

Security Solutions Today

May / June 2017

IMMIGRATION & BORDER CONTROL

Cover Focus

Protecting Borders from Vehicle Attack on Land and Sea

Inside Look

2017 Cybersecurity Predictions

Security Feature

Anatomy of a Secure Travel Document & More



Scan this code to visit our website









ONE STEP TO SMARTER Control Center Solution



End-end surveillance control center solution

- High-performance LCD panel with ultranarrow seam for vivid image presentation
- Various image control: split, merge and roam
- Multi-services: preview, playback & alarm linkage display
- Flexible operation for front-end devices via controller & VMS software
- Multi-screen inter-action to make your business easy

RELATED PRODUCTS

Video Wall	Matrix	Monitor & Display Bracket	Keyboard	VMS Software	STORAGE
					
- DHL550UCM-ES -	- M70-4U-E -	- DHL22/27/32/42/49/55 -	- NKB1000 -	- DSS4004 -	- EVS5024S-R -

CE FC CCC UL ROHS ISO 9001:2000



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



HD300 High Security Electronically-Controlled Barrier



DSC720 High Security Bollard



DSC1200 High Strength Surface Mounted Barricade



DSC2000 High Security Barricade



DSC501 High Security Barricade



DSC288 High Security Sliding Gate



DSC207 High Security Shallow Foundation Barricade



DSC7000 High Security Beam Barrier



DSC600 High Security Shallow Foundation Fixed Bollard



DSC1100 High Strength Portable Barrier



TT207SFM High Security Surface-Mounted Barricade



DSC7500 High Security Swing Beam Barrier



TT212 High Strength Beam Barricade



TT280 High Security Linear Crash Gate

Delta Keeps Them Stopped!

18,000+ Systems Deployed Around the World!

Stopping a bomb-laden car and SUV from penetrating the entrance to a consulate to guarding against vehicle assaults at dams, border crossings, court houses, embassies, capitol buildings, palaces, hotels, headquarters buildings and many other types of important facilities, Delta's bollards, barricades, beams, barriers, gates and guard booths keep vehicles stopped, keeping people and property safe in over 130 countries throughout the world since 1974.



CONTENTS

May-June 2017



6	CALENDAR OF EVENTS	
8	EDITOR'S NOTE	
	IN THE NEWS	
10	Around the World	
29	Eye on Asia	
	COVER FOCUS	
38	Protecting Borders from Vehicle Attack on Land and Sea	
	APPLICATION STORIES	
41	Biometric Scans Comply with Impending Privacy Legislation	55
43	Cognitec Face Recognition Technology Supports Growing Demand for eGate and Airport Security	56
43	Biometrics and Border Security	
44	First County in Maine Installs Body Scanner from Smith's Detection	58
45	Morpho Detection Wins Bristol Airport Contract For CTX Hold Baggage Explosives Detection Systems	60
46	Biometrics at the Borders	
48	Canadian Airports Implementing Facial Recognition Technology	
	CASE STUDIES	
50	Chile Adopts Modernised Electronic ID Documents	
51	Toshiba's Business Solutions (USA) Augments and Improves Headquarters Security with the help of Tyco	
52	Biometric System for Iraqi Border Patrol Security	
53	Swedish Epassport and National eID	
54	Arecont Vision Megapixel Cameras	
	SECURITY FEATURES	
62	Biometrics and Banking	
64	Get the Most Out of Your Security Cameras	
66	Anatomy of a Secure travel Document	
	INSIDE LOOK	
68	Extract from 2017 Cyber Security Predictions	
	IN FOCUS	
71	An Interview with Mr. Daniel Elvin, Regional Director – Asia Pacific, Oncam	
	SPECIAL PRODUCT FEATURE	
73		
	PRODUCT SHOWCASE	
79		
	AFTERTHOUGHT	
90	A Glimpse into the Next Frontier of Airport Security	
	POST SHOW REPORT	
92	Milestone America: 12th Milestone Integration Platform Symposium (MIPS)	



BOSCH

Invented for life

They see a fun day of shopping.

You see smart data to help increase sales.

Bosch empowers you to build a safer and more secure world. And with built-in video analytics as of the IP 4000 cameras, we allow you to use video data for more than security alone. Anything from improving sales to increasing customer experience.

Find out more at boschsecurity.com



People counting



Queuing alarm



Enforcing safety regulations



Publisher

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

Editor

Melissa Teo (sst@tradelinkmedia.com.sg)

Radio Technology Consultant

Martin Gillmon (martin.gillmon@tradelinkmedia.com.sg)

Group Marketing Manager

Eric Ooi (eric.ooi@tradelinkmedia.com.sg)

Marketing Manager

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

Marketing Executive

Racheal Chong (racheal.chong@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 Credit: Pexels.com
Globe Vector Credit: Freepik.com
Designed by Fawzeeah Yamin

Printed in Singapore by KHL Printing Co Pte Ltd.

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: 65-68422580 Fax: 65-68422581
ISSN 2345-7104 (Print)

The magazine is available free-of-charge to applicants in the security industry who meet the publication's terms of control. For applicants who do not qualify for free subscription, copies will be made available, subject to the acceptance by the publisher, of a subscription fee which varies according to the country of residence of the potential subscriber in the manner shown on the right.

The editor reserves the right to omit, amend or alter any press release submitted for publication. The publisher and the editor are unable to accept any liability for errors or omissions that may occur, although every effort had been taken to ensure that the contents are correct at the time of going to press.

The editorial contents contributed by consultant editor, editor, interviewee and other contributors for this publication, do not, in any way, represent the views of or endorsed by the Publisher or the Management of Trade Link Media Pte Ltd. Thus, the Publisher or Management of Trade Link Media will not be accountable for any legal implications to any party or organisation.

Views and opinions expressed or implied in this magazine are contributors' and do not necessarily reflect those of Security Solutions Today and its staff. No portion of this publication may be reproduced in whole or in part without the written permission of the publisher.

ANNUAL SUBSCRIPTION:

<u>Surface Mail:</u>	
Singapore	- S\$45 (Reg No: M2-0108708-2 Incl. 7% GST)
<u>Airmail:</u>	
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

ComNet is the Solution to Your Communication Challenge





GUARANTEED PERFORMANCE

TODAY - AND TOMORROW

When *network dependability is critical*, the *transmission products you choose today* affect how *your network performs tomorrow*.

ComNet - Communication Solutions for the Long Term

- Only ComNet Offers a Complete Fiber Optic, Copper, and Wireless Communication Solution
- ComNet Products are MADE IN THE USA 
- Exclusive **LIFETIME WARRANTY** 
- Experienced ComNet Customer Care Specialists Who Understand Your Application are Here to Support Your Every Need

www.comnet.net

comnet
Communication Networks
sales-europe@comnet.net
+44 (0)113 307 6400

See what ComNet can do for you.

Security Australia | Stand D16 | 26 - 28 July

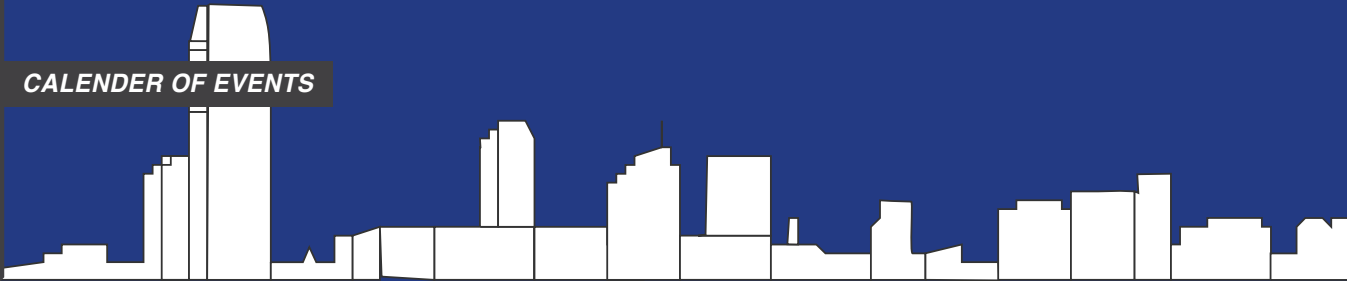
IFSEC SE Asia | Stand P121 | 6 - 8 September



WWW.COMNET.NET

MADE IN THE USA 

LIFETIME WARRANTY 



CALENDAR OF EVENTS 2017-2018

MAY

IFSEC Philippines 2017
 Date: 3 - 5 May 2017
 Venue: SMX Convention Centre,
 Pasay City, Metro Manila
 Organiser: IFSEC Philippines
 Website: www.ifsec.events/philippines

Communic Asia 2017
 Date: 23 - 25 May 2017
 Venue: Marina Bay Sands, Singapore
 Organiser: Infocomm Media
 Development Authority and
 Govtec Singapore
 Telephone: +65 6233 6638
 Website: www.ifsec.events/philippines
 Email: CommunicAsia@sesallworld.com

JUNE

Infocomm 2017
 Date: 14 - 16 June 2017
 Venue: Orange County Convention
 Center, Orlando, Florida, USA
 Organiser: InfoComm International and
 Samsung
 Telephone: +1.703.273.7200
 Website: www.infocommshow.org
 Email:
InfoCommAttendee@experient-inc.com

IFSEC International 2017
 Date: 20 - 22 June 2017
 Venue: ExCel London, London, UK
 Organiser: IFSEC International
 Telephone: +44 (0)20 7069 5000
 Website: www.excel-london.co.uk
 Email: ifsecustomerservice@ubm.com

JULY

INTERPOL World 2017
 Date: 4 - 6 July 2017 (Congress)
 5 - 7 July 2017 (Exhibition)
 Venue: Suntec Singapore
 Organiser: Interpol
 Telephone: +65 6389 6613
 Website: www.interpol-world.com
 Email: layeng.see@interpol-world.com

SEPTEMBER

IFSEC Southeast Asia
 Date: 06 - 08 September 2017
 Venue: Kuala Lumpur Convention
 Centre, Kuala Lumpur, Malaysia
 Organiser: IFSEC SE Asia
 Telephone: 6-03-2176 8788
 Website: www.ifsec.events/sea
 Email: tj.tan@ubm.com

OCTOBER

Safety and Security Asia 2017
 Date: 4 - 6 Oct 2017
 Venue: Marina Bay Sands, Singapore
 Organiser: Cems Conference and
 Exhibition Management Services
 Telephone: +65 6278 8666
 Website: www.safetysecurityasia.com.sg
 Email: info@cems.com.sg

China Public Security Expo 2017 (CPSE 2017)

Date: 29 Oct - 1 Nov 2017
 Venue: Shanzhen Convention and
 Exhibition Centre, Shenzhen,
 China
 Organiser: Futian District
 Government, Shenzhen Security &
 Protection Industry Association and
 CPSE Exhibition Co. LTD
 Telephone: +86-755-88309123
 Website: www.cpse.com.cn
 Email: overseas_market@cps.com.cn

NOVEMBER

Secutech Thailand 2017
 Date: 16 - 18 Nov 2017
 Venue: Bangkok International Trade and
 Exhibition Centre, Bangkok,
 Thailand
 Organiser: Messe Frankfurt
 Telephone: +66 2 726 1999
 Website: [www.secutechthailand.
 tw.messefrankfurt.com](http://www.secutechthailand.tw.messefrankfurt.com)
 Email: [jason.cheng@newera.
 messefrankfurt.com](mailto:jason.cheng@newera.messefrankfurt.com)

DECEMBER

IFSEC India 2017
 Date: 6 - 8 December 2017
 Venue: Pragati Maidan, New Delhi, India
 Organiser: IFSEC
 Telephone: +91 (0) 11 66517606
 Website: www.ifsec.events/india
 Email: pankaj.jain@ubm.com

JANUARY 2018

Intersec 2018
 Date: 21 - 23 Jan 2018
 Venue: Dubai International Convention
 and Exhibition Centre, Dubai
 Organiser: Messe Frankfurt Middle East
 Telephone: +971 4 389 4500
 Website: www.intersecexpo.com
 Email:
andreas.rex@uae.messefrankfurt.com

MicroEngine®

Integrated Security Systems

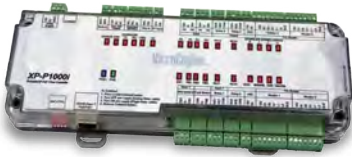
The Trusted Brand in Security Solutions

Plato DesFire Reader



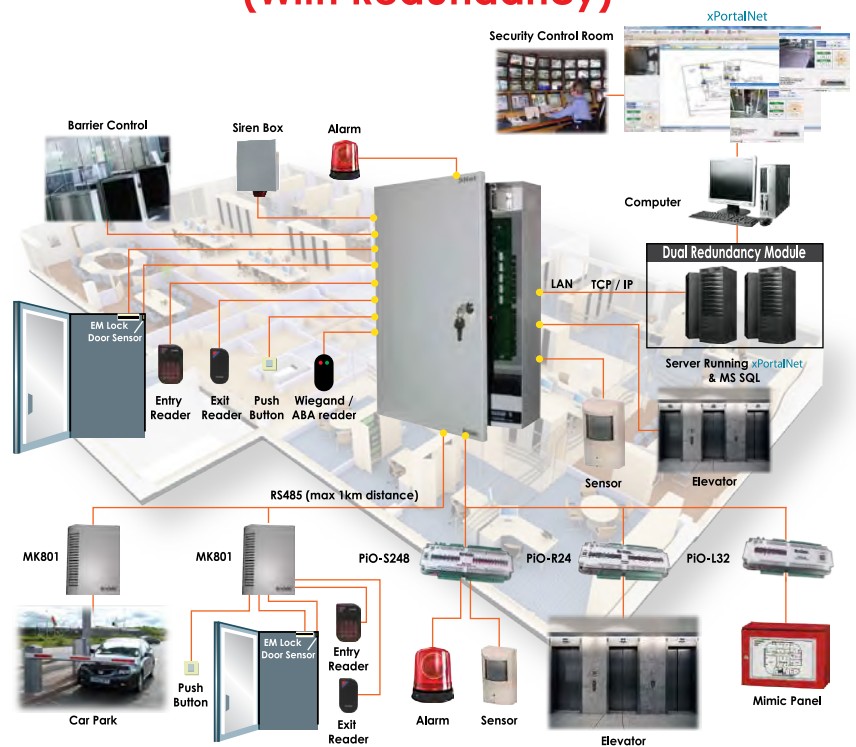
- ▶ 64 Bit Programmable Card ID
- ▶ Encrypted with 3DES
- ▶ Card ID Not by Serial Number

P1000i PoE Controller



- ▶ PoE with Battery Charger
- ▶ AES128 Encrypted IP
- ▶ Support 1 Door/2 Readers

Integrated Security System (With Redundancy)



Projects



Commercial /
Complex



Factory



Condominium



Plato Reader - Slim Card Reader



600+ readers ward access & security system on SQL Server for hospital and many more ...

enquiry@microengine.net
www.microengine.net



Our Office





Dear esteemed readers,

We welcome you to the May/June issue of Security Solutions Today. As always, it is our absolute pleasure to present you with the latest happenings in the security industry in concurrence with market trends and current events.

This focal point of this issue centres on a topic that has dominated the news in the recent months – securing America's borders. The issue of border security is multi-dimensional and leads us into a provocative portal of politics and precaution versus privacy and personal freedom. We present you with articles on the latest security solutions being implemented at airports in the United States as well as around the world, in light of President Trump's plans to tighten border security. This issue will also focus on case studies of how biometrics assists immigration officials in securing ports of entry as well as examine how state of the art passports are making a difference in travel today. Also featured are case studies on how security solutions implemented in banking and corporate offices have created safer working environments for staff and reduced liabilities at the same time.

Our Inside Look will focus on securing the cyber realms in terms of threat predictions in 2017. Our line-up of Security Features this month focus on biometrics in banking, specifically the measures being employed to prevent identity theft which has become commonplace in our era of internet dependency, as well as the problem of passport fraud and the technology that is used to eradicate it. Also included is an article by TycoIS advising organisations on security optimising strategies that make the best use of surveillance cameras.

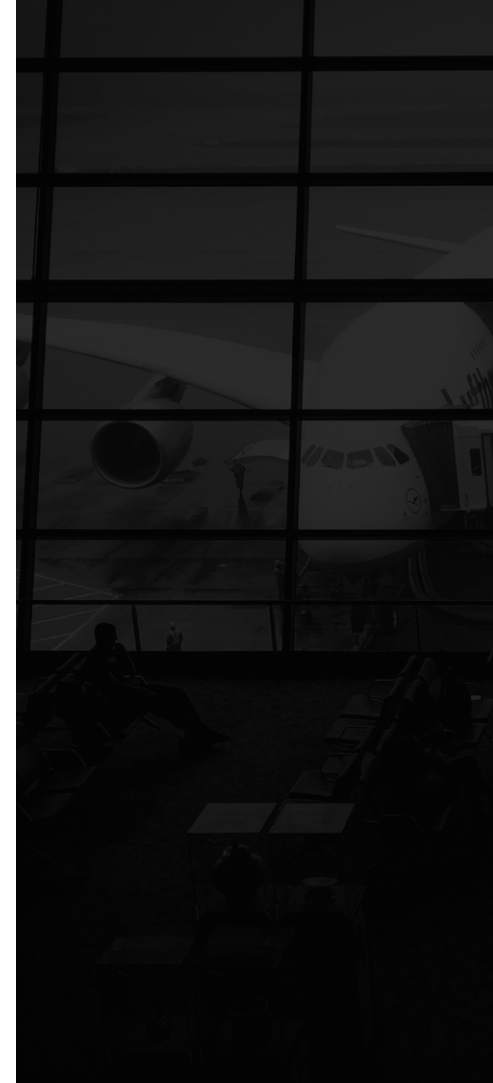
In line with the theme of airport and border security, we are pleased to present to you, an exciting array of products designed to assist homeland security agencies and immigration officials, such as chemical and explosive detectors, CCTV and IP surveillance cameras and biometric access control systems including a pocket sized iris detection device.

In this issue's In Focus, we present to you an interview with Oncam's APAC Sales and Business Development Manager Mr. Daniel Elvin on the company's cutting edge cameras and the company's wealth of experience in a diverse range of industries including the Banking sector.

We conclude this issue on a contemplative note with an exciting afterthought in the form of a futuristic feature on the next frontier of airport security that is currently being tested out by the Canadian Border Security. Robotic Detection could soon become a common fixture in airports around the world. Do read the back page for details on this science fiction reminiscent technology.

I certainly hope this issue proves to be as informative and intriguing for you as it was for me in researching and compiling it for your reading pleasure. SST looks forward to bringing you a kaleidoscope of interesting themes and stories in the year ahead.

Melissa T
Editor



YOUR SOURCE FOR SECURITY SOLUTIONS

Congress: 4-6 July 2017 | Exhibition: 5-7 July 2017
Suntec Singapore Convention & Exhibition Centre



EXHIBITION HIGHLIGHTS



PUBLIC SAFETY
TECHNOLOGIES



BIOMETRICS



IDENTITY
SOLUTIONS



FORENSICS AND
INVESTIGATIONS



CYBERCRIME

WHAT TO EXPECT

300

international solution
providers and
manufacturers

10,000

professionals and
buyers from public
and private sectors

30%

international visitors

20 hours

of informative sessions with
topics on cybercrime, safe
cities and identity management

INTERPOL World Congress registration is now open.

Register by 31 May 2017 to enjoy early bird rates.

www.interpol-world.com

E: visitor@interpol-world.com

[in](#) [t](#) [f](#) [v](#) [+](#) #INTERPOLWorld

EVENT OWNER



SUPPORTED BY



INDUSTRY INSIGHTS BY



HELD IN



MANAGED BY

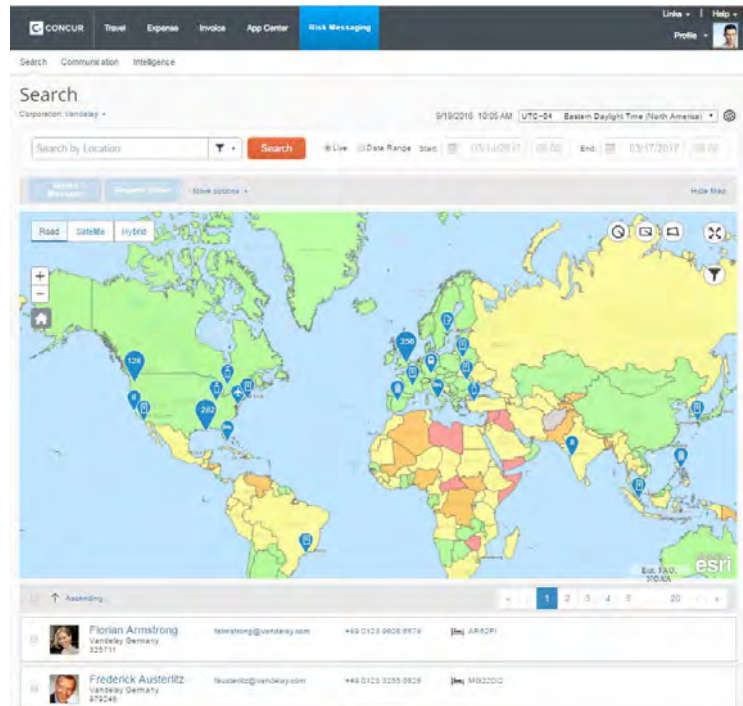




Concur Unveils First Integrated Traveler Risk Management Solution and Active Monitoring Service to Help Companies Manage Employee Safety 24/7, Anywhere in the World

Bellevue, Washington - Concur, a SAP company and the world's leading provider of travel, expense and invoice management solutions, has introduced the first integrated traveler risk management solution featuring the most comprehensive, actionable travel and expense data set in the industry. The new solution also includes an option for 24/7 monitoring services to help communicate with and assist employees at any time on a company's behalf, from pre-travel guidance to emergency safety information.

"With global uncertainties and business travel on the rise, Concur has a strong sense of responsibility for our employees and customers around the world," said Mike Eberhard, President of Concur. He elaborated that from civil unrest to natural disasters and terrorist attacks, businesses need to be sure they know where their employees are and direct them to safety as quickly as possible. Concur's data set extends beyond traditionally booked travel itineraries, maximising visibility and empowering businesses to take action in such situations. During recent global incidents, Concur was able to locate employees in affected areas within an hour.



Unlike other solutions, Concur Risk Messaging will capture unrivaled traveler location data via Concur Travel and Expense, Concur Mobile, Concur TripLink, TripIt from Concur, supplier e-receipts and more, providing travel managers immediate and unparalleled visibility into employees that may be at risk. Concur Active Monitoring, powered by HX Global will offer 24/7 monitoring, proactive communication capabilities and assistance coordination. This enables businesses to deliver on their commitment to ensure employee safety and well-being as they travel across time zones and outside of business hours.

In 2016, Concur issued more than 10 million alerts notifying business travelers of potential risks in locations they were visiting. The number of Concur users who received alerts also increased by 770 percent from 151,000 users in January 2016 to 1.3 million users in December 2016.

