Security Solutions Today

July / August 2018

BODY LANGUAGE

Security from your face, eyes, voice, fingerprints and emotions

Cover Focus

AI and the Quest for Improved Security

Inside Look

The Benefits and Challenges of Facial Recognition

Show Preview

ConnecTechAsia 2018 and Asia's Growing Economy

Download our new Tradecards Global App on iOS and Android to read the latest issue!

Lechange

It's Time for Lechange

Smarter Home Security

Protect your home with a smart security ecosystem that can be managed from anywhere. Lechange delivers a comprehensive series of cloud-connected home security products and solutions to keep your home safe in a variety of situations.

Lechange Products

Ranger/Ranger 1080P

Cue/Cue 1080P

Bullet

Doorbell

Scout

CE FC RoHS ISO 9001:2000

E service.global@lechange.com W www.lechange.com

Available on the App Store

GET IT ON Google play

DAHUA TECHNOLOGY SINGAPORE PTE. LTD.

Add: 62 Ubi Road 1 #06-15 Oxley Biz Hub 2
Singapore 408734
E-mail: sales.sg@global.dahuatech.com

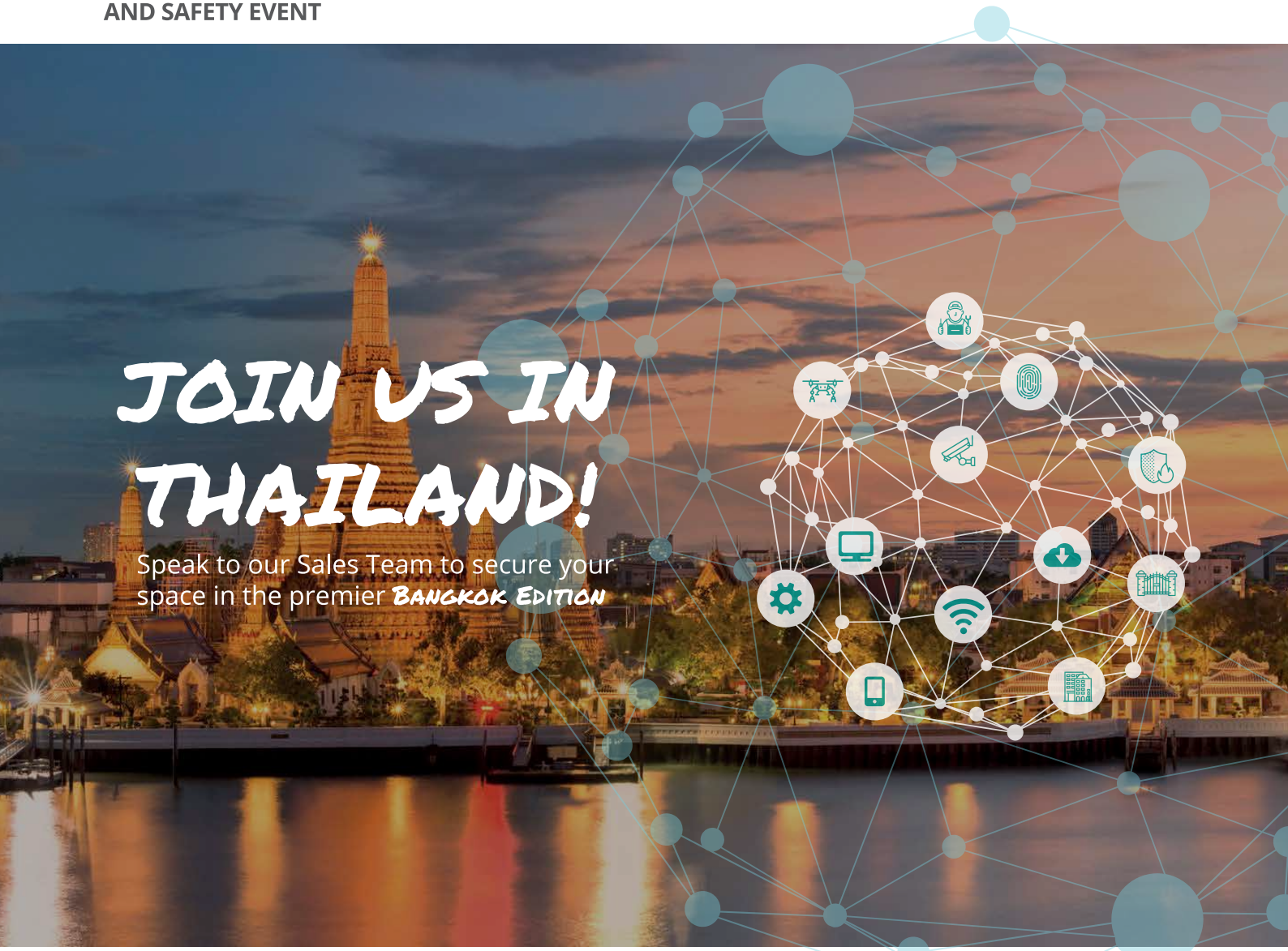
IFSEC
SOUTHEAST ASIA

25 - 27 OCTOBER 2018

IMPACT CONVENTION CENTRE, BANGKOK

SOUTHEAST ASIA'S LEADING SECURITY, FIRE AND SAFETY EVENT

CO-LOCATED WITH
POLSEC
POLICE SECURITY



CONTACT US

MR TJ TAN
PROJECT MANAGER
E: TJ.TAN@UBM.COM

MS ARIES KEE
ASSISTANT SALES MANAGER
E: ARIES.KEE@UBM.COM

MS RACHEL EATON
BRAND MANAGER
E: RACHEL.EATON@UBM.COM

SUPPORTED BY

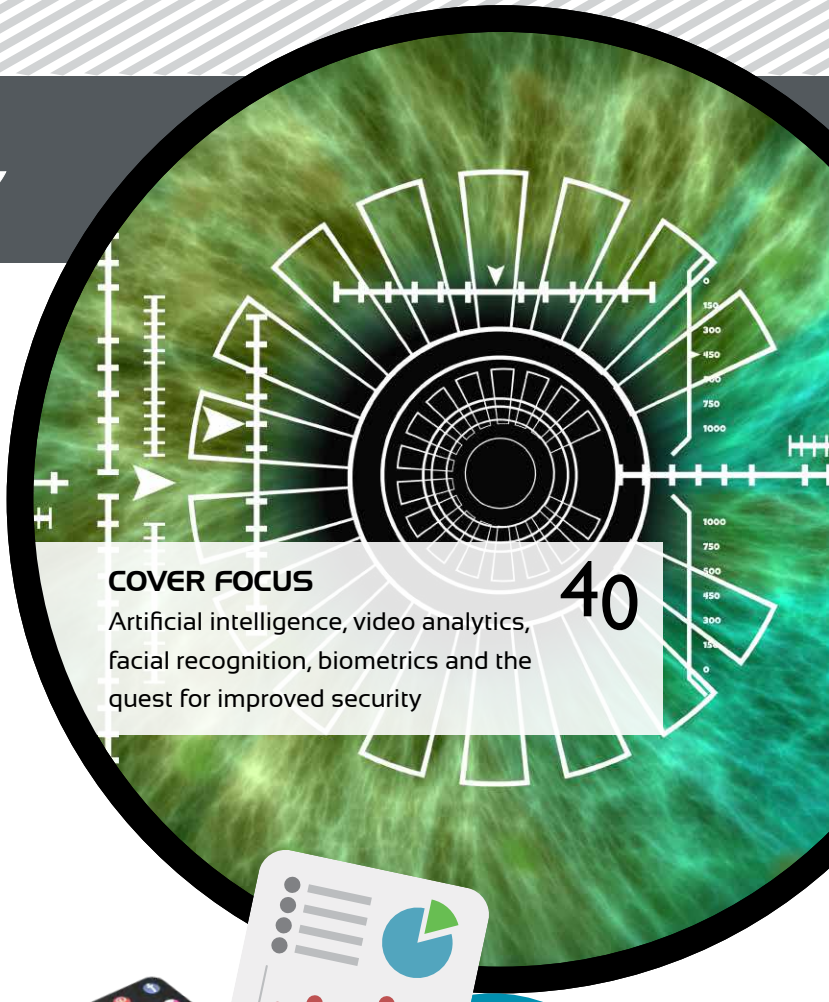
www.ifsecsea.com

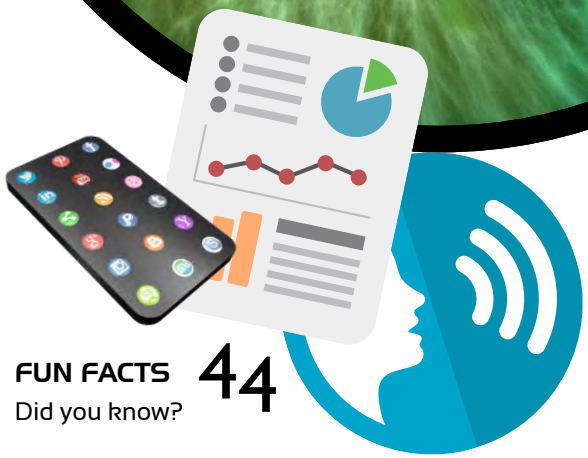
@IFSECSEA #IFSECSEA

IFSEC SOUTHEAST ASIA

UBM

IN THIS ISSUE





secutech
VIETNAM

fire & safety
Powered by Secutech Vietnam

SM home
VIETNAM

16 – 18 August 2018
Saigon Exhibition & Convention Center (SECC)
Ho Chi Minh City, Vietnam
www.secutechvietnam.com

Fast Growing Economy Enhances the Vietnam Security Industry

300+ Exhibitors I 13,000+ Visitors I 10,000 sqm Floor Space

- Growing sectors, including building, infrastructure, manufacturing and hospitality, make Vietnam the leading country in the security market in Southeast Asia.
- Continuing support from Vietnamese Government on city development feeds the increasing demand on security, smart home and fire safety systems.

Global contact I
Messe Frankfurt New Era Business Media Ltd.
Michelle Chu I +886 2 8729 1099 ext. 768 I michelle.chu@newera.messefrankfurt.com

VIETFAIR

messe frankfurt

CONTACT

PUBLISHER
Steven Ooi (steven.ooi@tradelinkmedia.com.sg)

GUEST EDITOR
Sheri Goh (sst@tradelinkmedia.com.sg)

GROUP MARKETING MANAGER
Eric Ooi (eric.ooi@tradelinkmedia.com.sg)

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

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

GRAPHIC DESIGNER
Siti Nur Aishah (siti@tradelinkmedia.com.sg)

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

Photos/Vectors Credit: Pixabay.com / Freepik.com

Designed by Fawzeeah Yamin

SECURITY SOLUTIONS TODAY
is published bi-monthly by
Trade Link Media Pte Ltd (Co. Reg. No.: 199204277K)
101 Lorong 23, Geylang,
#06-04, Prosper House, Singapore 388399
Tel: +65 6842 2580 Fax: +65 6842 2581
ISSN 2345-7104 (Print)

Printed in Singapore by KHL Printing Co Pte Ltd.

ANNUAL SUBSCRIPTION:

Surface Mail:

Singapore	- S$45 (Reg No: M2-0108708-2 Incl. 7% GST)

Airmail:

Malaysia/Brunei	- S$90
Asia	- S$140
Japan, Australia, New Zealand	- S$170
America/Europe	- S$170
Middle East	- S$170

ADVERTISING SALES OFFICES

Head Office:
Trade Link Media Pte Ltd *(Co. Reg. No: 199204277K)*
101 Lorong 23, Geylang, #06-04, Prosper House,
Singapore 388399
Tel: +65 6842 2580 Fax: +65 6842 1523, 6846 8843, 6842 2581
Email (Mktg): info@tradelinkmedia.com.sg

China & Hong Kong
Iris Yuen
Room 1107G, Block A,
Galaxy Century Building
#3069 Cai Tian Road,
Futian District
Shenzhen
China
Tel : +86-138 0270 1367
sstchina86@gmail.com

Japan:
T Asoshina/Shizuka Kondo
Echo Japan Corporation
Grande Maison, Rm 303,
2-2, Kudan-Kita,1-chome,
Chiyoda-ku, Tokyo 102,
Japan
Tel: +81-3-32635065
Fax: +81-3-32342064

Netway®
SPECTRUM

FIBER SOLUTIONS

Altronix's NetWay Spectrum series takes fiber and power to a new level. Indoor and outdoor models include hardened Ethernet PoE switches and multi-port media converters with or without integral power. Units can be deployed with conventional single or multi-mode fiber...or composite cable which combines fiber with copper to simultaneously deliver power and data. **Go further – with NetWay Spectrum from Altronix.**

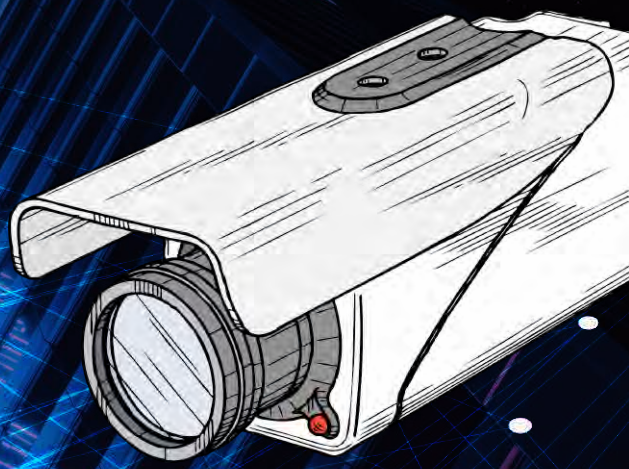
MADE IN THE U.S.A. & BACKED BY A LIFETIME WARRANTY

Altronix®

More than just power.™

altronix.com – info@altronix.com

COMING SOON...



OCTOBER

Safety & Security Asia 2018
Date: 2 - 4 Oct 2018
Venue: Halls B and C, Marina Bay Sands, Singapore
Organiser: Security Industry Institute
Telephone: +65-6278 8666
Website: www.safetysecurityasia.com.sg
Email: ssa@cems.com.sg

OCTOBER

Security China 2018
Date: 23 - 26 Oct 2018
Venue: China International Exhibition Centre (New Centre), Beijing, China
Organiser: China Security and Protection Industry Association (CSPIA)
Telephone: Tel: +86-10-6873 1701
Website: www.21csp.com.cn
Email: International@bizcspia.com

OCTOBER

IFSEC Southeast Asia 2018
Date: 25 - 27 Oct 2018
Venue: Impact Exhibition and Convention Centre, Bangkok, Thailand
Organiser: UBM
Website: www.ifsecsea.com

DECEMBER

Counter Terror Asia 2018
Date: 4 - 5 Dec 2018
Venue: Marina Bay Sands, Singapore
Organiser:
Fireworks Trade Media Pte Ltd
Telephone: +65-6100 9101
Website:
www.counterterrorasia.com
Email:
sg@fireworks.com

MicroEngine®

Integrated Security Systems

The Trusted Brand in Security Solutions

xPortalNet HS

High Security System Software

- 20 Digits (Full DesFire 64-bit CSN and Card ID)
- DesFire Security Profile Configuration
- Alarm Monitoring & Lift Controller
- CCTV Integration
- Visitor Management System (VMS)
- Dynamic Floor Plan for Real-Time Monitoring
- Web Server Support

Projects


Commercial / Complex


Factory


Condominium

500+ doors access & security system on SQL Server for factory and many more...


Plato DesFire Reader

1300-88-3925 or enquiry@microengine.net

www.microengine.net


Our Office


Service Centre

GlobalGROUP ISO 9001 5965 UKAS MANAGEMENT SYSTEMS

REG No. 749921389

EDITOR'S NOTE

Dear Readers,

We're whizzing into the second half of 2018, and it's been an eventful year so far. I'm standing in as guest editor for this issue of Security Solutions Today, and I've been enjoying all the exciting news that's been coming in about developments in the security world.

This issue's focus is on how your body talks—no, not necessarily in the ways you are thinking about! Technology and computers have collided with the world of physical security solutions, and your face, eyes, fingerprints, voice and even emotions have become an important part of keeping your world safe. With the uniqueness of each person's looks and personality comes the challenges of making security accurate but non-intrusive, which is what we discuss at some length in this issue.

In our cover story, Steve Reinharz lends his expertise as to how artificial intelligence (AI) can play a part in video analytics, facial recognition and biometrics. He also talks about the brave new world of AI in security solutions.

We also cover the gamut of technology, from phones to computers to smart video surveillance that quietly interact with people and keep them, as well as property, buildings and surroundings, safe. There are even facial recognition video cameras in China that monitor students' attentiveness in classrooms and take attendance!

As an important sidestep, we talk about how the European Union's General Data Protection Regulation (GDPR) affects us, even far away in Singapore.

This has been a fascinating venture into the world of security solutions, and I hope you enjoy reading this issue as much as I have enjoyed putting it together for you.

Sheri G

Guest Editor

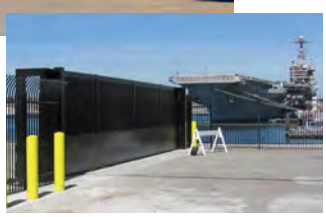
THIS IS NO TIME TO GAMBLE!

Delta's Crash-Certified Vehicle Barriers — People's **Lives Depend** On Them Everyday!

It's a fact. Since 1974, Delta Scientific has established the safety standards for high security vehicle barricade systems—barricades, beam barricades, bollards, portable barriers, sliding gates, surface mounted barriers—parking control equipment and guard booths. Delta systems can stop a 16,500 lb truck going 50 mph (7500 kg @ 80 kph)...and keep protecting.

Delta is also the acclaimed industry leader for customer service and technical support...the foremost choice of militaries, embassies, capitols, colleges, law enforcement agencies, auto lots, parking structures, international borders, airports, municipalities, public infrastructures and courthouses from Riyadh to Washington, London, Singapore and Rio de Janeiro. From protecting Presidents to pedestrians, Delta systems stop terrorists dead.

Bet your life on Delta.



DELTA

Visit **www.deltascientific.com** for details and specifications. ▲ **1-661-575-1100** ▲ **info@deltascientific.com**

IndigoVision announces new product to maximise security systems' potential

New Jersey, USA—IndigoVision, a leading developer of complete end-to-end video security solutions, announced in April that it has released the latest version of their Security Management Solution Control Center, a new cyber-security innovation CyberVigilant® in Camera, the Integra™ all in one device, and three additional products that strengthen their existing security offering.

IndigoVision's Control Center has long been regarded in the industry as one of the best, from its bulletproof nature to search and review forensic features; the software is intuitive and easy to use. The release of v15.2 is no exception with the introduction of Dynamic Profile Switching and improved support for analytics, both of which enable Control Center to grow with any business.

CyberVigilant® in Camera takes cyber-security technology within the industry to the next level. This unique and innovative cyber-security offering is a fantastic addition to IndigoVision's cyber range. Users can receive notifications direct to their Control Center user interface in the event that a cyber-attack takes place.

IndigoVision's Integra™ provides users with a Control Room in a box by combining Control Center, an NVR and the License Server into a single device. It is perfect for small to medium sites such as Retail, Education, Banking and Hospitality. View and manage multi-site installations easily from a central location using Integra™ View Workstation.

IndigoVision's existing security offering has also been further strengthened by the introduction of their new 200 Channel NVR-AS 4000, BX HD PTZ Dome Camera and a BX 4MP Microdome Camera which is available in two variants. Each of these products uses the latest technology in the industry to provide users with fantastic options for their security systems.

Pedro Simoes, IndigoVision's CEO, said, "The six products we are releasing are greatly enriching IndigoVision's security solutions offering. Each product enables our customers to address different market segments, always maintaining a focus on quality and important considerations such as cyber-security, to ensure potential issues are being addressed."

IndigoVision has more than 15,000 installations globally in markets including airports, casinos, education, government, health and industrial. In each and every one of these installations continual technology development, specifically in the area of cyber-security are crucial to user safety. It is essential that users are able to maximise their security systems potential by adapting to said threats and that is exactly what this latest release from IndigoVision enables. Combined with their commitment to open standards, integration and unique Distributed Network Architecture are what make IndigoVision an industry-leading video security solution.

For more information, please visit www.indigovision.com. SST

2018 SECURITY CHINA

the 14th China International Exhibition on Public Safety and Security 2018

New China International Exhibition Center

Beijing China

October 23 - 26. 2018

Wechat: cspmag

Wechat: securitychina

Approved by:
the Ministry of Public Security of the People's Republic of China
the Ministry of Commerce of the People's Republic of China

Organizer:
China Security and Protection Industry Association

www.securitychina.com.cn

Malwarebytes Introduces Easy to Use Endpoint Protection and Response Solution for Monitoring, Detection and Remediation

Most businesses don't have enough malware prevention infrastructure, solutions or expertise, says Malwarebytes.

SANTA CLARA, California—Malwarebytes, the leading advanced malware prevention and remediation solution, announced the release of Malwarebytes Endpoint Protection and Response in April. When it comes to Endpoint Detection and Response (EDR), most businesses fall into one of three categories: they either don't have EDR and have limited visibility into endpoint activity across their infrastructure; they have an EDR solution that provides visibility, but staff lack the time to gain the expertise necessary to leverage EDR data; or they have EDR and the expertise but the solution they are using simply provides alerts without resolution. Each of these circumstances often results in missed threats or extended dwell time.

"Many businesses don't have the resources to bring on dedicated, highly-specialised EDR technology and talent, leaving them with a tool that simply adds to a long queue of alerts, without fixing the underlying problems," said Marcin Kleczynski, CEO, Malwarebytes. "Malwarebytes Endpoint Protection and Response provides proven endpoint protection with integrated detection and response capabilities via a single agent, so organisations of all sizes can easily protect their endpoints from targeted attacks, thoroughly remediate systems and rollback ransomware."

Key features of Malwarebytes Endpoint Protection and Response protect across every stage of an attack including:

- Cloud-based single management console and a unified agent.
- Continuous monitoring and visibility of endpoints—Endpoint Protection and Response's flight recorder provides continuous monitoring and visibility into Windows desktops to obtain powerful insight. Businesses can easily track file system activity, network activity, process activity and registry activity. Flight recorder events are stored both locally and in the cloud, adding another sphere of safety.
- Multi-layered protection—Malwarebytes Endpoint Protection and Response's multi-vector protection (MVP) uses a seven-layered approach, which includes both static and dynamic detection techniques. This technique gives protection against all known and unknown threat types, from traditional viruses to tomorrow's advanced threats.
- Rapid identification and three modes of endpoint isolation—When an endpoint is compromised, Malwarebytes stops the bleeding by isolating the endpoint. Endpoint Protection and Response is the first product to offer three ways to isolate an endpoint. Network isolation restricts which processes can communicate. Process isolation to controls which processes are allowed to keep functioning. Desktop isolation alerts the end user and halts further interaction to limit damage. With these three controls, malware is rendered incommunicado and remote attackers are locked out.
- Complete remediation and ransomware rollback—Malwarebytes proprietary linking engine provides complete and thorough remediation to rapidly return an endpoint to a truly healthy state and minimise impact to the end-user, post-compromise. Rollback technology winds back the clock up to 48 hours, negating the impact of ransomware with just-in-time backups prior to infection.

Malwarebytes Endpoint Protection and Response allows organisations to proactively hunt for malware across all of their endpoints without the need for a dedicated resource. This increases the efficacy of protection and provides a lower total cost of ownership. The single console delivers significantly greater security visibility and direct drill-downs to explore and instantly manage all security events. All this is accomplished with reduced hardware cost and a reduced server footprint.

Malwarebytes proactively protects people and businesses against dangerous threats such as malware, ransomware and exploits that escape detection by traditional antivirus solutions. Malwarebytes completely replaces antivirus solutions to remove the personal obstacles and business interruptions caused by modern cybersecurity threats. More than 10,000 businesses and millions of people trust Malwarebytes innovative machine-learning solutions and global team of researchers to identify emerging threats and to prevent and eradicate malware that antiquated security solutions miss and leave behind.

For more information, please visit:
http://www.malwarebytes.com/ SST

The international exhibition & conference on building maintenance and facilities management

BMAM EXPO ASIA 2018

12-14 SEPTEMBER 2018

HALL 5-6, IMPACT, BANGKOK, THAILAND

INTEGRATED FM OF THE FUTURE

BMAM Expo Asia 2018 offers exciting possibilities for businesses keen to be at the forefront of innovation and technology in facilities management.

EXHIBIT NOW!

FM Products & Services I Plant Maintenance I Facilities Management Software
Workspace Management I Smart Building Solutions I Cleaning Products & Services
Security I Interior & Landscape Design I Green Building Technologies I Health & Safety

Scan to book your booth

Organized by IMPACT MUANG THONG THANI

www.bmamexpoasia.com

BMAM Expo Asia

+66 (0) 2833 5208

Security software detects friend, foe and accident

In addition to the sensor resolution of CCTV lenses, the accuracy of surveillance programs has been increasing for many years. Powerful computer systems run data-intensive applications for registering friend and foe, customer and thief.

But current systems are not the last word in accuracy, as clearly demonstrated by providers of state-of-the-art surveillance software at the recent Secutech Taipei and Intersec Jeddah trade fairs. Intelligent computer programs identify, inter alia, customer numbers, the length of their visit, gender and type of behaviour. The prerequisite for this is smart software and an ability to use deep-learning algorithms. Systems of this kind analyse data, e.g., images, videos, texts and signals, in real time. And, with time, the program analyses types of behaviour and becomes increasingly accurate.

The possibilities range from theft prevention, via an analysis of consumer interest, to accident recognition. Naturally, this is not only of interest to the retail trade but also to security-sensitive businesses, factories, the health-care system, smart cities and the transport sector, not to mention the own home.

Another benefit of using intelligent surveillance systems: to date, security experts have been forced to review hours of surveillance videos after an incident. However, reconstructing the past on film is much more efficient if the material has been smart tagged, i.e. linked with a digital keyword. To this end, the intelligent software behind the CCTV lens must be able to identify and classify objects automatically. The system then attaches specific properties as tags in real time. The user is responsible for determining what elements are to be tagged. Subsequently, the system shows all relevant results with a time stamp on the display.

