now our approach to protecting the IT infrastructure that supports our businesses must evolve," he continues. "Every IT organisation, large or small, needs security that is innovative, integrated and scalable. Sophos Central provides all of this, plus vital visibility into what's happening and where."

In addition to XG Firewall and artificial intelligence-driven endpoint security, partners and customers can manage web, email, wireless, server and mobile device protection through Sophos Central. A dedicated partner dashboard caters to business management for Sophos partners and enables multi-customer management for MSPs.

"By completing its vision to unify XG Firewall and Intercept X endpoint protection in Sophos Central, Sophos is putting us ahead of our competition," says Ryan Lipschitz, vice president of engineering, Virtual Graffiti, Inc., a Sophos partner based in Irvine, California. "The platform is now even more powerful because of the added benefits of Synchronised Security in an easy-to-manage cloud-based platform that seamlessly integrates with the entire Sophos security products portfolio. We are also excited about the lateral movement protection added to XG Firewall. We see a lot of cybercriminals trying to harvest credentials, which would allow them to move undetected through a network to steal and exfiltrate high-value data. With XG Firewall on Sophos Central, Sophos has made game-changing advancements no one else offers."

Recent threats like Emotet and targeted ransomware, such as Matrix and SamSam, demonstrate the ways cybercriminals are constantly changing their tactics to stay effective and profitable. The next-geneneration advancements of XG Firewall and Intercept X, combined with the intelligence of Synchronized Security and management of all products within Sophos Central, are described by the manufacturer as essential for maintaining protection and responding quickly to any attack.

"Our goal at Opus is to provide customers with simplicity and features that add layers of protection, so every area of their environment is secure," said Mehernosh Chemi, Senior Account Manager at OPUS Consulting Group, a Sophos partner in Vancouver, Canada. "With XG Firewall now on Sophos Central, Sophos is providing complete 'edge to end security' that is managed centrally in a cloud. This is the simplicity customers are looking for, and the addition of the XG Firewall means they have the benefit of Sophos' security heartbeat technology for bilateral communication between the endpoint and firewall. Moving forward, we are focusing our customers on Intercept X with EDR and XG Firewall. The two go together. Having these next-gen products integrated with Sophos' complete portfolio in Sophos Central is the protection customers need to stay secure."

www.sophos.com

Pulse Secure integrates SDP
architecture within its Secure Access platform

Pulse Secure says it is the first to deliver secure access for hybrid IT with Software Defined Perimeter (SDP) solutions delivering provisioning simplicity, scale and superior economics

Pulse Secure has integrated SDP (Software Defined Perimeter) architecture within its Secure Access platform and included Pulse SDP as an add-on within its Access Suite. By offering a flexible path to SDP, the company states that it has extended its foundation of Zero Trust access for hybrid IT and provided enterprises and service providers with unrivalled provisioning simplicity, security posture fortification and lower total cost of ownership.

SDP is an emerging security architecture that requires user authentication and device validation before a connection is granted. In other words, a deeper level of trust is established – before access – between users and resources. With this approach, network connectivity is based on a need-to-know model, in which device posture and identity are verified before access to applications is granted. Application infrastructure is effectively "dark" (a DoD term meaning the infrastructure cannot be detected) without visible DNS information or IP addresses.

Zero Trust is a next-generation security model based on the principle of "never trust,

always verify", offering capabilities such as extensive authentication, policy controls and data communication encryption. In effect, SDP is an enhancement of Zero Trust by including technical components directly into the architecture. It offers provisioning simplicity, security posture fortification, and lower total cost of ownership.

Ubiquitous access to applications and dynamic resource provisioning are the new normal, yielding an increase in advanced threats and massive data breaches. As enterprises embrace digital transformation and migrate their applications and infrastructure to multi-cloud, access requirements have become more stringent and complex to prevent attacks and data leakage. To reduce risk, organisations are applying a Zero Trust strategy of "verification before trust" by incorporating stronger user and device authentication, granular access control, and enhanced segmentation no matter where the application and resources reside.

"Business leaders face a digital imperative to boost user productivity, while also mitigating the risk of data breaches that are growing in size and frequency," notes

Sudhakar Ramakrishna, CEO of Pulse Secure. "From our inception, Pulse Secure has focused on providing a pragmatic approach to Zero Trust Secure Access that balances user experience with compliance. By incorporating SDP architecture within our Access Suite, we can deliver the deployment flexibility, scale and investment protection sought by enterprises and service providers."

Pulse Secure Access Suite provides remote, mobile, cloud, network and application security with comprehensive VPN, Mobile Device Management (MDM), Single Sign-on (SS0), endpoint and IoT device visibility, Network Access Control (NAC) and virtual Application Delivery Controller (ADC) capabilities. Pulse SDP complements this integrated solution set by offering direct device to application/resource secure connectivity only after successful user, device and security state verification including geo location and behaviour-based anomaly detection. As a result, the manufacturer states that organisations gain accessibility while streamlining access provisioning, improving performance and reducing the visible attack surface. More so, organisations reportedly gain greater economies and a non-disruptive way to readily implement SDP functionality when, where and how they require.

"Despite industry suggestions about VPN replacement, SDP is not a panacea for all applications and hybrid IT infrastructure as enterprises migrate to the cloud," says Jon Oltsik, senior principal analyst at Enterprise Strategy Group. "While deployments can offer comparatively simple, secure connectivity, SDP projects tend to be based on specific use cases and projects. VPN and SDP will likely co-exist for a while, so organisations need to keep an eye on joint usability, management and costs. By

offering an integrated secure access suite that supports VPN and SDP architectures for data centre and cloud, Pulse Secure can provide strong value that can be compelling for customers and service providers."

With SDP, Pulse is now the only Zero Trust vendor to provide a dual offering to customers: traditional secure access through VPN technologies, and SDP for customers looking to increase device-based security (given the prevalence of BYOD), centralise policy control and reduce the attack surface of their network.

Pulse Secure provides enterprises single pane-of-glass secure management and operational visibility across public cloud, private cloud and data centre. The manufacturer sees SDP as a logical extension of Zero Trust Secure Access that offers a lower total cost of ownership, streamlined configuration and policy controls and an increased security profile.

Most importantly, Pulse Secure's SDP does not force a rip and replace approach. Existing customers can leverage all or part of their already-deployed Pulse infrastructure to take advantage of SDP features and functionality. Similarly, new customers can deploy SDP immediately, or in silos. Other vendors require a more drastic approach that may not incorporate

every application a customer needs into the SDP installation.

Pulse Secure's existing integrations with identity providers such as Okta, Ping Identity and Microsoft ADFS continue to be relevant. The company states that customers need not re-integrate their toolsets with SDP. Moreover, SDP augments these identity-based integrations through additional multi-factor authentication (MFA) and device- and host-based security state checking. In this way, endpoints are checked prior to the connection for their security health, preventing malware spread within the network.

Pulse Secure's existing NAC-based integrations are augmented, too. By superimposing the Zero Trust and SDP features, policies and actions taken by enforcement points (such as firewalls) can be more granular and incorporate endpoint- and device-based information. Administrators can take action via policy, such as quarantining devices for remediation, based on this integration.