Additional Concur Risk Messaging and Active Monitoring features include:

- The ability to issue pre-travel advisories
- Two-way messaging via text, email, phone, and Concur Mobile
- Traveler location mapping and reporting
- Incident analysis and reporting
- Custom message and alert creation

Concur previewed new travel risk management capabilities at its annual Fusion customer conference in Chicago. Concur Risk Messaging and Active Monitoring will become available to global customers in 2017. **SST**



@IFSECSEA #IFSECSEA



IFSEC SOUTHEAST ASIA



IFSEC Southeast Asia

SECURITY • FIRE • SAFETY

PROVIDING GLOBAL INNOVATION AND EXPERTISE TO THE SOUTHEAST ASIAN SECURITY, FIRE AND SAFETY MARKETS

6 - 8 SEPTEMBER 2017
KUALA LUMPUR CONVENTION CENTRE, MALAYSIA

- More than **350** world-renowned brands on the show floor!
- Witness the latest products in CCTV, Access Control & Biometrics, Home Automation, Cyber Security, Perimeter Protection, Occupational Health & Safety, Fire Detection & Prevention and more!
- Join with over **9,000** industry experts and trade buyers coming from **51** countries!
- Obtain knowledge for **FREE** at the IFSEC Technology Showcase



More info at www.ifsecsea.com



UBM



Gemalto and IER Create The Complete Self-Service Airport Experience for Travellers

Amsterdam, Netherlands – Gemalto, the world leader in digital security, and IER, a leading designer of solutions that improve the flow of goods and people, have teamed up to create Gemalto and IER Fly to Gate, an end-to-end self-service airport experience for travellers.

Airport travel is booming and in 2016, there were 3.8 billion passengers. The International Air Transport Association (IATA) expects this to double by 2035. This means that the industry and authorities will need to deploy automated solutions to optimize the flow of passengers while guaranteeing stringent security.

Gemalto and IER Fly to Gate answers the growing need for a self-service experience that takes travellers smoothly from their home to the departure gate. A typical Gemalto and IER Fly to Gate departure solution gives the traveller the choice between mobile check-in or self-service kiosks and includes bag drop points, border control, security and boarding gates.

This innovative offer combining IER's self-service equipment and services with Gemalto's border management solutions opens a swift and secure biometric pathway through the airport.

Gemalto and IER Fly to Gate supports multimodal biometric verification including facial recognition, robust document verification and straightforward integration with immigration systems, enabling rigorous standards of security and outstanding operational efficiency for airports and airlines.

The solution offers complete flexibility to meet individual airport operator requirements, and the potential to make virtually all traveller handling processes automatic. By putting the passenger in control of their airport experience, Gemalto and IER's joined-up approach reduces queueing, as well as the stress and strain associated with air travel. Airports and airlines also benefit from the enhanced customer experience, with travellers enjoying more free time in leisure and retail facilities.

Maxime Boulvain, CEO at IER said that for airports and airlines alike, the opportunities created by strong growth in passenger numbers go hand in hand with the challenges of more stringent border and security checks. This new partnership between IER and Gemalto squares the circle, utilising world-class automation techniques



„FLY TO GATE“

Enabling speed and security at every passenger touch point with biometric authentication.



to improve customer satisfaction, implement consistent identity and document verification procedures as well as maximise commercial revenues.

Frédéric Trojani the Executive Vice President of Government at Gemalto said that the appetite for automated, self-service travel experiences is already evident in the success of electronic travel authorisation, online check-in and automated border eGates. He added that for the first time, Gemalto and IER Fly to Gate offers a chance to reap the full benefits of this trend, working with leading partners whose solutions have been proven in numerous deployments. **SST**



@IFSECPH #IFSECPH



IFSEC PHILIPPINES



IFSEC Philippines

SECURITY • FIRE • SAFETY

Providing global innovation and expertise to the emerging security, fire and safety market of the Philippines

3 - 5 MAY 2017

SMX CONVENTION CENTRE, PASAY CITY, METRO MANILA

- More than **150** world-renowned brands on the show floor!
- Witness the latest products in CCTV, Access Control & Biometrics, Home Automation, Cyber Security, Perimeter Protection, Occupational Health & Safety, Fire Detection & Prevention and more!
- Join with over **5,000** industry experts and trade buyers coming from from around the nation
- Obtain knowledge for **FREE** at the IFSEC Technology Showcase



More info at www.ifsec.events/philippines



UBM



Ideagen Launches New Enterprise Safety Management and Incident Reporting Software, Ideagen Coruson

Ideagen unveils “definitive and visionary” product in re-brand of flagship software application

Software firm Ideagen is delighted to announce the launch of launched Ideagen Coruson – a definitive and visionary re-brand of its enterprise safety management and incident reporting software.



Gael Enlighten, a cloud-based software solution used by some of the world’s leading brands including Virgin Trains, Telefonica and Haeco Group, will now be known as Ideagen Coruson from 22nd February 2017.

The re-brand project comes as Ideagen seeks to align its product portfolio following several successful acquisitions in recent years. The Gael Enlighten software was part of the intellectual property purchased in the £18million acquisition of Gael Ltd in December 2014.

Ideagen CEO, David Hornsby was quoted as saying that the time had come to “retire” the Gael brand. He added that Ideagen is delighted to announce the renaming of Gael Enlighten to Ideagen Coruson, which will modernise the product brand and bring it into conformity with the rest of the organisation’s product suite.



As an important part of Ideagen’s portfolio of governance, risk and compliance applications, Coruson has matured over the past two years and has many high-profile customers. The application is fully productised, commercialised and generally available. Given its visionary nature, the time had arrived to retire the Gael brand name and launch the definitive version of the product brand.

“These are exciting times for Ideagen as an organisation and we are looking forward to Ideagen Coruson playing an integral part of the company’s future success, said Mr. Hornsby.

Ben Dorks, Ideagen’s Chief Customer Officer added the ambitiously significant re-brand of one of the organisation’s most prominent, market leading products is truly an exciting event. Customers have also welcomed the re-branding project much to the delight of Ideagen.

Ideagen Coruson comes with a fresh new colour palette and appearance but the popular architecture and roadmap of the software remains entirely the same thus cementing its place as the most user-friendly enterprise cloud safety and incident reporting software on the market.

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

secutech

THAILAND

16 – 18 November 2017
Bangkok International Trade &
Exhibition Centre (BITEC), Bangkok
www.secutechthailand.com

SMART AND SAFE CITIES FOR TOMORROW

PREMIER PLATFORM FOR
SHOWCASING INNOVATIONS IN
SMART & SAFE CITY SOLUTIONS



Event Highlight of Secutech Thailand 2017 – Demo Zone

In the 2017 edition, Secutech Thailand will introduce real intelligent solutions – real world scenario display creating a smart city solution experience.

The Smart and Safe City Complex demo zone will feature various popular vertical solutions in the Thai security market, such as hotel, retail, city surveillance, transportation, etc.



Secutech Thailand — Bringing "Smart" into Security Solutions

In 2017, Secutech Thailand will
showcase six theme zones to meet
the market demands:

- Security
- Smart Home
- Smart Retail
- Safe & Smart City
- Fire & Safety
- Disaster & Prevention



Target Visitors

• **Business nature:**
systems integrators, installers,
importers, distributors, retailers,
developers, system designers,
security service providers and
manufacturers

• **Vertical Markets:**
government, transportation,
construction, enterprise,
finance, telecommunication,
retail, hospitality, public law
enforcement

Global contact

Messe Frankfurt New Era Business Media Ltd | Mr Jason Cheng | Tel: +886 2 8729 1099 ext 215 | stth@newera.messefrankfurt.com

WORLDDEX
Group of Exhibition Companies



messe frankfurt



Bosch Security Systems Drives Forward Its Video Security Business Together with Sony

Grasbrunn, Germany – After the official approval of the antitrust authorities, the business partnership of Bosch Security Systems and Sony Corporation in the field of video security solutions became effective by February 1, 2017 except for in China where the partnership will start on April 1, 2017.

Both companies will now focus on strengthening their collaboration that was first announced in November 2016. The partnership comprises of both a sales and marketing cooperation as well as a technical collaboration. As part of the sales and marketing partnership, Sony's video security sales and marketing associates joined a newly formed dedicated team within the Bosch Security System organisation. Sony's video security customers, in all markets except Japan, will be served and supported by this sales and marketing team.

“We are happy to welcome these experienced colleagues in our organization and are convinced we will further grow the business with Sony's products by providing excellent support and service to our customers”, says Michael Hirsch the Vice President for Sales and

- **Business partnership officially approved by antitrust authorities**
- **Bosch takes further steps in cooperation with Sony towards setting new standards in the field of video security solutions**
- **Sony's associates join new dedicated sales and marketing team within Bosch Security Systems.**

Marketing of the Sony Security Business within Bosch. “We are delighted that Sony's video security customers are now being supported by Bosch Security Systems. We are moving forward with this partnership which will feature jointly developed products that fully leverage our industry-leading expertise in video image quality and performance”, adds Toru Katsumoto, Deputy President of Imaging Products and Solutions Sector, President of Professional Products Group, Sony Corporation.

Regarding the technical cooperation, both companies are aiming to set new standards with regard to high resolution video imaging, combined with excellent light sensitivity, complemented by Bosch's expertise in built-in video analytics and latest bitrate management techniques.

In March 2017, Sony will launch eight new Full-HD (1080p) video security cameras within its sixth generation (G6) range of network cameras, meeting the ever-increasing demand for greater image clarity within the video security market. New G6 cameras' high sensitivity capabilities ensure that the color integrity of images is maintained even in extreme lowlight situations.

At the same time, Bosch is updating its portfolio concerning video analytics and bitrate management. Starting as of May 2017, all network cameras from the IP 4000 series will be equipped with built-in video analytics as a standard as well as latest bitrate management techniques combined with H.265 video encoding, reducing bitrate by up to 80 percent. Both Sony's and Bosch's innovations will be presented at the ISC West 2017 (April 5- 7) in Las Vegas, USA.

The first jointly developed products are expected to be launched in 2018. “We are looking forward to delivering best-in-class video security solutions to our customers for both existing and new market segments”, says Gert van Iperen, President of Bosch Security Systems.

*For more information, please visit: www.bosch.com **EST***



THE WORLD'S BIGGEST SECURITY TRADESHOW



THE 16TH CHINA PUBLIC SECURITY EXPO

Oct 29-Nov 1, 2017 | Shenzhen Convention & Exhibition Center

The 14th China Public Security Forum
The CPSE Golden Excellence Award 2017
GSIA Gold Shield Award 2017



Exhibition Area (m²)

110,000

Exhibitors

1,100

Visitors

130,000

Booths

6,000





High End Automobile Dealership Innovates with Morse Watchmans KeyBank® Touch

Oxford, Connecticut – As the saying goes, “You only get one chance to make a first impression” – and at Mercedes-Benz in Sydney, Australia, management makes every effort to ensure the first impression is a good one. From the luxurious showroom to the state of the art service bays, every detail throughout the three-story dealership is optimized for customer satisfaction in keeping with the brand identity.

To safeguard this quality and level of service, management relies on a number of technology innovations including the Morse Watchmans KeyBank Touch key management system. The system features aesthetically attractive cabinets that are used for storing and tracking vehicle keys. They are located throughout the facility and are connected on the internal network. Every time a key cabinet is accessed to remove or return a vehicle key, the activity is automatically recorded including the name of the individual and the time and date of the activity. Only authorized users can access the cabinets and they can only take keys they have been

pre-programmed to access.

“Key control is vital in an automobile dealership and our KeyBank Touch system more than meets our needs,” said Keith McArdle, General Sales Manager of Mercedes-Benz Sydney. “From its ease of use to the money saved in eliminating lost keys, it hits on all cylinders.”

KeyBank Touch cabinets for keys belonging to new and used car are located in the showroom and service department, while high volume KeyBank cabinets are installed in the warehouse and storage center. Keys are logged into the system upon vehicle arrival at the dealership and are then attached to a locking device with a unique identification chip and secured in the key cabinet. As the vehicle is moved about the facility, the system keeps track of its location and at all times, management knows the location of every key registered in the system such as who has which keys out and when they are to be returned. They can check the information in real time on their PC as well

as receiving an email alert when a specific key – such as one for a high value automobile – has been accessed or returned.

Management can quickly audit the status or history of any vehicle and custom reports provide insight into model popularity, employee performance and vehicle use. Key usage information can also be analysed for sales and marketing effectiveness, further adding to its operational value. Sales staff can reserve a demo car with the system or with the KeyFind feature, quickly check to see which automobiles are in and available for a demonstration or sale. A group release function lets management sequentially distribute keys for demo vehicles so they get equal use.

“Convenience and feature-rich capabilities are key to the success of KeyBank Touch at the dealership,” said Fernando Pires, VP Sales and Marketing, Morse Watchmans. “Together they increase the security and efficiency of the organization.”

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

Delta Scientific Announces Upgrades to Popular Portable MP5000 Barrier

Palmdale, California - Delta Scientific, the leading manufacturer of counter-terrorist vehicle control systems used in the United States and internationally, today introduced a new universal voltage DC power unit for its popular portable MP5000 vehicle barrier. As a result, the MP5000 can now be efficiently deployed in remote locations and areas that have limited power options but requires that same level of functionality that a hard wired pump-based portable

unit provides in a city setting, including Emergency Fast and multiple control options.

“For instance, the barrier plate will rise as fast as two seconds, creating a sound portable solution for final denial applications in remote locations such as dams or other sites needing protection from terrorist vehicle attacks,” reports Delta Vice President-Sales and Marketing Greg Hamm. “In addition, the control circuit

continue on page 19



in the new Hydraulic Power Unit (HPU) provides easy integration of various control options such as keypads, card readers, RFID, key fobs, wireless transmitters and computer networks.”

Along with the power unit upgrade, Delta also added a new safety option that builds upon that of traditional vehicle presence loop detectors. The new option provides self-contained IR beams into the portable barriers that will stop the barrier plate if a vehicle or pedestrian crosses the sensors.

Delta’s totally self-contained MP5000 mobile deployable vehicle crash barriers carry a K8 rating (M40 ASTM rating), stopping 7.5 ton (6400 Kg) vehicles traveling 40 mph (64 kph). They tow into position to control vehicle access within 15 minutes. No excavation or sub-surface preparation is required. Once positioned, the mobile

barricades will unpack themselves by using hydraulics to raise and lower the barriers off their wheels. DC-powered pumps will then raise or lower the barriers. Once the event is over, procedures are reversed and the barriers are towed away.

The MP5000s were recently used successfully in protecting attendees and spectators at the recent presidential inauguration of President Trump in Washington, DC. Delta always keeps an inventory of the MP5000s for purchase and quick delivery at their manufacturing facility in Palmdale, California. In many cases, they are needed for events that come up quickly such as politician or celebrity visits and other unexpected incidents.

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

Louroe Electronics Debuts Next Generation Advanced Audio Technology at ISC West

Verifact® A USB Microphone and AOP530 Speaker Microphone improve integration with network devices and enrich sound clarity

Van Nuys, California – Louroe Electronics, the world leader in audio monitoring within the security industry, will introduce next generation advanced audio technology at ISC West 2017 with two new products, the Verifact® A USB microphone and AOP530 speaker microphone. Both products boast new features that improve network device integration, installation time and sound clarity. The official release date for the Verifact® A USB and AOP530 is April 3, 2017 and both will be showcased at Louroe’s booth, number 8038.

The all-new Verifact® A USB microphone features a USB connection with architecture enabling direct connection to USB hubs or computers, simplifying installation and creating plug-and-play audio for almost any application. The microphone is

self-powered from the USB hub, eliminating the need for any external power source and includes a gain adjustment switch for sensitivity control. Additionally, the microphone incorporates Louroe’s new Smart Tube design that enables a wider frequency response capture for improved analytics performance.

The AOP530 is a two-way speaker microphone with echo cancellation and full-duplex communication. The AOP530 connects directly to IP cameras and encoders that support two-way, line level audio. The vandal-resistant housing makes it ideal for both indoor and outdoor applications and its blue illuminated pushbutton makes it easily identifiable in low-lit areas.

“Our new Verifact® A USB and AOP530 products improve audio monitoring while keeping current



with 21st century technology,” said Richard Brent, CEO of Louroe Electronics. “They require minimal installation, increasing the cost-savings. The overall value of the technology for both the integrator and end user is higher given its performance benefits.”

Both products are optimal for the law enforcement, commercial, education, banking and healthcare sectors.

For more information, please visit: www.louroe.com/iscwest2017 SST



Delta Scientific Gearing Up for Increased U.S. Border Crossing Vehicle Checkpoints

Palmdale, California - Delta Scientific, the leading manufacturer of counter-terrorist vehicle control systems used in the United States and internationally, today announced that not only is it developing new products to take on the increased protection of vehicle checkpoints between the United States and Mexico as part of the Trump Administration's plan to better secure the border but it is also designing new manufacturing flexibilities into its planning cycles. The projects will require growing numbers of hydraulic barricades, bollards, traffic control barriers, portable barricades, beam barriers, sliding gates and guard booths.

"While the projects have not yet been funded, plans are already being created to upgrade vehicle checkpoints along the 1250 miles of the U.S./Mexican border," reports Greg Hamm, vice president of sales and marketing for Delta Scientific. "Once building commences, the government wants all checkpoints operational in less than three years."

At present, the United States Border Patrol operates 71 traffic checkpoints, including 33 permanent sites along the border. Over the years, Delta has implemented vehicle crossing protection at many of the most secure sites including El Paso, San Ysidro, Calexico, Otay Mesa and Tornhill-Guadalupe.

The most recent Delta project at San Ysidro provides a glimpse into what future point of entry checkpoints will entail. Located between San Diego and Tijuana, it is the busiest land port in the world, processing an average of 50,000 northbound vehicles per day and features 50 custom-designed bullet-resistant guard booths, K4 rated swing gates, barriers and bollards.

In addition to the booths, products in the \$5 million project also included beam barricades that are counter-balanced, hinged semaphore type gates consisting of a crash beam, support and pivot assembly, steel foundation implants, cast-in-place concrete buttresses, and locking and anchoring mechanisms. The crash beam incorporates a high strength wire rope that is firmly attached to both buttresses when the crash beam is in the down position. In a collision, the energy of the impact is transmitted through the crash beam to the buttress and the foundation.

*For more information, please visit: www.deltascientific.com **ESST***

Oncam Expands Investment in India, APAC Markets with New Regional Directors

Emerging market share for comprehensive, intelligent video technology spurs growth

London, UK - Oncam, the leading provider of 360-degree video capture and business intelligence technology, today announced the promotion of sales leaders Daniel Elvin and Abhishek Kumar to Regional Directors in the APAC and South Asia regions, respectively. The move is in response to the overwhelming growth of the security and business intelligence markets in these dynamic regions, and increasing demand from target customers in both the private and public sectors.

In these roles, Elvin and Kumar are tasked with developing and implementing strategic sales and business development plans to increase market share that supports the overall corporate strategy in 2017. These leaders will also be responsible for building and maintaining strong relationships with regional partners, overseeing a sales team and coordinating marketing efforts. Elvin is based in Hong Kong, and Kumar is based in Delhi, India. They will both report to Scott Brothers, Executive Vice President - Corporate Development.

Elvin joined Oncam from Axis Communications where he served as the Regional Business Development Manager for the North Asia regional headquarters and previously held the positions of Business and Partner Development Manager and Lead Engineer for the video analytics team. Elvin brings extensive knowledge and experience in video surveillance technology to the Oncam team, with specialized regional expertise in Asia. He holds a Master of Science degree in

continue on page 21



electrical engineering from Lund University in Lund, Sweden.

Kumar also joined Oncam from Axis Communications, where he was the Regional Manager for Key Accounts in both the Delhi and Mumbai markets. Prior to Axis, he worked as the Assistant General Manager of Marketing and Business Head for Electronic Security Solutions at Godrej Security Solutions, where he was instrumental in building strategies to support ongoing sales success, including business planning and alliances, product management and pricing strategies. Kumar holds a Master of Business Administration degree in

international business and marketing from the Institute of Management Technology in Ghaziabad, India.

“Oncam has experienced significant growth in both the APAC and Indian markets, necessitating the need for strong leadership within these regions,” said Brothers. “The promotion of these dedicated industry professionals signifies our dedication to customers and channel partners, who see multi-dimensional video capture and business intelligence technology as the next step in more safety and security for a variety of vertical markets. We are excited about the continued momentum and expansion in these areas.” **SST**

JFK Terminal 1 Improves Security with Milestone Video

IP platform provides significant upgrade with increased usability, efficient storage and enhanced system integration with Agent Vi analytics

Copenhagen, Denmark - Milestone Systems open platform IP video management software (VMS) has been installed at JFK International Airport’s Terminal 1 to help manage the safety of more than 27 million passengers a year.

Previously, T1 at JFK relied on a limited analog surveillance system and an older IP system that were independent of each other. Both were inadequate and lacked some necessary functionality. Operators could only view video from specific workstations, it was difficult to replace or add cameras, and the system did not integrate easily with other systems.



Migrating the terminal’s old analog system to an advanced IP video management software platform was no small feat. Due to the airport’s high-security environment, the system and all of its cameras had to remain operational around the clock throughout the migration.

To design and implement the new solution, the airport worked with security integrator Media Wire, LLC, who designed and implemented a Milestone XProtect Corporate VMS solution to manage its 500 to 600 cameras, including the installation of 160 new network cameras from Axis Communications. Providing greater access to video, the Milestone Mobile client is used by air terminal managers to view video on their smartphones.

“We installed an extensive 10 gig fiber network to support the bandwidth needed for current and future cameras. All cameras provide video at the maximum resolutions and frame rates, no corners are cut,” said Laszlo Tordai, Owner, Engineer and Technician at Media Wire. “It is simply unacceptable to minimize the system’s capabilities and performance because a component is not up to par with the rest of the system. We are keeping this a top-notch installation.”

Migrating Terminal 1’s system required upgrades to ensure a solid solution from the ground up. New high-speed fiber optics, switches, PoE injectors, software, workstations and operating systems were installed. Tordai estimates the terminal has close to one Petabyte of storage due to both security requirements, and powerful analytics from Agent Vi that are used on recorded video and to search across camera views.

continue on page 22



The new system is easily scalable and can accommodate additional cameras at any time. Terminal 1's new Axis cameras easily integrated with the Milestone system and require less bandwidth that better allow the security team to meet the airport's lengthy storage requirements.

"When you look at a whole system and deploy the right parts, you actually save the customer a lot of money," Tordai said. "It's a win-win across the board."

*For more information, please visit: www.milestonesys.com **ESST***

SDI Statement on House Homeland Security Committee Report on America's Aviation Security

Edgewood, Maryland - Smiths Detection Inc. (SDI) President, Dan Gelston issued the following statement in response to a new report from the House Homeland Security Committee entitled, "America's Airports: The Threat from Within." This statement includes an announcement of a pilot project with Miami International Airport on a first-of-its-kind airport employee screening project.

"This report provides further evidence for what experts have known for a long time, that despite employee background checks and access control measures at airports, the 'insider threat' remains one of the greatest threats to aviation. As a result, technology solutions must play a key role in addressing this issue. We commend U.S. Representative John Katco (NY-24), Chairman of the House Homeland Security Committee's Transportation and Protective Security Subcommittee, for releasing this important report.