Thus, passive security and market research become a single entity if necessary—a milestone from the user's point of view because security now has the potential to change from being a pure cost centre to a profit centre by, for example, processing all the data collected.

In many cases, security is a regional or even national topic. On the one hand, this is due to regulatory differences and, on the other hand, the very different weighting given around the globe to security needs in relation to personal transparency. With ten strategically located trade fairs and forums around the world, Messe Frankfurt offers security platforms for greatly divergent needs. There, established manufacturers and innovative newcomers present their latest products and, increasingly, networked systems, which benefits a variety of companies, especially those wanting to fill the synergistic gaps between security technology and customer analysis.

For more information, please visit: www.safety-security.messefrankfurt.com SST

SAFETY & SECURITY ASIA 2018 SINGAPORE

THE 17TH INTERNATIONAL SAFETY & SECURITY TECHNOLOGY & EQUIPMENT EXHIBITION

in conjunction with

Security Industry Conference 2018

Halls B and C
Marina Bay Sands, Singapore
2 - 4 October 2018

Enhance your productivity with smart security solutions

SSA 2018 brings together the top security leaders in the field to showcase an extensive presentation on the latest security solutions, products and services.

Exhibit today to reach out to buyers of security solutions!

Seize the opportunity to :

√ connect with industry experts at the exclusive Security Industry Conference 2018.

√ meet your key buyers: Architects, Builders, Contractors, Developers, Engineers, Facility Managers, Government Agencies, Security Consultants and many more!

www.safetysecurityasia.com.sg
For more information, please email ssa@cems.com.sg
or call (65) 6278 8666

Organised by

CEMS Conference & Exhibition Management Services Pte. Ltd.

SIC 2018 Organiser

Security Industry Institute

Host

Security Systems Association of Singapore
www.ssas.org.sg

A Part of Architecture & Building Services 2018

ArchXpo 2018
The 5TH International Exhibition of Architecture & The Built Environment

iFaME INTERNATIONAL FACILITY MANAGEMENT EXPO 2018
The 6th International Facility Management Equipment, Products, Technology & Services Exhibition

LED+LIGHT ASIA 2018
5TH International LED + Lighting Technology Show

FIRE & DISASTER ASIA 2018 SINGAPORE
THE 15TH INTERNATIONAL DISASTER, EMERGENCY MANAGEMENT & FIRE PREVENTION TECHNOLOGY & EQUIPMENT EXHIBITION

WORK SAFE ASIA 2018 SINGAPORE
THE 5TH INTERNATIONAL WORKPLACE SAFETY TECHNOLOGY & EQUIPMENT EXHIBITION

Dahua Technology USA Introduces Advanced Artificial Intelligence Technologies at ISC West

New Dahua Deep Learning algorithms offer proactive approach to video surveillance

Irvine, California, USA—Dahua Technology USA, a leading video surveillance solutions provider, has introduced two cameras incorporating Artificial Intelligence (AI) technologies at ISC West, including front-end devices, back-end storage and platform management through Dahua's New DSS Pro.

Artificial Intelligence is on the cusp of becoming the next technology to disrupt the security industry. AI has the ability to perceive and learn the environment so that when something abnormal is detected, authorities can quickly respond before a situation arises. Similar to how the human brain remembers large amounts of data, AI has the ability to classify and recognise thousands of features and then perform corresponding actions based on what the system has learned. The more features the system can capture, the higher the accuracy.

The IPC-HF8242F-FR AI Network 2MP Box camera is a standalone front-end intelligent solution that performs complex facial recognition without additional licenses or servers. This camera features backwards compatible H.265 / H.264 smart codecs, Starlight Technology for low-light applications and True Wide Dynamic Range (120dB) for high contrast scenes. By interpreting video data at the source, the camera dissects and learns data for easier processing and higher efficiency. Since the analytics are done on-board, this camera is a perfect solution for small to mid-size applications that require advanced intelligence at the edge.

The camera includes human facial feature extraction, real-time facial snapshots and a comparison database of up to 10,000 face images and five libraries that are stored on-board. The facial recognition feature enables a proactive way to identify persons of interest before an incident occurs. For example, by simply adding profiles of known criminals, prior offenders, suspended students, sexual predators or disgruntled persons to the database, an alert will be sent if the person is detected on camera.

An additional feature the IPC-HF8242F-FR offers is accurate, real time facial analysis that includes six types of facial features: age, gender, expression, glasses, mouth mask and facial hair, and and five types of expressions including: happy, normal, surprised, sad and angry. This information can be valuable demographic information for profiling the type of customers a business attracts.

The IVSS7016 all-in-one 16 Channel AI NVR supports 4K ultra HD resolution for recording, live viewing and playback, and combines video management functions with traditional video storage, video decoding & deep learning in one device. With its integrated, high-performing GPU module, and Dahua's advanced deep learning algorithms, the device can perform a powerful video structure analysis using metadata and achieve high precision facial analysis.

The IVSS7016 features an Intel Dual-core processor and the AI NVR can store up to 100,000 faces in the image database and a maximum of 10 million face metadata or face images. The device offers RAID 0/1/5/10, redundant power, and backwards compatible H.265 / H.264 smart codecs and is compatible with any ONVIF camera.

"AI is changing typical passive video surveillance into a preventative approach. Dahua is excited to provide the most advanced technology for predicting incidents before they occur," said Jennifer Hackenburg, senior product manager at Dahua Technology USA.

A key facet of Dahua's new Facial Recognition technology is the alerting system that informs operators to persons of interest. Designed for places with high throughput traffic and risk of theft, such as casinos, this technology is a critical tool to prevent blacklisted personnel from entering a facility. For example, upon an identity match, security guards are alerted to the presence of a known offender, enabling security personnel to deny access into a casino to deter unlawful behaviour like cheating. This technology works equally well in preventing the admittance of known offenders into other venues such as education facilities, restaurants and sports arenas.

For more information, please visit: us.dahuasecurity.com SST

"Asia's Premier Counter-Terrorism and Internal Security Exhibition and Conference!"

CTAX

COUNTER TERROR ASIA EXPO 2018

4 - 5 DECEMBER 2018

Marina Bay Sands, Singapore

Co-Located With:

An International Conference on Counter-Terrorism and Internal Security

www.counterterrorasia.com

For more info, contact us:
Phone: (+65) 6100 9101 | Email: sg@asiafireworks.com

Organized by:

FIREWORKS® TRADE MEDIA GROUP

Fireworks Trade Media Pte Ltd

How CCTV OEMs increase video data capacity and reduce costs

Original equipment manufacturers (OEMs) working in CCTV and security are using Hewlett Packard Enterprise (HPE) OEM Solutions to expand data storage capacity, apply analytics and lower costs

The rise in global security threats has increased the demand for advanced video surveillance technologies that store and analyze large amounts of video data. According to research from industry analyst IHS Markit, the number of surveillance cameras to be shipped globally in 2018 is 130 million[1]. To put that into perspective, it was fewer than 10 million in 2006. Older storage systems, video cameras and servers are simply not designed to support the needs of today's CCTV industry.

Surveillance providers are demanding more storage capabilities from OEMs due to the growing volume of video data they need to store, and the ever-higher definition formats it's captured in. New data and compliance laws also require these surveillance companies to retain video data for longer periods of time.

These growing collections of data are also essential to businesses that want to drive value from predictive analytics. According to research firm MarketsandMarkets, the video analytics market alone is expected to grow to $8.5 billion USD by 2023[2].

To benefit from the growing security landscape, leading security surveillance OEMs are choosing to partner with Hewlett Packard Enterprise (HPE) OEM Solutions. By integrating HPE OEM Solutions' hybrid cloud technologies into their surveillance platforms, security OEMs can create new solutions that help companies increase video data capacity and leverage analytics, all while lowering costs.

Providing cost-effective predictive analytics

While security headlines often focus on cyberthreats, physical threats such as fire, theft and crowded gatherings are also increasing. For CUDO Communication, which specializes in state-of-the-art intelligent video surveillance, helping customers develop predictive analytic capabilities is paramount.

Their IntelliVIX software analyzes video signals in real-time to enable immediate threat response. This technology is run on HPE OEM Solutions servers which are purpose-built for high-performance computing and big data analytics. As a result, CUDO customers can rapidly analyze massive volumes of CCTV footage to meet their security objectives at a lower total cost of ownership.

Optimizing server performance and reducing complexity

Surveillance solutions developer Venzo Secure required a partner to help them reduce the complexity of technology implementation while lowering costs.

With the understanding that video surveillance solutions are not one size fits all, Venzo needs to deliver customized state-of-the-art platforms optimally configured for each individual deployment. That's why Venzo integrated HPE OEM Solutions servers that can be modified to meet the needs of each installation.

Being able to tailor solutions, backed by 24x7 onsite support, for specific customer needs has helped reduce costs by delivering the right server platform for each specific implementation. And Venzo customers benefit from a 30 percent increase in server performance.

Global, reliable support

As security surveillance providers expand into new markets, CCTV solution provider Vista needs to ensure on time deliveries and 24x7 support for customers all over the world, 365 days of the year.

Vista regards the reliability of their technology as a top priority. "If a customer has a problem with recording or accessing the video, it puts the entire purpose of our solution into jeopardy," said Gary Rowdan, Divisional Director at Vista.

HPE OEM Solutions offers global logistics and support to assure a consistent customer experience. This extensive supply chain and service network enables OEMs to expand their businesses across the globe at a reduced risk.

To keep up with the rapidly evolving security surveillance industry throughout the world, OEMs need to provide advanced real-time analytic capabilities, superior scalability and global support that meets the unique needs of every customer. Choosing a partner with the experience, portfolio and expertise to help deliver this package can make the difference between short-lived progress and long-lasting success.

Learn how HPE OEM Solutions are providing the backbone for security surveillance, and how we can help your business today at http://www.hpe.com/solutions/oem-cctv.

1 IHS Markit, https://technology.ihs.com/598815/market-for-storage-used-for-video-surveillance-worth-17bn-in-2017
2 MarketsandMarkets, https://www.marketsandmarkets.com/Market-Reports/intelligent-video-analytics-market-778.html

HERE, IDEAS ARE ALWAYS IN SIGHT

Your customers need security, surveillance, and analytical solutions that can help protect their people and their assets against an evolving world of threats. Staying ahead demands your constant innovation; **HPE OEM Solutions** has the highly adaptable compute, storage, and networking resources your customers need to keep an eye on everything that matters.

Hewlett Packard Enterprise

OEM

HPE OEM SOLUTIONS

Learn how we provide the backbone for security surveillance at:
hpe.com/solutions/oem-cctv

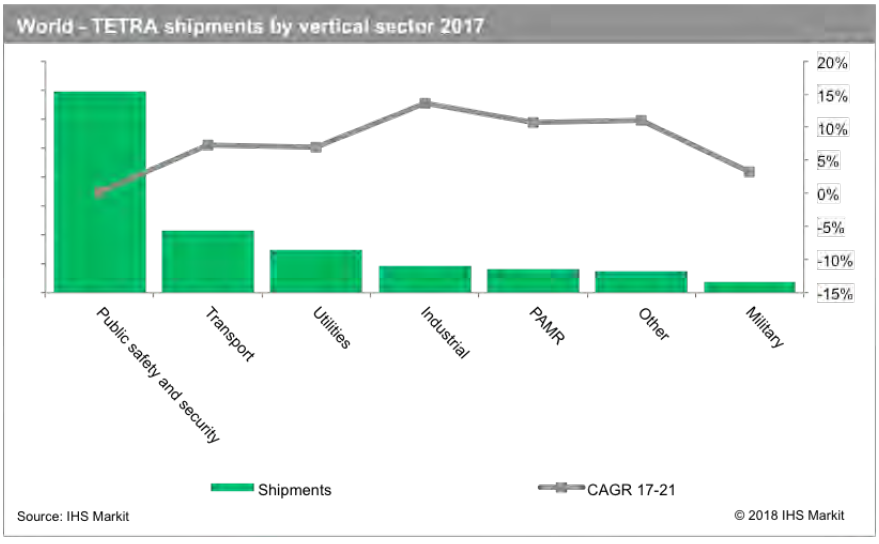
Led by Asia and the Americas, global TETRA shipments increased by 16 percent in 2017

Developed by the European Telecommunications Standards Institute, terrestrial trunked radio or trans-European trunked radio (TETRA) is a global standard for digital trunked radio. While adoption varies by country and region, growth rates of this magnitude for a mature technology are significant. While some people question its longevity, its presence on the world stage continues to grow. IHS Markit projects TETRA will continue to provide mission-critical communications well into 2020 and beyond.

TETRA has proven itself the technology of choice for emergency services, and the European public safety and security industry continues to be the backbone of the TETRA market. Unfortunately, in many parts of the world, there are persistent reminders of just how important the public safety and security market is, as people around the world face the threat of injury and loss of life from terrorism and anarchy. In 2017, there were more than 1,300 terrorist attacks around the world, including the Westminster attack in the United Kingdom in March 2017, the St. Petersburg metro explosion in Russia in April 2017, the attack in Stockholm, Sweden, in April 2017, not to mention the countless foiled terrorist attacks which security forces thwarted.

TETRA has been critical in coordinating the emergency services in many countries, and it will continue to provide mission-critical communications well into the future. The merits of TETRA in critical times are so apparent that Belgium's nationwide public safety network ASTRID received approval from the Belgian government to invest €117 million in improvements to its network infrastructure, following the bombings in Brussels in 2016.

Investment in both established and new networks are evident across Europe, with deployments continuing to grow in Western Europe. Parts of Eastern Europe are also investing in the technology, with Bulgaria procuring TETRA radios for its police forces and Hungary investing in its nationwide public safety network EDR. Furthermore, shipments destined for Russia increased, as Russia prepares to host the FIFA World Cup this summer. TETRA markets in Asia and the Americas are now expected to grow more quickly than in the past. In fact, Asia posted its largest growth in deployments in 2017, with airports, metro systems and other transportation hubs adopting the technology.



The Americas set for fastest procurement growth

Over the next five years, the fastest procurement growth will come from the Americas, as North America and Latin America continue to adopt the technology. Despite the extensive utilisation of P25 communications by emergency services in North America, TETRA continues to penetrate commercial organisations, adding many new users in the transportation and utilities sectors.

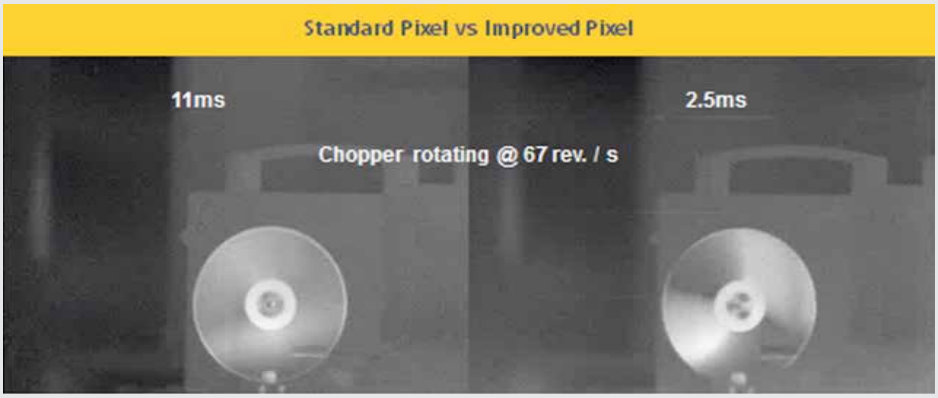
TETRA has also been very successful in Latin America, particularly in the public safety and security domain. Parts of Latin America have long suffered endemic corruption and increasing urbanisation. Weak states and disparate economic prosperity in the region underpin the need to invest in public safety and security. Latin America has just eight per cent of the world's population but 38 per cent of recorded murders, so investment in public safety and security is crucial. Latin America also has a very diverse licensed mobile radio (LMR) ecosystem, with no clear leading technology. P25, TETRAPOL, TETRA and cost-optimised digital technology all have a solid presence in this region, bringing with them many opportunities for growth.

Alongside the growth of LMR digital technologies, Long Term Evolution (LTE) technology has also developed on the world stage. Private LTE networks have emerged in China, South America, Australia, Qatar, United Arab Emirates, Saudi Arabia, Ghana, Kenya and Nigeria. National LTE networks are also planned in South Korea and the United Kingdom, while Angola

has opted for a TETRA and LTE convergence solution, for its national communications network. The United States has affirmed its commitment to rolling out its nationwide FirstNet LTE network, as AT&T secured a 25-year contract to build and maintain the network.

Despite the emergence of LTE technology, LMR adoption will continue to grow, as LTE becomes more established and proves its capability to meet the critical voice communications requirements of emergency services. Over the next few years, LTE will complement critical voice with data, rather than replace LMR altogether. Over the next five to ten years, LTE might be used as a substitute for TETRA, TETRAPOL and other high-end LMR technologies, as capital investments are considered in nationwide or large-scale deployments. SST

ULIS sets new performance record for bolometers; now match speeds of high frame-rate cameras



Veurey-Voroize, near Grenoble, France—ULIS, a designer and manufacturer of a wide range of thermal image sensors for commercial, defence and security applications, announced in April that it has achieved unmatched performance with its bolometer (a type of thermal sensor) that now meets speeds of fast imaging applications. It has gained a response time that is four-times greater than standard bolometers. ULIS has achieved this faster speed without any trade-off in sensitivity; the company is the first to overcome this technological challenge in its aim to significantly raise the overall Factor of Merit (FoM) of bolometers. FoM, a relative measure of thermal sensor sensitivity against response rate, is a key parameter camera makers use to compare the performance of thermal sensors.

In contrast to standard bolometers, ULIS' quicker response time means that it can detect fast-moving objects without producing a blurred image. This new pixel technology enhancement, in conjunction with the bolometer's comparably lower price, make it ideal for inclusion in machine vision cameras, where high frame rates for in-line quality inspection are required but previously the cost of adopting thermal imaging had been prohibitive. The bolometer will also have wider application in defence, such as missile warning systems.

"ULIS is thrilled with the outstanding results we have achieved in improving both the response time and sensitivity of the bolometer. This is proof of the continued strength of our affordable pixel technology and the skillset within our R&D teams," said Sébastien Tinnes, marketing team leader at ULIS. "We feel camera makers will benefit tremendously from thermal image sensors, which, when used in conjunction with visible or SWIR cameras, can provide valuable additional information on product quality. We look forward to exploring with customers, industrial partners and the scientific community attending SPIE Defense and Commercial Sensing in Orlando in mid-April, the potential of integrating this new pixel technology into future equipment requiring fast imaging capabilities."

ULIS' new pixel technology achieves an FoM of 125 to 150mK. ms, enabling sharper images that aim to improve the quality of in-line production controls, such as automated glass manufacturing line monitoring.

In a technical paper entitled, "ULIS Bolometer for Fast Imaging Applications Sets New Response Time Record," which they presented at OPTO2018 in Paris, UKIS showed gains in FoM performance from the standard NETD=50mk multiplied by TTC=10 to 12ms (meaning FoM 500 to 600mK.ms) to a new level of NETD=50mK multiplied by TTC=2.5 – 3ms (meaning FoM 125 to 150mK.ms), a four-fold improvement. SST

Feeling the Heat: Dahua Thermal Cameras Create Value with Temperature

Dahua Thermal Cameras for Perimeter Protection

HANGZHOU—Conventional surveillance cameras are already capable of capturing video in daytime and well-lit areas. However, in poorly-lit areas or at night, these cameras' video capture abilities begin to diminish as sensors must compensate for the lack of light by increasing sensitivity, thus producing a noisy image, if one is produced at all. Since clear day and night monitoring is an important benchmark in assessing a surveillance system's effectiveness, thermal imaging devices present a clear advantage in their ability to convert heat energy into an image visible to the human eye.

Leveraging its experience in camera image analysis and intelligent algorithms, Dahua Technology has developed a new generation of thermal imaging devices with innovative functions that balance visible light with infrared, enabling users to effectively monitor an area under all lighting conditions. In addition, these functions include advanced capabilities such as intelligent temperature measurement and behaviour analysis, further extending the scope of surveillance applications such as perimeter protection or equipment predictive maintenance in substations.

The new products adopt advanced uncooled infrared detectors with 400x300 effective pixels, realising a 40 per cent increase over the previous infrared detector with-336x256 effective pixels. The benefit is that the field of view is increased, for example, TPC-BF5400 with 13mm thermal lens, has a 29.7^0x22.3^0 field of view, and the older model TPC-BF5300 is 25^0x19^0 with the same lens. Meanwhile, newer models have received improvements in detailed information, contrast and other upgrades.

Thermal imaging is probably the most reliable security solution for perimeter protection. A thermal camera is less sensitive to changes in the environment. It detects moving people or objects even in total darkness, 24 hours a day and seven days a week.

The Dahua IVS (Intelligent Video System) is a built-in video analytics algorithm that delivers intelligent functions to monitor a scene for tripwire violations, intrusion detection, and abandoned or missing objects. It requires a certain number of pixels on the target to function properly. The DH-TPC-BF5400-B13 model can be utilised to form a perimeter intruder detection system, performing as an invisible wall. When installed at the recommended height of 5 meters, one camera can cover a 100 meters long fence. Whether it is day or night, if someone enters a targeted area, a warning will be sent to the control centre.

A thermal camera is not just for video surveillance; it is also suitable for remote temperature monitoring to prevent accidents. Calculating the corresponding relationship between received radiation energy and temperature, it shows the surface temperature of the target through different grey values. Currently, the temperature measurement tolerance is within a certain range- ±2°C, ±2%. It provides users with real-time information about substation equipment much more efficiently, saving time and labour. If the temperature of equipment or part of the station exceeds a pre-set threshold, the system will automatically trigger an alarm and alert management.

For a thermal camera, the radiation does not only depend

on the temperature, the surrounding environment also emits radiation, especially high temperature objects at close distance, which will be reflected by the target surface. The emitted radiation of the object and the reflected radiation are also affected by atmospheric absorption. Therefore, to measure temperature precisely, it's necessary to consider the effect of different radiant sources.

A precise temperature measurement should include these three steps:

- Excluding external temperature interference by placing a baffle or coat of high emissivity materials on the surface of the target to make the result as accurate as possible.
- Keeping appropriate distance to ensure the target occupies at least 10x10 pixels in the image.
- Considering energy transmission losses, especially in high temperature and humidity environments, the atmospheric transmission coefficient is obviously reduced.

Conventional monitoring methods are not sufficient enough in dealing with all kinds of threats. Cutting-edge technologies are necessary to effectively prevent and respond to threats in the shortest time possible. Dahua thermal imaging devices provide the tools required for ensuring security in a number of applications. With a mission of "Enabling a safer society and smarter living", Dahua will continue to focus on "Innovation, Quality, and Service" to serve partners and customers around the world. SST

Oncam Recognised for Multiple Awards for Innovative Products and Partner Solutions

LONDON—Oncam, the leading provider of 360-degree video capture and business intelligence technology, announced today it has been honoured with two awards for its innovative products: Most Innovative Online Solution from the 2018 North American Fraud Awards alongside its partners at Video Analysis Solutions (VAS) and a 2018 Money-Saving Products Award from BUILDINGS Magazine for its new Evolution 180 Indoor Camera. The recognitions demonstrate the company's continued dedication to innovation and the development of technology to address today's greatest security and business challenges.

At the 2018 North American Retail Fraud Awards dinner in May, Oncam and its partner VAS were recognised by Retail Risk for their retail-centric Cloud Searching Dashboard. Oncam and VAS have created a powerful and user-friendly analytics tool that leverages Oncam's high-quality 360-degree video and intuitive VAS analytics to allow store managers and staff to securely log in and view live or recorded images, as well as monitor customer behaviour and provide details on store traffic. The solution offers significant ROI by optimising store operations, improving customer service and growing sales.

The Evolution 180 Indoor Camera was recognised in the June 2018 issue of *BUILDINGS* Magazine for the features it provides building owners and facility managers for life safety and security. The Evolution 180 range uses a 12MP sensor for high-resolution panoramic video. Oncam's unique Angle Compensation Technology provides adaptive dewarping in the camera, eliminating the need for integration in video management software. The camera is ONVIF Profile S compliant, making it plug-and-play with the leading video management systems on the market today.

"Oncam provides innovation in the products we create, but more than that, our close collaboration with other technology leaders allows us to create solutions that enhance the abilities of our video capture tools to provide valuable insight to end users," said Jumbi Edulbehram, Regional President—Americas, Oncam. "These awards are an acknowledgment of the hard work and dedication of our team and we're honoured to be recognised."

About Oncam

Oncam is a global technology innovator offering a cloud-based business intelligence platform with industry-leading 360-degree video capture and analytics at its core. Founded in 2007, it is part of ONVUTechnologies Group, and is a leading innovator in 360-degree video technologies globally. Oncam is headquartered in Switzerland and operates from regional hubs in the UK, US, Turkey, Hong Kong and India.

Please visit oncamgrandeye.com for further information. SST

VTT Marilyn, a Finnish robot car, has taken a leap towards automatic 24/7 driving

Marilyn sees better than humans in foggy, and even snowy, conditions, and can now navigate without stopping—even in bad weather.

Finland—VTT's robot car, Marilyn can see a human through fog and avoid accidents automatically. This is enabled by the LiDAR mounted on the car's roof, which can see wavelengths that are beyond the ability of the human eye. As the technology evolves, this represents a big step towards a safe automated vehicle that is not even stopped by inclement weather conditions.

Most likely, for the first time, robot cars from different manufacturers will demonstrate their driving scenarios in the same arena at the RobustSENSE event in Ulm, Germany, where Marilyn will head with six other robots on 16 May.

The latest additions to Marilyn include optical component wavelengths via the new 1550 nanometre LiDAR and additional intelligence for its software, which improves sensor capabilities. Furthermore, software modules have been built in for the filtering of point clouds and the assessment of scanner reliability. This is to ensure the vehicle's ability to function, including in fog and powdery snow, under which conditions the LiDAR radar, which 'sees' in the visible and near infrared ranges of the spectrum, even enables the robot car to see people better.