Pulse SDP will be offered solely as a licensed component within Advanced and Enterprise Editions of the Pulse Access Suites in April 2019. Pulse SDP is comprised of an SDP Controller, SDP Client and SDP Gateway which are enabled within the Pulse

Secure software, hardware and cloud solutions. This approach allows SDP and perimeter-based VPN functionality to work in parallel and provides Zero Trust access security and essential operational flexibility for enterprises and service providers. With a software upgrade, customers can activate Pulse SDP using the latest Pulse Secure infrastructure.

www.pulsesecure.net

Data Protection Day: Cybersecurity and
compliance in an uncertain climate

This year's Data Protection Day provided the opportunity to raise awareness of what rights individuals have relating to personal data and privacy but are these rights being respected?

Over 2.5 quintillion bytes of data are created each day which will only continue to accelerate as new formats are being produced at a rapid pace. With this comes the ever-looming worry of privacy protection and just exactly how much information is being shared. Data Protection Day was the start of a challenging year for businesses, at a time of political and economic uncertainty, the opportunity for cyber-attack increases dramatically. This means that organisations must recognise that they face a growing number of sophisticated attacks, many of which will generate breaches that could result in a number of consequences ranging from regulatory action to class action lawsuits.

One may question if it is actually necessary to have a Data Protection Day in 2019 to which Colin Truran, Principal Technology Strategist, Quest answers: "We should ask ourselves, is an arbitrary day to simply raise awareness of data privacy really necessary in 2019? In the eras of GDPR, multi-million-dollar lawsuits and career-ending data breaches, awareness of data privacy is higher than ever. It may sound like a cliché, but every single day of the year should be a day for businesses and individuals to do more to protect personal data."

2018 saw more than double the number of data breaches of 2017, clearly demonstrating how important it is that businesses implement effective cybersecurity and data privacy strategies to mitigate the threat. Furthermore, with new legislation now in force, such as GDPR and PECR, companies risk severe financial penalties in addition to reputational cost if they are deemed to be non-compliant.

In the current climate of Brexit induced uncertainty, organisations should be taking both strategic and tactical steps to improve cybersecurity at all levels inside the organisation to a level commensurate with the heightened exposure to cyber risk which they currently have. A cyber resilience strategy with defence in depth is now a fundamental part of any organisation's approach to operational activity.

The recent example of Google's GDPR fine just a week before Data Protection Day clearly shows how the regulators are now starting to take action against companies that are deemed to be non-compliant. The record €50 million fine – issued to Google for lack of transparency, inadequate information and lack of valid consent regarding ads personalisation – makes Google the fifth organisation to be issued with a GDPR fine across Europe.

However, whilst a handful of other organisations have received penalties for GDPR breaches, the Google example is certainly the largest in terms of the financial penalty. Clearly, the size of the fine reflected the fact that Google is a major player in the online world, with a revenue stream to show, but also demonstrates how severe the penalties can be for not complying with the regulations.

This high-profile example is one reason why organisations must step up their compliance efforts because it is clear that regulators are paying attention and the potential penalties are substantial. Moreover, organisations should not presume that an effective cybersecurity strategy means they are also GDPR compliant or unlikely to face investigation. Google did not suffer a breach but by not complying with the law, it was hit with a significant GDPR fine.

For an organisation looking to increase their compliance efforts, it's more than just how you deal with consent. It's to do with the extent to which you have assessed risk correctly, identified appropriate controls and can demonstrate evidence that hose controls are working through ongoing audits.

Eight months after GDPR became law, one thing for certain is that we will see further investigations and fines being handed out to prominent brands, so all businesses need to get compliant now and demonstrate continuing efforts towards compliance.

Data Protection Day shines a spotlight on the need to protect the privacy and security of our data across the world and is a timely reminder for businesses to make sure they are fully prepared and compliant, by deploying robust technology and ensuring established processes are in place.

www.securitybuyer.com
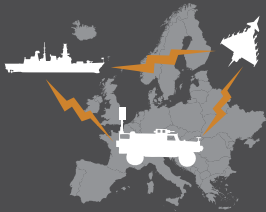
ASSOCIATION of OLD CROWS

Electronic Warfare Europe

13-15 May 2019
Stockholmsmässan, Sweden

Register online today

Unifying Electromagnetic Warfare in a Complex World – Together

In 2019, join us and connect with

- **70+** Sponsors & Exhibitors
- **45+** Countries Represented
- **2** Conference Streams
- **1,100+** Attendees

Get in touch

W: www.eweurope.com
E: eweurope@clarionevents.com
T: +44 (0) 20 7384 8246

Enquire about exhibition and sponsorship opportunities

Crown Copyright (2018)

Produced by	Headline partner	Event partner	Intelligence workshop sponsor	Gold sponsor
ASSOCIATION of OLD CROWS	SAAB	LEONARDO	PLATH	HENSOLDT Detect and Protect.

THE FONTENAY protects its guests
with Dallmeier video solution

The best is just good enough: Hamburg's new luxury hotel
THE FONTENAY relies on video security technology from Dallmeier

The completion of THE FONTENAY has enriched Hamburg with what is described as a timelessly modern, luxury class hotel. Standing directly on the shores of the Outer Alster lake, this "modern classic" succeeds in creating a remarkable blend of urban nature and cosmopolitan lifestyle. The hotel sets new standards not only in respect of its architecture and interior, but also in terms of guest protection and building security. For the latter aspect, the hotel relies on an innovative solution from Dallmeier.

The foundation stone was laid for the hotel in the spectacular Hamburg Alsterpark in August 2014. The ceremony took place on the property of its former owner, the man after whom the hotel is named: ship broker John Fontenay. After a construction period of about three-and-a-half years, the new five-star Superior Luxury Hotel with 130 rooms and suites finally opened in March 2018.

The striking architecture of the THE FONTENAY was designed by star Hamburg architect Jan Störmer. The basic layout of the hotel consists of three merged circles, so that no wall in the building runs parallel to another. It therefore goes without saying that a hotel of such distinctive form must also have a custom-designed security solution.

Naturally, the planning partner also has a critical part to play in implementing precisely this requirement. The choice was ultimately made for Dallmeier, and Dallmeier subsidiary DEKOM Video Security & Network GmbH (DEKOM) was tasked with management of the project – since its main offices are in Hamburg it is ideally positioned to ensure the requisite technical expertise and quality.

The first planning meetings were held as early as 2015, at which the customer laid out its strict specifications: Accordingly, the highest degree of security must be afforded without giving the guests occasion to feel importuned or under observation, and without detracting from the architecture. For example, visitors should be able to enjoy unrestricted views of the imposing, 27m high circular atrium and its 7m long light sculpture. Another important consideration was that the video security system should be sustainable into the future. The hotel also insisted that the solution should conform to data protection requirements.

"The entirely justified wish on the part of the customer to ensure security for all areas with video security technology often conflicts with the demands of data protection," explains Wolfgang Haack, Managing Director of DEKOM. "Our objective was to reconcile these concerns."

Based on the specifications, it quickly became clear that security must be assured for the expanses of the hotel using the smallest possible number of cameras. This meant that only ultra-HD cameras could be considered so that the entire video security system could be kept discreet and unobtrusive. For system planning purposes, this approach in turn entailed the use of appropriate network components and in particular of powerful servers for recording. The Dallmeier systems are capable of storing these enormous quantities of data and backing them up redundantly – also for prolonged periods of time.