"The report makes clear that only a two-pronged approach to combatting the 'insider threat' at airports - namely relying on people (background checks) and process (access control) -- is leaving a dangerous gap in efforts to mitigate the threat. A truly comprehensive approach to preventing criminal and terrorist acts in airports must include threat detection technology solutions with multi-view X-ray and Explosives Trace Detection (ETD), paralleling those seen at passenger checkpoints around the world. Such non-intrusive screening technologies assure greater security without sacrificing speed, accuracy or efficiencies.

"The report also correctly notes that targeted screening, which relies on the right technology solutions with portable capabilities, offers airport operators increased visibility into threats in their facilities. Furthermore, it provides effective deterrence while supporting

continued operational efficiency and minimizing costs.

"With over 40 years' experience, Smiths Detection has insight into the security challenges of regulators, airlines and airport professionals and has helped them to prevent explosives, chemical weapons, guns and other contraband from getting onto airplanes and crossing borders. We look forward to using that experience to work with Congress and airport operators to help them make the critical security improvements called for in this report."

Most recently, in a focused effort to assist U.S. airport operators with the myriad complexities associated with employee screening, SDI has partnered with Miami International Airport in a first-of-its-kind employee screening pilot project. The MIA pilot, launched in January of this year, deploys SDI's latest capabilities in multi-view x-ray and explosive trace detection equipment placed in one of MIA's industry-leading employee checkpoints. The pilot is designed to help develop a replicable concept of operations and demonstrate high-accuracy threat detection coupled with fast and efficient movement of employees through the screening experience.

"Over a decade ago, MIA made the commitment voluntarily to invest in employee screening absent any federal requirements because we felt it was the right thing to do," said Emilio T. González, Miami-Dade Aviation Director. "We have renewed our commitment to this important component of airport crime-fighting and anti-terrorism by partnering with SDI in an effort to again raise the bar and demonstrate the art of the possible."

*For more information, please visit: www.smithsdetection.com **ESST***



ENGIE Ineo, Milestone and Axis Secure the Council of Europe Buildings

The Council of Europe has upgraded its video safety solutions at the Strasbourg campus thanks to dedicated efforts by Milestone community partners

Copenhagen, Denmark - Milestone Systems, the number one open platform company in networked video management software (VMS), has collaborated with partners ENGIE Ineo and Axis to upgrade the Council of Europe's (headquarters in Strasbourg, France) video surveillance systems. The security project was managed by Milestone community partners Securitas and ENGIE Ineo.




The security solution, which has been live since January 2017, has secured the Council's vast campus including the Human Rights Building, European Directorate for the Quality of Medicines & Healthcare, the European Center for Youth and the Agora building. A security surveillance and monitoring solution was installed in all access areas including the entire external perimeter. The contract also includes a five-year maintenance agreement.

ENGIE Ineo partnered with Milestone and Axis for their video expertise (video management software and network cameras respectively). The legacy analog surveillance system has been replaced with a full network video surveillance solution that delivers better performance including ease of access and retrieval of video assets, as well as a flexible solution that allows the Council to tailor how locations are secured. With Milestone's XProtect solution, the organization is now able to handle all its video safety operations through a single management interface as well as manage other security devices such as gate control systems and thermal cameras.

The project was designed to keep disruption to a minimum, taking into account the busy schedule of the Council of Europe, particularly during parliamentary sessions.

Amine Sadi, Country Manager France, Milestone Systems, said: "This project has once again demonstrated how effective our partnerships are. The way that we work and collaborate with the teams at ENGIE Ineo and Axis has contributed significantly to the success of this impressive installation. With Milestone's solution, the Council of Europe now has the right surveillance management technology in place. It is perfectly tailored to their needs in terms of accessibility, scalability, cost, ease of use and performance."



For more information, please visit: www.milestonesys.com 



Palo Alto Networks Completes Acquisition of LightCyber

Bringing Award-Winning Automated Behavioral Analytics to the Palo Alto Networks Next-Generation Security Platform

California - Palo Alto Networks® (NYSE: PANW) the next-generation security company announced its acquisition of LightCyber®, a privately held cybersecurity company that has developed award-winning, highly automated and accurate behavioral analytics technology. Under the terms of the agreement, Palo Alto Networks acquired LightCyber for \$105 million in cash.

Recognised by Gartner in two recent market guides*, LightCyber has been leading the industry in the development of automated behavioral analytics capabilities through the use of sophisticated machine learning to quickly, efficiently and accurately identify attacks based on identifying behavioral anomalies inside the network.

Palo Alto Networks will continue to offer the LightCyber products and support existing customer implementations while it engineers the technology into the Palo Alto Networks' Next-Generation Security Platform by the end of the calendar year. Bringing behavioral analytics to the platform will enhance its automated threat prevention capabilities and the ability for customer organisations to prevent cyber breaches throughout the entire attack life cycle.

Mr. Mark McLaughlin the Chairman and CEO of Palo Alto Networks was quoted as saying that the

LightCyber team's vision to bring automation and machine learning to bear in addressing the very difficult task of identifying otherwise undetected and often very sophisticated attacks inside the network is well-aligned with their organisation's platform approach. He added that the technology will complement the existing automated threat prevention capabilities of Palo Alto's platform to help organisations improve and scale their security protections to prevent cyber breaches.

Palo Alto Networks has been driving a paradigm shift in the security industry with its natively engineered and highly automated Next-Generation Security Platform designed to change how organisations prevent cyber breaches. Gonen Fink, CEO of LightCyber said that the organisation is pleased to join the Palo Alto Networks team in combining the technology innovations of both organisations which will serve to accelerate the adoption of behavioral analytics to help organisations bolster their defenses against the advanced and sophisticated adversaries they are facing in current times.

Automated Attack Behavior Analytics Enhances Breach Prevention

According to a report by the Ponemon Institute, when attackers successfully find their way into a

network, there is an industry average dwell time of approximately five months to discover their activity. During that time, an advanced attacker can initiate command and control lateral movement and data exfiltration. This can lead to extensive damage and loss of confidential data.

Common approaches to this problem include third-party log-based collection and analysis tools that are often error-prone limited in visibility, lacking important context and are labor-intensive. They also require a data scientist to investigate false positives, tuning for accurate outcomes, and furthermore lack enforcement capabilities.

To address these challenges, reduce attacker dwell time, minimise damage done and prevent breaches, the LightCyber technology employs highly accurate and automated machine learning techniques to analyse user and entity activity and then identify and protect against anomalous activities that are indicative of an active attack.

This behavioral attack detection capability complements the existing protections delivered by the Palo Alto Networks platform to help security team members to focus on only the most meaningful alerts and improve the time to breach response and prevention.

For more information, please visit: www.paloaltonetworks.com 



RLHC Selects Hospitality Software Leader Cendyn for CRM and Loyalty

The cloud-based software company was chosen based on its ability to handle multiple, complex systems and leverage real-time data to heighten guest experiences

Boca Raton, Florida - Cendyn, a cloud-based hospitality software and services company was selected as the technology partner by RLHC (Red Lion Hotels Corporation) for the company's CRM and "Hello Rewards" loyalty program.

Cendyn was chosen for its ability to easily handle complex interfaces, leverage real-time data to drive true one-to-one communications, and provide sophisticated guest intelligence, reporting, and analytics.

"It's imperative for us to partner with companies that are at the cutting edge of their disciplines," said Bill Linehan, EVP and CMO for RLHC. "In trusting Cendyn with our CRM and the 'Hello Rewards' loyalty program, we anticipate ROI for our owners and satisfied guests at our hotels."

Cendyn will implement a state-of-the-art guest intelligence solution that will collect data from multiple property systems to provide real-time, personalized

communication to guests and roll out insight to staff for over 1,100 hotels within the RLHC portfolio.

The enterprise Hotel CRM solution combines first and third-party data sources to deliver dynamically generated, one-to-one marketing across digital marketing channels: Email, Web, Display, Mobile, and Social. The result is increased guest satisfaction and loyalty and significantly higher ROI for RLHC and its franchise hotel owners.

"We understand the relationship a company has with its guests is a highly-valued bond that we don't take for granted," said Charles Deyo, CEO of Cendyn. "That's why it was important for us to be a partner who not only is able to anticipate guests' needs in advance of their stay, but will use data-driven marketing to ensure RLHC guests are informed before, during and after their on-property experience."

*For more information, please visit: www.cendyn.com **ESST***

Sterlite Tech Showcases India's First Smart City Services Success at MWC, Barcelona

Integrated Smart Services Include IP Surveillance, Smart Lighting, Public Address, Face Detection, Command Centre and City-wide Wi-Fi at Public Places

Barcelona, Spain - Sterlite Tech, a global technology leader in smarter digital infrastructure announced deployment of first Smart City Services in India for the Government of Gujarat. Sterlite Tech led the end-to-end design, development and management of Gandhinagar city to be the first Wi-Fi Capital City of India with citizen-centric Smart City Services.

The successful deployment enables Gandhinagar with city-wide Wi-Fi connectivity and installation of integrated Smart City subsystems including IP-based CCTV Surveillance, Smart Lighting, Face Detection, Public Address System, Central Command Centre with Help Desk. A 24x7 call centre will address citizen complaints and queries. All Smart City Services implemented in Gandhinagar Smart City can be controlled and monitored through the Central Command Centre. This will help the government to offer citizen-centric efficient connectivity and innovative services as well as bring transformative changes in the everyday lives of the citizens.

Nikhil Jain, MD of Elitecore said that the Smart City Services project is a benchmark in digital infrastructure and

continue on page 26



brings smarter living experiences to the citizens of Gandhinagar. He expressed that the organisation is proud to be associated with Gandhinagar Municipal Corporation in the creation of high-end Smart City infrastructure.”

Sterlite Tech’s strong expertise as a System Integrator with leading government projects has enabled best practices in implementing standard procedures to meet smart city objectives. Gandhinagar Smart City Services, through urban infrastructure, is successfully addressing needs of the citizens and empowering them with easy access to real-time information.

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

New SentiVeillance 6.0 Improves Speed and Accuracy for Biometric Identification Using Surveillance Cameras

SentiVeillance 6.0 from Neurotechnology includes new face detection and tracking algorithms and support for up to 10 surveillance cameras with one GPU for faster, easier, more accurate identification.

Vilnius, Lithuania - Neurotechnology, a provider of high-precision biometric identification and object recognition technologies, today announced the release of the SentiVeillance 6.0 software development kit (SDK), which provides improved facial recognition using up to 10 surveillance, security and public safety cameras on a single computer.



The new version uses deep neural-network-based facial detection and recognition algorithms to improve accuracy, and it utilises a Graphing Processing Unit (GPU) for enhanced speed. Also, now users can more quickly and easily adjust the tradeoff between speed and accuracy as needed for different applications.

“We developed SentiVeillance 6.0 as a self-adapting system based on deep neural networks that were trained on a larger quantity of data, said Ignas Namajunas, surveillance technologies research lead for Neurotechnology. This ensures better generalisation for a variety of conditions. Additionally, by making use of the GPU processing capabilities, we were able to improve the processing speed significantly.”

SentiVeillance 6.0 can process information from up to 10 surveillance cameras with one GPU, it provides faster, easier, more accurate identification of faces against watch lists, making it suitable for a wide range of surveillance applications. As with previous versions, the new SentiVeillance also provides real-time moving object detection; tracking and classification for pedestrians, vehicles and other predefined object classes based on size and speed of movement; and area control that triggers events when people or objects enter, leave or stay in restricted areas.

The SentiVeillance 6.0 SDK is available through Neurotechnology or from distributors worldwide. For more information and trial version, go to: www.neurotechnology.com. As with all Neurotechnology products, the latest version is available as a free upgrade to existing SentiVeillance customers.

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



Toshiba Introduces High-Resolution 5MP Bullet Camera with Enhanced Nighttime Video Surveillance

Irvine, California - Deploying megapixel cameras in outdoor video surveillance applications can be a real challenge. While video during the day is typically crystal clear, at night it may be blurry, dark or washed out, making it useless for retrospective analysis.

To combat this all too common problem, Toshiba Surveillance & IP Video Group, a business unit of Toshiba Information Systems, Inc., today introduced its new J-WB51A five-megapixel IP bullet camera. Built rugged for outdoor deployment, it is specifically designed for 24/7 video surveillance with a powerful nighttime feature-set highlighted by adaptive IR LEDs, day/night IR cut filter and True Wide Dynamic Range that ensures forensic-quality video, even in complete darkness or adverse weather. The adaptive IR LEDs have a range of up to 30 meters or approximately 100 feet, plus will automatically adjust the LED intensity to avoid over-exposure of close objects.

Speed and Resolution

The J-WB51A's 5MP CMOS sensor achieves brilliant image quality whether monitoring large outdoor areas or when zoomed-in for the smallest of details. High frame rates of 30 fps at full resolution of 2560 x 1920 permits reliable capture of fast-moving objects, such as a car speeding or a suspect running. When combined, this speed and resolution delivers a superior level of detail that can make the difference when analyzing relevant information in the scene.

High resolution megapixel video presents serious limitations for network bandwidth and storage capabilities, especially when capturing moving objects. The J-WB51A leverages Smart Codec H.265 video compression to minimise video storage and bandwidth needs without sacrificing image quality by allocating bandwidth only to moving objects and not to the background. Multi-streaming in H.264, H.265 and motion-JPEG further optimizes the balance of video quality, storage and networking requirements. In addition, users are given the option of a 90° portrait view to only video stream narrow areas of interest such as a hallway, warehouse or retail aisle.

Weatherproof and Vandal-Resistant

Toshiba applied its vast experience in outdoor IP surveillance to the J-WB51A. Not only does it comply with the stringent IP66 weatherproof rating, it is also rated IK10 vandal-resistant as a precaution against tampering and theft. As such, the camera is highly resistant to impact, difficult to readjust or open by a non-professional, and its cabling is protected by a management bracket to minimise unauthorised access.

Advanced Features

Value-enhancing features of the J-WB51A include defogging and imaging stabilisation, PoE (802.3af), audio in/out and ONVIF Profile-S/Profile-G.

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



Toshiba's J-WB51A five-megapixel IP bullet camera is built rugged for outdoor deployment with a night time feature-set highlighted by adaptive IR LEDs, day/night IR cut filter, and True Wide Dynamic Range that ensures forensic-quality video in complete darkness or adverse weather. Also featured, is the option of a 90° portrait view to only video stream narrow areas of interest Rated IK10 vandal-resistant and IP66 for weather-proof performance. ONVIF compliant.



IrisGuard Releases its Avant-garde Outdoor EyeHood® Iris Camera for Speedy Iris Registration and Verification

Milton Keynes, United Kingdom - IrisGuard Inc., the world's leader in secure iris recognition payment technologies, today announced the introduction of the EyeHood® imager which is the latest addition to IrisGuards already extensive EyePay® Platform camera portfolio.

The unprecedented handheld EyeHood® device is the world's most accurate, portable and convenient Iris & Face imager, ideally well suited for outdoor enrollments and recognitions, where the camera fully shields the user from direct sunlight and other external lighting conditions both at mobile or stationary enrollment and verification stations, thus providing excellent iris quality images and subsequent pristine matching results which is of decisive importance in all-encompassing payment and identity systems.

The EyeHood® was specifically designed to meet the most difficult outdoor registration challenges such as humanitarian itinerant enrollment stations in harsh and severe operational settings where speed, accuracy and immaculate image quality are of prime relevance particularly in demanding financial payment applications for unbanked, non-banked and financially underprivileged communities such as vulnerable refugees and internally displaced person (IDP). The EyeHood® plays a preponderant role during the registration process, by faultlessly providing a unique identity record for each refugee / IDP person which in turn helps protect them and provide the needed access to financial services and food assistance which serves them with dignity and renders them

more independent.

The EyeHood® camera features patented IrisGuard countermeasures against all known vulnerabilities in combination with the avant-garde built-in cryptography hardware chipset rendering the EyeHood® camera the most technologically advanced, cryptographically secure and easy-to-use iris imager on the market presently (see brochure for details). Furthermore, the EyePay® Platform generates completely encrypted independent IrisPrints (iris templates) protecting users from identity thief and ensuring their privacy when using the system at all times.

The EyeHood® can speedily enroll and recognise eligible beneficiaries in real time outdoor situations anywhere in the world no matter the size of the database in less than three seconds. The EyeHood® performance and accuracy are unprecedented in the industry.

The EyeHood® hosts a newly engineered proprietary auto-focus lens together with a patented fast focus adjustment software capability to ensure rapid iris recognition in order to capture a user's in-focused iris image at extremely fast speeds, second to none in the industry. This is an essential component conducive



to streamlining the capture process and to ensure that only flawless iris images are captured hence reducing the overall acquisition time which is of critical significance in holistic iris recognition applications. Unlike other similar-looking imagers on the market today, the automatic "fine focus" feature with its amazing mega-pixel sensor ensures unprecedented quality suitable for amassing databases of millions of people in rapid time without sacrificing iris image quality unlike inferior fixed-depth-of-field iris cameras on the market today.

The primary purpose of the EyeHood® camera, according to Imad Malhas, CEO & Founder of IrisGuard Inc., is to be able to offer to our United Nations humanitarian agencies and international NGO customers a unique iris camera enabling operational staff to enroll and recognise millions of vulnerable beneficiaries they serve daily with perfect iris quality images for authentication services such as financial inclusion, remittances, cash withdrawals and food assistance in real time at remote locations throughout the world with ease and convenience meeting the highest industry standards in iris recognition obtainable today.

The cost-effective patented EyeHood® sets new heights in iris recognition camera technology and is globally available for IrisGuard worldwide deployments today. **SST**





Palo Alto Networks Opens New APAC HQ in Singapore

More Than Double the Size of Its Previous Floor Space, the New Office Will Provide Regional Customer Support, Training Facilities and an Expanded Cybersecurity Solutions Lab

Singapore – Palo Alto Networks®, the next-generation security company, today announced the opening of its new Asia-Pacific headquarters in Singapore. Located in the heart of the central business district at Guoco Tower, the new office spans a floor space of 35,000 sq. ft which is more than double its previous space at Millenia Tower and was officially opened today by Dr. Yaacob Ibrahim, Minister for Communications and Information and the Minister-in-charge of Cyber Security.

The new office will enable Palo Alto Networks to expand services and support for customers within and beyond the Asia-Pacific (APAC) region. The office will be the base for many cybersecurity personnel in the region including systems engineers, Unit 42 security analysts and threat intelligence specialists. It will provide regional support capability for customers of Palo Alto Networks, expanding the company's worldwide network of support centers.

Unveiled two years ago to provide opportunities for users to learn about cybercrime-fighting technologies, the Palo Alto Networks cybersecurity solutions lab has expanded to support a broader range of Palo Alto Networks technologies, including our next-generation firewalls, Aperture™ security offering for software as a service (SaaS), and WildFire™ cloud-based threat analysis service.

The Palo Alto Networks commitment to APAC is also underscored by its drive to promote cybersecurity education in this region. In January of this year, Palo Alto Networks released *Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers – Singapore*, providing a collection of actionable insights and advice from key cybersecurity stakeholders in the country.

Outside of Palo Alto Networks APAC headquarters in Singapore, the company has offices in Australia, China, Hong Kong, India, Indonesia, Japan, Malaysia, New Zealand, South Korea, Taiwan, Thailand and the Philippines. **ESST**





CA Technologies Positioned a Leader for Identity Governance and Administration

Gartner Recognizes CA Identity Suite for Ability to Execute and Completeness of Vision in 2017 Gartner Magic Quadrant

Singapore – CA Technologies (NASDAQ:CA) has been positioned by Gartner, Inc. in the Leaders quadrant of the 2017 Gartner Magic Quadrant for Identity Governance and Administration (IGA). The report evaluated CA Identity Suite, a comprehensive identity management and access governance solution with a simple, intuitive user experience.

Vendors were evaluated on their ability to execute and completeness of vision.

According to the report, “IGA Leaders deliver a comprehensive toolset for governance and administration of identity and access. These vendors have successfully built a significant installed customer base and revenue stream, and have high viability ratings and robust revenue growth. Leaders also show evidence of superior vision and execution for anticipated requirements related to technology, methodology or means of delivery. Leaders typically demonstrate customer satisfaction with IGA capabilities and/or related service and support.”

In a survey of more than 100 CA Identity Suite Users, 70 percent report that using CA Identity Suite has reduced costs more than 25 percent. The virtual appliance reduces costs even further with installation and configuration time going from days to minutes. Organisations also can avoid high recurring software licensing costs with the appliance providing pre-installed instances of an operating system, application server and directory.

“Identity and governance administration isn’t just about compliance; it’s also about protecting the expanded attack surface that we see in today’s hybrid IT environments,” said Lim Teng Sherng, vice president, Security, Asia Pacific & Japan, CA Technologies. “CA Identity Suite is a comprehensive IGA solution that helps our customers secure their enterprises by proactively managing identity and access rights for all their users and applications, whether in the cloud or on-premises.”

For more information, please visit: www.ca.com 

Star India Deploys HID Mobile Access to Improve Security and User Experience for 2,500 Employees at Their Corporate Headquarters

News Highlights:

- Star India deployed HID Mobile Access powered by Seos to secure doors at its 32-story building in Mumbai.
- The new mobile-centric solution eliminates the need for access cards and improves user experience while reducing costs related to card re-issuance.
- The demand for mobile access solutions gains momentum in Asia Pacific as smart organisations go mobile-first.

HID Global®, a worldwide leader in trusted identity solutions announced that its HID Mobile Access® solution, powered by Seos® had been selected by Star India, the country’s largest multimedia entertainment company to secure the entrances and doors of its Mumbai headquarters. Star India issued 2,500 mobile IDs to the smartphones of their employees and installed numerous mobile-ready iCLASS SE® readers at doors and gates throughout the 32-story building.

“As India’s largest multimedia company, we have extremely high security standards,” said Sumir Yadav, Senior Vice President (Administration and Facilities) with Star India. He added that HID Global known for being the market leader of access control solutions was able to fulfill all their requirements. With HID Mobile Access, it is now possible for companies to take advantage of the latest technology in our mobile-first era and achieve better security without being intrusive or compromising the user experience.

Mobile IDs, a core component of HID Mobile Access were provisioned via the solution’s robust online portal making it possible for Star India’s IT administrators to issue or revoke mobile IDs quickly easily and efficiently. Whenever a new employee joins the company, the IT administrators can

continue on page 31



effortlessly enroll them into the system by simply sending the employee an email invitation. The system-generated email contains directions and an activation code for the recipient to download and use the HID Mobile Access App. Upon entering the code and successfully activating the app,

the employee can then begin using their mobile device to unlock doors and gates at Star India.

50% of the world's companies will enact bring-your-own-device (BYOD) programs by this year, as predicted by Gartner resulting in increased employee satisfaction and cost reduction while driving innovation through countless applications and new opportunities transcending traditional mobile email and communications.

“As more businesses adopt bring-your-own-device (BYOD) policies and cloud initiatives, an increasing number of customers in the Asia Pacific look to us to

provide a modern and cost-effective solution for their mobile-driven and secure workplaces. HID Mobile Access supports the broadest range of mobile devices from smartphones to wearables. These can also be used in addition to traditional card access, giving companies the privacy protection and convenience they have come to expect from HID Global, at the pace that is aligned with their changing business goals,” said Alex Tan, Director of Sales, Physical Access Control System, HID ASEAN.