"Although Marilyn's vision is limited to roughly 30 metres in thick fog, the new LiDAR type allows the car to be driven slowly rather than it coming to a full stop," says Project Manager Matti Kutila of VTT's RobotCar Crew team.

The car also has traditional automotive radars and LiDAR, but their detection of non-metallic obstacles and resolution is limited, particularly when trying to recognise shapes.

"Marilyn can also combine radar and LiDAR technologies by optimising the best aspects of the different sensors. This makes the automatic vehicle safer than a car driven by a person—although there are still lot of obstacles in development path, a major leap has been taken in the right direction," Kutila emphasises.

"We still have a long way to go on the journey towards 24/7 automated driving, but we are now a big leap closer to achieving our dream. If we think of this as a 42km marathon, we are now perhaps 10km closer to our goal," he comments.

More and more driving scenarios involved

More and more scenarios (such as cities, main roads, snow,

exit ramps), which robot cars can manage, have been added. Marilyn will present her own special capabilities at the RobustSENSE event, along with six other robot cars.

"Marilyn will drive through a bank of fog created in a tent, which is so thick that the passengers cannot see through it. After passing through the chamber, the car will automatically avoid an obstacle in front—in this case, a dummy. Among Marilyn's sensors, the 905 nanometre LiDARs cannot see through mist—the new 1550nm LiDAR is the only sensor based on which a decision to swerve can be made," says Kutila, describing the driving scenarios of his protege.

This is probably the first time in Europe that six robot cars will drive through their different scenarios in the same campus area, in which also pedestrians are also moving around. Other cars will negotiate crossroads automatically, engage in route planning, and change between manual and automated mode, which makes this exceptionally fascinating day.

Marilyn, on the other hand, will profile the "see through" type of scenario, by driving through fog which even the observer cannot see through.

The LiDAR and sensor fusion technology of VTT Technical Research Centre of Finland, SICK, Oplatek and Modulight are co-created in Marilyn.

The project in overall is joint effort of Daimler AG, AVL, Bosch, Centro Ricerche Fiat, EICT GmbH, Fico Mirrors S.A., Fraunhofer FOKUS, FZI Forschungszentrum Informatik, Modulight, Inc., Oplatek Group Oy, SICK AG, University of Ulm and VTT.

"Members of the public will also be able to hop into a robot car at an event which could feature the world's first robot car traffic jam, but hopefully not chain collisions," Kutila adds.

Marilyn will next try out her skills in an automated parking exercise in the summer, based on commands from outside the car. Her husband, VTT Martti, will also be making the news in the north during the summer and in November, when he makes route selections based on friction data and LiDAR. SST

Essence works with the Google Assistant to Deliver Voice-activated IoT Control

Tel Aviv & Mountain View, USA—Essence, a leading provider of connected living solutions, announced in April that its WeR@HomeTM technology has been integrated with the Google Assistant, allowing WeR@Home customers to use the Google Assistant on their phone; voice-activated speaker, like Google Home; and more to operate their Essence-based IoT solutions.

Essence WeR@HomeTM Smart Living enables consumers to enjoy IoT's possibilities through seamlessly and remotely managing their connected homes. The comprehensive Security, Safety and Smart Home solution is easy-to-install and simple to use and leverages IoT and M2M communication technologies to deliver a complete connected-home experience.

Essence is one of the first Israeli OEM's to integrate a smart home solution with the Google Assistant. Essence has been a home security platform provider for more than 20 years—IoT before the term existed—delivering highly secure, easy to control and manage, and beautifully designed safety, security, and home management systems.

Essence brings significant added value to the table, as it offers end-to-end solutions, from complete connectivity with service providers' business and support infrastructures to a comprehensive platform on the customer side supporting API and local integration with Nest, IFTTT, Yale Lock, August Lock, and hundreds of other Z-Wave compatible devices.

"The integration of the Essence WeR@Home platform with the Google Assistant gives users even more choice when looking to create a connected smart home experience," says Mark Spates, Product Lead for Smart Home at Google. "We're looking forward to working together and bringing Essence technology to even more homes via the Google Assistant."
With the Google Assistant, consumers can control their home environments simply with voice commands, such as: "Hey, Google, turn on my lights."

A fully integrated WeR@HomeTM connected home experience can be achieved by controlling IoT devices or setting automatic event driven actions, supplemented by real-time voice commands, such as controlling lighting and smart switches and setting automation scenarios.

"Working with Essence gives Google Assistant customers the ability to use voice commands to control many aspects of their homes' security, safety and automation," said Ronnie Nir, Essence VP Sales & Marketing. "This is the first step in reducing our reliance on apps, with voice control ultimately being the main way we manage the multitude of IoT devices within our environments."

The combination of the Google Assistant and Essence opens significant business opportunities for service providers looking to differentiate their offerings, allowing them to deliver a connected-home system that can be managed by voice or apps on any screen from any location. Service providers using Essence's cloud platform can keep customers engaged 24/7 with advanced tools to remotely assist their customers, provide software upgrades, and deliver professional security services.

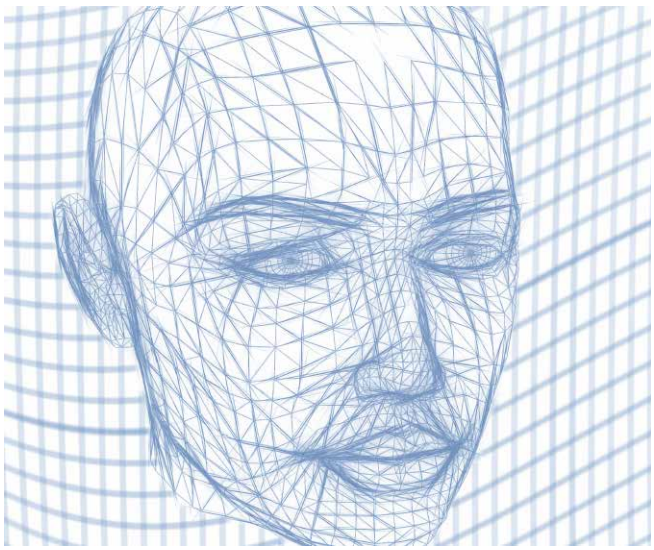
"Ultimately, the business of connected living is to offer technologies that let service providers deliver exceptional customer experience," concluded Nir. "The combination of the Google Assistant with Essence gives our integrators and distributors an advantage in the market." SST

Auxiliary Force is the First Security Force in Malaysia to Adopt Facial Recognition Technology to Combat Growing Security Threats

Malaysia—Auxiliary Force Sdn. Bhd. (AFSB), a member of Royal Malaysia Police Cooperative Bhd., is working with YITU Technology (YITU), a pioneer in Artificial Intelligence (AI) research and innovation, to transform and augment Malaysia's public safety and law enforcement efforts. As YITU's client in Malaysia, AFSB is the first security force in the country to integrate body-worn cameras with cutting-edge facial recognition technology.

In line with efforts to enhance the way auxiliary police safeguard the community, infrastructure and assets, AFSB has tapped YITU's facial recognition technology to allow officers to review captured video footage to positively identify persons of interest post-event. Implemented since February 2018, the body-worn cameras are currently in use by auxiliary police officers of AFSB at various critical infrastructure, with plans to increase the roll-out to more locations across Malaysia in the near future. YITU is working with its system integration partner in Malaysia, Build Technology Converge, to deploy the body-worn camera system.

"AFSB is committed to bring constant innovation and forward thinking to the security landscape in Malaysia. This is a significant step forward for us as we leverage artificial intelligence to increase public safety and security. Looking ahead, AFSB also intends to expand the capabilities of our body-worn camera system to include real-time facial recognition and instant alerts to the presence of persons of interest from criminal watchlists," commented Dato' Rosmadi Bin Ghazali, CEO of Auxiliary Force Sdn. Bhd.



Left: Auxiliary Force Sdn. Bhd. showcasing its body-worn camera system integrated with YITU Technology's facial recognition technology at National Security Asia 2018
Right: A mannequin displaying Auxiliary Force Sdn. Bhd.'s body-worn camera used by auxiliary police officers in Malaysia

YITU's facial recognition solutions are currently being used for security at Chinese tourist locations including ports, and public spaces which require high safety standards.

"AFSB leads the way in introducing new security technologies to transform the security landscape in Malaysia," said Lance Wang, YITU Technology's General Manager of Southeast Asia, Hong Kong and Macau. "We are committed to supporting AFSB in their journey to strengthen public security and to become a leading player in the security industry. Our work with AFSB builds on our joint belief that AI technologies will help bring about safer and more secure communities in Malaysia," Wang added.

YITU's state-of-the-art algorithm won first place in the globally-renowned Face Recognition Vendor Test (FVRT) organised by the National Institute of Standards and Technology (NIST) in 2017. It also won the face identification accuracy segment of the Face Recognition Prize Challenge, hosted by the Intelligence Advanced Research Projects Activity (IARPA) in the United States.

The company also opened its first international office in Singapore in January this year to bring its award winning facial recognition and intelligent business solutions to the Southeast Asian, Hong Kong, Macau as well as Oceania markets.

For more information, please visit www.yitutech.sg. SST

Citrix Expands Investment in Channel, Announces New Distributors for ASEAN

Four new distributors appointed in Indonesia, Malaysia, Thailand and Vietnam

Singapore—Citrix announced in April expanded investment in the ASEAN channel ecosystem with the appointment of four new distributors; including Synnex Metrodata in Indonesia, Netpoleon Malaysia in Malaysia, M.Tech in Thailand and VietSunshine JSC in Vietnam. Showing its deep investment in the channel ecosystem, the appointments will grow Citrix's distributor network in ASEAN and help partners in the region to increase the velocity of their business, with greater access to secure workspaces, networking and cloud solutions.

"Responding to our partner's feedback and the growth opportunities in ASEAN, the new appointed distributors will provide a wider coverage in the local markets," said John Lee, Director, Channel, ASEAN, Citrix Systems, Inc. "Each distributor announced today brings unique strengths and experiences to the table that will benefit our channel partners and mutual customers. We look forward to working with the newly appointed distributors to offer more value-added Citrix solutions and services to our ASEAN reseller ecosystem and to reach into new markets."

The four new distributors along with Tech Data, a Citrix's distributor operating across ASEAN, will service the channel in the region. The appointed distributors will provide Citrix's partner ecosystem with increased support in the key focus areas of; secure workspaces, networking and cloud, in addition to more enablement opportunities and expanded access to multi-vendor configurations.

Distributor Quotes

Synnex Metrodata Indonesia (Indonesia)
"We are excited to bring Citrix's solutions and services to our reseller base. Citrix is a strategic partner for us, and their suite of products complements our existing portfolio and will bring expanded opportunities to our resellers and customers" said Li Heng, Commercial Business Director of Synnex Metrodata Indonesia. "With more companies realising the benefits of cloud, we see the potential for digital workspace to redefine the way organisations do their business and we will work closely with our partners to tap into this tremendous opportunity."

Netpoleon Malaysia (Malaysia)
"With today's increasingly complex IT environment, businesses are looking for an integrated workspace that can proactively address security threats across its multi-device, hybrid-and multi-cloud environments," said Lester Song, Netpoleon Sales Director. "Aligned with our robust security practice, Citrix technologies will enable us to equip our resellers with the complete end-to-end portfolio that their customers are looking for."

M.Tech (Thailand)
"We are excited to be Citrix's distribution partner in Thailand. Citrix's technology has been recognised as one of the leaders in delivering the industry's most comprehensive and integrated platform for secure app, data and network delivery," said Stanley Foo, CEO, M.Tech Group. "Citrix's cutting-edge offerings coupled with our value-added approach and mid-market coverage will help to accelerate our Thai partners' business growth for mutual benefits."

VietSunshine JSC (Vietnam)
"Today we are very excited and honored to announce our new strategic partnership with Citrix," said Luong Bui, Technical & Product Director, Vietnam, VietSunshine JSC. "VietSunshine JSC has long been known as the leading ICT Value Added Distributor in Vietnam by bringing innovative technology vendors to the Vietnam market. With Citrix's wide and leading products portfolio and services offering, we believe we will be able to meet the growing customer demand in Vietnam and transform their businesses."

Taiwan Innovators Unveil World's First Security Solutions Poised to Transform Global Security Market

Las Vegas, USA—At ISC West 2018, insights and a first look at cutting-edge products from Taiwan's top innovators—EverFocus, GeoVision, PLANET and VIVOTEK—were the highlights of a recent press conference at ISC West 2018, organised by the Taiwan External Trade Development Council (TAITRA), Taiwan's foremost trade promotion organisation. These breakthrough products, with potential to transform the global security market, include a futuristic Virtual Reality 720° camera, a facial recognition dome camera, a cutting-edge Internet of Vehicle (IoV) fleet surveillance system, an IP camera armed with anti-intrusion software, and a next-gen intuitive color touch LCD switch.

Taiwan Products Launch at ISC West 2018. Speakers from left to right: EverFocus Regional Technical Sales Manager Marques Phillips, TAITRA Executive Director Simon Lai, GeoVision President David Huang, PLANET Sales Manager Tammy Huang and VIVOTEK Director of Marketing and Product Development Shengfu Cheng. (Photo: Business Wire)

"We are proud to showcase Taiwan's finest at one of the United States' most prestigious security tradeshows and look forward to having participants experience the future of security," TAITRA Executive Director Simon Lai said. "Today, the United States and Taiwan enjoy an ever-expanding relationship and extensive engagement in many fields, especially in electronic security. Our products launch event unveiled some of Silicon Island's most cutting-edge products and technologies in the areas of IoT and Internet of Vehicles (IoV), unmanned Security and Cyber + Physical integration. We are proud to showcase Taiwan's finest at one of the United States' most prestigious security tradeshows and look forward to having participants experience the future of security.

These Taiwanese ICT companies, all winners of the Taiwan Excellence Awards, generated a lot of excitement and buzz with the unveiling of their new products at the conference.

1. EverFocus Electronics Corp.
EverFocus demonstrated its engineering and research prowess as Regional Technical Sales Manager Marques Phillips unveiled details of the company's Xfleet Management Platform, which he described as not only transforming the IoV experience, but the future of vehicle fleet management. The new solution allows users to easily track, monitor and manage any type of fleet vehicles on a Web browser anywhere and anytime. With Xfleet, users can not only reduce overall costs by effectively utilising resources such as vehicles, fuel, and manpower, but also improve management efficiency and business performance by keeping and analysing the historical records of the vehicle data as needed.

2. GeoVision, Inc.
GeoVision showed off the VR 360, the world's first Virtual Reality camera that can provide a 720° view. President David Huang said it's the only camera with two Fisheye lenses to provide a floor-to-ceiling, 720° view with no blind spots. It's ideal for security environments such as airports, train stations, city streets, harbors and highways. The camera uses advanced computer vision technology to simulate a three-dimensional, highly realistic, and practical 3D space. It's water-proof, vandal-proof and dust resistant, making it ideal for outdoors. It also boasts IR Night Mode for clear images even in dark environments.

Huang also demonstrated new facial recognition IP dome camera with cutting-edge AI. It can recognise human faces in 1.5 seconds, making possible identification of authorised versus un-authorised personnel, creation of blacklists for restricted personnel, and VIP lists to improve relationship management.

3. PLANET Technology Corp.
PLANET explained how the Intuitive Touch LCD Switch makes it possible to easily manage powered devices in real time, greatly enhancing network management efficiency. Tammy Huang, Sales Manager, noted that it's the unique touch LCD that makes such management possible. In addition to the touch LCD interface, the solution features L2+ switching, intelligent PoE management and an ONVIF support function. An Industrial flat-

type touch LCD switch model is also offered, making possible management of large-scale networks.

4. VIVOTEK, Inc.
With the theme "Security within Security", Shengfu Cheng, Director of Marketing and Product Development, demonstrated the first cybersecurity enhanced network cameras in the IP surveillance industry. The three new cameras are armed with Trend Micro's anti-intrusion software, allowing them to automatically detect and prevent credential attacks and block suspicious events. They also feature VIVOTEK's Smart Stream II and H.265 technology, allowing users to benefit from reduced bandwidth and data storage demands by up to 90% more than systems employing H.264. Add to that a new generation of night visibility technology, Supreme Night Visibility II (SNV II), which allows them to reproduce high-quality color images, even in very low-light conditions.

In the security industry, the United States is the largest buyer of electronic security products and spent $12.3 billion on imports in the field in 2016. And Taiwan constitutes North America's 4th largest trade partner in the electronic security field, with an import value that was close to $1 billion in 2016.

Throughout ISC West 2018, Taiwan exhibitors presented their latest innovations. In pursuit of Asia's Silicon Valley vision of propelling Taiwan to the international forefront of technology, Taiwanese companies continue their pursuit of excellence and innovation. SST

Surveon Videos Keep Recording Continuously with Failover Solutions

New Taipei City, Taiwan—More and more problems such as conflicts and burglaries rely on the evidence of recording videos. Most applications thus require a stable surveillance system to keep recording videos continuously. Surveon Failover solutions have been deployed in public hospitals in Asia and the server rooms of internet service providers (ISPs), providing reliable methods to record videos.

Distinct from the usual Failover mechanism where Failover NVR can be used for failover purposes only, Surveon offers unique Peer Mode that supports mutual failover (one-on-one or multiple to multiple) among NVRs. This failover working model allows the system to record continuously for long time. Without having to set aside spare NVR or failover licenses, Surveon Failover solutions allows the licence of camera to be shared with the Failover ones, making it a superior C/P solution for projects with limited budgets.

If the protected server fails, the failover server will seamlessly clone the configurations and take over its recording work.

Catering to different vertical applications, Surveon offers a variety of failover solutions, not only in Peer Mode, but also in Dedicated Mode. The Failover NVR shares the same file space as protected NVR whether or not it is working, resulting in the protected NVR's video being recorded and saved to the same location once it has been taken over by Failover NVR, giving partners many options for their projects.

Surveon Failover solutions keeps the public hospital's surveillance intact. The Peer Mode supports mutual failover between two NVRs. If one of the NVRs fails, the other NVR will take over recording and save the failed NVR's videos to its internal storage. For the ISP that has adopted Surveon Failover solution as well, the Dedicated Mode makes a Failover NVR take over recording when protected NVR fails, keeping it safe in the server room of the ISP.

For more information, please visit: www.surveon.com. SST

Dahua Technology Enriches ePoE IP System

After introducing its ePoE (extended Power over Ethernet) IP system in in July of 2017, Dahua Technology, a leading solution provider in the global video surveillance industry, has extended ePoE technology to more products, including full range of network cameras with wide selection of form factors, 16/32/64 channel network recorders and 4/8/16/24 port network switches. The newly enriched ePoE IP system enables Dahua customers and partners to reduce costs and embrace more business opportunities.

ePoE IP System

These are the products that are equipped with ePoE technology:

Category	Model		
Eco IPC	IPC-HF5431E-E	IPC-HF5231E-E	IPC-HFW5831E-ZE/Z5E
	IPC-HFW5631E-ZE/Z5E	IPC-HFW5431E-ZE/Z5E	IPC-HFW5231E-ZE/Z5E/Z12E
	HDBW5831E-ZE/Z5E	HDBW5631E-ZE/Z5E	HDBW5431E-ZE/Z5E
	IPC-HDBW5231E-ZE/Z5E	IPC-HFW4831E-SE	IPC-HFW4631E-SE
	IPC-HFW4431E-SE	IPC-HFW4231E-SE	IPC-HFW4831T-ASE
	IPC-HFW4631T-ASE	IPC-HFW4431T-ASE	IPC-HFW4231T-ASE
	IPC-HDBW4831E-ASE	IPC-HDBW4631E-ASE	IPC-HDBW4431E-ASE
	IPC-HDBW4231E-ASE	IPC-HDW4831EM-ASE	IPC-HDW4631EM-ASE
	IPC-HDW4431EM-ASE	IPC-HDW4231EM-ASE	
Ultra IPC	IPC-HF81230E-E	IPC-HF8630F-E	IPC-HF8331F-E
	IPC-HF8232F-E	IPC-HF8231F-E	IPC-HFW81230E-ZE
	IPC-HFW8630E-ZE	IPC-HFW8331E-ZE/Z5E	IPC-HFW8232E-ZE
	IPC-HFW8231E-ZE/Z5E	IPC-HDBW81230E-ZE	IPC-HDBW8630E-ZE
	IPC-HDBW8331E-ZE/Z5E	IPC-HDBW8232E-ZE	IPC-HDBW8231E-ZE/Z5E
NVR	NVR5816-16P-4KS2E	NVR5832-16P-4KS2E	NVR5864-16P-4KS2E
	NVR5464-16P-4KS2E	NVR5432-16P-4KS2E	NVR5416-16P-4KS2E
	NVR5232-16P-4KS2E	NVR5216-16P-4KS2E	NVR5208-8P-4KS2E
	NVR5216-8P-4KS2E		
Switch	PFL2106-4ET-96	LR2110-8ET-120	LR2218-16ET-240
	LR2226-24ET-360		
Accesory	LR1002		

**LR2110-8ET-120, LR2218-16ET-240 & LR2226-24ET-360 will be released very soon.*

Product Features

Dahua ePoE IP system delivers transmission of up to 800 metres between ePoE camera and ePoE network switch or ePoE NVR at 10Mbps & 13W or 300m @ 100Mbps & 25.5W. It overcomes the limitation of traditional Ethernet and PoE (both restrict cable distances to 100 metres between network ports) and eliminates the need for Ethernet extension devices or additional network switches. Moreover, according to testing results, the ePoE IP system will not increase the transmission delay or package loss rate compared to traditional IP systems.

Application Scenarios

For surveillance of large spaces such as large warehouses, parks and outdoor parking, cameras are usually over 100 metres away from the control center. Conventional approaches, such as adding repeater devices and fiber optics, increase equipment and installation costs and complicated systems. Dahua ePoE IP system, with 300-metre transmission at 100Mbit/s via network cable and only one cable required to connect front-ends and back-ends, offers a simple, cost-effective and reliable solution.

A proper solution to migrate analog surveillance system to IP needs to adapt the IP video signal and RJ45 connection to coaxial cable, support the length of coaxial cable and transmit power over coaxial cable. Dahua ePoE IP system uses PoC Extender LR1002

to connect Ethernet port of IP camera or network switch on the one end and BNC connector of coaxial cable on the other, supports up to 1,000-metres transmission over coaxial cable at 10Mbit/s, and delivers PoE power to IP cameras. This is a simple and effective solution that significantly reduces the cost of analog-to-IP migration.

The enriched Dahua ePoE IP system, which will be on display in IFSEC International 2018 during from 19 to 21 June, offers a better way to accomplish long-distance transmission between IP cameras and network switches or recorders and allows more flexible system design, improves reliability and saves construction and wiring cost. With a mission of "enabling a safer society and smarter living", Dahua will continue to focus on "innovation, quality and service" to its partners and customers globally.

For more information, please visit: http://www.dahuasecurity.com SST

Eyeris Recognised as Finalist for Human Behavior Understanding AI at 2018 TU-Automotive Awards

Eyeris in-cabin vision AI software suite enhances safety, comfort and convenience through multimodal analysis of occupants' complex visual behaviour inside autonomous and highly-automated vehicles

Eyeris, a world pioneer and leader in deep learning-based vision AI software for face analytics, emotion recognition, body pose, and human action and activity recognition for the automotive industry, today announced that it has been honoured as a 2018 TU-Automotive Awards finalist in two categories for Best Auto Mobility Product or Service and Best Connected Product or Service. The TU-Automotive Awards are a highly-regarded recognition of excellence, innovative technology, and leadership in the connected car industry. The winners will be announced at the TU-Automotive Awards ceremony on 5 June 2018 in Detroit, Michigan.

This is the fourth consecutive year that Eyeris has been recognised as a finalist in the TU-Automotive Awards, including winning the Award for Best Connected Product or Service for the Commercial Market in 2017. Finalists are carefully selected by a panel of expert judges from the automotive industry based on four criteria: innovation, industry engagement, user experience, and market updates.

Eyeris offers the following new applications with its Human Behavior Understanding AI:

- **Safety:** Eyeris Driver Monitoring AI augments advanced driver assistance systems (ADAS), enhances seamless human-machine interface (HMI) and enables safe transition between different levels of autonomy.
- **Comfort:** Eyeris Occupants Monitoring AI offers in-cabin ambient intelligence and dynamic interior configurations such as lighting, seating, controls, etc.
- **Productivity:** Eyeris HBU AI enables mobility-as-a-service providers with hyper-targeted demographics and unique qualitative behaviour insights.

"We're certain that human-centered interior vision AI will be ground-breaking in defining the future of a safer, more dynamic mobility in this new consumer space," said Eyeris Founder and Chief Executive Officer Modar Alaoui.

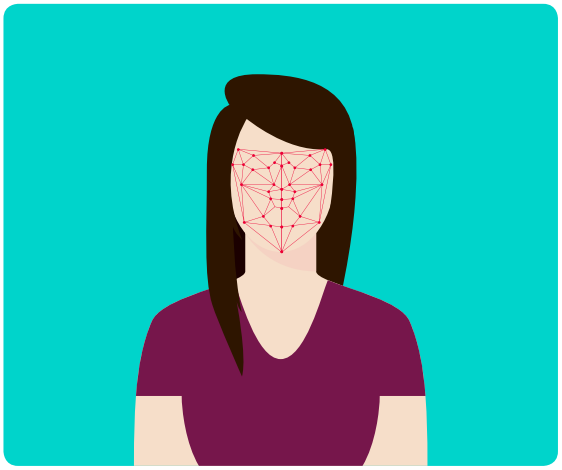
"Additionally, we are excited that with the convergence of our comprehensive 2D-based face and body reading AI, Eyeris has the final critical piece of the ADAS puzzle to achieve the level of safety consumers and regulators expect from highly-automated vehicles,"commented Glen Carroll, Eyeris Chief Operating Officer.