"Given the large quantities of sensitive data, it became clear very early that in this project data protection and data security must be considered very carefully," says DEKOM Project Manager Kai Gebhardt. "The combined data protection and data security module from Dallmeier guarantees secure operation and helps the customer to comply with all requirements of the GDPR."

In order to provide rapid orientation for the hotel staff in the new video security system, a team from DEKOM was deployed to the site and instructed the hotel security personnel thoroughly in the system and the management software. These individuals were also very impressed by the ease of use of the overall system.

THE FONTENAY not only represents the creation of a luxury hotel in which urbanity, nature and modern living are blended in one distinctive, exceptional style, at the same time it ensures that its guests can enjoy their stay undisturbed and in safety.

www.dallmeier.com
www.panomera.com
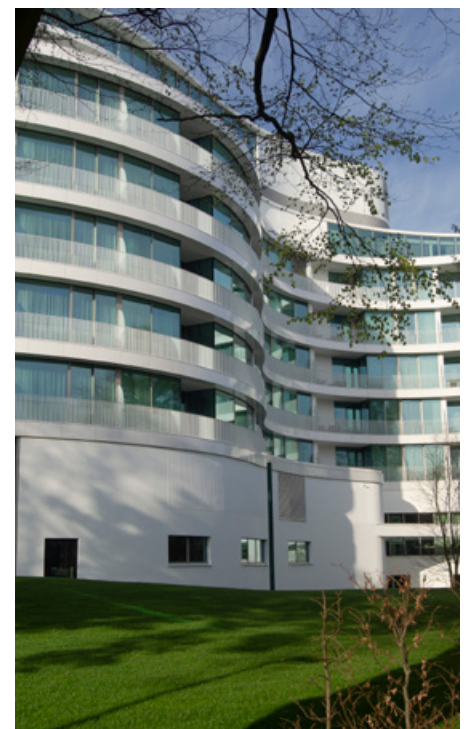
Nortech parking systems still the
best choice for top boutique hotel

With the latest specification of the Nortech FeeMaster system installed, the hotel staff can control any misuse of the car park and ensure there are enough parking spaces available

Access control system specialist Nortech has recently seen a luxury hotel in Bath update its car park by replacing its existing Nortech FeeMaster system with the latest specification.

Nortech's FeeMaster range was installed by access control system experts APT Security Systems, which is currently updating its past application of the FeeMaster system, so that staff can continue to monitor use of the hotel's car park.

APT Security Systems is the leading provider of vehicle access control and traffic management systems in the UK. Using its experience in designing and delivering practical and cost effective solutions, APT installed the updated system which includes the FeeMaster Smart Entry Station, FeeMaster Smart Exit Station and a FeeMaster Smart Console for inside the building. The console allows the staff to control any misuse of the car park and ensures that there are enough parking spaces for its guests.

Mary Lynskey, Operations Manager at APT Security Systems commented, "Nortech's systems have been used on our projects for a number of years and as with this hotel we are currently updating the equipment at these sites to the latest versions. We have worked with Nortech for more than 20 years and are very pleased with its equipment."

She continued, "The FeeMaster range has always worked well for the hotel and they were happy to renew the system as it's the right fit for their business. The client likes how the products work and we will always recommend Nortech to others looking to upgrade their car parking systems."

Nortech's FeeMaster Smart parking management system is a flexible, simple and cost-effective way of managing car parking access and controlling validity periods using Mifare smart cards. This avoids the need for expensive cabling between components and minimises disruption.

The FeeMaster entry station is designed o be used to record the date and time that a vehicle enters a car park. Located at the entrance of the car park, it issues tickets to visitors as they arrive, with each ticket containing a barcode, serial number and the date and time. Dispensing the ticket triggers an 'open' signal to the entry barrier.

The ticket is then taken to the hotel's reception desk where the date and time is used in conjunction with the FeeMaster Smart Console.

The FeeMaster Smart exit station prevents unauthorised vehicles leaving a car park or entering restricted areas. Located at the exit of the car park or the entrance to a restricted area, it validates the Mifare smart cards and exit tokens.

The exit station is equipped with a barcode scanner to read exit tokens issued by the FeeMaster Smart console, as well as entry tickets issued at the entry station. Each ticket is valid for single use at the exit station during the validity period assigned to it. The exit station controller checks the details on the barcode ticket and sends an 'open' signal to the barrier.

The FeeMaster Smart Console is a compact and easy-to-install device that reads barcode tickets issued at the entry station, calculates the fees based on pre-programmed tariff details, and encodes reusable Mifare access control cards with validity data. If necessary, the console can print customer receipts and/or barcode exit tokens. It can also control a till drawer and can optionally provide a relay output signal which can be used by third equipment i.e. barrier control whenever a card has been encoded or an exit ticket printed.

The console may also be connected to a PC so that transactions can be analysed and additional tariff management features may be used.

Nortech has supplied products and solutions to the security industry for over 25 years as an independent British company. The company uses extensive experience and expertise to create new security products to fit their clients' needs and designs everything with the customer in mind.

www.nortechcontrol.com

Protecting Super Bowl LIII
in Atlanta, Georgia

With the Super Bowl being one of the biggest sporting events of the year, security measures from law enforcement officials, surveillance and software solutions were the top priority

The Super Bowl is widely recognised as one of the most viewed sporting events in American culture and this year's event saw close to a million people in attendance over Super Bowl LIII weekend, in Atlanta Georgia. With this number of attendees and the world watching the New England Patriots against the Los Angeles Rams, law enforcement officials knew they couldn't afford to skip on any detail. The men and women at the Atlanta Police Department were working around the clock to ensure the safety of the fans. Around 75 to 100 officers and agents were manning the City's Joint Operations Centre, keeping a watchful eye on all Super Bowl activities.

Atlanta is no stranger to hosting large-scale events, which includes a previous Super Bowl, and has invested in a multitude of surveillance, analytic, data fusion and communications systems and technologies in recent years. The city has also established an innovative public-private partnership, known as Operation Shield, that effectively leverages the surveillance assets and infrastructure of other participating Atlanta metro area departments and agencies, including the City's Metro Atlanta Rail and Transit Authority (MARTA) and Hartsfield Jackson International Airport, as well as the City's business community, while also bridging communication gaps between and across them.

With 15 official event sites where teams and fans gathered throughout the week, securing Super Bowl LIII was an around the clock job involving 40 different agencies including the Department of Homeland Security. "Protecting the Super Bowl was no small task," states Kirstjen Nielsen, Secretary of the Department of Homeland Security. "I wanted to make clear that despite the lapse in funding DHS employees are and have been committed to keeping our nation and Super Bowl LIII secure. A great deal of work went in to reducing risk and vulnerabilities from any sort of incident. But as we continue to stress to our partners around the country, being prepared if an incident does occur is just as important."

Other key agencies involved in security for the event included the FBI, the Secret Service and the Federal Emergency Management Agency on the federal side, the Georgia Bureau of Investigation, Georgia State Patrol, Georgia World Congress Centre Authority Police and the Georgia Emergency Management Agency on the state side as well as the Fulton County Sheriff's Office, Atlanta Fire Rescue and Grady EMS on the local side.