Feedback on HID Mobile Access from Star India employees has been positive and the company is currently exploring options to deploy HID Mobile Access to secure its canteen and collaboration spaces. Star India is also considering expanding the scope of the solution to cover the management of visitors and enable secure printing in the future.

Star India received the IFSEC India Awards 2016 in “Excellence in Security Initiatives” for their implementation of HID Mobile Access with HID Global’s “Twist and Go” gesture technology. The award is a user implementation accolade that recognises the excellence and innovations of CSOs and security officers who work behind ensuring robust security for their organisations.

For more information, please visit:
www.hidglobal.com **SST**

Epsilon Launches Infiny On-Demand Connectivity Platform

Infiny delivers a comprehensive set of enterprise, voice, local access, Cloud and global connectivity services from a single self-service platform

Singapore - Epsilon, a privately owned global communications service provider, has launched its Infiny by Epsilon platform to give users on-demand access to its suite of connectivity solutions.

Users are able to procure and manage Epsilon’s services via Infiny’s web-based portal, APIs, and Android and iOS mobile apps. They can use the self-service platform to procure local, regional and global port-to-port, port-to-Cloud, port-to-Internet Exchange, SIP Trunking and last mile DIA and SD-WAN services.

“Infiny is the result of more than a decade of simplifying how our partners connect and deliver services around the globe. We have taken our core set of services and made them available via a simple and powerful platform. It removes the friction from voice, data and local access services and delivers truly Cloud-centric networking,” said Jerzy Szlosarek, CEO at Epsilon. “We have reduced the complexity of global networking to a mobile app and web based portal, delivering networking as a utility in the form of a fully adaptable API. This is a step change in our industry.”

From the Infiny.cloud web portal, partners gain complete visibility into their service status with click-to-connect

continue on page 32



provisioning and back end automation. Partners also have the option to use the Infiny.io API to plug Epsilon's services directly into their existing platforms.

"Infiny enables users to manage global connectivity on-demand. They can see network performance and analytics while adding new services directly from a smartphone. It is that simple. Infiny puts Data Connectivity, Direct Cloud Access, SIP Trunking and Last Mile services in the palm of your hand and removes the limits from networking," Carl Roberts, Chief Commercial Officer at Epsilon. "The user is in control of their services and gains a set of services that they turn up at the click of a button."

Infiny is supported with bespoke intelligent networking technology that enables it to offer guaranteed quality of service end-to-end and around the world. Each service is accessible from the platform in a modular format. Epsilon's Cloud Link eXchange (CloudLX) platform will become a module of Infiny. Its SD-WAN module will enable users to connect enterprise locations globally.

"When the network is a utility, it becomes easier to innovate. Software and application developers are no longer restricted by the lack of agility in traditional networks. They can rollout services knowing the network will be able to support them and offer the flexibility and adaptability they need. Infiny supports the entire ecosystem and turns the network into a driver for innovation," said Szlosarek.

Android and iOS apps will be available for download in March 2017. Users that pre-connected to Epsilon will be able to request a login into these apps, allowing them the ability to procure and monitor services, anytime anywhere.

For more information, please visit: www.epsilonintel.com **SSST**

NICE Survey Reveals an Opportunity for Contact Centers to Improve Customer Service by Using Voice Biometrics Technology

Singapore - NICE announced the results of its Asia Pacific Voice Biometrics Consumer Survey. The survey revealed



that consumers are overwhelmingly in favor of companies using voice recognition to authenticate their identity when interacting with a contact center. This saves times for both customers and contact center agents and eliminates frustration caused by forgotten passwords or wrong answers to traditional security questions.

NICE's survey of 900 consumers in Australia, Hong Kong, India, Indonesia, Philippines and Singapore discovered the following:

- 46 percent of respondents rated their current experience of authenticating themselves when engaging with a contact center as somewhere between neutral and terrible. Just nine per cent said it was 'great.'
- 55 percent of people said having to answer security questions (which are usually personal) to a stranger via telephone when they're in a public place is their biggest frustration when trying to authenticate themselves.
- Consumer readiness to accept voice biometrics for contact center authentication is high: 88 percent were open to voice biometrics. Of the people who had never heard of voice biometrics, 81 per cent were open to it once they understood what it means.

Raghav Sahgal, president of NICE APAC, said that once the respondents learned about the benefits of biometrics, their likelihood of performing transactions via the contact center increased by 1.5 times which demonstrates high levels of readiness and a huge revenue opportunity for businesses that can incorporate voice biometrics into their authentication processes.

Mr Sahgal also expressed that voice biometrics lets enterprises interact with their customers in a friendly and personalised manner by authenticating the customer on the background of a natural conversation, allowing service agents to immediately start helping the customer. This greatly improves customer satisfaction and reduces fraud. Organisations that implement voice biometrics technology can also dramatically improve customer service and reduce handle times resulting in increased sales and customer loyalty.

For detailed survey results, please visit: www.nice.com/websites/RTA_APAC/ **SSST**



Gartner Says Detection and Response is Top Security Priority for Organisations in 2017

Worldwide Spending on Information Security to Reach \$90 Billion in 2017

Singapore - Enterprises are transforming their security spending strategy in 2017, moving away from prevention-only approaches to focus more on detection and response, according to Gartner, Inc. Worldwide spending on information security is expected to reach \$90 billion in 2017, an increase of 7.6 percent over 2016, and to top \$113 billion by 2020. Spending on enhancing detection and response capabilities is expected to be a key priority for security buyers through 2020.

“The shift to detection and response approaches spans people, process and technology elements and will drive a majority of security market growth over the next five years,” said Sid Deshpande, principal research analyst at Gartner. He also added that this does not mean that prevention is unimportant or that chief information security officers (CISOs) are giving up on preventing security incidents but it sends a clear message that prevention is futile unless it is tied into a detection and response capability.

continue on page 34



UHF New Series from 840 - 960 MHz

We help to simplify your UHF application in all environment.

- ✓ 0.5W/1W UHF read/write modules
- ✓ UHF antenna OEM/ODM customized design:
 - Patch Antenna
 - Array Antenna
 - Ceramics Antenna
 - Chip Antenna
 - Paper Antenna
- ✓ UHF project consultation and design
- ✓ SDK/API available



GIGA-TMS INC.
Quality, Delivery & Service
Tel: 886-2-26954214

8F No. 31 Lane 189, Kang Ning Street,
Hsi Chih Dist, New Taipei City, Taiwan

<http://www.gigatms.com.tw/>
Email: promag@gigatms.com.tw

GIGA-TMS INC. © 2015 All Rights Reserved.



Mr. Deshpande said that skills shortages are further driving spending on security services. Many organisations lack established organisational knowledge of detection and response strategies in security because preventive approaches were the most common tactics for decades. Skill sets are scarce and therefore, remain at a premium, leading organisations to seek external help from security consultants, manage security service providers (MSSPs) and outsourcers.

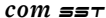
The need to better detect and respond to security incidents has also created new security product segments such as deception, endpoint detection and response (EDR), software-defined segmentation, cloud access security brokers (CASBs), and user and entity behavior analytics (UEBA). These new segments are creating net new spending, but are also taking spend away from existing segments such as data security, enterprise protection platform (EPP) network security and security information and event management (SIEM).

On the services side, the emergence of specialised managed detection and response (MDR) services is a threat to traditional MSSPs. The rising number of point solutions in the security market that address detection and response is creating sprawl and manageability issues for CISOs and security managers, driving spending for

management platforms and services that are better integrated with adjacent markets.

As enterprises shift toward balancing prevention with newer detection and response approaches, CISOs are changing how they measure the success of their security strategy. All security investments are being measured on how they contribute to the shift in mindset. Even preventive security controls, such as EPP, firewalls, application security and intrusion prevention systems (IPSS), are being tweaked to provide more intelligence into security operations, analytics and reporting platforms.

“CISOs are keen to communicate the return on investment of their security strategy in terms of the business value associated with quick damage limitation, in addition to threat prevention and blocking,” said Lawrence Pingree, research director at Gartner. “The key enabler for CISOs in this endeavor is to get visibility across their security infrastructure to make better decisions during security incidents. This visibility will enable them to have a more strategic and risk-based conversation with their board of directors, CFO and CEO about the direction of their security program.”

For more information, please visit: www.gartner.com 

ZTE Releases Industry's First IP+Optical 5G Flexhaul Transport Solution

Hong Kong - ZTE Corporation, a major international provider of telecommunications, enterprise and consumer technology solutions for the Mobile Internet released the industry's first IP+Optical 5G Flexhaul solution, a fronthaul and backhaul integrated solution based on Internet protocol (IP)+Optical technology at Mobile World Congress, Barcelona.

Adopting the new IP+Optical architecture provides unified transport of 5G fronthaul and backhaul services on one device as well as super-large bandwidth, ultra-low latency and software-defined networking (SDN)-based

traffic engineering. It is estimated that ZTE's 5G Flexhaul solution can reduce the total cost of ownership (TCO) by 30 percent compared to traditional solutions.

5G networks provide unparalleled experience for users in terms of bandwidth, latency and number of connections. Compared with the single scenario of 4G, 5G supports diverse scenarios including enhanced mobile broadband (eMBB)/massive machine type communications (mMTC)/ultra-reliable and low latency communications (uRLLC) and the key indicators of different scenarios vary significantly. Therefore, traditional networks face

requirements that include structure reconfiguration, equipment upgrade and performance improvement.

Building an efficient and cost-effective bearer network to meet the requirements for super-large bandwidth, ultra-low latency and cloudification of core networks and radio access networks (RANs) in the 5G era has become a huge challenge that global operators are facing.

ZTE's 5G Flexhaul solution combines Flex Ethernet and IP+Optical architecture and provides super-large flexible pipeline transport capability for 5G fronthaul and backhaul services. The 5G Flexhaul solution

continue on page 35

implements end-to-end (E2E) application of IP+Optical synergy and provides unified planning, scheduling, management and maintenance by SDN controllers. IP+Optical integrated devices are used in the mass access layer to reduce network construction costs and save equipment room space. It implements super-large-bandwidth transport by multi-wavelength connection between adjacent nodes. Additionally, with the FlexE feature, it can flexibly isolate sub-channels of different services to provide optimal forwarding plane support for 5G bearer network slicing.

The ZXCTN 6180H, a 5G transport pre-commercial equipment that is also showcased at MWC, is only 3RU high and supports up to 1T networking capacity of one access ring.

In addition to super-large pipeline transport capability, the 5G Flexhaul solution has flexible transport latency capability. The latency

budget allocated to the fronthaul network by 5G cloud radio-access network (C-RAN) is less than 100us. In the forwarding plane, the 5G Flexhaul solution supports fast forwarding and ordinary forwarding modes, which can be selected according to the service type. The fast forwarding mode is used for services that are time sensitive. The time sensitive network (TSN) technology is used to reduce the switching latency between the upper and lower service nodes from 30 microseconds to several microseconds. The intermediate node uses optical bypass technology to achieve a forwarding latency that is less than 1 microsecond. It effectively meets 5G low latency requirements and provides a powerful guarantee for new services and network architectures.

The cloudification feature included in 5G will bring flexible, ubiquitous connections. The 5G Flexhaul solution, based on SDN-based traffic engineering, can efficiently build ubiquitous connections and

dynamically optimise network traffic according to the information collected by the traffic monitor to match the tidal effect of the network and substantially increase resource utilisation.

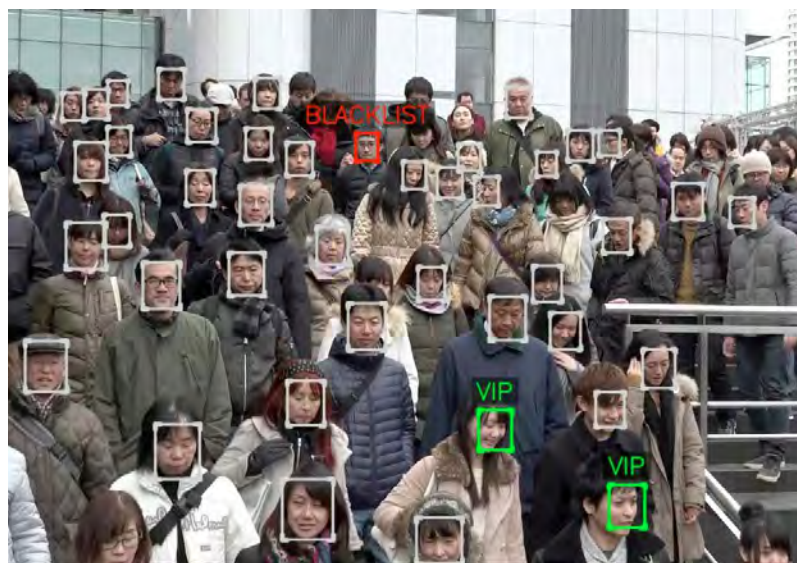
“ZTE continues its constant innovation to provide competitive solutions and products for global operators. As 5G technology is bringing in a new network revolution, ZTE responds actively and highly promotes the application and trial operation of 5G transport technologies. ZTE has carried out early-stage research and discussions with a number of operators about a cooperation in 5G fronthaul and backhaul technology. The 5G Flexhaul solution will greatly help global operators build a future-proof, flexible, cost-effective and integrated 5G transport network,” said Mr. Zhao Fuchuan, Chief Engineer of ZTE 5G Transport Solution.

For more information, please visit www.zte.com.cn 3ST

NEC's Video Face Recognition Technology Ranks First in NIST Testing

Tokyo, Japan – NEC Corporation announced that NEC's face recognition technology achieved the highest performance evaluation in the recent Face in Video Evaluation testing performed by the U.S. National Institute of Standards and Technology (NIST). Results were released in NIST's Interagency Report 8173: Face In Video Evaluation (FIVE) Face Recognition of Non-Cooperative Subjects.

NEC's face recognition technology took first place for the fourth consecutive time following the 2009 Multiple Biometric Grand Challenge (MBGC 2009), 2010-2011 Multiple



continue on page 36



Biometrics Evaluation (MBE 2010-2011), and 2013 Face Recognition Vendor Test (FRVT 2013).

Video face recognition technology identifies the faces of moving subjects in real-time as they walk naturally without stopping in front of a camera. The benefits of high-speed video analysis enabled by this technology include the prevention of potential incidents through detection of suspicious individuals and recognition of individuals at the gateways of critical facilities.

Using video images from standard cameras for face recognition requires highly advanced techniques when compared to still images. This is because images are greatly influenced by environmental conditions such as camera location, image quality, lighting and subject size, in addition to the behavior of a subject, including walking speed, face direction and sight line.

To achieve reliable face recognition of a video image, NEC developed feature point extraction technology that enables enhanced face recognition to a level where an individual can be identified with high precision from within a group, even if their face is partially hidden, or the image is taken from different angles. NEC's face recognition technology also uses deep learning technologies for face matching to increase accuracy to a level where an individual can be identified by a low-resolution face image captured by a distant camera.

"It is a great honor that our face recognition technology received a first place evaluation for the fourth consecutive time from the NIST," said Masakazu Yamashina, Senior Vice President, NEC Corporation. "We will further

expand global business by offering innovative biometric solutions, such as the video face recognition system, throughout a wide range of fields, including security, transportation, finance and retail."

Evaluation examples from the NIST FIVE testing:

Entry-exit management at an airport passenger gate

Tests were conducted to recognize one individual at a time as they walk through an area without stopping or acknowledging the camera. NEC's face recognition technology won first place with a matching accuracy of 99.2%. The error rate of 0.8% is less than one-fourth of the second place error rate.

Detection of suspicious individuals at an indoor stadium

Tests were conducted with an individual situated far from the camera with their face direction changing frequently. NEC's face recognition technology won first place with an error rate half that of the second place error rate.

For nearly 30 years, NEC has been developing face recognition technology by defining it as one of the key technologies to help achieve a safer and more secure society. The technology has now been implemented in more than 100 systems in 40 countries worldwide. NEC will continue to develop solutions that leverage face recognition technology as part of its portfolio of AI technologies "NEC the Wise" (*3) and to deliver the solutions for a wide range of fields, including social infrastructure and private sector facilities. **SST**

Honeywell Lights Way for Singapore Airport Expansion

New airfield lighting control and monitoring system will improve aircraft movement efficiency and safety at one of the world's busiest airports

Singapore - Honeywell has announced a multi-million dollar, multi-year contract to implement a new airfield ground lighting control and monitoring system at Singapore Changi Airport, Southeast Asia's busiest hub and one of the most frequented airports in the world. The Honeywell system will play a critical role in helping Changi Airport safely

and efficiently accommodate the expected increase in aircraft traffic.

The project is part of expansion efforts at Changi Airport, which include the development of a three-runway system. The new Honeywell system will cover all three runways and associated taxiways, taxi lanes and apron lighting as well as facility control and management.

Helping streamline operations and optimise ground traffic flow, Honeywell's advanced Individual Lamp Control and Monitoring System will allow the airport to get real-time information on approach and runway lighting lamp failures, including the precise location to facilitate fast response and repair.

"Since its opening in 1981, Changi



Smiths Detection Deploys First Smart Security Checkpoint at Kansai Airport in Japan

Osaka, Japan - Smiths Detection is working with Kansai Airport to deploy the first ever Smart Security checkpoint in Japan. The Smart Security Checkpoint is an integrated system that combines walk-through metal detectors with passenger security scanners, cabin baggage X-ray machines, an automated tray return system and an advanced image and checkpoint management platform to provide a seamless, more efficient, and less intrusive experience for passengers.

Built around Smiths Detection's X-ray scanner HI-SCAN 6040-2is X-ray scanner, an advanced dual-view X-ray inspection system with automatic explosive detection capability, the Smart Security system will significantly reduce waiting times at the security checkpoint, which means higher passenger satisfaction and improved operational efficiencies at Terminal 2 Kansai International Airport (KIX).

Nathan Manzi, Vice President of Asia Pacific at Smiths Detection, said: 'With passenger numbers expected to increase in this region, airports are under increasing pressure to move passengers quickly and seamlessly, whilst maintaining the integrity and quality of the security system. Innovative deployment of security technology such as this at KIX has been proven to do just that. We see Smart Security as the future of

airport security.'

Jeremy Goldstrich, Corporate Executive Vice President & Chief Operating Officer of Kansai Airports said, "The key to an effective security strategy is integration and Smiths Detection has been a good partner throughout the planning, design and implementation of the Smart Security system. Through such partnerships, we are able to bring innovations to Kansai International Airport, focusing our number one priority, which is keeping our passengers safe and secure".

"Smart Security" was developed by the International Air Transport Association (IATA) and Airports International Council (AIC), and is deployed in a number of advanced airports in Europe and the United States. Integral to the system are new "Smart Lanes", which increase the inspection capacity by 1.5 times to significantly improve the time it takes for passengers to move through the screening process. The "Smart Lanes" speed up cabin baggage screening by moving trays automatically, eliminating the need for passengers to have to move their trays manually. Passengers can instead proceed immediately through security and be screened by body scanners and walk-through metal detectors.

For more information, please visit:
www.smithsdetection.com **SSD**

Airport has been recognised for ensuring safety in its airfield," said Koh Ming Sue, managing director, engineering & development of Changi Airport Group. "The new Honeywell airfield lighting control and monitoring system serves as an important cog in our broader expansion plans to help upkeep our safety and efficiency performance even as air traffic demand grows beyond the capacity of our existing two runways."

"We are excited to have been chosen by Changi Airport Group and look forward to working with them to maintain the airport's high safety and efficiency record," said Raghu Seelamonthula, market director of Airport Systems,

Honeywell Building Solutions. "Airfield ground lighting, as a visual aid for landing and taxiing, is an important element of an airport's equipment. Honeywell's airfield lighting control and monitoring have proven to be highly reliable with equally high availability rates in operations throughout the globe."

Lighting installations for approaches, runways, taxiways, and aprons enable pilots to navigate the complex surface layouts of modern airports. Honeywell's computerised control and monitoring system facilitates the operation and observation of these lighting installations, and ensures that safety requirements

are met. This system provides workstations for tower and technical personnel to simplify daily operational processes and optimize maintenance activities.

Honeywell designs, manufactures and installs complete airfield ground lighting systems for airports. The systems range from individual lighting units to series circuit transformers and power supply systems to control and monitoring systems, including single lamp control and monitoring, routing systems, aircraft docking systems, and surface movement guidance systems.

For more information, please visit:
www.honeywell.com **SSD**



Protecting Borders from Vehicle Attack on Land and Sea

► *By Greg Hamm, Delta Scientific Vice President, Sales & Marketing*

It's almost a cliché in international spy movies. The good guys need to escape to the adjoining country to avert certain death. They pile into a car or truck and head for the border, which is defended by armed soldiers and a barricade consisting of a wooden bar the size of a broom handle. The car revs up, the guns begin shooting and the car roars through the barricade with splinters exiting out of the field of view.

Conversely, bad guys need to get that contraband out of the port. In the dark of night, they drive a big truck up close to the port, put

the medal to the metal and smash through the fence protecting the port's perimeter like a hot knife through butter. Exciting movie... bad security! Fact is, borders can be protected a lot better from vehicle assault.

Protecting the United States/ Mexico Border

Located between San Diego and Tijuana, the San Ysidro Landed Port of Entry (SYLPOE) is the busiest land port in the world, processing an average of 50,000 northbound vehicles per day. In a recent update to SYLPOE, security



was not overlooked. In a \$5 million project, the border crossing features 50 custom-design bullet-resistant guard booths, K4 rated swing gates, barriers and bollards.

The architect on the project, The Miller Hull Partnership, selected a combination of stock equipment for certain areas and custom booths and a tri-fold gate for other sections of the crossing to provide the U.S. government with a turn-key project.

The majority of the traffic lanes have two stacked bullet-resistant inspection booths created for northbound traffic, effectively doubling the capacity of the 24 existing booths. The highly energy-efficient structures have

a photovoltaic and Ethylene Tetrafluoroethylene (ETFE) roof structure that will shade cars and officers. It also provides for rain and sun protection for the officers in booths. Because of its translucent nature, it allows for natural light thereby requiring no artificial lighting during the day.

The booths also provide the typical specification found within a bullet-resistant booth including the following –

- Protection against
 - ▶ Impact – Level 1
 - ▶ Handgun – 9mm or .357 – Level 2
 - ▶ Handgun .44 magnum, 5.5 ammunition or 12g shotgun – Level 3
 - ▶ High-power rifle such as a

30.06, 7.62 ammunition, hand grenade, high explosive – Level 4

- All structural members meet or exceed ASTM A500
- Sliding or swing door fabricated from structural steel with heavy duty hardware for bullet resistance
- All electrical components will be UL approved and installed in accordance with the N.E.C.

In addition to the booths, products in the \$5 million project also include beam barricades. They are counterbalanced, hinged semaphore type gates consisting of a crash beam, support and pivot assembly, steel foundation implants, cast-in-place concrete buttresses, and locking and anchoring mechanisms. The crash beam incorporates a high strength wire rope that is firmly attached to both buttresses when the crash beam is in the down position. In a collision, the energy of the impact is transmitted through the crash beam to the buttress and the foundation.