Eyeris in-cabin vision AI solutions have been adopted by Toyota Motor Corporation, Jaguar Land Rover, Bosch, Honda Motor Co., Mitsubishi Motors Corporation, and Toyota Research Institute. Eyeris expects to go into vehicle mass production in 2019. SST

Facial Recognition Cameras Keep an Eye on Chinese Students

It's not so easy to take a nap in these new smart classrooms

Recently, there has been more than one pair of eyes in some classrooms in the 11th middle school in Hangzhou, the capital of the eastern province of Zhejiang. Three facial recognition cameras mounted above the blackboard in the classroom keep an eye on teachers and students throughout the day.



The country's first "Smart Classroom Behaviour Management System" was developed by Hikivision Digital Technology, one of China's biggest suppliers of security cameras and AI technology.

Facial recognitions tools are increasingly being used in China for more and more everyday security tasks, such as verifying payments, catching shoplifters and criminals, as well as recording faces at large-scale entertainment events.

At the Hangzhou school, a combination of three cameras keep track of students' attendance, analyse their behaviour and facial expressions, and provide feedback on their any abnormal conduct. The camera analyses and assigns values to facial emotions such as neutrality, happiness, sadness, dislike and surprise. If the inattentive behaviour reaches a certain value, the system's screen will display a real-time reminder, and the teacher can then correct the student's behaviour.

"The surveillance cameras are like a teaching assistant for teachers, and can improve the interaction between teachers and students," said the principal, Ni Ziyuan.

Some have raised concerns about the students' privacy issues. "Is this a concentration camp? They are kids, not the target of dictatorship," wrote one person on the Weibo social media platform. But the principal assured the public that the system only collects behavioural information and does not perform video recording in class. SST

Huawei Launches eLTE Multimedia Critical Communications System

eLTE Enables Comprehensive Awareness, Multi-Service Collaboration and Dispatching Everywhere and Anywhere

Huawei launched has its eLTE Multimedia Critical Communications System (eLTE MCCS) at Critical Communications World 2018. eLTE MCCS is an end-to-end solution equipped with ultra-reliable multimedia communications capabilities tailored for the public safety sector. Bringing together platforms, networks and terminals to achieve comprehensive awareness of situations, multi-service collaboration and capabilities enabling dispatching anywhere

as required, Huawei envisions that this solution will "help the public safety sector make every corner of our world a safer place to live in".

Dynamic development of ICT technologies supporting multimedia functions like transmission of voice, images and video, and real-time global positioning across an array of mobile apps has transformed the way people live through their smartphones and wireless technologies by making everyday activities such as shopping, dining, commuting and even accommodation arrangements more convenient than ever. But even as society has become more efficient, specialised domains such as public safety have lagged in the development of technology and apps and continue to rely on narrowband networks that essentially provide little more than voice, thus limiting response time, efficiency and decision-making precision in city management, incident management, emergency response and disaster relief.

eLTE MCCS enables creation of a unified service and closing of technological gaps by interconnecting narrowband systems, video surveillance and GIS systems through a mobile service convergence platform. This platform would enable gradual phasing out of existing narrowband networks and upgrading to new networks while maintaining provision of services and protecting the investments customers have already made in narrowband networks.

In consideration of the different conditions customers operate under, eLTE MCCS provides differentiated network products that meet different standards such as those by 3GPP, ITU and MulteFire. The solution also encompasses various series of terminals and equipment designed to be used for voice and video by individuals and on cars, motorbikes and others, covering the diverse scenarios in the public safety sector.

Eric Sun, President of Enterprise Wireless Business at Huawei, said, "eLTE MCCS has added value to services on three levels—Dispatching Anywhere, Comprehensive Awareness and Multi-service Collaboration—through its scenario-based design of platforms, networks and terminals."

eLTE MCCS launch ceremony at Critical Communications World 2018

But even as society has become more efficient, specialised domains such as public safety have lagged in the development of technology and apps and continue to rely on narrowband networks that essentially provide little more than voice.

eLTE MCCS' Dispatching Anywhere capability provides ubiquitous multimedia dispatching of voice, video and data that allows streamlining of the last kilometre in police cloud operations, enabling smart policing, and the agile use of resources such as police cloud video and data.

The Comprehensive Awareness product series includes equipment used by individual police officers, vehicle-mounted equipment, mobile control cameras, drones, IoT sensors and others gear that helps achieve comprehensive awareness of situations and a system of safeguards comprising voice, video and data. Synergising mobile video cloud, fixed video cloud and public social networks allows prediction of safety hazards rather than mere prevention, increases deterrence, raises efficiency and provides trustable multimedia evidence for law enforcement. The Multi-Service Collaboration solution makes smooth connections among public communications networks and current narrowband trunking systems (such as P25/Tetra/DMR) possible, safeguards installed base assets and allows convergence of data across different networks. With eLTE MCCS, data no longer needs to be exchanged between officers repeatedly; instead, a one-off exchange with the system will suffice. This simplifies the work of the police and raises the efficiency of collaboration.

By year-end 2017, Huawei cemented its position as one of the world's major players in private broadband networks with its eLTE critical communications solution successfully deployed on 233 public safety broadband networks worldwide. SST

Siemens drives digital transformation in buildings with acquisition of Enlighted

Siemens Building Technologies Division is acquiring Enlighted Inc., a leading provider of smart IoT (Internet of Things) systems in buildings, headquartered in the Silicon Valley. The company is a successful player in the smart building industry, bringing an advanced digital sensory system to market. Both parties have agreed not to disclose financial details. Closing is expected in the third quarter of 2018. Enlighted will be managed as an independent legal entity and wholly-owned subsidiary of Siemens Industry, Inc.

"Enlighted has a strong footprint in revolutionising building intelligence by developing a multi-sensor-based IoT platform, using the power of data," said Matthias Rebellius, CEO of Siemens Building Technologies. "With this move, we are demonstrating our commitment to drive digitalisation in the smart building industry."

Enlighted achieved its technological leadership with a world-class IoT platform for commercial real estate. The platform consists of multi-function sensors, distributed computing, its own network, and software applications. The beating heart of Enlighted's platform are smart sensors, securely streaming data to the cloud. In addition, the platform enables reduced energy use, improved space utilisation, better environmental management and greater asset utilisation.

"With Siemens as a global partner, we will both accelerate innovation and market adoption of our smart building technologies on an international scale," said Joe Costello, Chairman and CEO of Enlighted Inc.

Enlighted analyses and visualises the collected sensor data to drive down operating costs and improve the inner life of a building. These sensors can be installed in every light fixture with the ability to collect data 65 times per second to detect environmental and occupancy changes and react to lighting and HVAC (heating, ventilation, air conditioning) needs in real-time. Based on an advanced smart lighting control application, today, the Enlighted platform can lower lighting costs of a building up to 85 percent when combined with advanced LED fixtures. In addition, the platform is able to locate people and assets within a building and analyse the occupancy of floors and rooms. Finally, in combination with Siemens solutions, the Enlighted platform can optimise the energy efficiency of HVAC systems.

The interaction between buildings and humans is crucial to increase productivity, energy efficiency and comfort in a building. From its inception, Enlighted has been focused on understanding how buildings can be made more efficient and the people who work in them more productive. Enlighted's smart IoT platform with a digital sensory system applicable in any light fixture is a core element of revolutionising building intelligence by enhancing the dialogue between humans and buildings.

For further information, please visit: www.siemens.com/buildingtechnologies SST

Anti-theft sticker protects valuables without revealing their location

VTT Technical Research Centre of Finland and Streamr have developed a prototype adhesive ID tag based on blockchain technology, which enables valuable goods to be protected without revealing their location. Possible applications include electronics, jewellery and caviar.

The tag developed by Streamr and VTT is based on a smart contract, using blockchain technology, between the owner of the goods and the transport company. The contract defines the terms and conditions of transportation and storage, and the fee. For the purpose of monitoring the terms of the smart contract, a range of smart sensors are embedded in the tag which identify issues such as the location, acceleration and temperature. Parties previously unknown to each other can use blockchain technology to co-produce and maintain databases in a decentralised and reliable manner.

For example, the owner of the product cannot see accurate transport information on the goods unless the terms are violated. Data is processed either in encrypted form or managed by a third party, such as Streamr, which provides platform data and smart contracts for presentation and processing.

"In the future, there will be more demand for online applications of this kind, which ease everyday life based on decentralised technology and smart contracts. Similar systems have already been tested for the needs of the healthcare sector," says Research Scientist Visa Vallivaara of VTT.

The product concept was developed as part of the Towards Digital Paradise project funded by Tekes—now Business Finland—with VTT investing in the smart contract logic and ID tag. It was based on Tekes' major strategic research breakthrough, The Naked Approach, which explores the embedding of digitalisation and user interfaces in our everyday environment. Tampere University of Technology, Aalto University, the University of Oulu, the University of Lapland, Demos Helsinki, Nokia, Skandal Technologies, Nextfloor, Premix Oy and Napapiiri Hub are involved in the project alongside VTT and Streamr.

Tomorrow's safe and secure society demands means and tools to detect, prevent and recover from incidents. VTT envisages and develops technologies and systemic models for comprehensive safety and security. Solutions to counter threats provide opportunities for trouble-free life and business.

"The anti-theft sticker is a prime example of the importance of applied research and of the collaborative approach to developing new innovations. Streamr's ability to integrate and visualise smart contracts and real-time data combined with VTT's technology and blockchain expertise form an outstanding combination," says VTT's Tua Huomo, EVP of Knowledge Intensive Products and Services.

The anti-theft sticker should be ready this autumn. A prototype was presented for the first time at the Consensus Event for blockchain operators from 14 to 16 May in New York. SST

TBS Biometrics Introduces a Unique Device in the Field of Iris and Face Detection

Combining the best of both worlds of both eye and face detection

TBS Biometrics has introduced a revolutionary reader featuring combined iris algorithm and face detection. Its distinctiveness comes from the combination of eye and face detection that gives it an even more robust accuracy. The sensor captures the iris of both eyes while the face sensor is used to automatically distinguish the height of the users and other details.

All biometric devices have their advantages and limitations. Where popular face recognition still struggles is with high accuracy; however, it is very intuitive and simple to use. Iris recognition is extremely accurate but still not user-friendly.

The TBS 2D Eye overcomes limitations by combining the best of both worlds. Its face detection interaction is most convenient for users, while its iris-based identification guarantees highest levels of accuracy delivered by modern technology. For even further user comfort, the reader adjusts itself automatically to the height of users. Additionally, the 2D EYE allows multi-modal identification by PIN and RFID.

The 2D Eye is part of the TBS Ecosystem and manufactured by CMITech, a leader in the biometric Iris industry. All TBS Ecosystem products comply with TBS quality standards while developed by a third-party manufacturer and fully integrated by TBS R&D within the powerful TBS Biometric subsystems (web based software/server with biometric core). It adds an additional masterpiece to one of the most complete biometric portfolios.

Where popular face recognition still struggles is with high accuracy; however, it is very intuitive and simple to use. Iris recognition is extremely accurate but still not user-friendly.

With a sleek and attractive design, its screen allows for a great deal of interactivity, customisation and, notably, gives the opportunity for the user to see themselves during capture process, similar to facial recognition. Pilot users acclaimed the exceptionally comfortable experience as opposed to traditional iris-based technologies. This has established that the 2D Eye meets the expectations from the users for a "touchless", convenient and rapid identification.

From corporate offices to airports, government to healthcare, research centres and critical infrastructures, the TBS 2D Eye will be the right solution where security is paramount. With the 2D Eye, TBS is even more at the forefront of integrated biometric solutions. Two touchless biometric sensors and four different touch-based fingerprint sensor technologies complete a compelling portfolio at the disposal of countless system integrators to provide seamless biometric solutions for access control and attendance. TBS, Secure by Nature.

For more information, please visit:
www.tbs-biometrics.com SST

Face, Iris and Pulse Sensors on the Fast Track

Consumer Fingerprint Shipments Surpass 1 Billion Shipments but End-Users Ready to Adopt Multimodality

The battle for the future of biometric modalities in consumer electronics is expected to become fiercer with each passing year as face and iris recognition are continuously gaining strength, threating to soon cannibalise on fingerprint technologies. ABI Research, a market-foresight advisory firm providing strategic guidance on the most compelling transformative technologies, posits that as ASPs for iris modules drop, and the once-timid face recognition is continuously honed with more sophisticated machine learning algorithms, they will both slowly start to eat away at fingerprint implementations.

Apple's choice to forego fingerprints and focus on face recognition for the iPhone X and Samsung's choice to focus on iris recognition for the Galaxy S8 and S9 have fast-tracked this realisation. However, fingerprint technologies won't go down without a fight as multiple innovative vendors including FPC, Qualcomm, Synaptics and Goodix introduce more robust, spoof-resistant sensors and a brand new "poster-boy" for fingerprints: the invisible, under-display sensor.

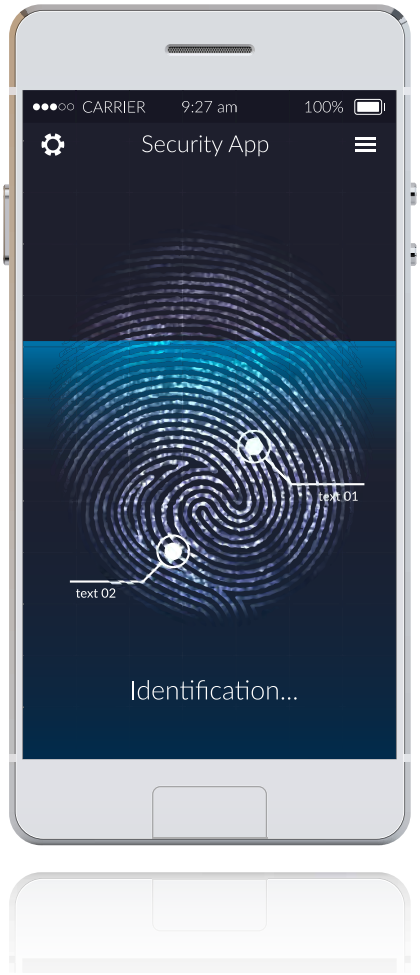
"Even though fingerprint sensor ASPs have taken a significant hit over the last couple of years, total fingerprint sensor shipments for the entire consumer market is still estimated to reach 1.2 billion worldwide for 2018, thus ensuring its market dominance," comments Dimitrios Pavlakis, Industry Analyst for ABI Research. "However, from established markets such as banking and payments to emerging ones like automotive and future-looking ones including robotics, we expect to see an increase in multi-modal applications and a scenario where biometrics is a critical component of a user's digital ID in the emerging IoT ecosystem."

"Even though fingerprint sensor ASPs have taken a significant hit over the last couple of years, total fingerprint sensor shipments for the entire consumer market is still estimated to reach 1.2 billion worldwide for 2018, thus ensuring its market dominance."

With the rise of card-less biometric ATMs developed by Diebold Nixdorf and Samsung, automotive investments by major car OEMs like GM, Nissan, BMW and Volvo, and governmental mandates in APAC seeking to expand biometrics further into banking, consumer, and telecoms, the single-modality pattern will shift radically.

"Multimodal user authentication in the Internet of Things will not be another gimmicky option—it will be the security norm," concludes Pavlakis. Established vendors are advised to plan accordingly and expand their biometric portfolio depending on the choice of market vertical.

These findings are from ABI Research's Biometric Technologies and Applications report. This report is part of the company's Digital Security research service, which includes research, data, and Executive Foresights. SST



Created by Macrovector - Freepik.com

a&s Security 50 Announces AI as Top Trending Technology of the Year

by the asmag.com team

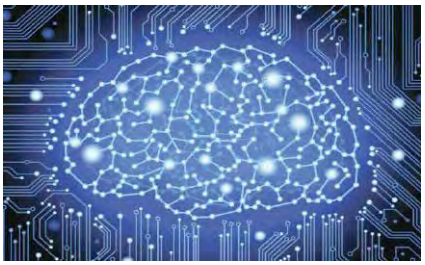
According to global security online platform asmag.com, the biggest trend and topic seen in the security industry this year is definitely artificial intelligence (AI) and deep learning. This year's Security 50 companies (the top 50 companies that either have the largest market share in the global market or the highest product shipment to its global partners) are embracing the growth opportunity in AI.

Jimmy Park, Senior Director of Strategic Product Management Team at Hanwha Techwin, revealed: "We are currently working on optimising Al technology for camera, recorder and VMS. We set scenarios in order to implement optimised functions for each vertical market as well as to reflect user-requested functions. When high-performance AI technology is applied, various functions can be practiced and utilised throughout all vertical areas with less expected errors and fail results."

AI-powered analytics

"Deep learning-powered analytics were a major trend which received a lot of interest and marketing activity this year. Increasingly vendors are launching smart network cameras and recorders with embedded deep learning capabilities," said Josh Woodhouse, Senior Analyst for Video Surveillance at IHS Markit.

"The next step in video analytics is to dive deeper to gain very specific insights into video content, including analysing human behaviour through the use of neural network video analysis. Video will not only be used to track the usual movement of cars and people or detect



items left behind, but will also be relied on more frequently to bring behaviours of interest to the attention of security personnel," said Jammy DeSousa, Senior Product Manager for Security Products for Building Technologies and Solutions at Johnson Controls.

Facial recognition applications

"Our facial recognition solution uses AI and deep learning. The ability to harness this technology has led to increasing performance levels and accuracy of detection for this solution and we are looking at ways to include this in our other technologies," said Marie Clutterbuck, CMO of Digital Barriers.

One company that has achieved a lot of success with facial recognition is China-based Videopark Technology, which has a strong focus on the banking industry. "Our facial recognition has passed tests by public safety and other agencies. We are one of the industry pioneers to roll out the facial recognition-supported NVR, as well as the ATM smart alert DVR. Our ATM smart alert system currently sees the most applications in China," said Luo Jun, Director and VP of Videopark Technology.

"One area we're focusing on is traffic where we're are giving those kinds of solutions supported with license plate recognition. We are also using it in the enterprise segment, giving enterprise-level solutions for visitor management. They are also using facial recognition from a deep learning perspective, receiving an alert when somebody is coming," said Yogesh Dutta, COO of CP PLUS.

Avigilon, which has put a strong emphasis on AI, explains how it can help solve some of the challenges and difficulties facing users. "Through the power of AI, we've developed technology that better focuses human attention on what matters most — enabling users to answer the critical who, what, where and when of an investigation with decisive action. For instance, innovative new technology like Avigilon Appearance Search technology, a sophisticated deep learning AI search engine that sorts through hours of footage with ease, allows users to quickly locate a specific person or vehicle of interest across all cameras on an entire site," said Willem Ryan, VP of Global Marketing and Communications at Avigilon. "Our technology will make searching for a person as easy as searching the internet."

Broader perspective

Johan Paulsson, CTO of Communications, meanwhile, has a broader perspective on this. "The surveillance industry has a history of sometimes overpromising with video analytics, and we are especially conscious of that when it comes to deep learning. We think deep learning has to mature further before it is ready for market in a broader perspective." SST

Global Emotion Detection & Recognition Market to Grow at a CAGR of 32.7% between 2018 and 2023

The global emotion detection & recognition market is estimated to witness a CAGR of 32.7% over the forecast period (2018-2023), driving the market to reach 24.74 billion by 2020. This is according to a recent report by ResearchAndMarkets.com, "Global Emotion Detection and Recognition Market—Segmented by Software and Services, End-user Vertical and Geography—Growth, Trends and Forecasts (2018–2023)".

The increasing demand for wearable devices and increasing penetration of Internet of Things (IoT) are the major determinants of the growth of the global EDR solutions market. Countries, such as China, India, Japan, and South Korea, which have a massive population, are putting extra efforts to implement EDR technology to meet the growing expectations.

Growing adoption of wearable devices, which include smart watches, fitness bands, smart glasses and smart textiles, will enable the growth of the EDR market over the forecast period. The usage of these devices has witnessed high growth rate in the past few years. According to Consumer Technology Association, the global shipments of smart watches have almost doubled from 38 million in 2016 to 75 million in 2017. High investments in the industry and large industry collaborations are resulting in innovations in wearable technology.

These wearable devices are equipped with biological sensors to monitor heartbeat and temperature, along with other components, such as microphones and cameras to capture human emotions, such as gestures, body postures, tone of voice, and facial expressions. Wearable devices continuously collect data from these sources and analyse the data to monitor health and other aspects of the user. Thus, the growing number of wearable devices is expected to drive the growth of the market over the coming years.

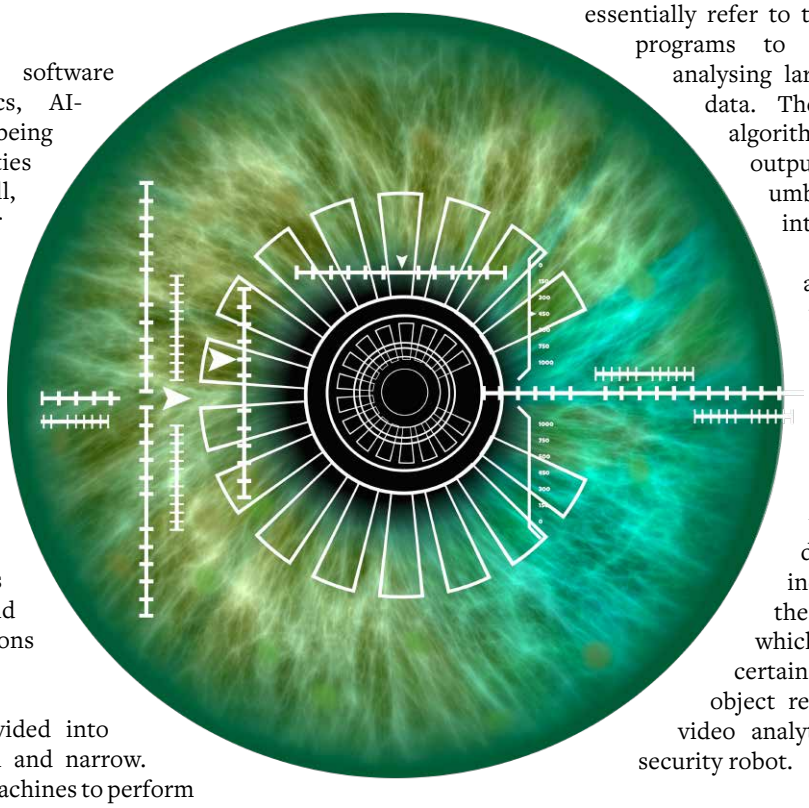
The government sector is expected to dominate the market landscape. SST

Artificial Intelligence Video Analytics Facial Recognition Biometrics and the Quest for Improved Security

►► *By Steve Reinharz, President and CEO, Robotic Assistance Devices*

Artificial intelligence (AI) is a continuation of the ongoing drive toward automation to make our lives easier and has become a part of our everyday lives in the form of social networks, Internet searches, Siri, Alexa, Google and other solutions. Without a doubt, we are living in the Age of AI, and the technology is advancing rapidly and has created fundamental and beneficial changes in human life.

From navigational software to advanced analytics, AI-based technology is being used in many capacities for security as well, and as this smarter technology becomes more mainstream, its use will only grow. We've seen AI usage in diagnostic applications within the healthcare industry and in the emergence of self-driving cars, and with the growth experienced in these areas, it's become hard to avoid AI's massive implications around the world.



AI can be roughly divided into two categories: general and narrow. General AI can enable machines to perform tasks at and beyond the quality of general human performance. But when it comes to security, the technology being developed falls under the category of narrow AI: focusing on executing certain defined tasks, such as object recognition in the case of video analytics or navigation for a security robot.

Defining AI and its Role in Security

By now, most people have at least read about or have some kind of vague idea about what AI is, but there is also a lot of confusion about some of the various terms that are used in conjunction with it. Among these include: machine learning, deep learning, neural networks, etc. All of these terms essentially refer to the capability of software programs to recognise patterns by analysing large amounts of collected data. These pattern recognition algorithms all produce an output that falls under the umbrella category of artificial intelligence.

And while the aforementioned science-fiction movies all deal with ideas surrounding general AI, which involves machines being able to perform any intellectual task that a human could, the technology being developed for the security industry would fall under the category of narrow AI, which focuses on executing certain defined tasks, such as object recognition in the case of video analytics or navigation for a security robot.

Video Analytics, Facial Recognition and Biometrics

Video analytics will be one of the first major domains within the security industry that will be radically transformed by AI. The rules-based analytics of old, such as virtual tripwire,

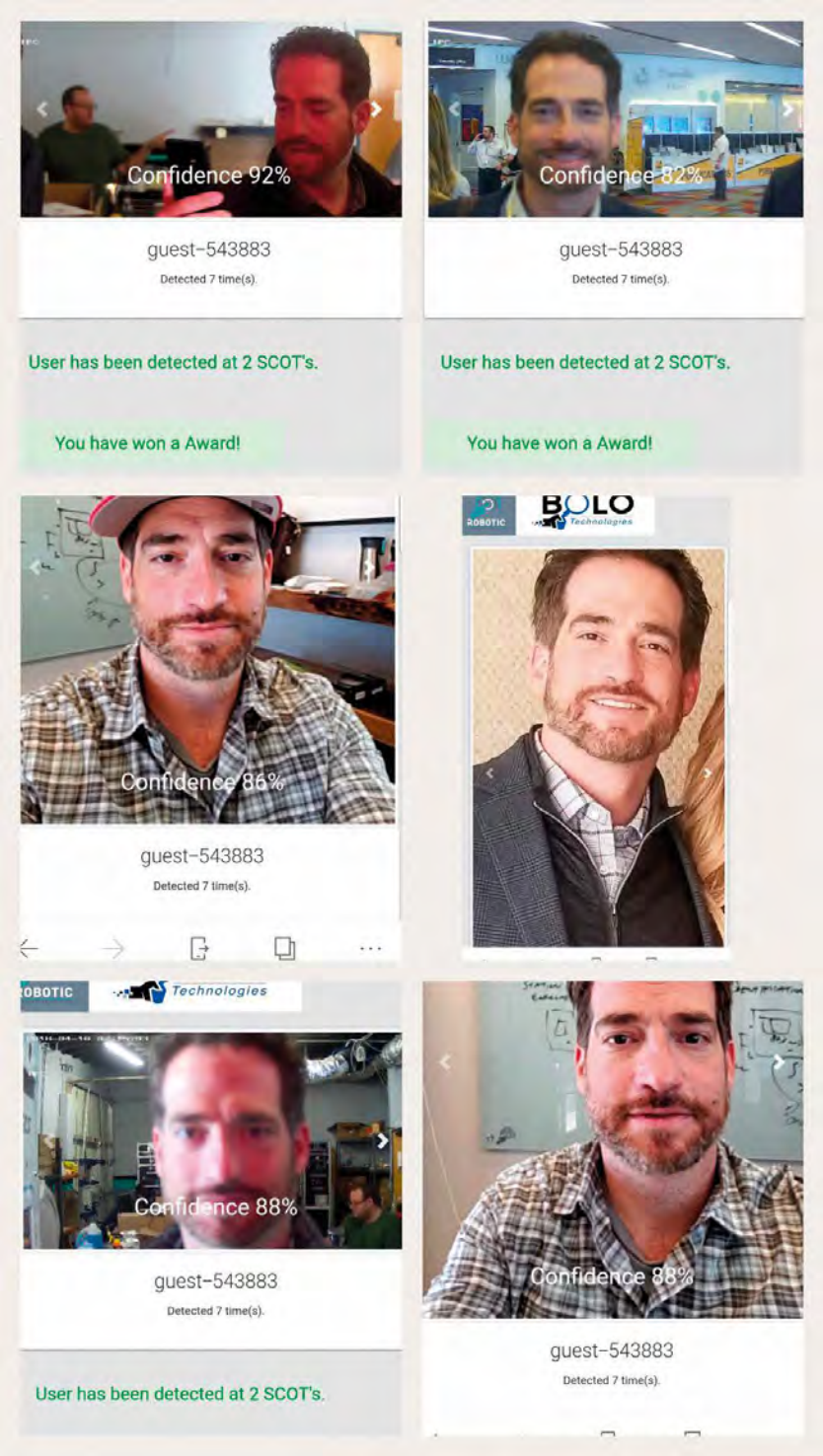
Technology is taking the next steps in developing portable AI-based solutions to identify issues before they arise, like the Robotic Assistance Devices Security and Observation Tower (SCOT).