Drone Concerns

Just two days before the game began, the sky above the stadium was being inundated with an alarming number of drones, despite a temporary flying restriction that prohibits their operation within the Super Bowl LIII footprint.

Officers had to confiscate half-a-dozen drones that were flown near the stadium. Law enforcement agencies were concerned a drone would crash and cause injury to spectators, collide with aircraft or be used to launch a terror attack. According to FBI spokesman, Kevin Rowson, the case was referred to federal prosecutors for possible charges and/or jail time.

"Law enforcement is spending way too much time on drones, when those resources could be used for other security," notes Rowson. "When we look up into the air and see a drone flying in the air, we have no idea if it's friendly, or if it's someone who has nefarious plans and it's weaponised."

Following the Super Bowl LIII, multiple helicopters were seen patrolling the air space above the stadium and surrounding area, often swooping below the tops of Atlanta's downtown buildings as part of a massive security operation. With the hundreds of flights being cancelled at

Gatwick Airport in London last December, the patrolling of drones is becoming an on-going issue for law enforcement officials.

Software and surveillance

CNL Software's PSIM technology was used to support a multi-agency security programme for the event. The company's IPSecurityCentre PSIM solution is installed in the Atlanta Police Department's Video Integration Centre (VIC) and helps secure the city and surrounding metro area, keep the metro area's transportation networks and systems safe, and to help law enforcement personnel make sense of the huge volume of video intelligence that is generated day-to-day and during large-scale events like the Super Bowl.

IPSecurityCentre from CNL Software integrates these disparate systems in the Atlanta Police Department's VIC to provide law enforcement and other public safety professionals with the data and video intelligence they need to effectively respond to incidents before they arrive on scene. "Estimates are that nearly one million people travelled to Atlanta for Super Bowl Week," comments Mike Mostow, General Manager – Americas at CNL Software. "As with all major events, ensuring public safety and security is a big job and huge concern. IPSecurityCentre was installed in the VIC by the Atlanta Police Department to provide the real-time situational awareness and decision

support they need to ensure public safety and security during large-scale special security events like Super Bowl LIII." IPSecurityCentre PSIM has been installed in some of the largest public safety and security programmes in some of the world's largest cities. The platform enables the most intelligent integration of the widest range of disparate public safety, security, emergency management, and homeland defence system and sensor technologies, including video and video analytics, facial recognition, license plate recognition, crowd size monitoring, gunshot detection, chemical, biological, radiological/nuclear and explosives detection, geospatial mapping and asset tracking.

In addition, the Mobile Advanced Security Tower – MAST for short – was deployed at the Super Bowl as part of the event's surveillance operations. The Security Centre is based in Cayman but also has a US headquarters in Chattanooga, Tennessee. The Tennessee branch of the company was awarded the contract to work at the Super Bowl, and 10 MAST towers were deployed to help in the overall security and monitoring effort.

"We kind of looked at the existing andscape for mobile video surveillance," recalls Stuart Bostock, President of The Security Centre. "Most of the existing systems were trailered and weren't aesthetically pleasing. They were very easily tampered with. They could be stolen."

Bostock said that the MAST alleviates a lot of the problems with mobile video surveillance technology. They can be set up in 30 to 40 minutes, and they operate on solar power. The vertical height of the tower also makes them difficult to tamper with from the ground. Bostock also added that once the security towers are installed, they can operate in two different modes. One allows the data feed to be pushed to an external command centre and another allows the operators of the feed to control the cameras and break down the data themselves.

In one case, said Bostock, the MAST cameras were able to focus 1.2 miles into the distance from the hub, and in another, they helped prevent a vehicle theft at the Super Bowl. The MAST can be deployed at construction sites or large development sites, and it can be used to provide security at night and also for time-lapse photography at a site. "The applications are endless in terms of where we put them," states Bostock. "Anywhere that eyes are needed on the ground."

CriticalArc now used at 30% of **Australian universities**

Three high-profile Australian universities have rolled-out SafeZone protection for students and staff As a new wave of adoptions reflects growingconcern to improve safety and security

A trio of leading Australian universities have announced that they are introducing SafeZone technology from CriticalArc in a drive to improve safety, increase their security teams' capabilities and provide better care for students and staff. With 30% of Australian universities now using SafeZone, the manufacturer believes that this latest wave of roll-outs confirms CriticalArc's position as "the most comprehensive safety and security management solution provider in the Australian market".

Adding to CriticalArc's growing network of customers are the University of Tasmania (UTAS), the University of Southern Queensland (USQ) and the University of the Sunshine Coast (USC). Combined, these establishments have more than 75,000 students and staff working in 33 campuses and associated facilities across four States. This means that SafeZone now serves the needs of 1.5 million students and staff at more than 500 locations across the world.

"UTAS, USQ and USC each have their own unique character and particular priorities but ensuring the best standards of care for students and staff is top of the list for all of them," says Robert Christie, CriticalArc's Customer Success Manager, Asia Pacific. "Preventing crime, managing public safety and handling emergencies are still the top concerns of university security teams, yet SafeZone is also enabling those teams do much more to address issues that are increasingly important. From improving support around mental well-being to tackling sexual harassment and making campuses inclusive environments where everyone can feel safe and welcome, security and response teams are playing a much bigger role than they traditionally did. SafeZone is a key tool in enabling campus

security to be more effective, more relevant and more approachable."

SafeZone puts individuals directly in touch with response teams at universities, hospitals, government departments and similar large organisations. This makes it easy for students or staff to use their mobile phones to request help, trigger an emergency response, receive rapid notifications in the event of emergencies and benefit from a wide range of customer-care services.
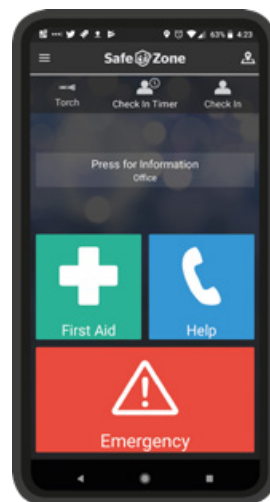
The technology also lets students and staff share their situation with response team members by checking-in when working alone outside hours or in higher-risk environments such as laboratories and workshops.

Further to this, with the ability to 'geo-fence' any location, each of the universities' security teams can now monitor care and safety of users wherever they are –including those working out-of-hours on campus, those travelling between campuses locally or on field projects, or travelling overseas for study or research placements.

With its global reach combined with its ability to precisely locate vulnerable individuals, SafeZone is helping universities around the world to better meet their duty of care obligations, says Darren Chalmers-Stevens, CriticalArc, Managing Director. "SafeZone offers all the functions that university teams want, in one easy package. It is not only helping them to deliver better care, it is letting them demonstrate this fact in an accountable way."

www.criticalarc.com

3xLOGIC improves video
surveillance capabilities KSBA

Video and audio verification plus glass break technology provide the educational organisation with what has been described as greatly improved images and priceless peace of mind

The Kentucky School Boards Association (KSBA) has recently-upgraded to a 3xLOGIC video surveillance system, installed and monitored by Sonitrol of Lexington. KSBA has been a Sonitrol of Lexington customer for around 25 years. Hence, Sonitrol and Danny Goodpaster, Security Consultant, were well positioned to understand the organisation's situation and recommend the solution best suited for its needs.