Contrary to the flimsy wooden bar in the movie borders, the high-strength wire rope of these beam barricades will stop a non-armored or non-tracked vehicle weighing 2721 kg at 64 kph. The barrier has been certified per U.S. Navy TM-56-86-05 to have a performance evaluation of 1/L3.0. A beam





barricade swing gate is used where vertical lifts are impractical and will stop a 6803 kg vehicle going 48 kph.

A crash rated swing gate eliminates the need for a ground track. It will stop a 2494 kg vehicle traveling 48 kph while providing a clear opening to 3.6 to 9.1 feet. Such barriers are found throughout the world protecting borders. In a novel approach, mobile barriers are used on the Israel-Palestinian border. Quick deployment, modular portable solutions can be rapidly set up within 15 minutes on existing concrete or asphalt roads, level compacted soils and other hard surfaces. No excavation or sub-surface preparation is required.

Protecting Borders on Water

The Port of Sydney Harbour installed anti-terrorist barriers to protect their international cruise ship terminal. The barriers will stop and destroy a 24,983 kg dump truck. They prevent speeding vehicles from getting past the guard post at the Overseas Passenger Terminal a Circular Quay, where approximately 90 vessels dock during the busy summer months. Nearly 160,000 passengers come through the Port, representing a major facet of Australia’s tourism industry.

In Hawaii, automated, linear gates are being used to protect vulnerable piers at Naval Station Pearl Harbor in Hawaii. The automated gates at the Navy piers create a protective barrier between terrorists and in-port assets. The equipment was installed as part of an overall regional effort to increase the force protection posture of critical assets at strategic locations.

“The Navy installed this barrier system in order to provide an adequate level of force protection while maintaining a high level of efficiency on the piers. In other words, we’ve been able to increase our force protection posture without impacting the mission of fleet support,” reports a director. “Before the gates were installed, as one approached the pier they came upon a swing gate guarded by a sentry. It was the sentry’s responsibility exclusively to assess and then grant or deny access. For a bad guy to access the piers,

“Contrary to the flimsy wooden bar in the movie borders, the high-strength wire rope of these beam barricades will stop a non-armored or non-tracked vehicle weighing 2721 kg at 64 kph.”

they only had to overcome the sentry.”

Now, the piers have a gate or kiosk system that protects the sentry, who remains in the gatehouse and cannot be touched. Anyone attempting to gain access has to slide credentials through a pass window to the sentry. However, even if someone could take out a sentry in the gatehouse, they still cannot get through the gates. The gates are ‘force multipliers’ for the Security Department when operating them in an automated mode during slow periods. An automated gate reduces overall manpower requirements and frees up a security personnel to perform other missions vital to force protection such as patrol, counter surveillance and random inspections.

As a result, Pearl Harbor’s piers are now less vulnerable to acts of terrorism. The automated gates provide an anti-terrorism force protection barrier between roadways and the piers which provide service to ships and submarines. Physical security upgrades such as this, combined with anti-terrorism awareness training, helps make Navy personnel less vulnerable from attacks and acts of terrorism.

In addition to the fixed crash rated gate, Pearl Harbor also uses portable barricades that are towed in place and set up in 15 minutes. The fixed barriers and portable barriers are integrated with a series of other force protection equipment and measures to achieve an antiterrorism system based on a defense-in-depth methodology.

Real Life Border Security Is Not a Movie

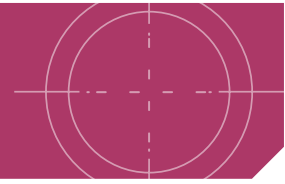
Some of the most secure 10 to 100 meters of property in the world are at border crossings. At crossings using the described barriers and gates, the odds of a vehicle penetrating to any extent are almost zero. Terrorists simply need to find another alternative.

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





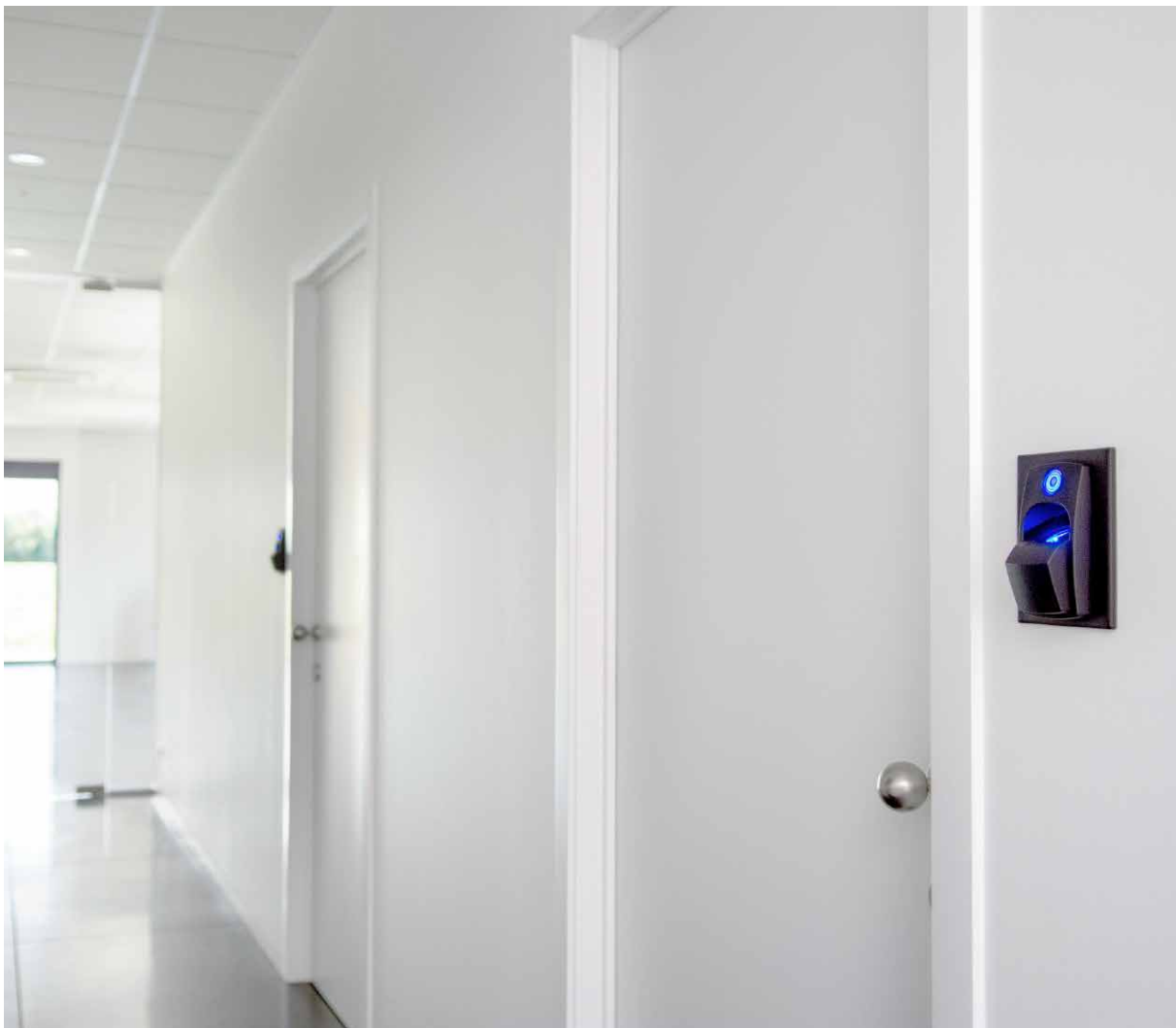
Biometric Scans Comply With Impending Privacy Legislation



Amidst the chaos of Brexit, many security minded organisations are concerned about the implications of the European Regulation on the Protection of Individuals with regard to the Processing of Personal Data, adopted in 2016 and planned to be enforceable in May 2018.

As an integral component of EU privacy and human rights law; it regulates the processing and distribution of personal data. In essence it will become illegal, or certainly contrary to the regulation, to link the stored data to the individual. Furthermore, the regulation states that personal data should not be processed unless the individual is informed and at least one of a set of strict criteria are met.

Whilst the regulations are designed to protect the individual's rights to privacy, they will have enormous implications for the security industry which now must adapt to comply.



continue on page 42



The process of data extraction from a typical fingerprint scan creates an encrypted pattern, no fingerprint image is stored.

Shaun Oakes, Managing Director of ievo Ltd, the Newcastle-based manufacturer of biometric recognition systems, explains, “The regulation is designed to prevent stored data being linked to individuals and used for purposes other than ensuring the security of whatever system it was designed for and transferring this data to third parties. Biometric data – fingerprint scans in our case – comes under the heading of a ‘special privacy element’ which are forbidden to use and process, unless, and this is very important, one of a number of criteria apply, the most pertinent of which is the data subject has given permission.”



As all scans are taken either voluntarily (after the individual has given his or her permission) or legitimately to ensure the safety and security of others, the ievo range of biometric systems fully comply with this legislation as they utilise feature-based matching. They do not store the raw biometric data or image but rather extract a salient set of features known as minutiae from which an individual template is generated.”

In essence, a system of ‘pseudonymisation’ is used where the data is processed in a manner which it can no longer be attributed to an individual without the use of additional information which is stored separately and subject to strict technical and organisational control.”

Following a High-Resolution scan of the finger ievo’s algorithms separate the foreground from the background of the image. It then enhances the image, detects minutiae points and creates a pattern. It is this pattern that is stored on ievo’s controller (which is installed separately from the sensor) which, when combined with encryption using AES (Advanced Encryption Standard) ciphers and further confidential safeguards serve to eliminate tampering.

It is important to note that the original scanned image of a fingerprint is never stored. As such, ievo biometric readers fully comply with the new legislation. However, many older systems which store biometric and/or personal data of card holders or those with knowledge of key pad combinations may well have to review their compliance.



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



Cognitec's Face Recognition Technology Supports Growing Demand for eGate and Airport Security Solutions

Cognitec continues to introduce new product features to advance its face recognition technology used in eGates for automated passport control procedures.

FaceVACS-Entry performs with reliable accuracy and speed in more than 150 installations at various European airports. The technology combines smart hardware for facial image acquisition with market-leading software for verification processes and is ready for integration into electronic gates (eGates) at border control checkpoints.

The product features Cognitec's latest matching algorithm and generates market-leading accuracy rates for passport images with low

resolution and other image quality problems. Cognitec continues to optimize the performance of FaceVACS-Entry's unique presentation attack detector, which recognises fraudulent attempts to use photos, videos or masks.

In addition, Cognitec has improved various user experience features. Persons entering the gate can overlay the moving contour around their live facial image with a static head silhouette in an optimal position for face recognition measures. The display also alerts users to remove sunglasses.

Cognitec's pioneering technology for real-time face recognition, FaceVACS-VideoScan allows airport security staff to detect and recognise

known suspects and receive instant notifications. The application detects people's faces in live video streams or video footage and stores video sequences of cropped faces for each appearance in front of a camera.

Anonymous analysis of all face streams over time allows the software to compute people count, demographical information, people movement in time and space, and to detect frequent visitors and crowds. Cognitec continually advances product utilities that respond to increasing demand for accurate, fast and convenient face recognition technologies at airports and borders.

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

Biometrics and Border Security

By: Rawlson O'Neil King Lead Researcher, Biometrics Research Group

United States and Border Security

Since the United States has stringent visa requirements on its inbound international visitors, which has been estimated as 88.3 million in number and growing, continued growth of biometrics usage for border security by the U.S. government is to be expected. The ongoing effects of these requirements are that other countries will also require enhanced travel documents that encapsulate biometrics.

The United States currently claims commitment to secure borders and open doors by welcoming and facilitating legitimate travel to the United States by

international visitors while maintaining the integrity of secure borders. By way of the Enhanced Border Security and Visa Entry Reform Act of 2002, the U.S. Congress mandated the use of biometrics for U.S. visas. This law requires that U.S. embassies and consulates abroad issue "only machine-readable, tamper-resistant visas and other travel and entry documents that use biometric identifiers" to international visitors.

The best known biometric is the fingerprint and the U.S. government has mandated that 10 fingerprint scans be collected at all U.S. embassies and consulates for visa applicants seeking to come to the United States. The use of the fingerprint identifier is an important tool

continue on page 44



for U.S. national security because fingerprints taken are compared with similarly collected fingerprints at U.S. ports-of-entry. This helps verify identity to reduce use of stolen and counterfeit visas and protect against possible use by terrorists or others who might represent a security risk to the United States.

These two important programs (collecting fingerprints for visa issuance and verifying travellers' fingerprints when they enter the United States) arguably makes travel to the United States safer for legitimate travellers, and also improves safety and national security. The 10-print system enables the State Department and the Department of Homeland Security to more effectively process visa applicant fingerprints.

As a consequence, travellers to the United States from a country without a visa waiver requirement must expect to be subjected to an application process whereby a digital photo is taken and electronic fingerprints are collected. All fingers of a visa applicant are electronically scanned in a quick, inkless process during the consular officer's interview with the applicant.

The electronic data from the 10 fingerprints collected is stored in a database and is made available at U.S. ports-of-entry to Department of Homeland Security immigration inspectors. The electronic fingerprint data

is associated with an issued visa for verification and the privacy of the data is protected by storage in the database.

Biometrics collected by the Department of Homeland Security and linked to specific biographic information enable a person's identity to be established, then verified by the U.S. government.



Border Security Impact on Biometrics Market and Other Countries

Due to the extensive use of fingerprint recognition for border security with the United States and throughout the world, the market for automated fingerprint identification systems and fingerprint biometric technologies will continue to account for the greatest share of the global biometrics market and is forecast to continue to be the main source of overall market revenues from 2015 to 2020.

Biometrics Research Group Inc. estimates that the market for fingerprint recognition was valued at US\$10 billion in 2012 and was predicted to reach nearly US\$25 billion in 2015. One of the main drivers for this revenue sector growth continues to be biometric requirements for travellers.

For more information, please visit:
www.biometricupdate.com **SSR**

First County in Maine Installs Body Scanner from Smiths Detection

Madison, Maine – Smiths Detection Inc. (SDI), in partnership with its Northeast distributor, Access Control Systems Inc announced that the Somerset County Jail in Madison, ME is the first county correctional facility in Maine to install a body scanner. The Somerset County Sheriff's Office has conducted more than 1,000 scans to date, significantly reducing the amount of contraband being brought into the facility, while greatly improving efficiency and reducing costs.

Sheriff Dale P. Lancaster of the Somerset County Sheriff's Office commented, "We are very pleased with the effects that the B-SCAN has had on safety and security for both staff and inmates. The body scanner has detected multiple occurrences of drugs and weapons concealed internally and has greatly reduced the cost previously spent watching inmates in dry cells. From procurement through installation and training, Access Control Systems and Smiths Detection provided the expertise and oversight necessary to ensure our success with this project."

continue on page 45



Smiths Detection Inc.'s b-scan transmission X-ray body scanner is a major deterrent in helping correctional facilities keep drugs and other contraband out. It can detect concealed

contraband that has been ingested, hidden in body cavities, or beneath clothing, greatly reducing the need for manual searches. This system is easy to integrate into an existing checkpoint and requires minimal training to operate. It is also backed by Smiths Detection's 24/7/365 technical support call center. There are hundreds of B-SCAN systems deployed around the world, largely in correctional facilities.

Dan Gelston, President of SDI, said, "Somerset County is a pioneer in the State of Maine. They were the first to install a B-SCAN body scanner to help enhance the safety of their staff and inmate population and serve as a role model to other counties in the state. We continue to work with organisations to help them implement our world-class technology to meet their requirements of increasing security and improving safety."

"Smiths Detection Inc.'s b-scan transmission X-ray body scanner is a major deterrent in helping correctional facilities keep drugs and other contraband out. It can detect concealed contraband that has been ingested, hidden in body cavities, or beneath clothing, greatly reducing the need for manual searches."

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

Morpho Detection Wins Bristol Airport Contract For CTX Hold Baggage Explosives Detection Systems

Source: Safran Group

Safran Identity & Security, through its subsidiary Morpho Detection UK Ltd, announced that following a comprehensive competitive tendering process, UK's Bristol Airport has selected Morpho Detection's CTX 9800 DSi™ and CTX 5800™ Standard-3 Hold Baggage Explosives Detection Systems (EDS).

Scheduled for deployment over a two-year period to meet UK Department for Transport mandates effective September 1, 2018, five high-speed CTX 9800 will screen all in-gauge hold baggage. In addition, one compact CTX 5800 will screen all Out-of-Gauge hold baggage. To ensure their CTX fleet is continuously up and running, Bristol Airport will utilise Morpho Detection's trusted, onsite service network to facilitate preventative and rapid-response capabilities for a minimum of 10 years.

Currently undergoing a £24 million terminal extension, Bristol Airport has grown to serve 116 destinations



across 30 countries and handled more than 7 million passengers in 2016.

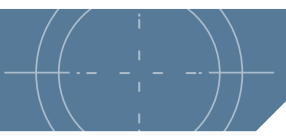
Commenting on the new hold baggage screening infrastructure and the airport's growth, Fraser Dury, Head of Engineering at Bristol Airport said that Bristol airport is committed to leveraging the most effective technologies and solutions to ensure high standards of security are maintained with minimal impact on passengers. Working with Morpho Detection helps ensure continued regulatory compliance as the airport develops and enhances their terminal infrastructure.

Both CTX 5800 and CTX 9800 are approved by the European Civil Aviation Conference (ECAC) as meeting Standard 3 requirements and certified by the U.S. Transportation Security Administration (TSA) and Civil Aviation Administration of China (CAAC).

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



Biometrics at the Borders



By Isabelle Moeller, Chief Executive of Biometrics Institute

While policy creation for the use of biometric technologies at national borders remains a matter for government, best practices and guiding principles for effective deployment can be built through collaboration between the industry's global stakeholders, says Isabelle Moeller, Chief Executive of the Biometrics Institute.

The adoption of biometric technologies at national borders around the world raises some important questions. National security and personal privacy sit at the heart of the debate, but there is much more to it than this; the speed and efficiency of border checks together with the cost of deployment and the accuracy and reliability of the technologies are also key factors that weigh heavily on the minds of border agencies across the globe. Although biometrics are undoubtedly a valuable addition to the evaluation of human identity, every biometric has vulnerabilities, which must be carefully managed when the technologies are being deployed and the resultant data is used.

The advantages and benefits that can be gained by conducting biometric checks in the border control environment are considerable. Each border works differently, of course, but when compared to traditional manual border controls, few would contest that the security process can be enhanced with biometric technology, be that through the comparison of the face (beyond the traditional visual review of a passport photo), a fingerprint, the iris or another biometric 'modality'.

The arguments for using biometrics to enhance the speed and facility of border controls are also compelling. Replacing six officer-manned passport manual control gates, for example, with six automated e-gates (supervised by one officer) will enable international border controls to scale up their operations at peak travel times, reducing delays and responding to traffic fluctuations much faster than can be achieved by



Isabelle Moeller, Chief Executive of Biometrics Institute

training and deploying individual officers in the conventional manner. The e-gate model also promises to reduce the operational costs of border management considerably.

What's more, the capture and/or the exchange of an individual's biometric data between countries (and domestic authorities) enables additional checks to be conducted before that individual reaches the port of entry, or border control point. Here, the biometric identity can be used in post entry scenarios to control access to services, and even to verify compliance and departure. Such practices require governments to align on biometric data management

policy (which is currently far from consistent between nations) but, nonetheless, has the potential to reduce the risk of a suspicious individual passing undetected through immigration and customs. It may also substantially cut the delays that travellers experience at the border, since many of the required checks will have already been performed in advance.

There are fears too, of course, particularly among implementing governments. These focus on uncertainty and risk. Putting aside the creation of national policy to determine how biometric data at the borders around the



continue on page 47



world is captured, stored and exchanged (a debate that sits right at the heart of government), it is important to acknowledge that all biometric technologies are fallible, including those deployed by border agencies. In this way, biometric technologies should be considered as one layer in a multi-layered security environment. Vendors have finite resources to test their solutions. Hackers and fraudsters are perpetually probing and testing to identify and exploit weaknesses. Simulated deployments invariably deliver different results to those generated by a solution which is live 'in the field'. Significant 'live' trials are required before real-world data can be collected, which disrupt border operations and cost taxpayers millions. In short, failure can come in various forms, but is always both expensive and unpopular.

There is also a 'knowledge gap' to consider. Government authorities, by definition, are not biometric technology specialists and can neither understand nor account for every potential vulnerability. Instead, they must trust in the models proposed by academics, brought to life by vendors and, at least in part, managed by service providers. It's worth remembering that the check-in process at an airport – the first step in the border security chain – is managed by the airlines, not the border agencies themselves.

What we can be sure of, however, is that the use of biometric technologies at national borders has arrived and is now in a perpetual state of evolution. Academics will continue to innovate, vendors will continue to sell and governments will continue to buy.

What, then, can the global biometrics ecosystem do to mitigate the risk and uncertainty felt by border agencies and their governments? Clearly lawmakers can and should continue to debate the moral and ethical questions that underpin their national policies for biometric data collection, storage, interrogation, and dissemination. Aiming for universal consistency across policy, deployment approach, and international border cooperation is far too big an 'ask'. Different countries have different motivations for introducing biometrics, which direct their strategies and define their appetite (or lack of) for shared border engagement with other nations.

Beyond this, however, there are easy wins that can

be obtained through international stakeholder collaboration. By bringing together government agencies, vendors, academics, specialist consultants, privacy advocates and industry watchdogs in a commercially neutral environment, problems and concerns can be explored and addressed through the sharing of expertise, 'live' field data, use cases and deployment experience.

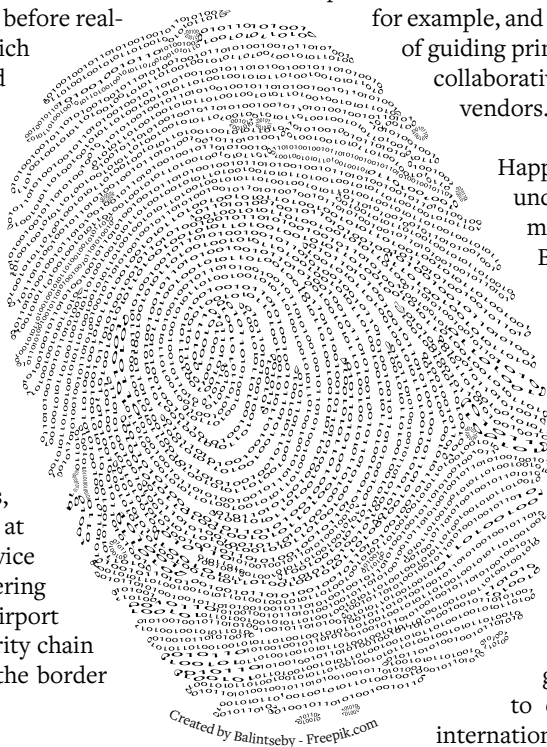
When convened, these stakeholders can work together for the benefit of the whole market, establishing best practices for secure and responsible deployment, for example, and working toward defining a set of guiding principles which can support the collaborative efforts of governments and vendors.