Video can be used in new and unique ways to aid officers in investigations.

SCOT watches over large-scale businesses to protect them from threats, using advanced analytics and AI-based functionality.

wrong-way motion detection and object left behind, will soon be rendered obsolete by AI, which completely eliminates the need for pre-programmed algorithms. In fact, sensor technology available today can capture an amount of metadata on people in real time, including their identity, gender and age. With such capabilities already within reach, the video analytics of tomorrow will be able to do much more than just alert users when a person, animal or vehicle has crossed an invisible barrier.

With regards to video data being collected by an end user, AI makes it possible to administer facial recognition—that is, a technology capable of identifying or verifying a person from a digital image or a video frame from a video source. Where this becomes especially helpful is in identifying persons of interest in incidents of fraud or theft. Repeat offenders, once identified through facial recognition software, can be placed on a designated watch list using this kind of AI-



Facial recognition software is emerging as a method to use artificial intelligence to identify persons of interest in the event of an incident.

based software so that if they re-offend, security teams can be notified. The embedded intelligence in the software makes this possible. And this is just one use case. There are many others that have been proven effective in security and beyond.

Biometrics is another area of security where AI can be helpful. Biometric authentication is used as part of access control systems as an added control on the basic premise that human characteristics of an individual are unique and therefore able to be used access to authenticate identification. Biometrics include fingerprint identification, as well as iris recognition—that is, using your eyeballs for identification. Iris recognition uses mathematical pattern-recognition techniques on video images of one or both of the irises of an individual's eyes, whose complex patterns are unique, stable and can be seen from some distance. This and other methods of biometric access result in added protection for critical and sensitive information and locations.

The Future of AI

As AI grows in scope and becomes more mainstream in practice, so too does the applicability it has in the security industry. At this point, the sky is the limit as more and more manufacturers begin to harness the power of AI to effectively make decisions related to the safety of people and assets from threats.

It's clear that AI provides end users and security professionals with a wealth of advantages when it comes to increasing operational efficiencies, proactively identifying risks and ensuring informed, rapid responses to security incidents. While nothing can substitute human-to-human interaction, combining AI-enhanced technology with traditional security measures can radically improve functionality and help organisations reach their security goals. SST

About the Author:
Steve Reinharz is the President and CEO of Robotic Assistance Devices (RAD), where he oversees the development, sales and marketing, and strategic vision for the company. Reinharz has more than 20 years of experience in various facets of the high-tech industry. Reinharz is a native of Toronto, Ontario, Canada, and attended the University of Western Ontario, where he earned dual Bachelor of Science degrees in political science and commercial studies. Follow him on Twitter @SteveReinharz.

Did you know?

The world's largest Internet retailer, Amazon, has been urged by the American Civil Liberties Union and other privacy advocates not to sell its powerful facial recognition tool, Rekognition, to law enforcement agencies. Privacy advocates are afraid that the tech giant's reach could vastly accelerate a dystopian future in which camera-equipped officers can identify and track people in real time, whether they're involved in crimes or not.

Police in China have nabbed three fugitives using facial-recognition technology at a series of concerts in Eastern China at performances by Hong Kong pop star Jacky Cheung, also known by his nickname, "the God of Songs", police were able to use facial recognition technology to a 31-year-old man in a crowd of 60,000 concertgoers, according to state media. At another concert, the technology recognised a man who had allegedly failed to pay for USD17,000 worth of potatoes in 2015 and had since then been living under a pseudonym. The state media claims that the technology is accurate 99.8 percent of the time, although Advocacy groups like Human Rights Watch having been flagging China's use of facial recognition systems as a flagrant abuse of its citizens' privacy.

Your next bank card could have a built-in fingerprint scanner. Mastercard says it is ready to issue thousands of biometric bank cards as its fingerprint scanners can be used everywhere. "A four-digit PIN is pretty good security—obviously, six, seven or eight digits are better, but it is very hard for people to remember," says Bob Reany, an executive vice president at Mastercard, who is working on the firm's biometric cards. "The security is going to be better than a PIN."

The Yale School of Medicine is reducing physician fatigue by using voice recognition, so that doctors can spend less time typing on a computer, and more time with patients. The move has saved physicians between six and 20 minutes daily—that's about 20 to 140 logins per physician each day.

According to a new market research report published by MarketsandMarkets, *the fingerprint sensor market is expected to grow from USD4.25 billion in 2018 to USD8.80 billion by 2023, at a CAGR of 15.66 per cent. The growth of this market is mainly driven by factors such as the proliferation of fingerprint sensors in smartphones and other consumer electronics, government support for the adoption of fingerprint sensors, and use of biometrics in mobile commerce.*

Pixel comparison can be the future of AI in detecting mood patterns. *Researchers can make sense of the microexpressions on a facial image using the pixel comparison method. The geometrical alignment in this method leads to create a meaningful correspondence at the level of pixels. It also removes the problem of expression-variation and pose-variation. Research studies have corroborated this concept showing that mood pattern recognition improved using this method. The method of pixel comparison for detecting the mood in a person is currently still a concept, but it can very much be the future of mood pattern detection using artificial intelligence.*

Fans of Android phones, rejoice. *In new Android P (Android mobile phone operating system) Developer Preview 1, Google announced the new Fingerprint Dialog API. With the second P preview, this is now being replaced with the BiometricPrompt API. This API is more general and allows for developers to support all forms of biometric unlock methods. Whether a device has an iris scanner, fingerprint scanner, facial recognition, or even in-display scanners, Google wants all biometric security measures to be supported by the new API, so that its phones are more secure but still convenient to operate.*

A novel idea for voice recognition technology is gaining traction *with the news that digitally enhanced storytelling start-up Novel Effect has just closed a $3 million series-A funding round. The app is designed to play ambient music and sound effects as parents or other caregivers read books aloud to kids, with the music and sounds dynamically changing depending on the part of the book being read. It assesses the unique characteristics of a reader's voice to provide the appropriate soundtrack for whatever is happening in the story.*

Scan to visit our website

Security Solutions Today

Security Solutions Today (SST) is a leading publication on the latest security information, trends and technology, and products that include Access Control, CCTV/IP Surveillance, Intrusion Detection and Integrated Security Systems.

SST is packed with the latest developments in security technologies and trends, events, previews and reviews of major global trade shows, product launches and security installations worldwide.

WE ALSO PUBLISH

bathroom + kitchen today

SEAB SOUTHEAST ASIA BUILDING

SOUTHEAST ASIA CONSTRUCTION

lighting today

CREATOR OF

TRADECARDS GLOBAL

TRADE LINK MEDIA PTE LTD

101 Lorong 23 Geylang #06-04 Prosper House Singapore 388399 Tel: (65) 6842 2580 Fax: (65) 6745 9517
info@tradelinkmedia.com.sg | www.tradelinkmedia.biz

Qognify Situator the Technology Enabler at the Heart of the Gatwick Airport Integrated Security Project

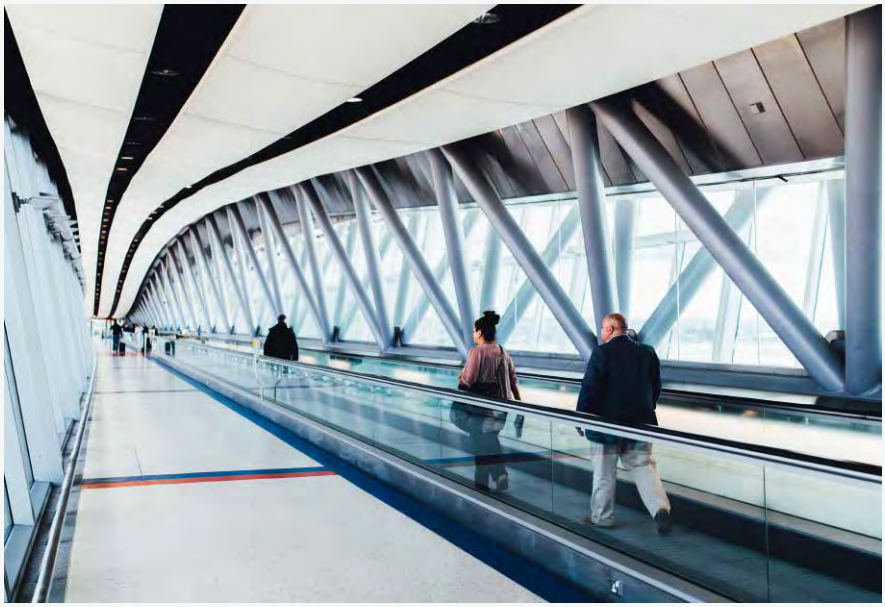
Gatwick Airport is the UK's second largest airport and the most efficient single-runway airport in the world. It serves more than 228 destinations in 74 countries for 45 million passengers a year on short and long-haul point-to-point services. It is also a major economic driver for the UK, contributing USD7.4 (£5.3) billion to national GDP and generating 85,000 jobs nationally.

As key national infrastructure and a major transport hub, Gatwick Airport takes the challenge of maintaining the safety and security of its passengers, visitors and employees seriously. It delivers on this challenge through people and process change, combined with powerful technology enablement and a standardised set of operational procedures and ways of working. This brings together the airport security and operations teams, Sussex Police, Border Force and many more interested parties.

The aim of the Gatwick Airport Integrated Security project was to use all available security elements to deliver a fully automated and rapid response solution for this state-of-the-art facility.

Qognify Situator is the technology enabler at the heart of the Gatwick Airport Integrated Security project. It provides a consolidated view and full management of any situation or emergency. The additional integration of Qognify's Suspect Search real-time video analytics proprietary software to this closely integrated network of security systems, means Gatwick Airport is now able to rapidly identify and pinpoint a suspected criminal/terrorist, or find a lost person in real-time.

A key aim of the project was the standardisation of operations and management across the airport. Security teams throughout the terminals and facilities collaborate effectively, ensuring the full safety of people and assets, along with full compliance and auditing abilities. The whole project helps to support smooth operations and minimise downtime in an intensely busy environment.



> "The power of the CCTV solution is that it gives Gatwick Airport superior situational awareness and allows us to command, adapt and respond to any security event, before, during and after it occurs."

By using a combination of Qognify's situational management and real-time video analytics solutions, the airport has a most powerful, automated and rapid response security system. From fighting terrorism, to combatting crime, or locating misplaced items and even finding a lost child, the security team at Gatwick Airport can now identify any issue and mobilise to wherever it is needed faster than ever before.

Robin Lomax, IT Project Manager, CCTV Refresh Project Gatwick Airport explains: "The power of the CCTV solution is that it gives Gatwick Airport superior situational awareness and allows us to command, adapt and respond to any security event, before, during and after it occurs. It enables a quicker speed of response, a more appropriate size of response and it allows us to play back and learn lessons from the incident after the fact." SST

High-tech Solutions to Homelessness in Scotland

Developer of complete end-to-end video security solutions, IndigoVision, along with their Authorized Partner Boston Networks and valued Technology Partner Dell Technologies, has provided Social Bite with a security system for their Social Bite Village.

Social Bite is on a mission to build a collaborative movement to end homelessness in Scotland, and thanks to recent fundraising efforts the Social Bite Village has become one of their many projects to help achieve this goal. The idea is to bring people from all walks of life in Scotland together to ensure that no one ends up homeless.

The Social Bite Village aims to provide a low cost, innovative and safe environment for up to 20 people for 12 to 18 months. Residents will be provided with the support, community and skills required to get their life back on track, including work placement opportunities and employability support. After the 12 to 18 months, the residents will transition to permanent accommodation and receive support in gaining employment, supporting their return to society. As one group of residents leaves the village, another can then enter and begin their journey. Residents will be selected from individuals in temporary and unsupported accommodation. The ambition behind this project is to create a full circle solution to the issue of homelessness—from housing to support to employment.

> Social Bite is on a mission to build a collaborative movement to end homelessness in Scotland, and thanks to recent fundraising efforts the Social Bite Village has become one of their many projects to help achieve this goal.

IndigoVision, Boston Networks and Dell Technologies have worked together to help Social Bite reach their goal by installing a security system to provide surveillance for the village site, specifically during the evening hours to ensure all people on site were kept safe.

Commenting on our involvement with this project IndigoVision's Chief Executive Officer, Pedro Simoes, said, "IndigoVision is proud to have been a part of a project that will contribute with such a positive change in Scotland. It's been a great privilege to work along with Boston Networks and Dell Technologies to provide the Social Bite Village with innovation that makes you safe."

Social Bite Village

As part of the installation IndigoVision provided 11 state of the art BX HD Vandal Resistant Minidome Cameras, which deliver high quality video and audio in all environmental conditions.

Boston Networks provided a survey of the Granton Road site, following which they laid cabling and set up point-to-point links to provide backhaul connectivity to support the network, before installing the cameras and configuring the security system. Purdicom and InfiNet, Boston Networks's distribution and wireless partners, provided the back-to-back wireless kit and licence.

Finally, a Hybrid NVR Workstation, which allows Social Bite to save recordings from the site, and a Workstation Monitor have been provided by Dell Technologies to complete the security system.

Founder of Social Bite, Josh Littlejohn MBE, said: "Companies such as IndigoVision, Boston Networks and Dell Technologies have gone above and beyond in supporting Social Bite to create the Social Bite Village in Granton, Edinburgh. We are deeply thankful – your contribution will help ensure that we are able to support people towards independence, changing lives for the better."

For more information, visit: www.social-bite.co.uk/the-social-bite-village/ SST

Taktis Detection Solution for "Church for the 21st Century"

Kentec Electronics Ltd., one of the world's leading manufacturers of life safety systems, has had its highly acclaimed Taktis® fire detection and alarm technology chosen to help protect an iconic new £4.7 million flexible use community hub development for Scotland's Dumfries Baptist Church.

The church for the 21st century in Dumfries, Scotland, is a £4.7 million community facility and will be a new home for the Dumfries Baptist Church's congregation. The church had long outgrown the building where the congregation had met since 1873, so suitable land had to be secured and funds raised before this ambitious project could be realised.

The recently completed new building, a 2,000m² community hub, comprises a main church hall seating around 500 and conference facilities including full catering, youth facilities plus a full specification games hall and multi-use games area. A central full height "Avenue" links all spaces, allowing light to flood the building, with rooms over two storeys offering flexible use of space options.

Such a busy, multi-use facility demands a fire safety system of the highest pedigree, performance and reliability, which is why leading specialists JJ Group (Contracting) Ltd. opted for an open protocol L3 system built around the sophisticated features of the new Taktis Technology Platform, and comprising a Taktis two loop fire control panel connected to a range of Apollo addressable loop powered devices including multi sensor detectors, sounders and beacons.

Kentec's Taktis fire detection and alarm system combines the very latest in hardware and software to produce a control and indication system that is both powerful and sophisticated, yet simple to understand. Available in 2-8 loop or 2-16 loop versions and certified to EN54-2 and EN54-4, Taktis is ideal for installation in larger buildings. Its capacity to be networked up to 128 panels and repeaters gives reassurance to all building owners/operators that they're in safe hands. Not only does Kentec's Taktis provide solutions to the most technically challenging applications in life safety, it delivers added value through ease of use, displaying clear information to ensure that when an event occurs appropriate action is taken swiftly. SST

Kentec's Taktis Technology Platform helps protect an iconic new £4.7 million community hub development for Scotland's Dumfries Baptist Church.

"Taktis is ideal for installation in larger buildings. Its capacity to be networked up to 128 panels and repeaters gives reassurance to all building owners/operators that they're in safe hands. Not only does Kentec's Taktis provide solutions to the most technically challenging applications in life safety, it delivers added value through ease of use, displaying clear information to ensure that when an event occurs appropriate action is taken swiftly.

Texas lieutenant governor's proposal to remove exits from school buildings is a bad idea, safety experts say

by Megan Cerullo

Lt. Gov. Dan Patrick from Texas said state schools should have fewer entrances and exits after a 17-year-old gunman went on a shooting spree that left 10 people dead at Santa Fe High School on 18 May 2018.

"We have to look at the design of our schools moving forward and retrofitting schools that are already built. There are too many entrances and too many exits to our over 8,000 campuses in Texas," he said.

Patrick made no reference to gun control in the wake of the mass shooting, instead insisting that limiting access to school buildings is the key to keeping Texas students and teachers safe.

"There aren't enough people to put a guard at every entrance and exit—you would be talking 40,000 people," he said. "But if we can protect a large office building or a court house or any major facility, maybe we need to look at limiting the entrance and the exits into our schools so that we can have law enforcement looking at the people who come in one or two entrances."

He also suggested staggering students' arrival times so that they're not all "trying to get in the door at once."

> "But if we can protect a large office building or a court house or any major facility, maybe we need to look at limiting the entrance and the exits into our schools so that we can have law enforcement looking at the people who come in one or two entrances."

The shooter, Dimitrios Pagourtzis, hid a shotgun and a .38 revolver belonging to his father under a trench coat he wore "almost every day," student Mateo Twilley told CNN.

But school safety experts say Patrick's logic is flawed. "That's a horrible idea," said school security consultant Steve C. Kaufer. "The likelihood of an incident like the one that happened today is very, very small compared to the likelihood of a fire or some kind of other incident, so you don't want to preclude people from getting out."

He added that removing a building's passageways would likely violate fire codes. "That would never fly because there are fire codes that require a certain number of exits by square feet and occupancy of the building."

Instead, Kaufer suggested that some entrances to school buildings be locked once the school day is underway. "Schools with several entrances typically have an administrator at the door screening people and once school starts they lock them down."

David Perrodin, an Expert Institute consultant, said Patrick's response to the tragedy didn't surprise him. "It's a very typical response that came out after Sandy Hook and the push is definitely going to be toward fortification," he told the Daily News. "But I don't believe that's an answer at all."

Instead, Perrodin emphasized the importance of having trained school resource officers on campuses nationwide. "We are at a point where school resource officers need to be a funding priority," he said.

He said the focus on facility design won't likely translate into safer schools. "It's just an initial reaction to create prison-like environments," he said. SST

A smart access control solution targeted at hotels, Airbnb

By William Pao, a&s International

Opening doors, but safely

Needless to say, the concept of opening doors with one's smart device has gained popularity. The convenience associated with it is certainly one driving factor. Also, the rise of Airbnb and autonomous hotels has also triggered demands.

Taiwan-based Nestech is a company that provides mobile access control solutions for hotel and Airbnb owners. According to Martin Prise, Business Developer at Nestech, the burden of always having to carry mechanical keys was one factor that drove them to create the solution.

"The thing is you have a lot of problems with your keys. A lot of people struggle to find their keys, and sometimes they lose them. Sometimes your guest or tenant loses your keys, and you have to make another set of keys or even replace your lock. This can be quite expensive, and everyone has had this kind of frustrating situation from time to time," Prise said. "We provide something that allows people to enter their flats or other properties without keys, just their phone."

> Sometimes your guest or tenant loses your keys, and you have to make another set of keys or even replace your lock. This can be quite expensive.

Nestech's solution entails an app that allows the hotel or Airbnb owner to create a QR code as well as a six-digit passcode, both of which will be sent to the guest or tenant. Once they receive the QR code, they can go to the hotel front desk and activate their smartphone's NFC function with an iPad-like device. Then, they can check in to their room with their smart device. In the event of Airbnb properties that do not have an NFC activation device, the tenant can opt to enter the six-digit passcode to unlock the door.

"We provide the locks, too. You can buy them online, like on Amazon, or you can buy them from our website. What is good is that you can install it pretty easily on your door. It's pretty simple to install. Anyone can do it," Prise said.

According to him, the solution is not reliant upon Internet, a feature that makes it unique.

"We provide a system without any Internet connection, as you already have the QR code. That's pretty unique. When you come from abroad you don't always have a connection with the Internet, which is ok. It works with Bluetooth and NFC, so it's pretty convenient," Prise said.

Hotels, Airbnb targeted

The solution primarily targets two verticals: hotels and Airbnb, where users can benefit, Prise said.

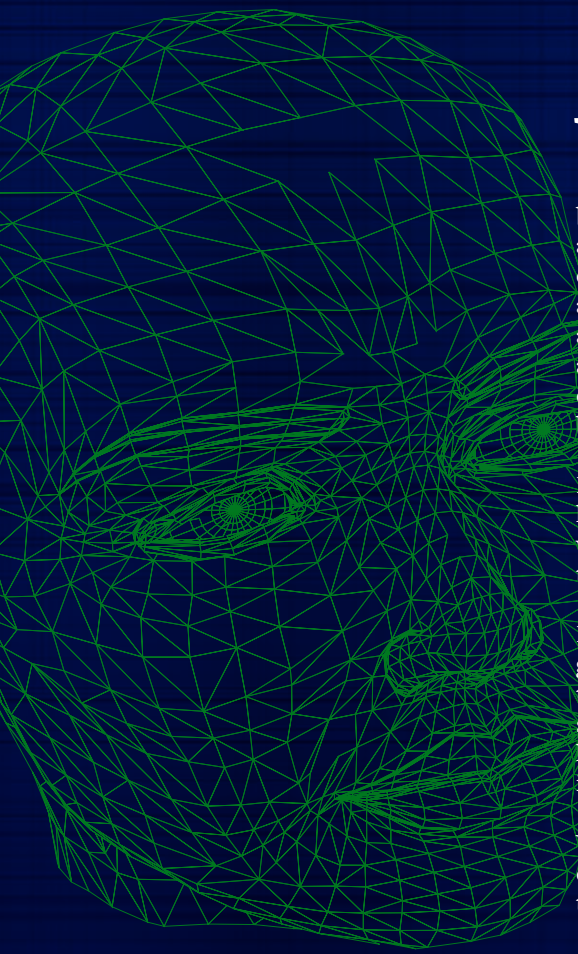
"We don't target luxury hotels. When people go to a luxury hotel they expect people to take care of them. Rather, we target small- to mid-sized hotel owners who want to remove the receptionist service. So even if there's no receptionist there you can still go to your room," Prise said. "Our solution also addresses the needs of Airbnb owners who, for instance, don't have time to do check-in each time because their guest may be late. With our solution you don't have to come to a place to meet guest. You just need to give them the QR code."

The solution has already been deployed in certain hotels in Taichung and Taipei. Besides Taiwan, the company aims to push the solution to overseas markets as well, one being Paris.

According to Prise, opportunities in Paris abound for this solution. "It's a pretty good niche for us to go there. People in Paris, they care a lot about security. Also, for Airbnb, the system removes the need to hand over mechanical keys to the guest. In Taiwan, you usually give the key to a neighbour or relative. But in Paris we don't have people nearby and we don't trust our neighbours. That's why in Paris it would work well," he said. SST

FACIAL RECOGNITION:
Benefits and Challenges

►► *By Navin Parti, Vice President, Q3 Technologies*



With state-of-the-art technology giving full reins to wishful fantasies that we could only imagine in the world of fairy tales, our digital communication and its after-effects have revolutionised the way one thinks, works and behaves—not just at workplace, but at every step that governs our life. As technological advancement follows high-tech expertise and is seen percolating down to different echelons of society, it also reigns supreme and becomes the keyword, and has become a must for all businesses of all kinds to take on the growing challenges of newer digital areas. Keeping up with such trends is the advent of facial recognition, which uses AI and Machine Learning, and has worked wonders in the use of security systems and other biometrics, such as fingerprint or eye iris recognition systems, in addition to becoming extremely useful as a commercial identification and marketing tool.

By definition, a face recognition system is just another computer application that helps in identifying or verifying a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the image and a face database.

Resultantly, multifarious applications across numerous sectors like retail, healthcare, government, travel and tourism, and many other industries, have benefitted tremendously with the use of facial data for various applications. Combined with the stupendous growth in population and the common man getting access to what was hitherto a reserve for the affluent, the functions of facial data seem to have magnified its strengths to unlimited usage.

With competition adding more zing to make devices cheaper, the consequences could extend to other recognition algorithms, such as three-dimesional recognition, thermal cameras and skin texture analysis, to name a few.

> *"Besides security systems, many governments have gained using a number of other applications for face recognition systems, but because of their covert nature, many such deployments are not in the public domain."*

Besides security systems, many governments have gained using a number of other applications for face recognition systems, but because of their covert nature, many such deployments are not in the public domain. Suffice it to say that every authority—be it the government or a corporate house to even institutions—earns rich dividends that go a long way to establish them as an incredibly data-rich law-enforcement and security agency, with a wide remit for data collection.