"About three years ago, during the budgeting process, we had an incident in our parking lot in which there was a minor fender bender," recalls Jeff Million, Print Shop and Operations Manager for KSBA. "The camera watching the parking lot was only 30 feet away, but I could not even make out identifying writing on the car that struck the other car. On another occasion, we had a break-in and from three feet away I could not make a positive ID on the perpetrator. After these incidents, things got rolling and we soon embarked on upgrading our video surveillance capabilities."

Goodpaster wrote the first upgrade proposal in 2016. After some discussion about installing a hybrid DVR, KSBA at Goodpaster's urging decided to remove the analogue cameras and go full IP. Now, the organisation has four static cameras and two 3xLOGIC Multi-sensor devices, trained on the front door and the back door, loading dock and parking lot. The Multi-sensor device is a camera with a unique set of capabilities, it is also equipped with impact-activated audio, glass break, and motion detection along with video and audio verification of alarm activations.

The Multi-sensors are connected to an updated Sonitrol panel and they provide video feeds, as well as glass break and audio verification for both entrances. "With our former system, I'd get the first call on alarm, but often I did not have enough video information to make an informed decision," explains Million. "Now, I have the data and the images I need to deal quickly with any situation."

Goodpaster recalled that there was a lot of competition for this business and that "KSBA really did their homework". At the end of the day, it was the Multi-sensor's video and audio verification that provided KSBA with real, tangible benefits it could feel. Further, between the Sonitrol app and VIGIL Client software installed on Million's laptop, KSBA now has a fully-integrated solution, as opposed to the two separate systems it had before. The four non-monitored cameras are overseen by 3xLOGIC VIGIL Central Management software (VCM), so if any equipment issues arise, Sonitrol knows immediately and can act to proactively solve them.

As noted earlier, the Multi-sensor devices monitor the front and back entrances, as well as the parking lot. The other four 3xLOGIC cameras are trained on the front door reception area and down the hallways away from the front and back entrances, to provide visibility on where any visitor or employee is going. These cameras are viewed live and used for incident review. The receptionist at the front desk has a dual screen that shows her the approach to the building and who is coming through the door before that person reaches her desk. This creates full situational awareness and keeps the receptionist safe.

"We really do like our new cameras, and we are light years ahead of where we were as far as quality and ease of use with the 3xLOGIC system," reflects Million. "We now have video verification capabilities. Before I'd get a phone call, while away from the office, providing video images but I couldn't make anything out. I'd have to head home to view the video and I still didn't have sufficient resolution to make out what was happening. The new cameras also provide a better field of view, I'm picking up my entire parking lot, before I could only see half of it.

"Recently, we had a forced entry attempt on the front door, and we went to the video," Million continues. "We could immediately resolve what had happened – that's real peace of mind. We have to make quick decisions, and in the event of a real incident, we're shaving at least 10 minutes off police response times. We don't want to call on false alarms, we want to make certain. Now we can and the video quality is about 10 times better."

www.3xlogic.com

Blighter's e-scan radar selected by
Dat-Con Defence for Indian Border pilot

Dat-Con Defence has deployed the Blighter B400 series radar as part of a pilot of the Indian Government's Comprehensive Integrated Border Management System (CIBMS)

Blighter Surveillance Systems Ltd, a British designer and manufacturer of electronic-scanning (e-scan) radars and surveillance solutions, is supplying its Blighter B400 series e-scan micro Doppler ground surveillance radar to Dat-Con Defence for deployment along the Indian border.

The Blighter radar was supplied to and deployed by Dat-Con Defence during 2018 as part of the Indian Government's Comprehensive Integrated Border Management System (CIBMS). CIBMS is designed to establish a multi-tier security ring – ground surveillance radar, thermal cameras, unattended ground sensors, seismic vibration systems, fences and fence protection systems – to protect the country's long international borders.

Dat-Con has integrated the Blighter radar, cameras and other sensors into its own command and control (C2) system. Sensor information from its C2 system is integrated with the CIBMS system to alert quick response teams (QRTs) of the Indian Border Security Force for action. Dat-Con has partnered with in-country Pune-based Ador

Powertron for this pilot project.
"The Blighter B400 micro Doppler radar is best-in-class as was demonstrated when it outperformed all the other radars in an Indian Government-sponsored trial," revealed Stane Plaskan, CEO of Dat-Con Defence. "Also, we know that this radar is highly effective in difficult terrains – such as mountains, plains and coastal areas, as it has been deployed for many years now along the 250km Korean DMZ, in what is considered one of the world's most mountainous countries with environmental extremes of -30°C in winter and a humid +40°C in summer."

The Blighter radar's wide elevation beam was reportedly a key feature for the Indian CIBMS project as it ensures that the radar can operate effectively in all terrains allowing the hills, mountains, plains, riverine territories and marshes to be scanned simultaneously, without the need to tilt the radar. The wide beam also provides detection of low flying manned and unmanned aerial vehicles (UAVs) and drones.

The solid-state passive electronically scanned array (PESA) radar has been

designed to detect small and slow-moving targets, even in cluttered environments, due to the radar's coactive frequency modulated continuous wave (FMCW) micro Doppler fast-scan processing. The radar delivers a 24x7x365 all-weather persistent surveillance capability. It can detect and track a walking person at 11km (6.8 miles), a crawler at 4.6km (2.9 miles) or a large moving vehicle at 25km (15.5 miles) and then cue a camera system to follow and identify targets.

"This is our second contract win for pilot projects linked to the Indian border security CIBMS initiative – further proof of the quality of our ultra-reliable, zero-maintenance Blighter B400 series radar," states Mark Radford, CEO, Blighter Surveillance Systems.

Blighter Surveillance Systems has now sold hundreds of its e-scan ground surveillance radars across 35 different countries. It has systems deployed along the Korean demilitarised zone (DMZ), on the US Southern border, in several Middle Eastern countries, and now in India too.

Blighter Surveillance Systems delivers an integrated multi-sensor package to system integrators comprising the Blighter radars plus cameras, thermal imagers, trackers and software solutions. Its ITAR-free systems are used worldwide in commercial, government and defence markets in area and asset protection for national border security, homeland security, critical infrastructure protection such as oil and gas facilities, coastal surveillance, and in military applications.

www.blighter.com

What can visitors expect from
The Security Event?

Aiming to be the must-visit commercial and residential security exhibition, The Security Event will bring together education, market leaders and industry experts to Birmingham

The Security Event is a major new exhibition created for the commercial and residential security market. Taking place from April 9 to 11 2019 at The NEC Birmingham, the event brings together a world-class education programme, market leaders and industry experts, to make it what the organiser calls the most hotly anticipated exhibition for UK security professionals in 2019.

Hosted by Western Business Exhibitions (WBE), part of Nineteen Group and powered by Security Essen, The Security Event offers the opportunity for direct engagement across the supply chain, by bringing together the best and brightest the industry has to offer.

An event designed by the industry, for the industry

The Security Event has been developed with support from a key group of the industry's major players, to deliver a world-class exhibition dedicated to UK security professionals, installers and integrators. The Security Event is proud to have support of its 10 founding partners – Anixter, ASSA ABLOY, Avigilon, Comelit, Dahua, Honeywell, TDSi, Texecom, Tyco and Videcon. This level of involvement ensures the exhibition covers the latest trends and innovations whilst addressing the evolving challenges facing the industry today.