Happily, this work is already underway, but there is much more that can be done. The Border and Travel Major Programmes expert group within the Biometrics Institute is an international group of border agencies, vendors and academics which exists to facilitate dialogue, exchange information and keep its members apprised of major border system projects currently underway. The group has evolved from government-only meetings to encompass a wide range of international experts, decision makers and influencers.

Biometric technology will continue to play a major part in the development of future Immigration and Border Controls, affording border agencies process efficiencies, enhancing security and making the border experience more traveller-friendly.

Using these sensitive, personal identifiers, however, requires an effective privacy ecosystem where the data is protected and where its usage is disclosed through the enforcement of robust retention policies. Only through collaboration between control agencies and technology suppliers can the industry develop the mutually beneficial guiding principles and best practices that will drive the development of borders capable of supporting the growth in global travel despite the increases in complexity and risk posed by 21st century living.

For more information, please visit:
www.biometricsinstitute.org **SSST**





Canadian Airports Implementing Facial Recognition Technology

Source: CBC News

Facial recognition technology is coming to major Canadian airports as part of a new traveller screening program under development by Canada Border Services Agency, CBC News has learned.

The technology will be part of a new generation of self-service border clearance kiosks for travellers entering or returning to Canada. The kiosks are being pitched as part of a broader effort to modernise and streamline clearance procedures at Canadian airports and will eventually replace the more limited kiosks currently in use.

“The new kiosks will improve border security as well as assist in reducing wait times and congestion at Canada’s busiest airports,” a statement from CBSA reads.

The kiosks will begin appearing at Ottawa International Airport this spring, according to multiple sources and the rollout will continue into 2018, CBSA says. The Primary Inspection Kiosk (PIK) program as it is called, has been in the works since at least 2015, and will provide automated traveller risk assessment” a CBSA tender describing the program reads.

The facial recognition feature appears to be similar to the U.S. Department of Homeland Security’s 1-to-1 Facial Comparison Project which uses facial recognition to compare a traveller’s face with the image stored on their electronic passport.

In that case, images are not retained unless the two images do not match very well.

In Canada, however, little is known about how the new kiosks will actually work in practice.

CBSA declined to answer specific questions about the PIK program stating that “further details will be announced publicly before the official launch,” with an announcement to follow “in the coming weeks.”

Very Much About Biometrics

International airports in Toronto, Quebec City and Ottawa are all preparing to install the new kiosks and have tendered requests for suppliers according to public records while Vancouver International Airport is developing its own self-service kiosks.

A Portuguese company called Vision-Box is installing 130 kiosks at Toronto’s Pearson International Airport. In an interview with CBC News, it offered a glimpse into how the new program will work.

“In terms of features to the benefit of CBSA, it’s very much about biometrics,” said Jean-François Lennon, the company’s vice-president of sales and business development.

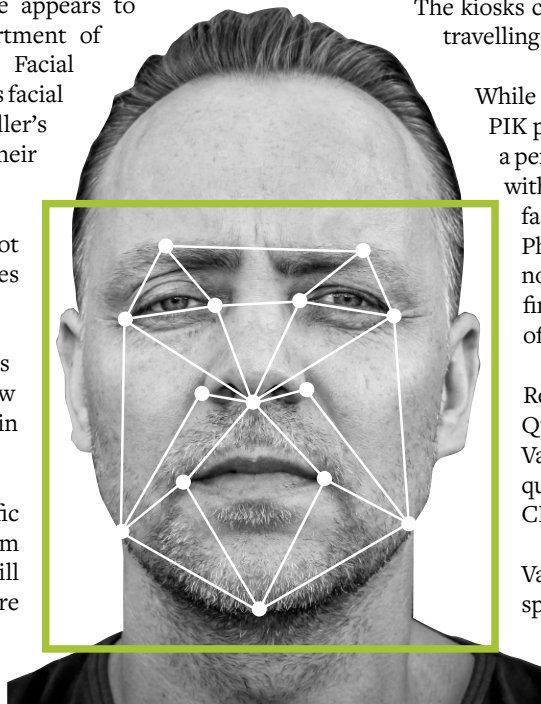
Vision-Box has been working closely with CBSA on research and development for two years, he says and expects its kiosks to begin appearing at Pearson in May. According to Lennon, the specifications for CBSA’s PIK program outline two phases — facial recognition and fingerprint biometrics.

The kiosks can also capture iris data for those travelling under the NEXUS program.

While CBSA would not elaborate on the PIK program’s biometric requirements, a person in the airline industry familiar with the new kiosks confirmed that facial recognition will be part of Phase One. The person could not however, confirm whether fingerprint biometrics will be a part of Phase Two.

Representatives for the Toronto, Quebec City, Ottawa and Vancouver airports referred all questions about the PIK program to CBSA.

Vancouver Airport Authority spokesperson Tess Messmer would only say that the group’s Borderxpress technology which is already



continue on page 49



used in some airport kiosks across Canada “has the capability to meet any government’s Canadian or other biometric requirements including facial, iris and fingerprint recognition.”

Privacy Impact to Be Assessed

Privacy experts will be watching the program closely to ensure that the kiosks’ facial recognition capabilities are being used as intended.

“The problem’s going to be, once that’s created, the capability is a general one that can be used in other contexts,” said Tamir Israel, a staff lawyer with the Canadian Internet Policy and Public Interest Clinic. “historically, once we have the technical capability, we haven’t been very good at limiting it to that use.”

In 2011 for example, the Insurance Corporation of B.C. offered to give Vancouver Police access to its database of driver licence photos so that facial recognition software could be used to identify people who participated in that summer’s Stanley Cup riots, Israel said.

Though Vancouver police did not accept the ICBC’s offer, B.C.’s Information and Privacy Commissioner ruled that such information cannot be freely provided by a public agency without a court order — especially if it was originally collected for a different purpose.

The Office of the Privacy Commissioner of Canada was consulted in the fall by Immigration, Refugees and Citizenship Canada about a biometric expansion project that involved something called Primary Inspection Kiosks, or PIK,” spokesperson Tobi Cohen wrote in an email. “We understand this also involves CBSA which committed to conducting a PIA on biometric expansion.”

Cohen said the office has not received a PIA or Privacy

Impact Assessment, and had no further details to share. Immigration, Refugees and Citizenship Canada meanwhile, had not responded to a request for comment at the time of publication.

Rise Of The Machines

The kiosks are also expected to further decrease the number of traveller interviews with border agents at primary inspection, offloading much of that work to the new machines.

“Customs agents are expensive and this allows them to focus their attention on the passengers that need greater attention while allowing legitimate travellers easier access through the customs process,” said Chris Phelan, vice-president of security and industry affairs for the Canadian Airports Council, which counts all of Canada’s major airports amongst its members.

When asked whether the new kiosks would replace the existing Automated Border Clearance (ABC) kiosks in use at Canadian airports, “Yes,” Phelan replied, “and as rapidly as they can.”

Jean-Pierre Fortin, the president of the Customs and Immigration Union which represents 10,000 front line customs and border agents is concerned that the new machines won’t be as effective at screening travellers as agents can be.

In a meeting with CBSA president Linda Lizotte-MacPherson last August, Fortin raised the safety concerns members have with the implementation of new technologies which includes the new kiosks.

According to Fortin, “there are a bunch of things that we’re trained to do that a machine cannot replace.”

For more information, please visit: www.cbc.ca ESR



Chile Adopts Modernised Electronic ID Documents

In 2012, Chile partnered with Safran to update its identity management system and produce new electronic IDs and passports. In 2013, Chile went live with its new national ID and passport program, following a massive modernization project.

Today, almost 60% of Chileans have an e-ID card. This electronic document eases access to online public services and secures private data. Over one million e-passports have also been delivered.

An E-ID Card for All Chileans by 2022

In 2012, the Chilean government awarded a 10-year contract to Safran to provide Chile's Civil Registry and Identification Service (Servicio de Registro Civil e Identificación) with a new national ID and passport structure.

In charge of the deployment and providing end-to-end secure ID management and document production, Safran updated two central sites and 380 regional offices with the latest technology. Around 825 enrollment stations for capturing biometric data of both citizens and immigrants were delivered.

To ensure a quick and easy identity document renewal process, an online reservation system was implemented, allowing citizens to order and track documents.

Since the beginning of the project, over 10 million e-ID cards and over 1.3 million e-passports have been produced. By 2022, almost the entire Chilean population will have an electronic national ID card.

Ultra-Secure Identity Documents

These electronic documents have some of the highest levels of security and robustness available on the market, thanks to their polycarbonate construction.

Manufactured in the Netherlands at a secure Safran production site, these cards include some of the latest technological advances, like Match-On-Card technology. This technology enables highly secure access to e-services and data protection thanks to strong authentication.

An Ambitious Project

Thanks to this project, on March 31, 2014, Chile became the first country in Latin America to qualify for the American Visa Waiver program. This program allows for travel to the United States without a visa

for a stay of a maximum duration of 90 days. Canada also adopted this program thereby eliminating Chilean's need to have a transit visa between the two countries.

The Safran contract with Chile's national records administration has enabled the deployment of a state-of-the-art identity information and production infrastructure, among the most modern in the world. The new system is faster, more efficient and more reliable, with Safran technology facilitating the issuance of e-ID cards and e-passports that address privacy concerns while also helping prevent identity theft. In recognition of the customer-first service model, the National Records Administration received the 2015 Annual Institutional Excellence Award.

For more information, please visit: www.safran-identity-security.com

SST





Toshiba's Business Solutions(USA) Augments and Improves Headquarters Security with the Help of Tyco

Situation

With Texas market headquarters in San Antonio, Toshiba Business Solutions (USA), Inc. (TBS) – a subsidiary of Toshiba America Business Solutions – employs approximately 1,100 people and provides application solutions including industrial power systems, transmission and distribution systems and lighting systems to a wide range of industries. The company was in the process of relocating its Texas market headquarters and had an aggressive timeline for moving into both the new headquarters and a secondary location.

While we had a relationship with our former security provider for a number of years, we decided to seek quotes and proposals from several other providers to see how security in the new facilities might be augmented,” explained Evan O’Mahoney, Director of Solutions and Professional Services for TBS. TBS decided to work with Tyco Integrated Security (TycoIS) because of its “detail-oriented and comprehensive approach” to security.

Solution

In determining the right solution for TBS, TycoIS first worked to understand the company’s core business to identify how various security offerings could positively impact operations. “This laser-focused approach and awareness of the bigger picture was something other vendors didn’t outline in their proposals,” said O’Mahoney. After a full review of inventory, TycoIS determined that Mobile Security Management would be an excellent

solution for enabling TBS’s security team to manage security operations when off site. “Mobile Security Management allows customers to work smarter and more efficiently by providing visibility and remote control of intrusion systems,” explained Troy Clendenin, National Account Manager for TycoIS and the sales representative closest to the TBS project. The TycoIS team also recommended hosted access control to give employees greater flexibility when traveling between locations.

Implementation

TycoIS installed hosted access control with swipe cards at the exterior and in-suite doors at both locations so employees don’t have to use multiple cards or codes when frequenting both facilities. TycoIS also ensured dual control for the headquarters location – one set of controls for the first floor sales showroom; and a second set for the second floor administrative and operations offices, as the two areas are not always open at the same time. “One of the most exciting aspects of the security solution for us is that our senior management team can now monitor the security status at these locations and take action as needed when they’re off-site, all from a mobile device,” said O’Mahoney. Should a breach occur during off-hours, management is notified according to business requirements and the solution, says Clendenin, “eliminates the extra step of speaking with an administrator and alarm company to ensure someone can travel to the facility to assess the situation.”

While the project timeframe was accelerated due to the timing of the

“Mobile Security Management allows customers to work smarter and more efficiently by providing visibility and remote control of intrusion systems,”

**- Troy Clendenin,
National Account
Manager for TycoIS**

new headquarters move, TycoIS completed the implementation flawlessly, on time and on budget. In fact, “the final invoice matched the proposal exactly, which we were thrilled about,” said O’Mahoney.

Results

TBS now limits liability and loss via a more controlled environment and employees report feeling empowered. Furthermore, TBS employees and management find the integrated solution helps streamline business operations. “The ability for employees to move around various facilities without running into any issues allows for greater flexibility, convenience and ultimately, improved productivity,” said O’Mahoney. Working together, the customer and TycoIS installed the integrated solution at the new headquarters and the secondary location, and are now in the process of implementing the solution at a third service center location, with plans for upgrading all 10 Texas TBS locations in the next five to eight years.

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



Biometric System for Iraqi Border Patrol Security

Government Border Control in Iraq

M₂SYS works closely with its clients enabling them to capitalise on the benefits of using biometrics for security and accelerating their return on investment (ROI). These case studies of multi-modal biometrics security deployments for various verticals show how biometric security software solutions can protect the welfare of citizens, stop corruption and fraud and create efficiency.

Over one million registrants and 100 terminal checkpoints with plans for future project expansion to 400 terminal checkpoints, the Iraqi Kurdistan Province of Sulaymaniyah currently uses the M₂SYS AFIS/ABIS biometric identification system to protect their borders from insurgents and terrorists. The Government of Sulaymaniyah Province are using M₂SYS fingerprint biometric technology to automate border control check in, boost security, increase efficiencies by eliminating paperwork and enhance staff productivity.

Challenge

Prior to implementing the biometric border control software system, border control agents were manually recording visitors and processing the corresponding administrative paperwork manually by hand which caused major delays. The entire process was extremely time consuming often taking staff 15 – 20 minutes to complete the registration process for each visitor. In addition, there were security concerns due to the absence of a virtually foolproof means of verifying an individual's identity. Worries over insurgents and terrorists infiltrating the city and jeopardising the safety of residents were a big concern for the government.

Sulaymaniyah Province realised changing to a more modern, technologically advanced border control management system that automated the check-in process was a priority. As part of this transition from manual and paper to automated and electronic, they decided to use the M₂SYS AFIS/ABIS solution which includes Bio-Plugin™ biometric fingerprint identification technology.

Solution

Having already captured over one million biometric identification templates, Sulaymaniyah Province utilises Hybrid Biometric Platform from M₂SYS



Technology through 100 fingerprint terminals (with plans to expand to 400 fingerprint terminals) and the M₂SYS web based border control management software application to record and manage visitor traffic flow into the Kurdistan Region.

In addition, Sulaymaniyah Province also uses a web based application at all border points and the airport which all connect directly with the main datacenter. This helps to more effectively coordinate database sharing to control border security and facilitate visitor management at centers throughout the country.

Benefit

Now with over a million visitors in their biometric fingerprint database, the project increased staff productivity by 70%, minimising paperwork for visitor processing that previously caused major delays. The biometric border control technology achieved the objective to convert provincial workflow from manual and paper based to an automated and electronic system. Sulaymaniyah Province now fully controls the database, reducing fear of threatening visitors entering the premises. As part of their counterinsurgency operation, using biometrics for identification has significantly increased citizen security and safety, virtually preventing Improvised Explosive Devices (IEDs) and terrorist attacks from insurgents.

For more information, please visit:
www.m2sys.com **ESST**



Swedish Epassport and National eID

Swedish epassports are regarded as one of the world's most secure travel documents and enjoy a strong reputation. It is also ranked as one of the most powerful as Swedish citizens can enjoy visa-free travel to many countries around the world.

According to goeuro and its 2015 Ultimate passport ranking, the Swedish electronic passport is ranking #1. The factors taken into account included visa free access, the ability of a citizen to obtain a passport and the amount of hours a citizen must work to obtain their passport.

A Global Infrastructure for Electronic Passport and National eID

In January 2012 Sweden started to issue the new generations of its electronic passport and national electronic ID card.

Gemalto manages the end-to-end delivery process including the live enrollment solution in Sweden, production of all secure travel documents, as well as operated issuance services.

The contract signed in 2011 with the local authorities includes the enrollment solution including the software for registering the applicants' personal data, along with enrollment kiosks for instant capture of the holder's photograph, fingerprints and electronic signature. Gemalto supplies the operated issuance services which ensure document personalization from its premises based in the Stockholm area.

The same infrastructure and procedures are maintained for the National eID card as for the ePassport. This leads to significant savings in terms of equipment, processes, systems and staff training.

The Operating Model: Outsourcing
The Swedish police put paramount importance to expertise in performing service functions, treating each citizen as a customer who needs to be served with utmost competence and efficiency. This is precisely what Gemalto offers to Sweden through its operation center in Stockholm.

Gemalto is delivering a solution that improves the



efficiency and effectiveness of new Swedish national document production, personalisation and issuance. Security level is high and collaboration is a daily reality.

The Police bottom-line of providing quality service and optimising taxpayers' money were the primary drivers for outsourcing. The Police are also maintaining a fundamental characteristic of its own operations.

Authority and the Control that Such Authority Guarantees

Outsourcing production and personalisation services to Gemalto is a model that combines the use of latest technology with technical expertise.

The Swedish police have been able to free their resources from being bogged down by functions that do not enhance their core competencies such as printing documents and management the logistics to distribute them.

The increasing complexity of the technical environment; the difficulty hiring qualified candidates, particularly for IT operations; and the lengthy procurement cycle to upgrade technology were all valid reasons for the Swedish police to consider outsourcing to Gemalto.

As the scope of the Swedish Police continues to grow, they now have the industry best processes and scalable model to ensure continued efficiencies.

The Swedish Passport: A Distinctive Design

The Swedish ePassport is certainly one the most advanced secure travel documents rolled out in the recent years and definitively a piece of art. Collaboration with the Royal Swedish Police was key to deliver a unique and distinctive passport and a symbol of pride in the hands of millions of Swedes.

This combination of stylish design and passport security features both illustrates the Swedish identity and makes the passport one of the most secure in circulation.

For more information, please visit:
www.gemalto.com



Arecont Vision Megapixel Cameras Prove to be a Valuable Asset in the Banking Environment

South Africa's Absa Bank Evaluates Arecont Vision Megapixel Panoramic Model

Megapixel Solution

The new security surveillance system at Absa Bank was installed by AV Enforce Electronics (AVEE) of South Africa. The system employs Arecont Vision's 2.0 and 3.0 Megapixel Cameras positioned behind teller stations to closely monitor transactions between bank employees and clients. In addition, Arecont Vision's 8 Megapixel 180-degree and 360-degree Pan-oramic Cameras (AV8185 and AV8365) watch over customer queues, automated teller machines (ATMs) and the general banking hall with extreme image detail.

The Absa Group Limited is one of South Africa's largest financial services groups offering a complete range of banking and wealth management products and services.

Each Arecont Vision megapixel camera at the Absa Bank installation is connected to a power-over-Ethernet network switch that serves as the network video connection and also as the power source to the camera. Cameras are recorded on Luxriot network video recorders. The system is monitored locally by authorised management personnel. Arecont Vision's AV3105 3-Megapixel Camera uses a 1/2-in CMOS sensor to provide 2048x1536-pixel progressive scan images at up to 15 frames per second (fps). The camera is built with Arecont Vision's massively-parallel MegaVideo® technology, providing image processing at billions of operations per second. It can output multiple image formats of larger areas to allow simultaneous viewing of the full resolution field of view and regions of interest. The Arecont Vision AV2105 2-Megapixel Camera provides 1600x1200-pixel video at up to 24 fps, with light sensitivity of 0.1 lux at F1.4. Features include forensic zooming on archived video, region of interest views as well as image cropping and motion detection.

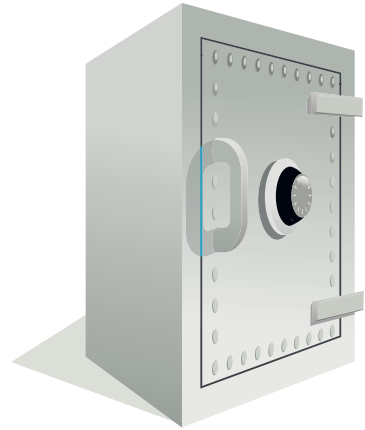
The panoramic view cameras used at the Absa Bank proof of concept installation are the 180-degree Arecont Vision AV8185 and 360-degree Arecont Vision AV8365 8-Megapixel Cameras. Both models employ

four 2-megapixel sensors enclosed in 6-inch IP66-rated domes and provide up to 6400x1200-pixel images at 5.5 fps. The cameras can be set for lower resolutions at

higher frame speeds such as 1600x1200-pixel images at 22 fps or 800x600-pixel images at 88 fps. The cameras also use Arecont Vision MegaVideo® video processing at billions of operations per second. Light sensitivity is 0.2 lux at F2.0 and the cameras provide image cropping and up to four regions-of-interest. "Arecont Vision outperforms all the current competitors," said Alex De Barros of AV Enforce. "The price compared to analog cameras is better considering the fact that you gain so much. We were able to capture images for the bank that were never achieved before."

Megapixel Benefit

Arecont Vision megapixel network cameras use H.264 compression to minimise bandwidth and storage needs and are available at costs comparable to standard-resolution alternatives. Mega-pixel images provide much more detail in playback mode for forensic investigations. Operators can zoom in for up-close views on stored images. They can view specific parts of a larger image such as a person's face. A benefit for Absa Bank is creation of a database of suspected criminals to allow operators to identify them easily. The use of megapixel video enables a larger area to be covered with fewer cameras, which reduces overall system cost which make



"The price compared to analog cameras is better considering the fact that you gain so much. We were able to capture images for the bank that were never achieved before."

- Alex De Barros of AV Enforce



“There is a lot at stake in the banking environment, and mega pixel imaging can vastly improve the performance of the video surveillance systems in this important market.”

- **Ethan Maxon,**
Middle East and
Africa Regional Sales
Manager of Arecont
Vision

it easier to realize ROI. Higher-resolution images boost the functionality of systems, enabling pristine image quality at industry-leading high frame rates, while minimising bandwidth usage with H.264 video compression.

The proof-of-concept system at Absa Bank has demonstrated that megapixel cameras are suitable for applications in the banking environment and represent a significant upgrade in system functionality compared to standard-resolution cameras. In addition to lower bandwidth and storage requirements, megapixel cameras can dramatically decrease costs related to other elements of a system such as fewer software licenses, less cabling fewer lenses, and a decrease in man-hours needed to bring it all together. “There is a lot at stake in the banking environment, and mega pixel imaging can vastly improve the performance of the video surveillance systems in this important market,” said Ethan Maxon, Middle East and Africa Regional Sales Manager of Arecont Vision. “We continue to spread the word about the unparalleled image quality and resolution of Arecont Vision’s megapixel IP video cameras. It’s good to know that Absa Bank has experienced those benefits first-hand.”

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

Countering a Proliferation of Threats

By Mark Desmarais, Clear View Security Solutions Program Manager of Raytheon Company

The global proliferation of terrorist threats is undeniable and unprecedented. The perpetrators of these threats specifically select targets to cause maximum harm and inflict local, regional or even global economic damage. To counter these threats and mitigate the corresponding personal and economic consequences, governments and business are selecting integrated security solutions that leverage existing investments with new capabilities to provide situational awareness at a glance based on robust collection, correlation, analysis and metrics.