Although concerns about biometric data used in fingerprint and facial recognition systems are unavoidable because it is indelible, and is being used in authoritative identity registers, and is featured on identity documents such as passports and driver licences, by 2020, the facial recognition software market will be worth $6 billion. With the help of smartphones, major giants like MasterCard and Facebook—using predictive intelligence—have used selfie payments and tagging features respectively. Snapchat's geo filters and special facial recognition effects are also aimed in this direction.

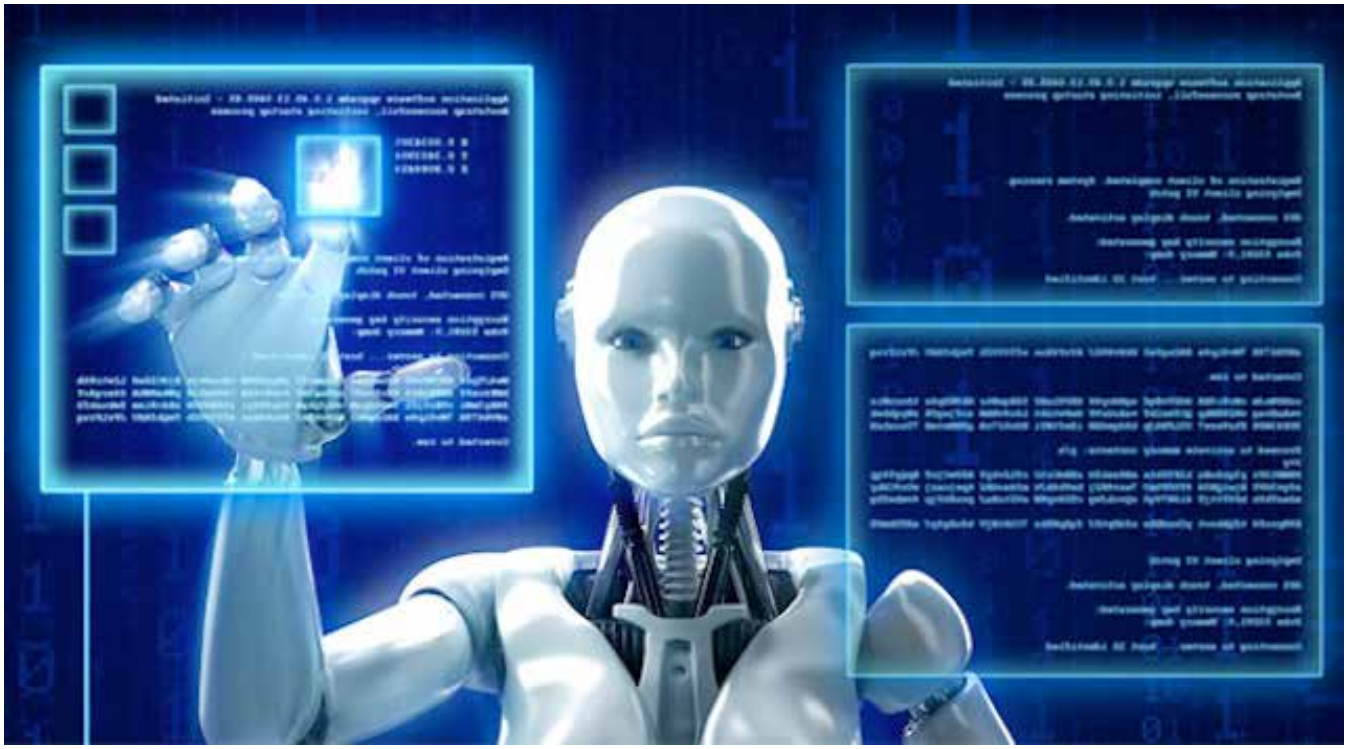
If we take a closer look at other areas, such as industries where more innovative applications could determine the course of action and assist in going forward, we could look at the ramifications it may have:

Government/ Identity Management

The governments in Australia have built large biometric databases through registration of people as drivers with a photograph of the driver through registration for passports, aviation/maritime security and other purposes.

The US Department of State, with 117 million American adults in its database, is one of the largest face recognition systems in the world.

For general management and running one can use these systems for census studies, voter identification, census studies, healthcare interventions, BPL handouts, law and



order management etc. Particularly in a country like India, with all its diversity, where there may not be a coherent enforceable right to privacy, this application could have far-reaching significance. But, with a rider, that it is judiciously and effectively implemented.

Retail / Emotion and Sentiment Analysis

Computational methodologies leveraging techniques from multiple areas, such as signal processing, machine learning and computer vision, could have tremendous positive outcomes for private enterprises as well. Systems now provide complete and accurate facial expression detection and frame-by-frame measurements of key emotions, as well as attention, engagement and positive or negative consumer sentiment.

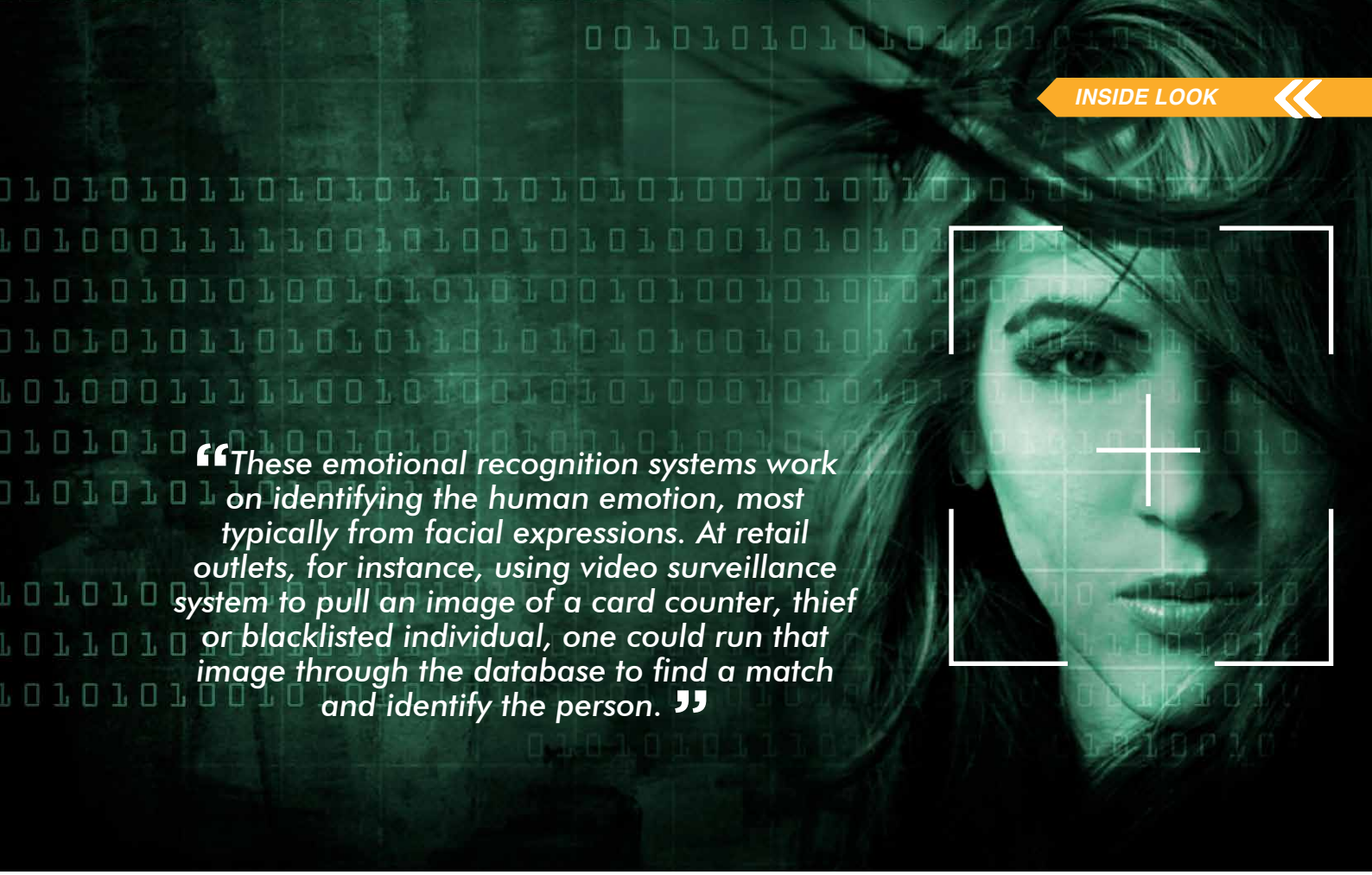
These emotional recognition systems work on identifying the human emotion, most typically from facial expressions. At retail outlets, for instance, using video surveillance system to pull an image of a card counter, thief or blacklisted individual, one could run that image through the database to find a match and identify the person. There could also be a non-intervention based attendance system, where retail stores could detect repeat customers and prompt salespersons to greet them by name.

Marketing / Product portfolio management

While humans may have had the innate ability to recognise and distinguish between faces, computers showing the same ability have taken giant leaps forward and developed by analysing what catches the eyes of customers in the public spaces, malls, showrooms etc. One could, thus, remotely conduct extensive market research and usability studies on how a user browses web pages, views advertisements and reads text through the webcams of participants sitting in the comfort of their homes. Obviously, this ensures a natural environment for a widespread high-fidelity data collection.

Healthcare / Healthcare provisioning

Facial recognition has great advantages over other biometrics solutions. Face recognition technology is contactless with the target, making it convenient for wide-ranging applications. The potential application of facial recognition technology used for genetic screening is an easy identity management facilitating easy check into hospitals, clinics and other medical facilities. MR records could be fetched in a flash, and insurance companies could check and authorise transactions in minutes instead of hours or days. Besides, facial recognition could also power emotional and sentiment analysis in mental healthcare



environments, as well add another piece to telemedicine to make it a real possibility. In addition, face and head tracking can be utilised for physiotherapy treatment through measuring and recording of head position, gaze direction and eye closure.

Financial services / Authentication systems

Since facial recognition could ease point of sale payments, with no swiping of cards, and potential of reducing lines at retails counters, financial services industry has been remarkably disrupted by the new business model, with customers are demanding more customer-centric, digital solutions and expecting banks to create solutions that not only solve the problem of security but also increase the level of customer satisfaction. Significantly, mobile banking could use a high-value second factor for authentication, as also, ATMs from faster access and disbursement. As an added advantage, it could also reduce spend and inconvenience for pension and other financial disbursements that require Proof of Life for older citizens who often have to manage this with difficulty.

Challenges

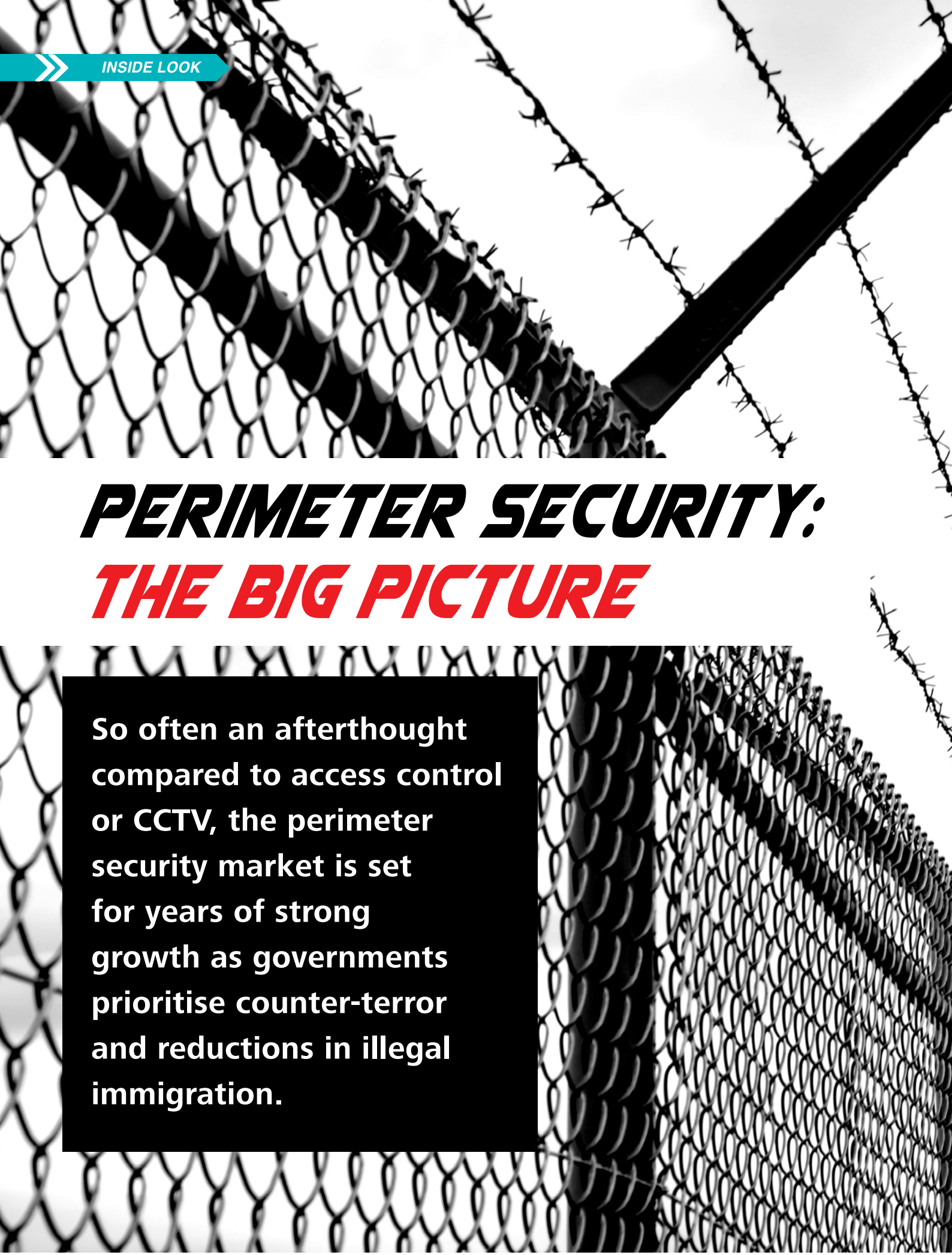
It's customary in any other novel approach to business—new or established—to field questions on the effectiveness of face recognition software too, particularly in cases of railway and airport security. And, therefore, a technology this promising has to have some hiccups. There are areas where this software may have its restrictions since accuracy in facial recognition technology remains less than desired. Fearing malfunction occurring, it may often create a problematic situation for a consumer.

Other important issue is that of privacy and consent, which we have touched upon earlier also. Many consumers are concerned about the privacy and consent or acquiring permission for facial recognition technology usage that may be difficult to accomplish. The silver lining is that with Snapchat's over 200 million, Facebook base exceeding two billion people, LinkedIn acquiring two new users every second with a projected goal of three billion (currently 467 million) this concern may be genuine but not something impossible to accomplish.

In conclusion

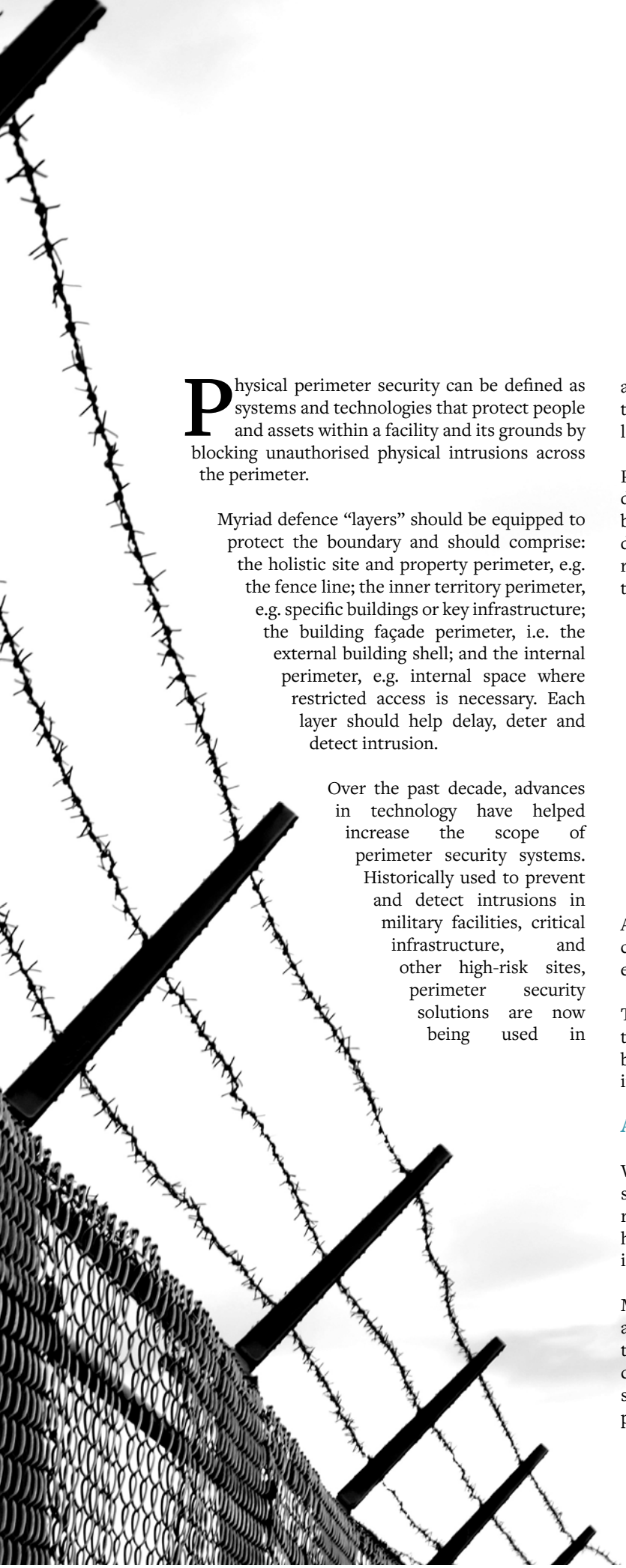
Despite demonstrating robust authentication methods, many companies are hesitant towards early adoption for valid reasons and other unforeseen deficiencies.

However, a core conclusion of this technology is that deployments of face recognition are diverse and differentiable, but that should not deter users from adopting the challenge. And while the debate still rages, what is important to recall is that the physiological characteristics of the human face with relevance to various expressions such as happiness, sadness, fear, anger, surprise and disgust are associated with geometrical structures which restored as base matching template for the recognition system call for an early adoption of technologies that invariably makes the difference between your business thriving or dying. The core technologies have evolved and the cost of equipment is going down dramatically due to the integration and the increasing processing power. Certain applications of face recognition technology are now cost-effective, reliable and highly accurate, and there are no technological or financial barriers for stepping from the pilot project to widespread deployment. SST



PERIMETER SECURITY: THE BIG PICTURE

So often an afterthought compared to access control or CCTV, the perimeter security market is set for years of strong growth as governments prioritise counter-terror and reductions in illegal immigration.



Physical perimeter security can be defined as systems and technologies that protect people and assets within a facility and its grounds by blocking unauthorised physical intrusions across the perimeter.

Myriad defence "layers" should be equipped to protect the boundary and should comprise: the holistic site and property perimeter, e.g. the fence line; the inner territory perimeter, e.g. specific buildings or key infrastructure; the building façade perimeter, i.e. the external building shell; and the internal perimeter, e.g. internal space where restricted access is necessary. Each layer should help delay, deter and detect intrusion.

Over the past decade, advances in technology have helped increase the scope of perimeter security systems. Historically used to prevent and detect intrusions in military facilities, critical infrastructure, and other high-risk sites, perimeter security solutions are now being used in areas such as commercial and residential sites, retail spaces, transportation sites, and many other urban and remote locations.

Perimeter security can include video detection, intrusion detection, access control, security fencing and gates, and barriers and bollards. The type of systems and technologies deployed will depend on the likely intrusion risks, which can range from vandalism and protests from activists, to criminal theft, espionage and, at worst, terrorism.

> *"While there has been huge investment in CCTV and electronic security systems, physical perimeter security hasn't always received the same attention. This is beginning to change."*

A robust perimeter barrier aimed at impeding intruders should combine a fence or wall with security lighting and surveillance, e.g. a perimeter intruder detection system (PIDS) and CCTV.

Toppings, including barbed wire and spikes, act as a deterrent to climbing a fence or wall by increasing the height of the barrier, as well as providing the opportunity for a would-be intruder to become entangled or injured.

A neglected market no more

While there has been huge investment in CCTV and electronic security systems, physical perimeter security hasn't always received the same attention. This is beginning to change, however, as perimeter security systems become embedded into integrated security strategies.

Market drivers include: the growing terrorist threat; increased awareness of issues around illegal immigration; technological trends in video surveillance; the need to reduce manpower costs; investment in smart city infrastructure; and more stringent government regulations and industry standards for perimeter security.

"Self-driving security patrol vehicles with CCTV, sensor and audio/visual capabilities may be on the horizon soon."

PAS 68 and hostile vehicle mitigation

PAS 68, for example, is a Publicly Available Specification for vehicle security barriers, which the UK government developed in partnership with perimeter security manufacturers. It has become the UK's standard and the security industry's benchmark for hostile vehicle mitigation (HVM) equipment.

It is also the specification against which perimeter security equipment is tested as part of research to prevent vehicle-borne improvised explosive device (VBIED) attacks. If a product meets the PAS 68 standard, end users can be confident that it is high quality and will operate as expected.

Multi-layered perimeter protection

With growing perimeter security threats, demand for multi-layered perimeter protection has increased. Technologies growing in popularity include next-generation fence-mounted sensors, infrared, and integrated fibre-optic PIDS. Thermal cameras and video analytics are also popular solutions, while intrusion detection technologies such as microwave, seismic sensors and radar are also experiencing high growth.

Indeed, radar has the advantage of working in most lighting and weather conditions, while it can also survey large areas that might otherwise require numerous cameras to achieve the same detection coverage. Nevertheless, video surveillance cameras are being deployed for perimeter security at a high rate and are an integral part of most perimeter security strategies.

Designing a perimeter security solution

When considering how to design a perimeter security solution, it is worth considering factors such as: visibility—what perimeter protection is visible and what it looks like, and if any critical assets are visible and could be hidden away; local information and statistics—local crime rates, first-responder locations, etc.; landscape and environmental conditions—terrain, weather, lighting, etc.; power requirements—e.g. for certain barrier systems.

How you respond to a detected intrusion should also be considered—how well trained and equipped are your responders?

The future of perimeter security

While perimeter security has an obvious deterrent purpose, its increased use in urban areas, and in commercial, retail and public applications, has focused attention on marking territories in a non-aggressive way through landscaping and other softer design elements.

In the case of vehicle barriers, for example, users should consider their materials and finishes, and whether they are low maintenance and are suitably sensitive to the surrounding environment.

Such is the importance of design that some perimeter security products, such as security planters, are being manufactured with an aesthetic purpose in mind.

The high cost of perimeter security systems can be a constraining factor in market adoption, however, costs are falling, particularly in respect of thermal cameras. Perimeter intrusion detection systems are also susceptible to false alarms caused by animals, weather, etc.

Improving reliability is therefore a key challenge for the sector, and will also be important in ensuring that perimeter security and business continuity strategies are aligned and don't conflict with one another.

In the future, perimeter security could become part of a connected technology system, which is able to profile specific locations, and match the skills and competencies of manpower required for each area.

When disruptions occur in different parts of an organisation, this connected technology will be able to analyse and identify information that could point to a serious threat, and raise alarms when business safeguards and operational processes are compromised.

Other innovations include aerial surveillance, via balloons and drones. The latter, in particular, may become popular if manufacturers can extend their battery life and if analytic capabilities can be integrated.

Robotics could also be part of future perimeter protection strategies. Indeed, there are already devices that can travel along monorails and patrol perimeters, as well as respond to suspected intrusions.

Self-driving security patrol vehicles with CCTV, sensor and audio/visual capabilities may also be on the horizon soon. SST

Interview with

SID DESHPANDE, RESEARCH DIRECTOR AT GARTNER, INC.

In March, the news about a major data scandal involving Facebook and Cambridge Analytica broke. Accused of improperly obtaining personal information on behalf of political clients, Cambridge Analytica announced it was shutting down its operations on May 1 and filed for bankruptcy. More than 87 million Facebook profiles were found to have had their information harvested—65,000 of which were users in Singapore. Sid Deshpande, Research Director at Gartner, tells us more about the Facebook and Cambridge Analytica incident on industry players and consumers.

How is this incident impacting companies in Singapore?

Regulators and government bodies in Singapore are taking this very seriously. The big question for them is how they can regulate data driven companies (such as Facebook and their developer partners) effectively while still allowing their business models to flourish. The need of the hour is for regulators to fully factor in social media business models into their regulatory planning exercises.

> *"Regulators need to to fully factor in social media business models into their regulatory planning exercises."*

Companies collecting data from users/consumers need to ensure they only collect data they absolutely need to provide a service. The consent they seek from the consumer for usage of the data should be clearly articulated and the consumer should be made fully aware of the various possibilities that may arise out of the usage of this data by the company in question. Furthermore, while such companies need to follow all local legislation and guidelines, they need to realise that they have a moral obligation towards their users when they collect data. Therefore, companies should not try to hide behind legal loopholes of the companies they are operating in to avoid disclosing an unintentional or intentional misuse or breach of consumer data.

How about social media companies? Do you expect them to tighten privacy controls further?

Yes. Such companies are already beginning to change their privacy regulations to make them more user friendly and provide users more visibility and control into how their data is handled. Users of social media platforms are already seeing notifications coming through from their social media platforms about updated privacy terms, and this trend is expected to continue. The major difference will be in how the information is presented—social media platforms are moving away from using complicated legal language in their terms and conditions to make it easier for users to understand.