The event has already created a buzz within the industry. "We believe The Security Event is exactly what the UK security industry needs and are excited to come on board as a founding partner," says Gareth Ellams, Group Sales Director at ASSA ABLOY. "At ASSA ABLOY, we are looking forward to the opportunity to engage directly with security professionals as well as end users, to present our industry-leading solutions."

"Comelit are extremely excited to become a founding partner of The Security Event 2019," adds Francesca Boeris, Managing Director of Comelit. "The events concept and UK focus aligns perfectly with Comelit's aims moving forwards. We look forward to showcasing Comelit's constant innovation and friendly technology to the UK Security Market at the NEC in 2019."

"Honeywell Security is delighted to be joining The Security Event as a founding partner," notes Mick Goodfellow, GM Honeywell Security EMEA. "This event provides an excellent opportunity to showcase our leading-edge security portfolio and in a location that allows us to enhance our relationships with our installer base."

A tailored seminar programme

The highly focused programme investigates the evolving challenges and opportunities involved in the delivery of security projects throughout the supply chain. The Security Event will tap into the expertise of leading security professionals and explore the latest innovations from suppliers. Visitors will have the opportunity to participate in a broad but relevant programme of presentations and seminars which will offer insights and ideas on the latest solutions available for any type and size of project.

The Security Event will welcome high-profile speakers such as Professor of Criminology, Martin Gill and Philip Ingram MBE former Senior Intelligence and Security Officer. Gill will be chairing a Keynote Panel offering insights direct from research on the trends impacting security installers and integrators, conducted on behalf of The Security Event. The session aims to explore the ongoing challenges within the security sector, how these are perceived, their impacts and in what ways might this

determine who thrives and who does not.

Addressing the ever-growing cyber threats organisations now face, Ingram will chair a panel entitled Convergence: The challenges for installers and integrators in the increasingly cyber enabled age covering important restrictions, threats and ultimately considerations which virtual platforms present to the security industry.

Throughout the three-day event, The Security Event's Innovation Theatre will feature presentations from some innovative manufacturers on the cutting edge of their field, covering topics such as CCTV, access control, integration platforms, automation, intelligent locking systems. In addition to their exhibition presence, all 10 founding partners will be welcomed into the Innovation Theatre, hosting seminars on a broad range of current, relevant topics to industry.

Seminars highlights from our founding partners include: The door was open…: a look at the cyber gaps in your building systems by Tyco; Using digital services to add value to intruder alarms from Texecom; TDSi will discuss Deliver Business Efficiencies by deploying innovative integrated security systems; The revolution created by Cloud based security management will be presented by Honeywell Security & Fire; while Using technology and AI innovations to improve local public services is a scheduled talk from Dahua.

A range of sessions covering vital industry updates, standards, regulations and

business advice from leading bodies including ASIS, The Security Institute, SSAIB and the FSA will also be presented in the Security in Practice Theatre, available for all visitors as part of their free admission.

Giving you more for less

The Security Event recognises it can be costly for security professionals to take a day out of their schedule to attend an exhibition. That's why The Security Event is providing free parking for visitors at the NEC. Once more, there's no need to rush off – as part of the free registration, visitors can enjoy a drink or two on the organiser straight after closing time at the on-site bar.

Location, location, location

The NEC Birmingham provides The Security Event with the most accessible exhibition venue in the UK. Its location is described by the organiser as perfect for visitors and exhibitors arriving from across the country and further afield. With an international airport, mainline train station, easy access to the UK's motorway network and over 16,500 car parking spaces, the NEC is the number one option for both exhibitors and visitors alike arriving from all directions.

Even more value from your visit with co-located events

The Security Event is co-located at the NEC Birmingham alongside three other highly successful and established exhibitions from the WBE portfolio: The Fire

Safety Event, The Health & Safety Event and The Facilities Event. This enables security professionals to get the most of their visit, by investigating integrated security solutions and networking with these closely related industries, to gain a wider picture of the services and technologies on offer as part of their free registration for The Security Event.

One Industry. Two Unique Audiences. The best of both worlds.

The acquisition of WBE by Nineteen Group at the end of November 2018 creates an unrivalled exhibition portfolio for the UK security market, with two complementary security events focused on two unique audiences. With International Security Expo focused on serving Government and End Users, The Security Event is placed to deliver the UK's number one channel focused event for the UK commercial and residential security market.

Tristan Norman, Event Director of The Security Event sums up why the security industry should be excited: "It is not often that the security sector gets to experience a brand-new event of this type and size. There has clearly been demand for a fresh event and we are enjoying tremendous support from the security community since announcing it. We believe this is a 'must see' event for anyone and everyone in the UK security industry and are excited to welcome visitors and exhibitors to Birmingham in the Spring."

www.thesecurityevent.co.uk

Intersec 2019 brings the world's
security industry to Dubai

With its diverse floor plan comprising security, fire and safety companies from around the world, the 21st edition of Intersec helped to focus minds on the year ahead

Every January, the global security industry heads to Dubai for three days of technology demonstrations, industry education and networking at Intersec. The 21st edition of the show once again succeeded in attracting a high-level audience with the vast majority of exhibitors happy with the conversations they were having.

The event featured 1,212 exhibitors from 54 countries spread over the 60,000m2. Security made up a considerable proportion of this number with Commercial Security (375 exhibitors), Information Security (120 exhibitors), Homeland Security & Policing (90 exhibitors) and Physical and Perimeter Security (54 exhibitors) all forming major elements of the event.

Nearly two-thirds of the world's top 50 security manufacturers took space at Intersec 2019, including 17 of the top 20 incumbents. This comprised the likes of Hikvision, Dahua, ASSA ABLOY, Bosch Security Systems, Axis Communications, FLIR Systems, Hanwha Techwin, Tiandy Technologies, Avigilon, Infinova, Optex, VIVOTEK, CP Plus, Nedap, Raysharp, Milestone Systems, and Kedacom.

All of these exhibitors showcased their latest solutions, from Artificial Intelligence (AI)-based safe city services and smart home security products, to the latest high definition IP-Network cameras and analytics software used across industry verticals from banking and retail to hospitality and oil and gas.

One of the regular comments made by exhibitors covered how important the Middle East was as a region. "This is an important show for us because this region really values what Flir has to offer," said Frederik


Wallberg from Flir. "Our equipment is not the least expensive on the market but perform at the best rate. This region and a lot of the installations that we have in this area value reliability and performance over the price war that we are seeing in other regions."

"The show attracts visitors not only from the Emirates but also from other Gulf countries as well as countries in Africa and Europe, which is fantastic," agreed Jaroslav Barton from Vanderbilt. "I think it really belongs amongst the best security shows in the world."

"This is a great show," stated Avigilon's Paul Such. "It gives us the chance to reach our EMEA customers and international customers and to show them the products. This is what we class as a tier one show and we get great return on investment from it.