Raytheon has successfully applied its extensive international, military, federal, and commercial expertise to the development and deployment of Clear View™ security solutions. The Clear View system is a comprehensive, fully integrated security management system for critical infrastructure protection, aviation security, border security and other security applications. The system includes several incident management tools; video management, resource management, asset



management, knowledge management, and advanced collection, correlation, analysis, forensics and metrics. The system instantly detects and assesses intrusions for a quick and effective response.

Complete Situational Awareness

Whether it’s securing a refinery, port (air, sea or rail) or a national border, the Clear View system is a highly efficient and easily configurable solution to manage complex security challenges. The system interconnects sensors, cameras and other business systems to enable comprehensive situational awareness at a glance and robust command and control of security resources. All events are displayed on a geospatial display using flexible, standards based symbols.

The system supports multiple Geographic Information System display formats including Google Earth and ESRI. Every event is displayed in context so the operator can immediately know where the event is occurring, see events in the area and locate responders. The system

continue on page 56



can automatically slew a camera to the event for immediate operator identification and assessment. Furthermore, all of the associated information is presented in the live video frame. The operator can coordinate response personnel and forward real time event information to responders without taking his eyes off of the video feed, ensuring safety for all responders. The user interface provides information layers.

Low Total Cost of Ownership

Based on an open industry standards and service oriented architecture, the Clear View system is affordable, flexible and scalable. The system is vendor neutral, and was designed to protect the customer's security investment by offering a solution that seamlessly integrates commercial off the shelf hardware and software. Compatible with industry standards, the system enables "plug and play" upgrades of sensors, cameras, radars, closed circuit television and other system components providing a cost effective security solution. An adapter library simplifies integration with existing customer components that are not standards based. Security systems need to evolve as threats change. The Clear View system includes modeling and simulation services that enable planners to analyse the effectiveness of proposed changes (policies, procedures, resources, placements)

before upgrades are purchased or installed.

Unique Sensor Management, Correlation and Tracking

Leveraging Raytheon's expertise in capturing and integrating sensor data, the Clear View system provides tracking and correlation capabilities that are unique in the industry. Multi sensor correlation enables the system to automatically correlate events from dissimilar sensors to form a single event and common database. This allows the system to maintain a high probability of detection. It also reduces the number of false alarms and better manages nuisance alarms; freeing up the security operator to focus on real intrusions.

Flexibility to Meet Changing Conditions

The Clear View system was designed to easily adapt to specific customer environments and evolving threats without modifying software. The system features workflows and rules to implement customer concepts of operations, policies and procedures. Work flows translate business processes and policies into automated actions. Work flows are developed using a standards-based business process engineering language that is automatically converted to Clear View system operations.

Work Flows and rules are easily defined by the operator using a drag and drop graphical user interface. Most work flow and rule changes can be implemented in a matter of minutes or hours instead of days, weeks, or months frequently required for source code modification. Work flows and rules simplify operator interaction with system devices.

In addition, work flows and rules provide specific step-by-step action plans, based on pre-determined rules and policies. It responds and manages the threat and control response operations, including automated escalation and notification if the appropriate actions are not performed in a timely manner. The system enables operators, shift supervisors and senior leaders to proactively monitor work flows and rules in real-time to ensure events are being processed appropriately.

Securing Valuable Assets

Regardless of the complexity of the challenge, Raytheon's Clear View security solutions provide rapid situational awareness and accurate threat assessment to enable informed decision making so vital to saving lives and protecting valuable assets.

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

Blank Rome Law Firm Migrates to Symmetry SR Solution

When Blank Rome, a 70 year old prestigious law firm, learned its existing access control system was end of life, Director of Information Security, Robert Weaver was faced with a decision. Should Blank Rome continue using its current

system, Facility Commander where getting replacement parts would become expensive and difficult to source or should they consider a new alternative?

Weaver turned to its long time partner and integrator,

continue on page 57



The Protection Bureau for an answer. Together, Weaver and The Protection Bureau President, J. Matthew Ladd reviewed the pros and cons of staying with Facility Commander or upgrading their system and installing AMAG Technology's Symmetry SR Retrofit Controller system. The Symmetry SR Retrofit solution offered an easy and affordable upgrade path. Blank Rome could keep their existing hardware, saving thousands of dollars, and upgrade to a state of the art access control system that would expand as their company grew. Having a system that could grow with them was important as the company is currently adding more offices. "We wanted to present Blank Rome with the best option that would fit their needs," said The Protection Bureau President, J. Matthew Ladd. "We worked with the Protection Bureau to identify an upgrade path that was going to be effective, cost efficient and provide us with the functionality that we were looking for.

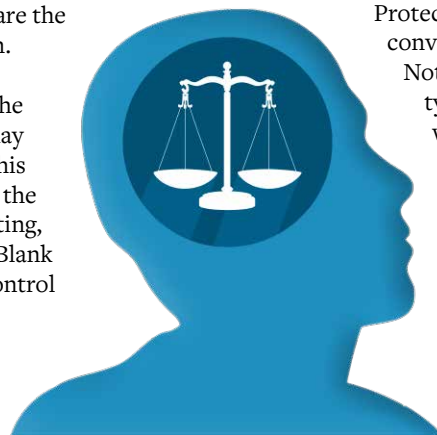
They recommended AMAG's SR system," said Blank Rome, Director of Information Security, Robert Weaver. Blank Rome required a centralised enterprise access control system to limit access throughout their offices and protect their physical assets. Symmetry would secure nine locations and be managed from one office. Remote monitoring and identity management were critical requirements for the system.

The Symmetry SR Retrofit solution allowed Blank Rome to use their existing card readers, cards, locks, request to exit devices and enclosures. The Protection Bureau converted their database and easily changed out every controller. The Protection Bureau and Blank Rome worked closely throughout a lengthy preplanning phase to ensure project success. The conversion would be done live while the current system was running. This was no easy task.

A conservative hardware timeframe was established, and the Protection Bureau was able to accelerate that dramatically once they saw how quickly the panels were swapping out. The Protection Bureau built a parallel system, installed the new software and approximately seven clients to prepare the environment prior to the conversion.

A month before the conversion, The Protection Bureau provided a one day training session for Weaver and his security team where they learned the system and went over troubleshooting, maintenance and badge creation. Blank Rome found Symmetry access control software easy to learn and use.

Cloning the environment took a week of reprogramming hardware components using the



"There was no downtime and no data reentry; all the data was converted over for us. The reporting capabilities are easy to use and provide the data I need."

- Blank Rome's Director of Information Security, Robert Weaver

old system as a template. All cardholders and access levels were migrated from the old system to the new Symmetry SR system. Once the migration was complete and Symmetry software online, The Protection Bureau manually programmed each site location including each controller, reader, input and output.

"It went so smoothly that we didn't need to get involved," said Weaver. "From the integrator side, we couldn't have asked for a smoother conversion," said Ladd. The Protection Bureau and Blank Rome carefully timed the card export to coordinate with business operations.

The card export of 1200 cardholders took a day and a half which was quick, and the staff didn't notice the seamless changeover. "The whole project went very quickly," said Weaver.

Blank Rome was the first large scale SR retrofit opportunity for The Protection Bureau. They dove in and completed nine sites throughout the US and one in Shanghai, China. Their familiarity with the product helped make the conversion go smoothly.

"From our standpoint, it just went beautifully. We had to tweak one or two small things, but nothing major," said Ladd. "It's hard to keep two systems operational at the same time, but this conversion process is literally plug and play, just like AMAG said it was." "The Protection Bureau managed the database conversion well and converted it quickly. Not just any integrator can perform this type of conversion. We've been working with The Protection Bureau since 1997 and are always pleased with the level of service we receive from them," said Weaver. "The entire staff is top notch. They are knowledgeable about the product. They help us on the spot and we have a very positive relationship."

For more information, please visit:
www.amag.com 



JFK Terminal 1 Improves Security with Milestone Video

JFK Terminal One Upgrades to IP Video for Improved Functionality, Image Quality

The Challenge

Previously, Terminal One at JFK International Airport relied on a limited analog surveillance system and a separate, older IP system that were independent of each other. Both were inadequate and lacked the functionality that Terminal One needed. Users could only view video from specific workstations, it was difficult to replace or add cameras, and the system did not integrate easily with other systems. Migrating the terminal's old analog system to an advanced IP video management software (VMS) platform was no small feat. Due to the airport's high-security environment, the system and all of its cameras had to remain operational around the clock throughout the migration.

The Solution

To design and implement a new solution, the airport worked with security integrator Media Wire, LLC. The New York-based integrator designed and implemented a Milestone XProtect Corporate VMS system to manage 500 to 600 cameras, including the installation of 160 new Axis cameras. Providing users with greater access to video, the Milestone Mobile client is used by air terminal managers to view video on their mobile devices. The Milestone VMS is integrated with Honeywell's Pro-Watch access control system so all alarms and door information can be easily accessed from one centralised system.

Additionally, the advanced VMS integrates via Milestone Interconnect with the video from the Milestone Husky network video recorders (NVRs) used by the terminal's restaurants and vendors, enabling broader coverage of the entire terminal.

Advantages

Milestone's IP VMS provided a significant upgrade to the terminal's analog system and greatly enhanced the ability to monitor and efficiently respond to incidents. The system's search capabilities enable users to quickly find and identify camera views. It provides users with the flexibility to view any of the nearly 600 cameras from any workstation throughout the airport, even from



continue on page 59



their mobile devices. Greater video coverage means the terminal can be protected against a range of threats including security breaches, aggressive actions and injury and liability issues. With many agencies requiring access to the system, from the FBI to building maintenance, the terminal's new system is more user friendly, making it much easier for operators to manage.

Institution Profile

JFK International Airport has been at the forefront of aviation since its first commercial flight in 1948. Located 12 miles southeast of Lower Manhattan, the airport has expanded to include six airline terminals operated by the Port Authority of New York. Terminal One opened in 1998 and includes 11 gates and two hardstands controlled by its own ramp control tower, which is equipped with state-of-the-art radio communications, weather information and gate video cameras. It is one of two terminals at JFK that has the capability to handle the world's largest passenger aircraft, the Airbus A380 aircraft. In 2013, Terminal One had 2.5 million international passengers. According to Timo Kapulainen, Maintenance Supervisor at Ekokem, the innovative initiative has been

very well received by Ekokem's customers: "Our customers are very satisfied with the initiative and it has helped raise customer satisfaction. It sends a very positive signal about us keeping our promises and being totally transparent".

Migrating an Around-the-Clock System

The biggest challenge of migrating JFK's Terminal One analog system to IP was keeping all cameras operational throughout the transition. To do so, technicians took each live camera and connected it to an additional working system. In the process, video from the camera was recorded by both systems. Once the camera was migrated and ported to the Milestone VMS, the camera was then decommissioned from the analog system.

Migrating Terminal One's system required upgrades to ensure a solid solution from the ground

up. New high-speed fiber optics, switches, PoE injectors, software, workstations and operating systems were installed. The terminal has close to one Petabyte of storage due to both security requirements and powerful analytics from Agent Vi that are used on recorded video, and to search across cameras. Much of the management structure is built on existing Dell servers (approximately 14 recording servers as well as the supporting storage) but all new servers are being custom built with close support from Milestone Engineering.

Since the migration involved multiple VMS clients managing video from cameras throughout the terminal, technicians set up a multicasting network to reduce bandwidth. It allows multiple users to view the same video stream without taxing the server, which was lacking with the old analog system. "We installed an extensive 10 Gig fiber network to support the bandwidth needed for current and future cameras," added Tordai. "All cameras provide video at their maximum resolutions and frame rates, no corners are cut."

Milestone Open Platform Meets Tough Demands

The Milestone VMS was selected in large part due to its easy integration with nearly any third-party system. In Terminal One the new VMS had to support older analog systems and cameras via encoders, also supporting a variety of IP cameras, integrating with access control and the NVRs used by vendors. The result has been a system that provides JFK International Airport with greater access to video and

"From a security standpoint, we can capture what we need on a daily basis and it gives us great visibility into areas we never had before."

- Head of Security for Terminal One Management

continue on page 60



advanced capabilities, including viewing video on their mobile devices. "The versatility of the system is great and it's so easy to use," said the Head of Security for Terminal One Management.

"From a security standpoint, we can capture what we need on a daily basis and it gives us great visibility into areas we never had before." The Milestone system is easily scalable and can accommodate additional or new cameras at any time. Terminal One's new Axis cameras easily integrated with the Milestone system and require less bandwidth that better allow the security team to meet the airport's lengthy storage requirements. Since Axis also provides a wide range of cameras for many applications, Tordai says he was able to use them in many areas where lighting was a concern, like near windows or in stairwells.

Robust, Easy-to-Use System

Terminal One's Milestone VMS provides broader coverage and features that make it easier to automatically monitor possible security concerns, such as an item left unattended. It also allows the security team to watch for suspicious people, monitor situations and

investigate after the fact.

Milestone is a great system and a drastic improvement over our previous analog system," added the Head of Security for Terminal One Management. "It allows us to deploy tools that are allowing us to mitigate risk and do our jobs more efficiently." The Milestone VMS provides users with shortcuts and keyboard assignments so they can easily change views or create camera setback positions. Through integration with its access control system, the display system will also automatically show all alarms and doors being accessed.

A Soaring Success with Tech Support

Tordai added that Milestone has provided excellent technical support throughout the installation. Cameras are currently being installed in jet bridges, the enclosed connectors that extend from a

*"It allows us to deploy tools that are allowing us to mitigate risk and do our jobs more efficiently. The Milestone VMS provides users with shortcuts and keyboard assignments so they can easily change views or create camera setback positions."
- Head of Security for Terminal One Management*

terminal gate to the airplane. About 10 cameras are being installed in each jet bridge and when they ran into a software issue, Milestone addressed it quickly. "I contacted Milestone tech support and they got it done," said Tordai. "The tech took it over and did a great job at solving the problem quickly." He says the airport has been extremely pleased with the Milestone VMS and Axis cameras. About 160 new Axis cameras are being installed throughout the terminal for better security and liability purposes.

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

Service Works Inc. and Honeywell Partner to Provide Cutting-Edge Security for Morristown Municipal Airport in Morristown, New Jersey

The Client

Conducting more than 220,000 flight operations a year, Morristown Airport is a general aviation reliever airport in the New York metropolitan area. They accommodate a mix of international and domestic corporate flights as

well as charter air carriers that rely on the airport for a safe, efficient and hassle-free travel experience.

The Situation

Currently, general aviation airports are not subject

continue on page 61



to federal mandates to provide security. However, Morristown Airport officials wanted to add a camera and gate access system to increase security for the public use areas of the airport so the tenants, users, and surrounding community would feel more safe and secure.

The airport had an existing system that wasn't able to address their specific needs, so airport management was looking for a security integrator who could create a web-based system that had the capability of expansion without additional capital costs.

"After we looked at the different products that were out there, we found that Honeywell really had the cutting-edge technology that we wanted. Their system has the capability to expand very easily and is web-based, which were two of our main criteria," said Maria Renner, Manager of Government Affairs for Morristown Airport.



The Solution

The airport contracted security integrator Service Works, Inc. (SWI) of Farmingdale, NJ. SWI reengineered the project, along with Honeywell, to address the airport's specific needs. They removed the existing products and created a Honeywell solution that includes IP-based video as well as card access control. "Honeywell worked with us on the project from the beginning. We started off with the new Digital Video Manager (DVM) product, which is exceptional, added the Pro-Watch line and we integrated that with other Honeywell products to give the airport one complete solution," explained Stephen Govel, President of SWI.

The airport wanted to make sure the system complemented the aesthetics of the facility and the entrance road into the property. SWI custom-matched all of the Honeywell domes and housings to the existing décor. In addition, SWI designed the system ergonomically so that the operators could efficiently answer issues or protocols by exception rather than having to manage a very involved process.

The Benefits

Everything is scalable and on an IP-based system. Honeywell's Digital Video Manager, an IP-based video management solution, is integrated with Pro-Watch, the access control solution. With the integration, operators do not have to manage several disparate systems. "By

allowing Pro-Watch to integrate with the IP solutions, intercoms and other solutions, we save the airport significant dollars and provide them and their customers with the security of having a solution that fits their needs," explained Michael Thomas, Vice President of Engineering for SWI.

For the access control solution, they used multi-technology readers that involve compliance with smart cards and/or HID multi-technology cards for their customers and staff. They also have Smart Pass readers for emergency vehicles and snow removal vehicles. If an airport employee approaches a gate, they have a Smart Pass, which is an unobtrusive but secure mode of entering the facility. When a non-employee approaches any of the gates, a motion detector senses the person and will train every camera to that person and capture video. The system allows that person to easily call the administrator or the Operations Center for access to the facility.

SWI designed a system that improves security in an emergency. In addition, the future system design will save additional money. A wireless mesh networking will allow for mobile applications such as roving patrols to see video or exception alarm routing at any point in the airport facility.

"One of the things that SWI and Honeywell have provided for us is the ability to do more with the manpower that we have. We have been able to make our operations coordinators who also act as our security coordinators, more efficient and effective in their jobs because they use the technology to supplement their need to be out on the airfield," explains Renner. By instituting these security improvements, the airport is setting an example for all general aviation facilities. "It gives an overall sense of security for our tenants and our users, that they're at an airport that has taken security very seriously and is looking to be on the leading edge of general aviation," concluded Renner.

The Product

- Digital Video Manager (DVM)
- Pro-Watch
- HD6 Domes
- HD4 Interior Fixed Vandal Proof
- Color Cameras

For more information, please visit:
www.honeywell.com **ESST**



BIOMETRICS AND BANKING

By HID Global

Ensuring Biometric Data is Useless to Identity Thieves

HID Global notes that biometrics is the only authentication method that binds a myriad of digital and physical credentials to a person. Biometrics plays an important role in eliminating digital identity theft in today's increasingly complex and vulnerable digital environment. Fingerprint images were among the sensitive information that was stolen in the 2015 U.S. Office of Personnel Management (OPM) breach.

Conceivably, this biometric data could be used by the perpetrators to hijack a user's identity and gain fraudulent access to security systems. It is important to understand that biometric characteristics are not secrets. Facial characteristics are quite public. Not only observable, but also generally associated with our names and other personal information. In the OPM example, now that fingerprints have been stolen from government databases and can never be taken back, the key question becomes what can or should be done to render this information useless to any would-be impostor? Given the premise that databases are inherently vulnerable to attack, the challenge is one of minimising negative impacts of a breach on individuals and organisations. As always,



the answer depends on the use case and each category of applications must be examined individually and its associated threats assessed. In this complex and interconnected digital world, systems must be thoughtfully designed and deployed in order to protect user identities and ensure appropriate levels of security within the context of the application.

In the case of biometric data that is already “in the wild” (such as that stolen from the OPM), numerous tactics and best practices should be considered in order to render identities useless to anyone but the legitimate owner. Of critical importance is the ability to detect fraudulent attempts to use biometric data. Liveness detection, the real-time determination that the biometric characteristics presented are genuine and not fake is a highly effective design feature in solutions where users physically interact with authentication systems. Augmenting biometric liveness detection with other security layers for multi-factor authentication greatly enhances digital security and renders the theft of any one personal data element inconsequential.

Improving Liveness Detection

HID Global notes that one of the most effective liveness detection approaches for fingerprint biometrics uses Lumidigm® multispectral imaging technology, which virtually eliminates the possibility of counterfeit fingerprints being used for authentication. The technology is used to compare the complex optical characteristics of the material being presented against known characteristics of living skin.

Multispectral imaging sensors are different from competitive offerings in that they:

Liveness detection, the real-time determination that the biometric characteristics presented are genuine and not fake is a highly effective design feature in solutions where users physically interact with authentication system.

- Use multiple sources and types of light along with advanced polarisation techniques to capture information from the surface and subsurface of the finger all the way down to capillary beds and other sub-dermal structures.
- Utilise advanced machine learning algorithms that can be updated in the field as new threats and spoofs are identified, enabling the sensors to very quickly respond and adapt to new vulnerabilities.

Multi-Factor and Multi-Modal Authentication

For strong and reliable user authentication, organisations should consider, where practical, multi-factor and even multi-modal authentication. Today's authentication technologies enable solutions that can enhance security while replacing passwords and improving convenience in a seamless way that is non-intrusive to the legitimate user. For example, personal devices like smartphones,

wearables, RFID cards and other intelligent personal devices can all generally be used as factors of authentication.

When identity is firmly established, the use of mobile devices in authentication solutions offers the opportunity for greater personalisation and a seamless experience for legitimate users. Information systems can be tailored to each user's need, resulting in enhanced, individualised security, allowing individuals to fully control their real identity.

Robust Biometric Templates

It may be desirable in some application-dependent situations to construct and enforce the use of enhanced biometric templates. The use of a “super template” that uniquely combines biometric data with other information, perhaps even an OTP or other out-of-band data enables the system to recognize and reject a biometric template that was created from a stolen fingerprint image. Templates can reside on a card or chip or in a smartphone or personal wearable.

Identity Proofing

Lastly, it's important to remember that the chain of trust is only as strong as the weakest link. The biometric solution used in identity-proofing must interoperate with trusted devices at each verification point. An example of this approach is HID Global's Seos™ based solutions which create a device-independent, trusted physical identity verification process. Additionally, the physical devices themselves must be tamper-resistant to ensure that all transaction integrity is preserved.

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



Get the Most Out of Your Security Cameras

By Tyco Integrated Security (© 2017 Tyco Integrated Security)

Many business owners know that video surveillance is an important part of a comprehensive security plan but knowing where to place cameras and how to leverage unique camera capabilities can help you get even more out of the technology. From infrared camera models to IP-networked setups, video surveillance can help to better deter theft and burglary and provide valuable insights to make operational changes.

It is important to note that each country has different laws regarding workplace surveillance, and cameras should not override workers' rights to privacy. Be sure to consult a security professional who is aware of your local regulations before installing cameras or upgrading your current system.

Four places to leverage video surveillance cameras in your business:

Tighten Security at Entry/Exit Points

One of the most obvious places to place cameras is at your business' entry and exit points because this placement offers several advantages. Not only can these cameras be used in conjunction with security systems like alarms, badged entry and keypads to record movement but they can also be used to visually identify personnel and customers prior to entry, putting the business owner in control of the traffic moving in and out of the business.

Cameras at these points can also provide a record of visitors, which can be useful if a theft or other event were to occur.

In cases where a warehouse has high-value stock, monitoring entry and exit points can reduce shrinkage when loss prevention experts are present. In pharmacy and healthcare settings, for example, costly products and patient privacy can be better safeguarded with passageway monitoring.

Increase Awareness at POS Station/Cash Register

Positioning cameras so they focus on locations where currency is handled can help verify that staff is following opening and closing procedures. Managers can review footage with employees to highlight opportunities for improvement and are able to directly train employees on best practices.

With the right setup, these images can also provide a record in cases of burglary for law enforcement. In busy retail environments, cameras can help





protect staff and offer an additional deterrent against theft, even during high-traffic times. In restaurants, for example, cameras above cash registers capture cash handling, providing a record in cases of discrepancy.