Ultimately, governments around the world have to assess what the level of risk is that they are willing to expose their users to and regulate accordingly. The upcoming General Data Protection Regulation (GDPR) by the EU will be a good regulation in this regard. Social media platforms' compliance with GDPR will have side benefits for non-EU citizens as well. However, it is only enforceable by the EU for EU citizens' personal data. Therefore, country level regulators do need to step in to review their risk tolerance for personal data privacy.

Targeted advertising has its benefits for consumers, but the lack of privacy often becomes something intimidating. How can social media companies like Facebook work to balance both sides?

Social media companies like Facebook need to offer more information in a proactive manner about how types of profiles they are building about users and how those are

being used to serve ads. Social media platforms sometimes track users' behaviour outside their platform using cookies—while this is a common practice in the online advertising industry, not many users know about it. Users can opt out of such mechanisms on some platforms but the option to do so is sometimes buried so deep under user settings that it is hard for users to discover such a capability.

What are some advice you can share with consumers about security and privacy when using social media platforms?

Consent Matters: Read the terms and conditions very carefully and understand what data is being collected and how it is being shared with third parties. If you are not comfortable with it, don't use the platform! Consent is also what Facebook used as a defence in the early days of the CA scandal—the fact that users accepted the T&Cs at the time meant the onus of responsibility was purportedly on them. Upcoming regulations will mean social media providers need to offer a more easily understandable and simple set of terms and conditions, which will be a welcome change from the "legalese" that most consumers just gloss over.

> *"If a "news aggregator" app asks for access to your photos and videos on Facebook, don't install it!"*

Privacy vs. Convenience Trade Off: You could choose to be drastic, give up modern civilisation and retire to the hills to seek higher truths through meditation (arguably an attractive option for many, yours truly included!), but that is not a practical option for most people. Living in a city, you will most likely rely on technology in small or large measure. Modern technology you can bring great conveniences to your life but you need to pick and choose where you share data, how much you share and whether the benefit in return is worth it. Also, it is a good idea to remind yourself that anything you share on a public platform is probably being used in some way that you don't know. So, discretion is the better part of valour.

Review App Permissions and Default Settings: Ensure the apps that you are installing on Facebook (or other platforms) or on your mobile device actually need the permissions they are asking for to perform the functions they claim. If a "news aggregator" app asks for access to your photos and videos on Facebook, don't install it. Further, always go into the default privacy settings of a platform or app and choose the privacy options that you are comfortable with. New regulations are expected to mandate more granularity here so you can actually exercise more control.

Healthy Paranoia: We trust technology a lot because it is passive. It is important to apply the same principles of trust that we do in the real world, in the digital world as well. For example, if you are walking down the street and someone walks and asks you the name of your first pet, you would probably laugh them off. However, when a quiz app on Facebook asks you a similar question to "unlock" the next level, many (if not most) users would unthinkingly answer the question. These innocuous questions are often the "secret questions" to reset your password for online platforms.

Profiles

About Sid Deshpande

Sid Deshpande is a Research Director at Gartner. His areas of expertise include security infrastructure and services for both technology providers and buyers.

About Gartner

Gartner, Inc. (NYSE: IT), is one of the world's leading research and advisory company and a member of the S&P 500. They equip business leaders with insights, advice and tools to achieve their mission-critical priorities and build successful organisations with a combination of expert-led, practitioner-sourced and data-driven research. ***To learn more, visit www.gartner.com.*** SST

6 METHODS TO ENHANCE YOUR FACILITY'S ACCESS CONTROL

By Michael Elias, Director Of Business Development at Global Net Solutions (GNS)

Security has never been more important, as every company is challenged by how to track and secure customers, employees, property and assets once they're past the front door.

Whether you're a large corporation, small company, organisation or government agency—a security breach can deal crippling damage to one's brand and reputation, as well as leave consumers as prey to scenarios like identity theft, virtual robbery or even physical injury. Yet despite new technology, protocols and security best practices, breaches—both virtual and physical—are all-too-common scenarios.

And while many articles understandably focus on ways to protect organisations against hackers and other off-premise dangers, too few are looking at the more immediate threat: access control. Access control is undergoing a rapid evolution—just look at how the US Department of Defense is exploring the use of biometrics. But how else can organisations leverage the latest technology to improve their own security? I'd like to pose some new axioms, best practices and technology capabilities that I believe will act as drivers to improving access control in the immediate future and become the standard in the coming years.

1. Security must encompass more than the front door: Most security checkpoints are located just beyond the front entrance. But today's solutions also need to track what's happening

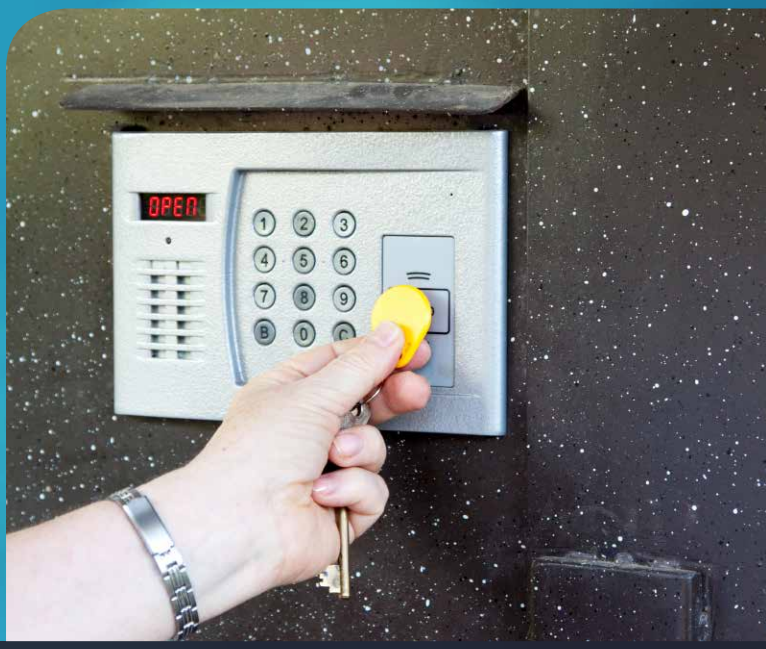
> Technology is never a cure-all. Implementing the best security for public facilities and commercial businesses still requires effective processes and people.

once an employee is inside. To effectively enhance security, we need to know who is doing what, where and when at all times. Ignorance isn't bliss, and it can quickly leave you maimed if you're not careful.

2. Solving lost and stolen badges: Human error can quickly lead to a large break-in if just a single badge is misplaced or stolen. And the RFID badge system is riddled with flaws. In 2015, for example, more than 1,400 security badges went missing from Atlanta's Hartsfield-Jackson International Airport, which could grant access to private baggage areas, tarmacs and other secure locations. Even if they're not physically stolen, most RFID badges can be quickly cloned undetected by the user. Eliminating this challenge requires more than a simple PIN number—we need multiple authentication methods that cannot be counterfeited.

3. Eliminating badge abuse: We like to believe that an employee won't abuse their badge and security clearance—but all it takes is one rotten apple to spoil the whole bunch. A unique PIN can be assigned to prevent the use of stolen badges, but what if an insider decides to sell that information? There are several ways to be nearly 100 percent sure the person opening the door is who they say they are—and they don't require implants. Biometric authentication—such as retina, fingerprint or facial recognition—is just one way to prevent this type of badge abuse.

Graphic Credit: freepik.com



4. Preventing tailgating and piggybacking: A badge system can prohibit an intruder from entering, but not if someone on the inside opens the door first. These types of scenarios happen all the time—both intentionally and unintentionally—and leave otherwise highly secured areas extremely vulnerable. To solve this, it's not enough to just know who scanned the badge—we need to know who (and how many) actually entered with them.

5. Improving emergency response: Unfortunately, the need for emergency response has become an all too common occurrence. And response times have a direct correlation to the severity of damage from a breach. Systems today lack the most critical feature to improving response time—which is identifying and relaying the exact location of the emergency. First responders would benefit greatly if they could verify the authenticity and exact location of an emergency at any time. It's not enough to know which building, but rather which room and which level.

6. Building business intelligence: For good reason, our world is becoming more and more data driven. And by improving the way we monitor employees and access control, we can unlock a huge stream of untapped information. These insights could range from better understanding the routines and processes of staff to improve productivity, to better identifying threats and breaches before they have a chance to strike.

Technology is never a cure-all. Implementing the best security for public facilities and commercial businesses still requires effective processes and people. That said, if an organisation integrates the right solutions within an effective governance framework, technology can augment and streamline security to be more effective and efficient. SST

Risk Mitigation Strategies

A Variety of Levels to Securing Entrances to Public and Private Buildings and Facilities

By Gary Schreiber, a Security Entrance Authority from the Boon Edam Global Network

Graphic Credit: freepik.com

Holding a door or gate open for another person is a nice thing to do — but it's certainly not good security

Something we should never complain about is that people are too nice. They let people in behind them without a second thought in most cases. Most of us are not brought up to close a door in someone's face, so we hold a door open for them, or we let them in behind us—especially if they have forgotten their personal authorisation or access device at home. Good manners indeed, but certainly not good security.

These weakness in a company's security—at an entrance point—are part of what makes an organisation aware that they need to find an even safer way to secure their space and keep their valuables safe as well. Several solutions are often considered such as: locks on doors or gates, access control systems to control electronic door locks, security officers posted at key locations and security cameras to monitor access.

Mitigating Risk with Security Entrances

As with all things in life, all of the above-mentioned options have their flaws. An access control system can manage who can open a door, but once it is open, anyone is able to freely enter or exit. Adding security cameras does not necessarily ensure security either—it often just makes it possible to replay what happened after the security breech has actually taken place. Employing security officers is expensive, and these guards may have a limited impact as they can be distracted, misled or overwhelmed.

Security entrance solutions provide the most effective way to allow passage of authorised people, while acting as a deterrent or a physical barrier for unauthorised people. More than that, security entrances can provide companies with valuable metrics to determine the traffic flow, monitor tailgating statistics, biometrics, and more.

You can think of security entrances in terms of four groupings to achieve a variety of risk mitigation strategies: crowd control, deterrence, detection and prevention.

Crowd Control

The lowest level of security entrances, such as waist-high turnstiles, can count the number of people exiting or entering a facility, which helps staffed entrances to cope with a large numbers of authorised people who have to enter or leave a secured area in a short space of time. These low security systems are designed to slow down and organise the entry point, while also serving as visual deterrents to potential infiltrators and preserving a relatively open appearance for authorised people. Typical applications include sports stadium entries, factory shift changes, transit terminals and high-occupancy skyscraper buildings.

Crowd Control technologies include Boon Edam's Turnlock turnstiles

Deterrent technologies include Boon Edam's Lifeline Speedgates

Deter

The next level up in the security entrance grading is designed with an increase in the deterrent factor. These incorporate a full-height barrier that deters casual attempts to defeat the system by means of climbing or crawling. A full height barrier is often installed at a perimeter fence line as a first layer of physical security, or an "exit only" to allow people to leave—but deter them from entering. Here, when integrated with an access control system, metrics such as the number of inbound and/or outbound people, in addition to credentials, can be tracked.

Photo Credit: Evening_tao / freepik.com

Detect

Medium level security entrances rely on sensor technology to accurately detect objects moving through an opening, and can determine whether one or two people are passing through. In this way, they can detect when a tailgating or piggybacking incidence occurs. If this happens, an audio, visual and silent alarm are activated to alert the right security personnel quickly. At this security level, speed gates, which are particularly popular in corporate reception areas or foyers, can be equipped with presence detection sensors, and can provide accurate metrics including the number of authorised personnel inbound and outbound as well as the number of tailgating incidents or alarms. Certain models equipped with dense sensor arrays and can be set up to alarm and count jumping or crawling attempts.

Detection technologies include Boon Edam's Tourlock security revolving door

Prevention technologies include Boon Edam's Circlelock high security portal

Prevent

This is the highest level of security entrances available and it introduces true tailgating and piggybacking prevention. We see products such as high security doors and portals typically fall in this area. The solutions in this category are most suitable for facilities such as data centres, and for locations where security staffing is impractical. These security entrances not only serve as a visual deterrent, but also physically deny all forms of unauthorised entry completely. By integrating facial recognition analytics, it is possible to ensure that the person traveling through the entrance matches the credentials which have been presented. Biometrics serve the same function by utilising the individual's face, iris or fingerprint as their credentials.

With the integration of sophisticated near-infrared sensors and optic technologies, such as the StereoVision, these entrances can provide a rich assortment of metrics, including authorisation received, passage completed, tailgating / piggybacking rejections inbound or outbound, biometric access control rejections, safety rejections, and emergency button rejections. They can also detect and send alerts for a variety of events such as an object left behind.

Securing an entrance can take many forms, but the overall goal is to establish risk mitigation strategies to keep unauthorised entry at bay. Security entrance solutions are the answer for protecting a company while, at the same time, providing critical metrics to further reduce risk. At the end of the day, security entrances are a good investment for any organisation that needs to control access to any points in their facilities. SST

Graphic Credit: freepik.com

GDPR: Noise or Necessity?

By the Infosecurity Magazine Team

Photo Credit: kjpargeter / freepik.com

> GDPR is predominantly solved through first understanding where the biggest risk and gaps lie, then addressing those through the implementation of processes and procedures, documented to demonstrate compliance, and finally reinforcing through specific technologies.

Understanding the fuss behind the European Union's General Data Protection Regulation

There is, and has been, a lot of noise around the European Union's General Data Protection Regulation (GDPR) that came into force in May of this year. Even Singapore, as part of the global business community, will be affected. Much of noise has involved scare-mongering with the prospect of large fines brought to the fore, primarily by organisations looking to promote their magic pill to solve the compliance challenge in one hit. Unfortunately, no such thing exists. GDPR is predominantly solved through first understanding where the biggest risk and gaps lie, then addressing those through the implementation of processes and procedures, documented to demonstrate compliance, and finally reinforcing through specific technologies.

The unfortunate consequence of this becomes a level of fatigue and scepticism around the subject which is extremely unhelpful because GDPR, in its essence, is a change for good. The UK Information Commissioner's Office (ICO) website is an independent and superb source of analysis and advice on the subject and should be reviewed by any business looking to understand the regulations. The ICO will act as the Supervisory Authority for the UK and is therefore the body that will audit companies for compliance.

GDPR: How It Benefits You

So, why is GDPR a change for good? Our world is becoming increasingly digitalised and our identity often represented by ones and zeros. Nowadays, we can bank, shop and work without leaving the house. When we do venture out, we can jump in a taxi without any money in our pocket, potentially to stay in somebody else's house with a pre-agreement conducted online all because our identity is validated on someone else's server. Everyone is drilled to protect their own online and physical critical security details, such as bank

card PIN numbers, passwords and credit card information. As part of our daily lives, we are frequently requested to hand this information over to a third party and blindly assume that they are taking as much care of our information as we do.

GDPR aims to ensure that this is no longer an assumption, but fact. The information referenced earlier falls under the definition of personal data and would require protection under GDPR. However, the regulations are wider than just a framework definition for data protection and address areas around the collection of that data, bestowing new rights upon consumers including decisions on how their data is handled. For example, you have the right that your data is collected only with your explicit consent, you have the right to request any and all data a company holds on you is permanently deleted (your right to be "forgotten") or for it to be provided to you in a portable format. No longer will you have to scrutinise every form you complete to determine if you have already been opted in to further marketing—are you opted in by default, do you need to check or uncheck a box to opt out or to opt in? Currently there is no consistency around how these requests are presented to you.

Under GDPR, your data can only be collected with your explicit consent and, when deciding whether to opt in or out, a clear description of how that data will be processed and used will be provided. For the person on the street, this is all positive. The companies that consume our data are now required, under GDPR, to take a responsible attitude to the collection, storage and processing of that data. The regulations adopt a pro-active stance to data protection in that they allow for organisations to be audited to check they are in compliance and, in the event they are not, will apply and monitor remedial action. This is another step forward as currently we only tend to discover a company's lax data protection strategy at the point our data has been breached, which is far too late.

Graphic Credit: freepik.com

> GDPR is predominantly solved through first understanding where the biggest risk and gaps lie, then addressing those through the implementation of processes and procedures, documented to demonstrate compliance, and finally reinforcing through specific technologies.

If you have suffered as a victim of a data breach, a best-case scenario is that you will need to cancel credit cards with the worst case requiring you to reclaim your identity. Anything that is put in place with the sole mission to avoid this type of situation should be welcomed.

Taking a Step Toward GDPR Compliance

As a business, there will undoubtedly be some effort required to ensure compliance with the regulations. If a strong data protection policy is already in place, it could just be a tweak. For others, it may involve a bit more work. A simple step towards GDPR compliance and its challenges is to ensure that every business is aware of GDPR and what it entails. Apricorn's survey, conducted by Vanson Bourne, uncovered the fact that 24 per cent of surveyed companies were not aware of GDPR or its implications, whilst 17 per cent of those who were aware had no plan for compliance.

However, GDPR provides an opportunity for businesses to clean up their house, and to really understand what data they hold, whether it is all necessary, how it is

processed and to re-confirm their relationship with their customers and partners. The first and most important piece of work is to analyse all personal data that is collected, stored and processed and to understand where it is located and who has access to it. All data deemed irrelevant to the business should be deleted and the remainder tested in support of the new rights individuals will have under GDPR—has the subject explicitly consented to the collection of their data, are you able to delete it or provide it in portable format on request? Once the data is understood and the processes around it documented, the next step would be to protect it both at rest and on the move in order to defend against any potential breaches.

GDPR is non-specific in terms of prescribed technologies. However, Article 32 does go a step further, requiring "the pseudonymisation and encryption of personal data". This would seem an obvious requirement, but there are still frequent examples of the use of unencrypted media at the centre of a breach played out in the media. The recent discovery of Her Majesty the Queen's security details on an unencrypted USB stick outside Heathrow airport is a case in point. Furthermore, Article 34 notes that, in the event of a breach, if the data at risk is encrypted, the requirement to contact each data subject affected is no longer mandated, thereby avoiding the resultant administrative costs. Therefore, it would appear prudent to apply encryption to all personal data within corporate systems and even more so on any media that is used to take the data outside of the business.

Spread the Word

Finally, once a business has these two pieces of the puzzle in place, an employee education and awareness programme must be put in place. As home based and mobile workforce numbers continue to grow, so does the number of locations and devices on which corporate data is carried. Each employee has the responsibility to ensure that they follow corporate data protection policy and to understand their role in ensuring any personal data they carry remains safe at all times. The aforementioned survey found that 48 per cent of the surveyed companies said employees are their biggest security risk, and as many as 44 per cent expect that employees will lose data and expose their organisation to the risk of a data breach. Therefore, this should be an area of focus—not only to equip the workforce with easy to use tools that support the data protection policy but to ensure everyone understands the policy and is aware of their obligations under it.

> "To the businesses — it is time to take your obligations seriously. GDPR is an opportunity for both sides of the data exchange relationship to get their house in order.

We are headed to a perfect storm where business will be legally required to implement data protection best practice and audited against that, individuals will become more aware of their rights, take more ownership of their data and expect companies to be doing everything GDPR mandates.

Everyone should embrace GDPR regardless of whether they are a citizen or a multi-national conglomerate. To the citizen—this is your data, you have every right to expect it to be treated responsibly and with your permission. To the businesses—it is time to take your obligations seriously. GDPR is an opportunity for both sides of the data exchange relationship to get their house in order. It's about time, wouldn't you agree? SST

PAVING THE WAY FOR SMART CITIES:

The Smart Sensor Platform Network

ConnecTechAsia Summit speaker, Yao Shih Jih, General Manager, ST Electronics (Info-Comm Systems), shares about how smart street lighting could be a key to unlocking the potential of a smart city

The cost of Internet of Things (IoT) sensors has decreased remarkably over the past decade, heralding new possibilities of a renewed push for smart cities. With worldwide spending on IoT predicted to surpass the USD$1 trillion mark by 2020, this has increasingly attracted attention within the various sectors.

With that tied in line with the strong push towards smart cities, seen through the recent piloting of Smart Cities Network by 26 ASEAN cities, more cities are looking towards developing more in-depth frameworks to improve the lives of citizens through the use of technology such as IoT solutions. This gives rise to an abundance of opportunities it can bring to governments and businesses—implementing further Smart Cities initiatives, such as smart street lighting, to drive efficiency and better quality of life for citizens.

Cities of tomorrow

Connectivity is a fundamental aspect of a smart city and implementing a smart network nationwide is a challenge. Step forth—the street lamps. As the number of street lights globally is set to grow to 363 million by 2027, it makes sense to consider this as a platform to kick start the smart city network. With street lamps typically dotted at walking distances apart from each other, we can leverage on existing street lighting infrastructure to affix smart sensors instead of constructing a smart network from scratch.

Through the incorporation of IoT sensors within smart street lighting, it can offer benefits for citizens such as:

Environmental monitoring: Sensors built into street lights to monitor real time environmental factors such as air quality, UV-ray levels and noise levels. Control allows the monitoring to be done over specific locations or citywide.

Traffic monitoring: Traffic sensors in street lighting to provide more precise traffic updates and congestion levels.

Smart parking and metering: A variety of sensors can be used to track parking lot availability and records for fee collection, and occupant's vehicle information.

Public Wi-Fi and HD video surveillance: High bandwidth wireless networks to provide citywide Wi-Fi access. Utilising of high bandwidth wireless networks to match the bandwidth requirements of HD videos and GPS for emergency response.

Through these solutions, governments and citizens can be kept informed of information in real time, enabling them to solve everyday issues in betterment of their daily lives.

Furthermore, governments and businesses can utilise the data to tackle issues such as public safety, traffic congestion and enhance emergency response. For instance, the transmitted data from the HD video surveillance could possibly inform emergency units of a casualty by identification through facial recognition, allowing the casualty to be identified remotely amongst the crowd.

Integration and interoperability

While governments and city planners are aware of the benefits of a smart sensor network, many face challenges in its implementation, particularly in the integration of solutions and interoperability. This is mainly due to the myriad of technologies and solutions involved which will require the complementation to each other.

To ensure optimal outcomes, both private and public parties need to work together to bring the right set of capabilities to ensure the various smart platforms can be successfully implemented. These partnerships can further unlock new innovations and opportunities—something as simple and apparent as the extended use of street lamps for smart networks. This will ensure that the smart cities do not end up turning into a mix of mini ecosystems that will only work in silos.

Aside from public-private partnerships, governments also play a role when it comes to implementing regulations and policies within a smart city. In doing so, it enables the objectives of the smart initiatives to be successfully met, and not faced with misuse. In the case of smart parking solutions, sensors are embedded in or on top of pavements to collect data such as parking lots availability and vehicles' parking duration for automatic charges. Through that, it aims to automate processes and take away the redundancies of manpower. Regulations can be considered to be imposed in order to prevent issues such as illegal parking, and ensure that parking authorities still have control on the parking situation despite reduced physical surveillance.

Privacy and data-hacks

As such, while great strides have been made in smart city developments, data privacy and cyberattacks is still seen as a key concern. The focus of smart cities initiatives tend to solely be on the implementation of the solutions, while overlooking the aspect of cybersecurity. As the complexity of cyberthreats continuously increases, it is even more important to prioritise cybersecurity in smart cities planning—particularly smart street lightings and sensors which are in the public space.

As cities continue their push towards being a smart city, we look forward to more possibilities beyond the horizon. However, greater involvement of stakeholders will prove essential to drive innovation and collaboration to realise the smart city goal.

For all we know, the springboard to smart cities could very well be right under our noses—with something as simple as a street lamp. SST

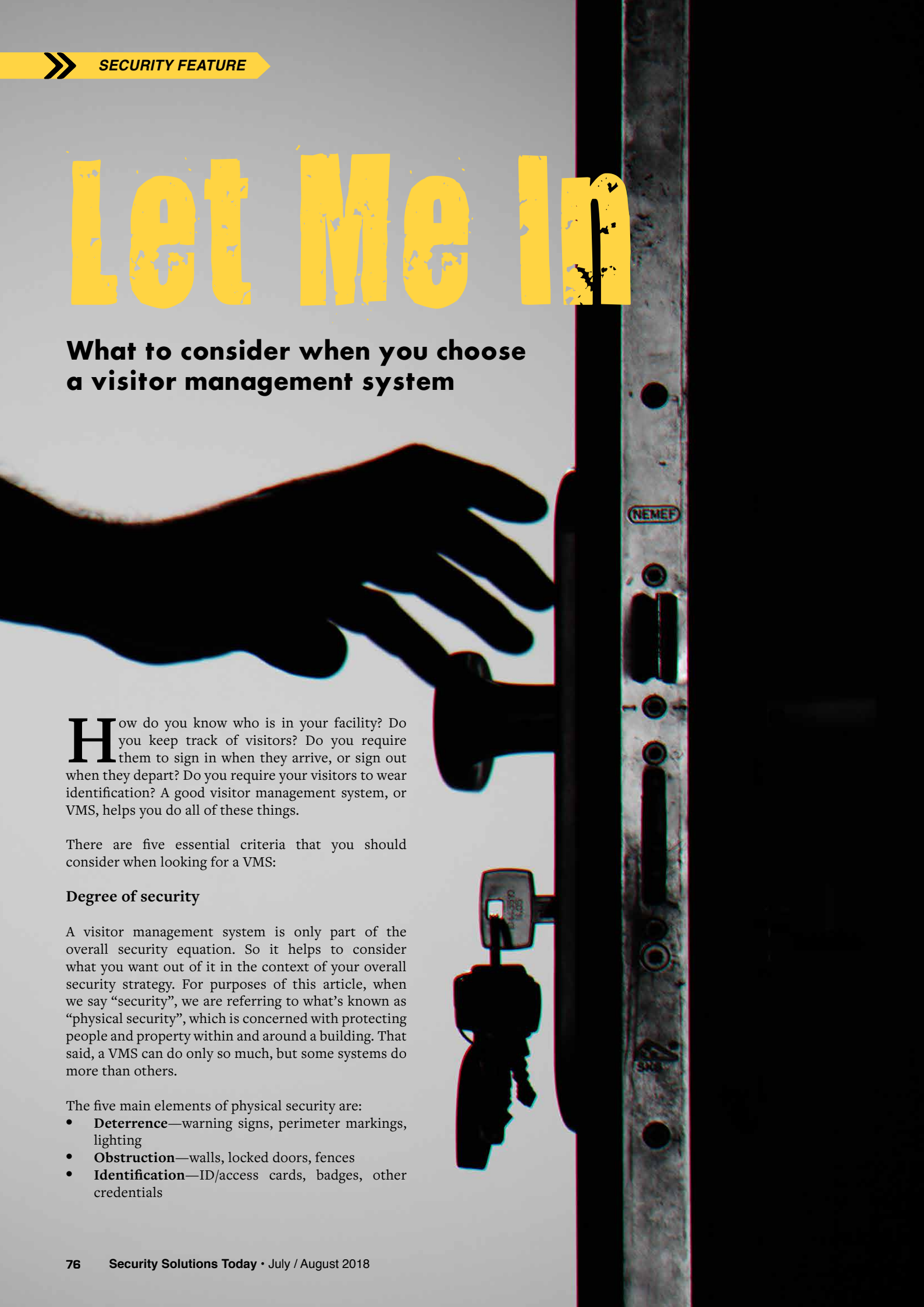
> "While governments and city planners are aware of the benefits of a smart sensor network, many face challenges in its implementation, particularly in the integration of solutions and interoperability."