"Intersec Dubai is not only for the Emirates, it's also a very international show where we have a lot of people from a lot of countries around the Middle East and Africa," added Christian Ringler from Milestone. "We meet with our partners and with potential customers and ensure that we
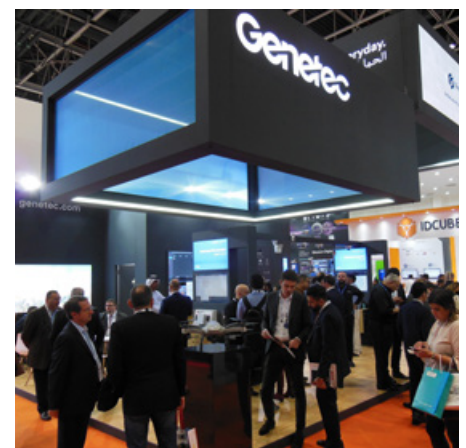
Dubai Police is one of Intersec's key government partners

are delivering the right messages and to demonstrate that our platform is the right solution in order to secure our customers premises with our technology partners."

Another key word that was mentioned across the show floor was quality, with both the level of booth design and the visitors coming in for particular praise. "I had some fantastic customers from all the regions we want them from, and it has been busy, busy with quality," observed Craig Kennedy from KBC Networks.

"It's been insanely busy with really good quality people," agreed Pelco's Stuart Rawling. "It's been really strong this year, Messe Frankfurt do a good job and this year it's been great for us."

Importantly, the event also succeeded in providing a strong platform for business discussions. "I think this is one of the most relevant events that we see because there are very few events that focus on AV security and surveillance," says Mohammad Meraj from Ring. "We think having our presence is very relevant and we are seeing a lot of traction from customers, resellers and partners who really love what we are doing."

"It's been a very positive result for us," stated Vanderbilt's David Sullivan. "We have people coming in and very interested in learning more about

> "INTERSEC DUBAI IS NOT ONLY FOR THE EMIRATES, IT'S ALSO A VERY INTERNATIONAL SHOW WHERE WE HAVE A LOT OF PEOPLE FROM A LOT OF COUNTRIES AROUND THE MIDDLE EAST AND AFRICA."

Vanderbilt products and so it's a very productive show for us."

"We've seen a lot of potential clients, a lot of existing clients that are coming here to celebrate the success of their previous projects with us," revealed Ali Al-Sohaini from Frontier Pitts. "It's a good place to find out about existing and upcoming projects and clients and it's nice to see British manufacturing as popular as ever."

"We had a good show," reflected Fadi Kanafani from NetApp. "We saw customers and partners, and we had new relationships established as well, so it is very interesting. These events are really a good platform for us to allow us to touch as many customers as we possibly can but also invite our install base to come and see some new initiatives that we are doing."

Away from the products on display, education played a vital role at the show. The launch of the three-day Intersec Future Security Summit, where Future Foresight on Security, Artificial Intelligence, along with the Internet of Things (IoT) and Intelligent Systems were among the central themes.

Martin Gren, Co-Founder of Axis Communications, and the inventor of the world's first IP-Network camera, was among the headline speakers. "We see security needs increasing and new applications are enabled by new and complementing technologies. Everyone expects to see industry disruption from AI and Deep Learning, and this is an area that Axis are heavily investing in, but I think the true benefits are still several years away. Instead you will see AI help with regular basic algorithms, and personally, I think the market for audio is going to move from analogue to IP as it's still currently 98 percent analogue."

With its popular features such as the Drone Zone, an Outdoor Demo Area, and the Safety Design in Buildings Pavilion also remaining a real draw for the crowds that filled the aisles at Dubai's World Trade Centre, it is easy to see why so many people came away from the event happy.

www.intersecexpo.com

ADECS 2019 brings the Asian
defence elite to Singapore

With four events covering related disciplines taking place all under one roof, ADECS 2019 succeeded in creating a platform for the Asian defence industry to talk and learn

Singapore's position at the entrance to the South China Sea, and its political neutrality, made it the perfect venue to discuss the development of military capabilities within in the Indo Pacific region this January. Delegates and exhibitors from 43 countries gathered for two days to share challenges and solutions around four key subjects: training and simulations, maritime patrol capabilities, underwater defence technology and developments in electronic warfare.

The Electronic Warfare Conference, organised by the Association of Old Crows, welcomed Air Marshal Daljit Singh, former Director General of Air Operations with the Indian Air Force, as the keynote speaker. Air Marshal Singh gave an assessment of the various international assets operating in the region, and the challenges posed by EMI and interoperability of systems.

In the Undersea Defence Technology conference track, the discussion repeatedly focused on waterway management and the development of procedures for de-escalating unexpected encounters. Commodore Paul Hornsby of the Royal Australian Navy, Director of the Autonomous Warrior 2018 exercise, opened the floor with a look at the vital role of unmanned and autonomous vehicle operations in littoral waters. AW18 was the largest activity of its kind conducted by regional allies, and the first autonomous exercise involving all domains. Commodore Hornsby forecasted a significant growth market in autonomous military assets going forward.

The second day began with a guest speaker from the German Navy, Rear Admiral Ulrich Reineke, who outlined the German approach to conventional submarine operations and offered some thoughts on

how that framework might be adapted. He also looked at how international training in the submarine environment might be achieved, including bespoke aspects for unique regional challenges.

Of particular interest in the military training seminar was the presentation by Vice Admiral Dr Sahapong Kruapach, Advisor to the Thai Permanent Secretary of Defence, who outlined plans for future training systems capability development. Dr Kruapech compared the costs and benefits of imported versus home-grown simulators, explaining that, while in-house development was cost-prohibitive, imported systems were unable to deliver the highly tailored requirements that regional forces must deliver in their training programmes.

He was followed by Janesh Janardhanan, Consulting Director at Frost & Sullivan, who reviewed some of the latest capabilities that will shape future training and simulation development. Nano devices are having a rapidly growing impact on military tech, as are human-machine interfaces and personal HUDs. The use of these systems requires specific and detailed training around an increasingly connected battlefield. Australia has already announced plans to migrate legacy training devices to systems that can accommodate these new requirements, and more are expected to follow.

The Maritime Patrol conference track had a welcome last-minute addition in the form of First Admiral Bambang Irwanto from the Indonesian Navy, who presented Indonesia's approach to coastal and EEZ security. He listed piracy, terrorism and IUU Fishing as the three most prevalent threats to maritime security – all issues that require a unified international effort to combat. He called for a regional framework to be

developed at the policy level to enable this, with coordinated patrols and shared intelligence. As an example, he shared a recent success story from the Sulu Sea off the coast of the Philippines where the IndoMalphi Operation has led to a significant decrease in marine robbery and kidnappings.

Dr Chris Merritt, Maritime Technical Advisor to the US Mission to ASEAN, made the same point in his talk around enhancing cooperative maritime situational awareness. "The end state," he said, "is a safe and secure maritime domain that is governed by an international rules-based order." Cooperation is clearly the name of the game, but the challenges in achieving that – given different legal systems, national priorities, and military capabilities – are significant

The conversations continued outside the conference rooms, and the show floor was constantly buzzing as visitors from regional military and industry crowded round the 35 exhibitors to view the latest technological developments.