What is the Internet of Things?

The term was most likely coined by Kevin Ashton, a British technology pioneer, in 1999, who was then a brand manager with Proctor & Gamble. He co-founded the Auto-ID Center at the Massachusetts Institute of Technology. He used the "Internet of Things" to describe a system where the Internet is connected to the physical world via ubiquitous sensors.

Let Me In

What to consider when you choose a visitor management system



How do you know who is in your facility? Do you keep track of visitors? Do you require them to sign in when they arrive, or sign out when they depart? Do you require your visitors to wear identification? A good visitor management system, or VMS, helps you do all of these things.

There are five essential criteria that you should consider when looking for a VMS:

Degree of security

A visitor management system is only part of the overall security equation. So it helps to consider what you want out of it in the context of your overall security strategy. For purposes of this article, when we say "security", we are referring to what's known as "physical security", which is concerned with protecting people and property within and around a building. That said, a VMS can do only so much, but some systems do more than others.

The five main elements of physical security are:

- **Deterrence**—warning signs, perimeter markings, lighting
- **Obstruction**—walls, locked doors, fences
- **Identification**—ID/access cards, badges, other credentials

- **Detection**—cameras, alarms, or other forms of surveillance for people who are coming in, as well as those who are going out
- **Response**—by security guards and/or police

There elements are not mutually exclusive. Of these five elements, the third one is most concerned with the management of visitors, providing identification that is temporary, as well as that of more permanent occupants, like employees. Identification also acts as a deterrence, and helps with detection, but in varying degrees of effectiveness. For example, identification cards that can unlock doors are more secure than adhesive badges that merely show a visitor's name. Still, even requiring a name badge makes it harder for intruders to roam a facility unescorted (deterrence). And a surveillance camera can tell if a person is wearing approved identification (detection).

Ease of use

Generally, the ease of using a visitor management system is directly related to the degree of security it provides. If you want your VMS to scan identity cards or driver's licences and maintain a database of troublemakers, you would expect a longer and more complicated installation and training process than that of a simple sign-in book.

Cost

What is security worth to you? So many organisations say they can't afford a visitor management system. But, as soon as there is an incident, security becomes more of a priority and budget is allocated to it.

In the scheme of things, visitor management is "soft" security. It likely won't prevent an armed intruder from wreaking havoc. But it provides other benefits:

- Encouraging visitors to check in and out at the front office
- Allowing the front office to authorise visits (and to refuse them if necessary)
- Helping staff to identify and assist strangers in the halls
- Knowing who is in the building at all times
- Keeping a record of who visited whom, and when
- Assuring building occupants that a security procedure is in place

Speed

There needs to be a balance of the various criteria you are considering for your VMS. Speed is a good example. How quickly do you need to be able to sign visitors in to your facility? Do you entertain a lot of visitors and vendors every day? If so, how do you register everyone completely without creating a long line of people at the front desk waiting to be processed? Fortunately, there are ways to sign in your guests, with either a manual or electronic solution, that are both thorough and quick.

Image

For some organisations, more so than for others, how the product makes your company look matters. You might think, "Who cares, as long as we're secure?" But there are two aspects of "image" as a criterion when considering visitor management solutions: Does the product literally "look good"? Does the product convey the appearance of added security?

Most visitor management systems include a visitor badge of some kind. These range from a plain, generic badge that just says "visitor", to a custom-printed badge with the facility's logo and a colour photo of the visitor. Custom-printed badges that contain a name and logo help to promote an organisation's "brand". More important, from a security standpoint, they make it harder for intruders to falsify their identification. So when employees they see a stranger wearing a custom visitor badge, they can more safely assume that person has permission to be in the building.

There are three important questions to ask yourself when considering a visitor management system:

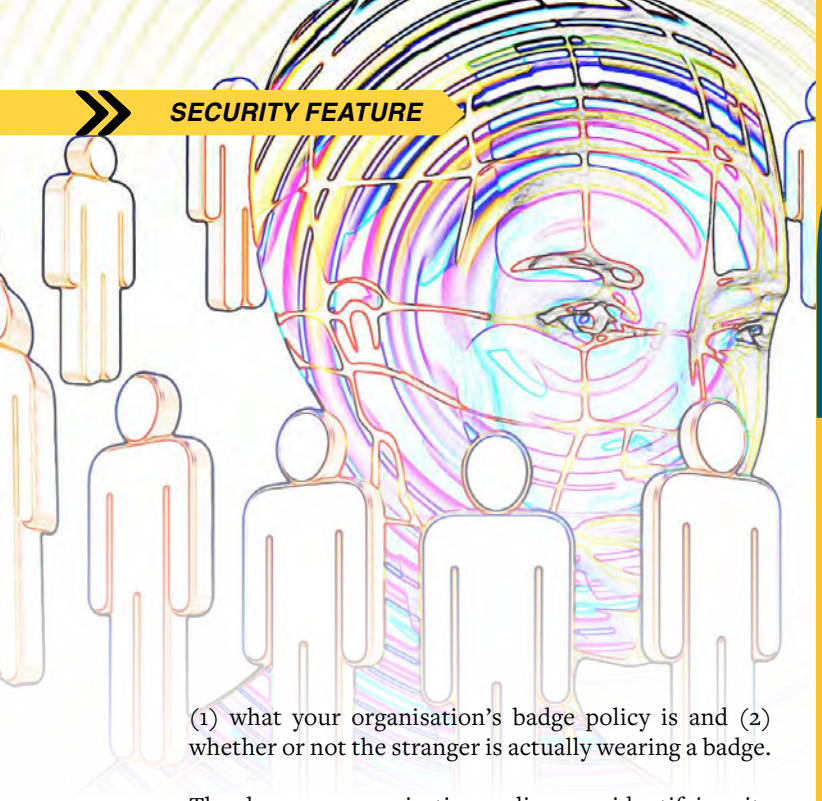
1. What do you want your visitor system management system to do?

Not all visitor management systems perform the same tasks, so it's worth thinking about what those tasks are and if they are important to you.

Identification

Do you know everybody at work? If you do, you can tell the employees from the visitors? If you don't, a stranger you encounter could be anybody. Either way, if they aren't wearing a badge, you may wonder who they are and what they are doing there.

Who you think the stranger is depends on two basic things:



(1) what your organisation's badge policy is and (2) whether or not the stranger is actually wearing a badge.

The less an organisation relies on identifying its building's occupants, the more mystery there is about their identity. At best, not identifying visitors arouses employees' curiosity and, at worst, leaves people and property exposed to potential harm.

Tracking

Whether you work in a school, a hospital, a business, or a government or non-profit agency, the occupants of your building fall into four distinct categories: (1) People who are there full time and permanently, e.g. employees, students, patients, clients or residents; (2) people who are there full time or temporarily, e.g. contractors, temporary help, relief teachers; (3) people who are there part time and frequently, e.g. vendors, volunteers; and, (4) People who are there infrequently or just once, e.g. visitors, students on a field trip.

The first category above falls out of the scope of most visitor management systems. But it is good policy to know, at all times, which of these people are in your building and, better yet, where these people are in your building. In an emergency evacuation, everyone needs to be accounted for.

The more sophisticated your visitor management system and policy are, the better you can verify that a visitor is who he says he is. Asking him to produce some government-issued identification, like a driver's licence, is a good start. But some organisations—especially those, like schools, with vulnerable occupants—require more information about their visitors. This can be accessed through online databases, as well as from an audit trail maintained by your own computerised VMS.

Record-keeping and Reporting

While a VMS's tracking capability lets you know who is (or isn't) in your facility now, its record-keeping and reporting function should tell you who was in your facility, as well as when, how often, and who they visited. This helps complete a visitor's background (was there any trouble last time?) and provide evidence for liability or confidentiality issues. For schools and hospitals, a "watch list" can help identify potential custodial issues.

> The less an organisation relies on identifying its building's occupants, the more mystery there is about their identity. At best, not identifying visitors arouses employees' curiosity and, at worst, leaves people and property exposed to potential harm.

2. What do you want your visitor management system to comprise of?

Just as different visitor management systems perform different functions, they also, understandably, comprise different components, depending on your needs and preferences.

Badges

It is not only important to consider whether to have badges as part of your security process, but also how secure they ought to be. The more distinctive you make your badges, such as with your organisation's name and logo, and corporate colours, the harder they are to copy, but they will cost more.

You can buy a bunch of plastic or cardboard badges that just say "visitor" on them, hand them out at the front desk, and require that they be returned when visitors

leave. These badges would be worn with a clip or a lanyard. If visitors forget to return their badges, you eventually have to replenish your supply. Disposable badges are cheaper to replace, but every time a badge leaves your facility, there's the risk it may be reused by someone with dishonest intentions.

Customised badges that expire visibly cannot be reused as easily. By expire, we mean it changes colour over time so that, even from a distance, you can tell the wearer should, at the very least, be stopped and questioned.

Information about the visit

In addition to the style of badge used, you need to decide if you are going to include information about the visit on the badge, such as: visitor's name and organisation, date and time of arrival, person and place being visited, and purpose of the visit. You might also need to record the visitor's photo, the visitor's time of departure, or even, in high-security facilities or high-risk areas, require a behaviour/confidentiality agreement and/or a waiver of liability (signed by the visitor).

3. How do you want your visitors to be processed?

Manual visitor management systems

A manual visitor management system usually consists of a log book, which the visitor fills out, that provides a record of the visitor's stay, including such details as name, company (when appropriate), the date, time in, time out, and destination (a person, floor, or room number). Often a visitor's badge is used, in addition to (and sometimes instead of) the log book. Many manual visitor badges are custom-printed to include an imprint of the facility's logo and name. Some types of badges have "time-expiring" technology, which means the badges change colour overnight to prevent visitors from reusing them the next day.

PROS and CONS:
A manual system is low-cost, and nothing beyond a log book or sign-in sheet. There are no software licensing fees or additional system components to purchase. Your staff would require minimal training and the list can be quickly consulted during an emergency.

However, if a visitor has bad handwriting, their particulars might be difficult to read. Also, most log books are not confidential and the visitor's information will there for all visitors who follow to see. The sign-in process might be time-consuming if there is a crowd of visitors, and all their credentials will need to be verified manually. Also, there will be no photo on the visitor's bad, making verification of identity difficult and badges interchangeable.

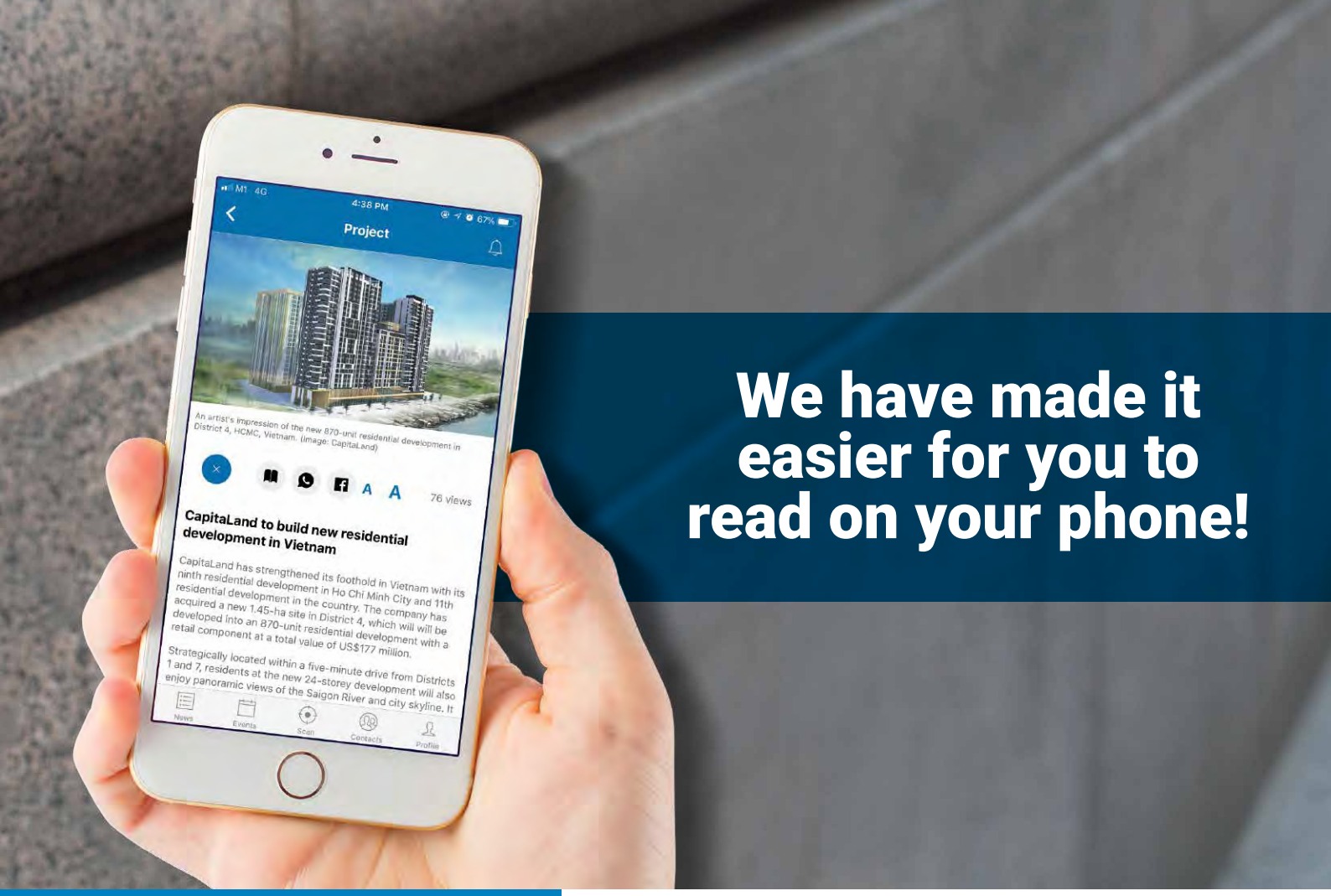
Electronic visitor management systems

Some organisations prefer to sign in their visitors by computer, which can save time at the front desk. This method typically provides an I.D. badge, often with a photograph, as well as a record of the visit that becomes part of the organisation's database

PROs and CONs:
Visitor information is recorded more uniformly, correctly and quickly when using a computerised VMS, especially when a driver's licence reader or business card scanner is used to record the information, versus having it typed in by hand, and you can include photos for better identity verification. Visitor information stored in a computer database, internal or external, allows you to search, sort, analyse, and retrieve data, helping you to keep track of current visitors and spot trends. And if you know that a particular visitor or group of visitors is coming in for a meeting, their information can be added to the system ahead of time.

But such a sophisticated system can cost thousands of dollars. This includes hardware, software (initial and license renewal fees), installation, networking, training, and support. Unlike a manual sign-in book, a computerised VMS takes time for staff to learn and troubleshoot. The more complicated a system the more pieces of it can malfunction, and it needs to work independently of your own computer network and internet connection, and even work during power outages. Then there are privacy concerns: the more information that is captured about visitors, the more they need assurances their data is protected and not wrongfully used.

It's hard to know how much security is enough. But visitor management is among the most affordable, easiest, and quickest ways to improve your security. SST



We have made it easier for you to read on your phone!

TRADECARDS GLOBAL

App features include

- Digital issue browsing
- Industry news update
- Events update
- Organisation listings

and more...

VISIT OUR WEBSITE AT
www.tradecardsglobal.com

Download **Tradecards Global** mobile application to browse and read our current and past issues of

bathroom +kitchen today
SEAB SOUTHEAST ASIA BUILDING
SOUTHEAST ASIA CONSTRUCTION
LAVA Lighting Audio Visual Asia
lighting today
Security Solutions Today

GET IT ON Google Play

Download on the App Store

Subscription Form

Fax your order today
+65 6842 2581

(Please tick in the boxes)

Southeast Asia Building

SINCE 1974

☐ 1 year (6 issues)

Singapore	S$45.00
Malaysia / Brunei	S$90.00
Asia	S$140.00
America, Europe	S$170.00
Japan, Australia, New Zealand	S$170.00
Middle East	S$170.00

Bathroom + Kitchen Today

SINCE 2001

☐ 1 year (4 issues)

Singapore	S$32.00
Malaysia / Brunei	S$65.00
Asia	S$80.00
America, Europe	S$130.00
Japan, Australia, New Zealand	S$130.00
Middle East	S$130.00

Southeast Asia Construction

SINCE 1994

☐ 1 year (6 issues)

Singapore	S$45.00
Malaysia / Brunei	S$90.00
Asia	S$140.00
America, Europe	S$170.00
Japan, Australia, New Zealand	S$170.00
Middle East	S$170.00

Lighting Today

SINCE 2002

☐ 1 year (4 issues)

Singapore	S$32.00
Malaysia / Brunei	S$65.00
Asia	S$80.00
America, Europe	S$130.00
Japan, Australia, New Zealand	S$130.00
Middle East	S$130.00

Security Solutions Today

SINCE 1992

☐ 1 year (6 issues)

Singapore	S$45.00
Malaysia / Brunei	S$90.00
Asia	S$140.00
America, Europe	S$170.00
Japan, Australia, New Zealand	S$170.00
Middle East	S$170.00

IMPORTANT

Please commence my subscription in _____ (month/year)

Personal Particulars

NAME: _____

POSITION: _____

COMPANY: _____

ADDRESS: _____

_____

TEL: _____ FAX: _____

E-MAIL: _____

Professionals (choose one):

☐ Architect ☐ Landscape Architect ☐ Interior Designer ☐ Developer/Owner

☐ Property Manager ☐ Manufacturer/Supplier ☐ Engineer ☐ Others

☐ I am sending a cheque/bank draft payable to:
Trade Link Media Pte Ltd, 101 Lorong 23, Geylang, #06-04, Prosper House, Singapore 388399
RCB Registration no: 199204277K * GST inclusive (GST Reg. No: M2-0108708-2)

☐ Please charge my credit card (circle one): Amex / Diner's Club
Card Number: _____ Expiry Date: _____

Name of Card Holder: _____ Signature: _____

ConnecTechAsia Summit
26–28 June 2018
Marina Bay Sands and Suntec City

New Mega Technology Event ConnecTechAsia Addresses Role of Accelerated Digital Change in Asia's Growing Economy

ConnecTechAsia, combining the strengths of industry stalwarts CommunicAsia, BroadcastAsia and the newly-launched NXTAsia, is the region's latest Mega Technology event, and will stage its inaugural edition from 26 to 28 June 2018 in Singapore.

With legacy events CommunicAsia and BroadcastAsia having served the telecommunications and broadcast media sectors respectively for nearly 40 years, the new NXTAsia builds upon this to bring new technologies that are shaping Asia's increasingly innovation-driven economy. With the advent of the Industry 4.0, ConnecTechAsia will present a holistic ecosystem of infrastructure, technology, and services that businesses and governments in Asia need to thrive in this new era.

"As Asia pursues digital transformation at an accelerated pace, it is critical that the event evolves alongside the dramatic shifts happening in the spaces we serve," said Mr Victor Wong, Project Director, UBM, organiser of ConnecTechAsia. "The new event reflects the pulse of Asia today, and is the only business platform covering the converging ecosystems of communications, broadcasting and emerging technologies connecting the physical and digital worlds."

At NXTAsia, industry professionals will catch the newest innovations and thought-leadership in areas such as Artificial Intelligence (AI), Augmented and Virtual Reality (AR/VR), Cyber Security, IoT, Robotics, Cloud and Data among others. NXTAsia will host promising start-ups, and the Singapore-leg of renowned start-up competition SeedStars, at tech showcase Disrupt+.

CommunicAsia, Asia's most established international industry event for the telecommunications sector, will focus on Network Infrastructure/FTTx, satellite communications and telecom software and services—the latest technologies to help companies and governments in Asia prepare for the coming of 5G and maintain a competitive edge in the communications and digital world.

With on-demand and streaming services surging in popularity, BroadcastAsia will shine a spotlight on the future of broadcasting, exploring how we have consumed news and entertainment over the past decade, and the challenges and opportunities this creates for traditional broadcasters and OTT players. BroadcastAsia will highlight

technologies that are reshaping the value chain, such as the latest innovations in UHD/HDR, IP Broadcasting, Live Production, Content Media Security, OTT and Alternative Content Platforms.

ConnecTechAsia Summit—Digital Business Transformation

The ConnecTechAsia Summit this year centres on Digital Business Transformation, covering the hottest trends across ICT, broadcasting industries and enterprises to enable a digitalised future. The three-day summit comprises three tracks—NetworkComms, BroadcastMedia and EmergingTech—that will drive business growth and sustainability.

5G, Network Virtualisation, Satellite Communications and Network Slicing will be the main topics in the NetworkComms track, while The Future of Television, Monetisation Strategies, Social Video, IP Broadcasting, 4K, AI and Immersive technologies for broadcasting will feature in the BroadcastMedia track. Topics of the EmergingTech track will include: Artificial Intelligence/Machine Learning, Blockchain Technology, Cybersecurity, IoT, Data Analytics, Seamless Commerce/Digital Payments, Connected Industries, IoT, Augmented, Virtual and Mixed Reality, and Smart Cities.

Key speakers include:

- Professor Howard Michel, CTO, UBTech
- Jassem Nasser, Chief Strategy Officer, Thuraya Telecommunications Company
- Geert Warlop, Chief Operating Officer, TrueMoney International

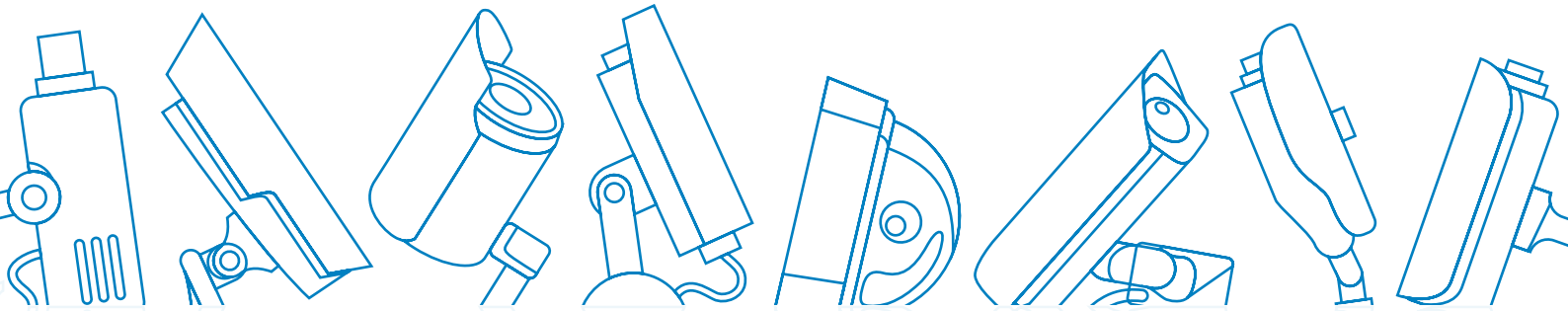
- Rene Werner, Chief Customer Service & Customer Experience Officer, Celcom Axiata Berhad
- Leah Camilla R. Besa-Jimenez, Chief Data Privacy Officer, PLDT
- Ian Yip, Chief Technology Officer—Asia Pacific, McAfee
- Arvind Mathur, Chief Information Technology Officer, Prudential Assurance
- Bill Chang, Chief Executive Officer—Group Enterprise , Singtel
- Parminder Singh, Chief Commercial and Digital Officer, Mediacorp
- Sanjay Aurora, Managing Director—Asia Pacific, Darktrace

"Presenting a holistic ecosystem of digital convergence and a platform for the discovery and understanding of new frontiers of innovation to elevate the global standing of Asian business and governments sits at the heart of what ConnecTechAsia stands for," adds Mr Wong. "Continuing the 40-year legacy of CommunicAsia and BroadcastAsia, the new ConnecTechAsia will continue to serve Asia as we embark on the journey of the Fourth Industrial Revolution."

For more information, please visit: www.connectechasia.com SST

ADVERTISERS' INDEX

Our tribute to Safety & Security...



TradeCards Global mobile application is offering **50% discount** for one-year organisation listing to suppliers and service providers that serve our Safety & Security Community. With the reduced price of USD500 / *SGD700 for one-year organisation listing, suppliers and service providers get to enjoy an ***additional 10MB of product listing*** tagged to your organisation listing.

Visit **www.tradecardsglobal.com** to sign up for a new account and your organisation listing. Input "**SECURETRIBUTE**" as promo code before proceeding to payment page. The promo code is valid until 31 December 2018.

*Rate excludes 7% GST applicable for Singapore-registered companies

TRADECARDS GLOBAL

Supporting mobile version of:

SEAB · Southeast Asia Construction · Security Solutions Today · bathroom + kitchen today · lighting today

GET IT ON Google Play

Download on the App Store

BOSCH
Invented for life

MIC IP Cameras

Find out more at **boschsecurity.com**

Intelligent Video Analytics in the most demanding environments