ADECS will return to Singapore in 2020, supported by a new Advisory Board of regional experts to ensure the show continues to meet the complex challenges of operating in the Asia Pacific.

www.asia-decs.com

THE MAGAZINE FOR A
CONVERGING WORLD

INTERNATIONAL BUILDING TECHNOLOGY
- A NEW PUBLICATION DEDICATED TO THE GLOBAL
SMART HOME AND CONNECTED BUILDING INDUSTRY.

INTERNATIONAL BUILDING TECHNOLOGY

SUBSCRIBE ONLINE
TO FIND OUT MORE

www.internationalbuildingtech.com

IBT

BOON EDAM

A global market leader in entry solutions
www.boonedam.co.uk

)eyevis
PERFECT VISUAL SOLUTIONS

First-Class Visual Display
Solutions for Control Rooms
www.eyevis.de

KERISYSTEMS
INCORPORATED

World leading manufacturer and supplier of
integrated access control solutions
www.kerisystems.co.uk

CEM SYSTEMS

Leading provider of access control and
integrated security management systems
www.cemsys.com

HIKVISION

One of the world's leading suppliers of video
surveillance products and solutions
www.hikvision.com

OPTEX
Sensing Innovation

Leading sensor manufacturer providing
perimeter protection, intrusion and
piggybacking detection solutions
www.optex-europe.com

dahua
TECHNOLOGY

Leading Video Surveillance Solution Provider
with IP Camera, NVR, Analog, DVR, Speed
Dome, HD-SDI and NVS
www.dahuasecurity.com

Genetec

Leading provider of IP video surveillance, access
control and license plate recognition solutions
unified in a single platform
www.genetec.com

rayTEC

Raytec are the World leader in LED
lighting for security and safety
www.rayteccctv.com

Cognitec

Cognitec develops market-leading face
recognition technology and applications
for facial image database search
www.cognitec.com

AXIS
COMMUNICATIONS

Leading manufacturer of network
cameras for the physical security
and video surveillance industries
www.axis.com/gb/en

BCDVIDEO

BCDVideo best in class IP video surveillance
systems. BCDVideo - simplicity, scalability, &
reliability for the video surveillance market
www.bcdvideo.com

KBC

Manufacturers of transmission equipment,
Fibre Optic, Wireless, IP and Encrypted
Secure Transmission
www.kbcnetworks.com

Dallmeier

P cameras, Panomera, network
cameras, security cameras, HD cameras,
DVR, NVR, software
www.dallmeier.com

MOBOTIX

MOBOTIX is known as an innovative
producer of smart and autonomous IP
cameras since the year 2000
www.mobotix.com

BOSCH
Invented for life

For security and communications
products, solutions and services, Bosch
Security Systems is the preferred partner
www.boschsecurity.com

HID
Powering Trusted Identities

We power the trusted identities of the
world's people, places & things with
solutions like access control, identity
management, asset tracking & more
www.hidglobal.com

NVIDIA

NVIDIA takes security concerns seriously and
works to quickly evaluate and address them
www.nvidia.com

Quantum.

Quantum Corporation is a manufacturer
of tape drive, tape automation, data
deduplication storage products
www.quantum.com

NOCTURNA
ILLUMINATING SECURITY

We provide hardware to security, military
& blue light industries worldwide with our
range of night vision products, providing
low light imagery
www.nocturna.co.uk

COP
Professional CCTV

The UK's premier CCTV distributor, offering
high quality CCTV products and industry
leading service & support
www.cop-eu.com

YOU'VE SEEN THE NEWS...
NOW DISCOVER THE STORY

Subscribers Know More. **Subscribers Get More.** **Subscribers Save More.**

Subscribers get **10 issues** for just **£99**

Subscription features:

s   Exclusive online content

s   Fully integrated into the industry

s   Digital & Print editions

SECURITY BUYER
FOR TODAY'S SECURITY PROFESSIONAL

Subscribe now to instantly start saving.
Call **01622 823 920** or visit **www.securitybuyer.com**

This package is a unique offer for those who see this advert. Shipping costs apply for those who are outside the UK. Full details can be found online via www.securitybuyer/subscriptionoffer

What's On?

Our latest round-up of recommended shows and exhibitions

Securika Moscow
19-22 March
Moscow, Russia
www.securika-moscow.ru/en-GB/
Securika Moscow is the largest exhibition of security and fire protection equipment and products in Russia and is an effective tool of security equipment and products promotion at the Russian market.

GISEC
1-3 April
Dubai, UAE
www.gisec.ae
With over 7,000 cyber-specific visitors and co-located with IoTX and Future Blockchain Summit, GISEC's mission is to bring the most innovative and game-changing cyber technology to each industry it covers.

The Security Event
9-11 April
Birmingham, UK
www.thesecurityevent.co.uk
This major new exhibition created for the commercial and residential security market aims to deliver a world-class exhibition dedicated to UK security professionals, installers and integrators.

ICS Cyber Security Conference
16-18 April
Singapore
www.icscybersecurity
conference.com
Industrial Control Systems (ICS) Cyber Security Conference is the longest running cybersecurity-focused conference for the sector. The event focuses on energy, utility, chemical, transportation, manufacturing and other industrial and critical-infrastructure organisations and leaders.

UDT Technology
13-15 May
Sweden
www.udt-global.com
Undersea Defence Technology brings together professionals from the military, industry and academia to focus on cutting edge technologies and developments within one of the harshest environments.

ITEC
14-16 May
Sweden
Celebrating its 30th anniversary in 2019, ITEC is an annual event held across different locations in Europe. The event presents the industry's latest innovations and provides a platform to discuss developments and exchange ideas about future requirements for military, education and simulation.

EW Europe
13-15 May
Sweden
www.eweurope.com
Electronic Warfare Europe 2019 will cover the future of EW and EM Operations in the changing light of current and emerging threats, including Hybrid Warfare, Information Operations and Cybersecurity.

The European Information Security summit 2019
Amsterdam
teissamsterdam.com
Award-winning TEISS Amsterdam 2019 will welcome 40 speakers from around the world for one day of high-level presentations, panel session, roundtables and workshops. The event will focus on key themes and challenges faced by CISOs, CIOs, CTOs and Heads of Information Security.

InfoSecurity Europe
4-6 June
London, UK
Infosecurityeurope.com
One of Europe's biggest and most-attended information security industry event, attracting more than 400 exhibitors and more than 19,500 information security professionals.

ITEC

14-16 May 2019

Stockholmsmässan, Sweden

REGISTER NOW

TRAINING AND EDUCATION TECHNOLOGIES FOR THE DEFENCE AND CIVIL PROTECTION COMMUNITIES

UK MOD © Crown copyright 2018

2,000
industry specific attendees

60+
countries represented

4
conference streams

100
exhibiting companies

80
international VIPs

For further information or to complete your registration, visit www.itec.co.uk

To discuss sponsorship and exhibition opportunities, contact us today at team@itec.co.uk

Organised by
NTSA

Organised by
CLARION EVENTS

Headline partner
SAAB

Gold Sponsor
hp

Gold Sponsor
THALES

intersec
AWARDS
2018

20 SEPTEMBER 2018 | HABTOOR PALACE, DUBAI

WINNER
Access Control
Product of the Year

Showcasing Aperio® H100:

Product of the year 2018

campaigns.assaabloyopeningsolutions.eu/aperio-h100

ASSA ABLOY

The global leader in
door opening solutions