Gain Insight into Common/Outdoor Areas

Monitoring open areas like common office space and retail floors can serve dual purposes: Cameras can offer increases in productivity and efficiency while also creating an additional layer of protection. With analytics programmed into IP cameras, a business owner can evaluate traffic flow, line queuing, dwelling on a product or display and team dynamics. Knowing which product is garnering attention, where customers tend to linger and when customers come into the business offers business owners additional insights into their operations which can translate into increased efficiency or even more revenue.

Placing cameras in parking lots and external areas helps to better protect both employees and customers, particularly in locations with low light. Infrared cameras have the ability to show detailed, full-color images during the day and high-definition black and white images at night, when burglary is more common.

Cameras can also be installed to offer views of a larger area or to focus on areas that employees on the ground might have difficulty viewing. When strategically placed, cameras can give security personnel the ability to look around corners, pan in and out of locations and monitor areas.

Foster Compliance in Backrooms

Beyond entry and exit points, locations where material

goods are held offer an opportunity to create additional layers of security. IP-networked technology allows businesses to review several locations at once, and to stay in control of business operations more efficiently.

Placing cameras to record backrooms can provide additional protection against theft and create a record should liability become an issue. These images can also allow businesses to ensure that employees are performing their jobs and following safety protocol. For instance, in situations where volatile or sensitive materials are handled, cameras allow management to track procedures to better ensure that processes meet industry and government guidelines.

In locations where materials must be kept warm or cold, like in a kitchen at a restaurant, thermal imaging can give additional insight into product integrity. By increasing awareness of a facility, these cameras can help businesses proactively address conditions that are not optimal for goods and protect against costly losses when conditions for stock are not met.

Using cameras to monitor backroom activity, give business owners the ability to address procedure deviations and correct them before they interfere with meeting customer or partner demands.

Video surveillance technology is an important part of any security system, as it can help businesses meet compliance standards, review multiple locations at a time and offer opportunities to gain operational insight. When used in conjunction with a Mobile Security Management system, access control or a burglar alarm, the technology helps create an additional layer of security.

*For more information, please visit: www.tycois.com **ESST***



PASSPORT SECURITY DESIGN:

ANATOMY OF A SECURE TRAVEL DOCUMENT

By: © 2006- 2017 Gemalto NV

The resistance of your passport can be increased dramatically, using a series of field-proven and cost-effective techniques.

The Five Major Passport Fraud Techniques and How to Deal With Them

Passports and ePassports are not immune to attack. Increasing use of microprocessor technology has raised the bar but not put off the fraudsters. To ensure robust protection, authorities must focus on the design and processes when creating their new national travel documents.

The new passport is protected properly against the five main threats.

1. Counterfeiting

- Counterfeiting is the complete reproduction of the document which involves:
- Using substitute materials to imitate original documents (paper, polycarbonate)
- Scanning valid documents for modification using computer software
- Reproduction of background and logos using alternate printing technologies
- Final lamination using commercial laminates
- Re-creating document using computer software
- Using commercially available original material

The key is to design a document that is very difficult to copy, produce and



personalise which can be achieved by multiplying effects, combining tactile and optical features, different technologies, and using material and inks not available in the public domain within a complex design.

2. Alteration

Alteration is where fraudsters try to change the data in a genuine document such as:

- Photo alteration or substitution
- Alteration of the biographical data, in the visual or machine readable zone (MRZ)
- Deletion of entries on visa/ observations pages
- Mechanical and chemical erasure of biographical data
- Delaminating attacks
- Alteration of the personalisation data on the data page.

Personal data should be:

- Inserted inside the document structure, not just on the surface, to make it difficult for fraudsters to reach, alter or recreate it.
- Interlocked with security features. The forged passport will therefore show clear and visible traces of alteration.
- Duplication of the personal data, using various techniques,

also makes the work of the fraudster much harder.

3. Recycling

This involves the creation of fraudulent documents, using material from legitimate documents, and the removal and substitution of entire pages or visas.

- Removing security features from a genuine document for reuse in a falsified one
- Using “recycled” genuine passport security features in a new falsification
- Interchanging pages between one passport and another

To prevent this kind of attack, all elements have to be closely interlocked and integrated. A holistic passport security design is therefore critical.

4. Stealing

This is the theft of an original, genuine blank document. Fraudulent passports in that case can be very hard to detect because they are genuine documents.

The integrity of manufacturing, transportation, storage and accounting of blank documents is critical to the entire security chain. Using a combination of advanced technologies for personalisation forces fraudsters to try and master them all.

5. Misuse of A Genuine Document Belonging to A Similar-Looking Person

Examples of this include:

- An unauthorised person using a valid genuine passport
- Use of registered lost or stolen documents by look-alikes of the real holder
- Cloning logical data from a similar looking person

It might appear difficult to address these threats at the document level. However, the danger of a stolen passport can be minimised by using a high quality personalisation technology to additional personalised elements including the repeated occurrence of the holder’s portrait in several places in the document.

The core benefit of an ePassport is that it allows the identity of the holder to be compared with his/her biometric data (such as finger prints and facial image), as stored in the microcontroller and the convenient use of databases such as Interpol ‘s Stolen and Lost Travel Documents database.

The Keys to Passport Security Design

Combine and connect all the elements into a single strong document

- Define the right materials (parts), unique processes and product construction that will be used
- Mix the artwork and security design as early as possible
- Protect the document and the citizen’s data
- Remember “less is more” A high level of conformance between all genuine documents will also make copying and counterfeiting more difficult
- Create passports combining several techniques
- Count on the electronic passport *SST*



EXTRACT FROM 2017 CYBERSECURITY PREDICTIONS

By: Stroz Friedberg



In 2017, IoT devices will be compromised, harnessed as botnets and used as launching points for malware propagation, SPAM, DDoS attacks and anonymising malicious activities.

Predictions

Criminal Activity Will Intensify Against Vulnerable IOT Devices

Gartner predicts there will be nearly 26 billion internet-connect devices by 2020 and the smart home market alone is expected to reach \$121.73 billion by 2022.

Verizon reported that IoT revenues were \$217 million in Q3 of 2016, up 24 percent from the comparable period last year. With such a huge market opportunity and no baseline security regulations or standards in place for manufacturers, the number of everyday objects that present serious security risks will increase materially in 2017. At the same time, the number of DDoS attacks will grow.

Rising Ransomware Resulting in More Extortions and Disruptions of Businesses via Connected Devices

In 2017, we predict that internet-connected hospital technology such as the HVAC system will likely be held hostage in demand for bitcoin payment.

Despite calls from the security community for government regulation and set security standards to address the unprecedented risks posed by IoT devices, nothing significant has been issued.

Security Communities' Outcry for Government Regulations and Set Security Standards to Address Risks of Iot Devices Have Been Ignored

There continues to be little financial incentive for conducting standard security assessments or integrating firewalls into IoT devices and manufacturers focused on getting products to market efficiently and profitably won't proactively drive improvements to security standards or take the lead in integrating security into design. Many prominent consumer technology associations view consumer-led best practices, rather than government intervention, as the way forward.

Data Integrity Attacks Rise

Data sabotage as the next big threat will become a reality in 2017. Criminals will seek to sow confusion and doubt over the accuracy and reliability of information, impairing decision-making across the private and public sector.

In 2017, organizations will prioritise protecting themselves against data integrity and sabotage after an incident in which criminals successfully manipulate information such as company earnings, news announcements, voter information or the operational controls of a system such as energy grids.



CYBER CRIME

Advancement Of Spear-Phishing And Social Engineering Tactics

As organizations continue to migrate to and embrace evolving technologies, including the cloud and IoT and in parallel shore up perimeter defenses to raise the bar on network security, criminals will increase their focus on the human element as an entry point to pivot into broader network systems. In 2017, advanced social engineering tactics will become more targeted, cunning, and more effective, exploiting the weakest link – employees that organisations always find challenging to safeguard.

Defenses are improving around protecting infrastructure and new technologies that organisations are increasingly adopting such as cloud services. Providers like Amazon, Microsoft, and Google continue to bolster security to help protect companies that migrate their critical data to the cloud. As a result, in 2017 attackers will continue to increase their focus on targeting the human element, especially at the executive level of organisations. We will see an increase in spear-phishing attacks directed at insiders, third-party service providers and business partners, aimed at gaining wider and faster access to data, such as information on a company's R&D, M&A activity, strategy, employee data, customers or other critical assets. The individual, device and the interface in between the user and the cloud will become the primary targets for criminals hoping to obtain credentials. Therefore, employees will continue to be the Achilles heel of any security program and the critical line of defense against such attacks.

Criminals will broaden the range of social engineering and phishing tactics they employ, including spear-phishing attacks to increase their chances of success. We will see cases of phishing tactics that will continue to be more authentic in appearance with embedded malware that once clicked will infect or spread through an organisation's system. We will also see an uptick in phishing scams targeting mobile devices as well as social media sites that are accessed by employees on company mobile devices. Employees accessing social

media at work has become part of routine business operations for most organisations and the increasing reliance on accessing social media sites via mobile devices and apps, has created multiple security gaps ripe for exploitation by attackers. Adversaries will use more sophisticated coercion techniques to target employees using knowledge gained from their social media profiles to extort them or exploit their human vulnerabilities to deceive them into providing sensitive information.

To build a more robust profile of a target, criminals may even conduct a series of smaller attacks to gather personal information before launching one major attack to gain network credentials.

In 2017, we expect to see adversaries hone in on "high value" targets, which no longer only means high net worth individuals or board members but also those targets who can be used as entry points for access into systems and other critical assets, including heads of business units and employees. Attackers will build automation into their tools to more efficiently exploit credentials, company data, and sensitive information once credentials are obtained. Security breaches of this nature are more likely to succeed in environments where there is negligence, carelessness and lack of awareness regarding security and social engineering exploits.

Regulatory Pressures Make Red Teaming the Global Gold Standard With Cybersecurity Talent Development

Recognised As A Key Challenge.

Increased pressure from regulators worldwide will push in-house red teaming capabilities to accelerate in 2017 and companies that are not in the cyber business will face a different challenge: recruiting, motivating, and retaining highly technical cyber talent to keep their red teams at the forefront of cybersecurity. This push will likely first occur in financial hubs such as Hong Kong, Singapore, the EU and even the United States.

In 2017, regulatory pressure on financial institutions to conduct red teaming will spark an uptick in the number

```

    ,,)}},c.prototy
    and('[data-toggle="tab"
    idClass("in")):b.removeClass(
    ia-expanded">
    ngth&&h?g.one bsTransitionEnd",f)
    onstructor=
    .data-api",
    each(function
    ){this.opt
    "click.bs.affix.data-api",a.
    tion();c.VERSION="3.3
    rollTop(),f=th
  
```





of organisations across sectors establishing programs and bringing these capabilities in-house. To meet the demand for these skills, there will be a concerted effort to build new marketplace strategies and education programs to strengthen the talent pool. Companies will face pressure to retain talent as forward-thinking competitors will be aggressively seeking out security professionals with this skillset.

Industry First-Movers Embrace Pre-M&A Cybersecurity Due Diligence

The financial services industry will be the early-adopters of making cybersecurity due diligence a critical part of the pre-M&A due diligence process, learning from high profile transactions that were derailed in 2016 following the exposure of cyber vulnerabilities. While 2017 will see one to two additional high profile instances that impact the deal process outcome, only the financial services industry will react accordingly and conduct judicious cyber assessments.

In 2017 we expect the financial services industry to adopt cutting-edge due diligence techniques such as searching the dark web for company data, seeing if employees are using their work email to set up online accounts, reviewing external facing intellectual property (IP) for evidence of persistent malware attacks and talking to employees and former employees about how operations actually work with regard to information security.

Recommendations and Actions

Optimise Your Cybersecurity Posture. Continually Assess and Prioritize Cyber Threats and

Vulnerabilities and Improve Incident Response (IR) Readiness.

Have an IR retainer in place to help minimise response times when an incident does occur.

Shift your mindset from conducting testing of a final version of a product to testing earlier in the development process. Conduct holistic testing, particularly when new technologies are introduced into an organization's ecosystems. Work with an outside provider on designing and implementing red teaming programs and bringing them in house.

Evaluate Insider Risk to Ensure Your Formal Program Is Current

Implement training and awareness around the current tactics and strategies that cyber criminals are using.

Conduct spear-phishing campaigns in your organisation to help educate employees around what they should be looking out for.

Conduct M&A Pre-Deal Cyber Due Diligence Early and Perform Alongside Compliance And Financial Due Diligence

Get your CISOs at the table early in the process.

Provide adequate time to identify and remediate vulnerabilities in the cybersecurity posture and products of the company being acquired.

Assess, Protect and Leverage Intellectual Property and Commercially Valuable Information

Design and implement a strategy to proactively identify trade secrets.

Ensure the most effective protections are in place and maximize the company's ability to respond rapidly and effectively when IP is misappropriated or infringed.

Consider Self-Regulation by Adopting Higher Security Standards in Products and Services Prior to Going to Market, Even if Cost is Prohibitive

It's no longer just the role of government or law enforcement to stop cyber criminals since networked technology can be weaponised and used against individuals and third parties.

It's in a business's best interest to be a good corporate citizen.

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





AN INTERVIEW WITH

MR. DANIEL ELVIN,
REGIONAL DIRECTOR – ASIA PACIFIC, ONCAM

As someone who is highly knowledgeable in both the customer and business development aspects of the rapidly flourishing tech industry, please tell us more about your aspirations with regards to taking Oncam to the next level.

Elvin: Oncam has long been a global company, with presence in a number of countries and regions, including Asia Pacific. With the potential and growth in the markets within APAC, the company saw an opportunity to strengthen its partner base in an effort to broaden the market reach for panoramic video and business intelligence solutions in the region. Oncam is committed to growing our business in burgeoning regions, like Asia Pacific and India.

As an innovative leader in the field of IP video and Technology, how does Oncam plan to establish its identity in the Asia Pacific market?

Elvin: Oncam strives to be the 360-degree camera of choice for our partners and customers by creating security and business intelligence solutions for specific industry sectors. We achieve this by building on our strong relationships with partners, consultants and customers – and that is at the core of our plans to expand our Asia Pacific presence. Nurturing relationships with partners, offering training and support, and working with customers alongside our partners to deliver the best possible solution that utilises our unique video capture technology.

Oncam is reputed for its personalised expertise in various sectors such as retail, gaming and education. Tell us more on how Oncam has assisted the retail sector in enhancing their security systems.

Elvin: Oncam provides a robust, highly reliable and cost-effective method for retailers, such as chain stores with multiple outlets and shopping malls. The image quality offered by Oncam 360-degree technology allows security directors to realize total situational awareness, which is critical to address loss prevention. Coupled with retail analytics software Oncam's technology provides merchandising leaders the best tool for the holistic understanding of customers behavior





“Security in today’s world requires the view and understanding of the “big picture.” Oncam’s 360-degree cameras capture the entire scene – not bits and pieces – offering a full view of any given situation with no blind spots.”

in the store to improve store efficiency.

Oncam’s state of the art cameras comprise of distinguishing features such as minimal maintenance, total situational awareness and even provide the user with the luxury of discreet surveillance thanks to technology that minimizes the number of cameras required in any given space.

What security challenges do you expect to face in the Asian market? How do you plan to meet these challenges?

Elvin: Throughout the world, some of the biggest markets include transportation, retail, healthcare, government and casinos – and the Asia Pacific region is no different. Each one of these markets have their own set of challenges that can be met and addressed by incorporating Oncam video capture and business intelligence technology. As previously mentioned, Oncam is uniquely qualified to offer industry-best 360-degree technology that works with a host of technology offerings that allow customers to custom-build a solution that meets their specific needs. That’s what sets

Oncam apart: the willingness and ability to tailor solutions to fit our customer’s needs and challenges each organisation faces with regard to their business goals and security posture.

In the recent years, the world has unfortunately seen an increase in acts of terrorism carried out in areas with high volumes of human flow such as airports and train stations. How does Oncam plan to address this issue in terms of securing airports and border control zones, for the safety of all commuters?

Elvin: This is a critical component of what Oncam offers. Security in today’s world requires the view and understanding of the “big picture.” Oncam’s 360-degree cameras capture the entire scene – not bits and pieces – offering a full view of any given situation with no blind spots. Coupled with today’s leading video management systems and analytics software, customers within the transportation and government sphere have the ability to monitor high-traffic areas clearly and effectively. The holistic view and understanding of the situation

is key in creating a safer world. Where narrow-field-of-view and PTZ cameras are best used for critical “chokepoints” where traffic is especially heavy and additional coverage is needed, Oncam’s 360-degree cameras gives the understanding of the whole scene at once. This creates multiple ways for a security director to gather critical information for an investigation.

What message do you wish to convey to our readers who are interested in utilising Oncam’s cutting edge technology for the safeguarding of their esteemed establishments?

Elvin: Oncam provides a unique perspective to the market through specialized expertise in retail, transportation, gaming, education, safe city and more. Oncam also has a number of technology partners that allow a seamless integration between our video capture technology and the leading VMS, analytics software, access control and PSIM solutions (to name only a few). This means Oncam has the ability to address our customer’s most critical challenges and develop practical solutions that deliver real impact. *SST*



Honeywell Digital Video Manager

Improve Operator Efficiency and Mitigate Business Risk

Honeywell Digital Video Manager (DVM) releases the power of the latest industry trends and innovations in surveillance and integrated security to deliver broad benefits to the business.

Honeywell DVM supports a multi-server environment with enhanced protection against system hardware failures.

Large system support: Honeywell DVM is based on a flexible, expandable system architecture. A single Database Server supports up to 4000 cameras spread across a number of Camera Servers and solutions can be further expanded by adding additional Database Servers. Multiple systems in one or more locations can be linked together in a federated architecture allowing centralised system monitoring via DVM's Distributed Video Architecture.



Mission-critical sites have the option to deploy high availability solutions with redundant database and camera servers as well as the ability to configure cameras to stream and record video to multiple locations simultaneously. This provides a high degree of fault-tolerance and allows continued use of the system even when a physical storage location has been destroyed by continued use of the secondary location.

Smart Surveillance Software Helps Boost Reliability and Enhance Operator Efficiency with Mobile and Voice Control.

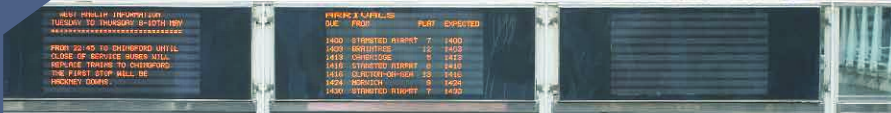
DVM enables organizations to more efficiently manage their security system with enhanced mobile capabilities and voice control, and mitigates business risk via support for current IT platforms.



DVM delivers enhanced system access and usability



SPECIAL PRODUCT FEATURE | HONEYWELL DVM



“DVM has been designed to offer quick, real-time support to operators to improve efficiency and mitigate business risk. It helps operators identify and mitigate the impact of an issue for safety and business continuity — no matter if they are in front of a central workstation or on the opposite side of a campus, connected with a smartphone.”

- Aseem Joshi, Regional General Manager, Honeywell Building Solutions, India.

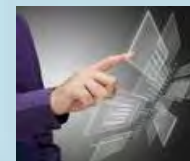
and Honeywell’s focus on User Experience ensures a simple and intuitive user interface designed to improve operator efficiency and reaction time.

Security personnel now can access high-definition, full-frame-rate video on a mobile device, for example, enabling continuous monitoring of live and recorded video from almost any location on site. Operators can also interact with DVM using voice commands to more easily manage multiple video feeds and request near-real-time system updates.

Security operators can export footage from multiple camera feeds in unison to streamline incident response and workflow, and quickly collect and archive forensic data in the event of an incident. Dynamic adapter installation, video analytics, edge recording and backfill, camera feature support, device capability discovery and video wall integration provides higher flexibility to customers to add new custom features.

Along with an improved user experience, DVM promotes IT integration and compliance with support for current Microsoft operating systems and databases, including Windows Server 2012, Windows 10, Internet Explorer 11 and SQL Server 2014. In addition, DVM allows customers to deploy and intelligently group multiple back-up servers to boost system robustness, which helps prevent loss of view and reduces the risk of missing – or mismanaging – critical incidents.

DVM provides a more efficient approach to incident response and investigations with flexible, multi-camera video export, helping to reduce operator workload and ensuring more





productive use of valuable operator time. Features such as the flexible workspace, instant and synchronized playback, motion searching and integrated analytics continue to empower security operators to better manage threats and reduce response time.

“DVM has been designed to offer quick, real-time support to operators to improve efficiency and mitigate business risk. It helps operators identify and mitigate the impact of an issue for safety and business continuity — no matter if they are in front of a central workstation or on the opposite side of a campus, connected with a smartphone.” Aseem Joshi, Regional General Manager, Honeywell Building Solutions, India.

Honeywell Digital Video Manager is a component of Honeywell's Enterprise Buildings Integrator (EBI), an award-winning building management system that unifies all aspects of a security solution, including video surveillance, access control and intrusion detection. EBI also integrates comfort, life safety, energy and other core facility controls providing users a single point of access to the essential information and resources needed to monitor, manage and protect a facility, campus or multi-site operation. As a result, security operators have optimised visibility and intelligence and the ability to deploy their staff and resources more efficiently and effectively.



Additional Key Honeywell Digital Video Manager Features:

- **Edge Recording and Video Backfill:** Ensure reliable collection of video in the event of network failures by recording to the camera's SD Card and then backfilling to the server once communications are restored.
- **Operator Bookmarking:** Allow operators to intelligently tag recorded video for easier search and reference
- **Camera Tamper Detection:** System monitors for blurring, blinding/covering and field of view changes to maintain the integrity of the live and recorded video
- **Advanced video analytics:** Support for video content analysis solutions – beyond simple video motion detection – from multiple vendors to notify operators of potential incidents
- **Image Blocking:** Restricted user access to PTZ cameras during critical event response.
- **Image enhancement features:** Brightness, Noise, Contrast and Sharpness adjustment
- **Voice Control** for camera selection, control and diagnostic reporting
- **User interface optimised for touch-screen monitors**
- **Reducing storage requirements** - Dynamic recording leads to reduction in cost up to 40% by enabling the system to capture critical video under higher frame rates, while collecting less important footage at lower frame rates, trimming storage requirements, reducing network bandwidth requirement and allowing edge recording playback from network video recorders, digital video recorders. It is easy to engineer and leverages the full capability of video encoding devices that support multiple streams.
- **Alarms and Reports** - Alarm monitor for automatic pop-up of alarm. Enables queuing of cameras in alarm monitor in case of multiple alarms. Alarms and event summary with attached video clips for quick verification of alarm. Audio alert in different tones for Low/ High/ Urgent priority alarms. Dashboard for system health status. Provides system reports including comprehensive audit report, system activity report, user activity report, camera configuration report, clip summary report, storage usage report, video analytics event report, point status report and diagnostic framework for logs and information collection and fault finding. *SST*



Dahua Introduces the Smart Thermal Network Camera Series

Dahua Technology, a world-leading manufacturer of video surveillance products headquartered in Hangzhou, China, introduces the smart thermal camera series that provides superior image quality and advanced features for perimeter, electric industry and manufacture security applications. The camera series is designed to find heat sources, offer highly detailed images and is equipped with an extensive feature set.

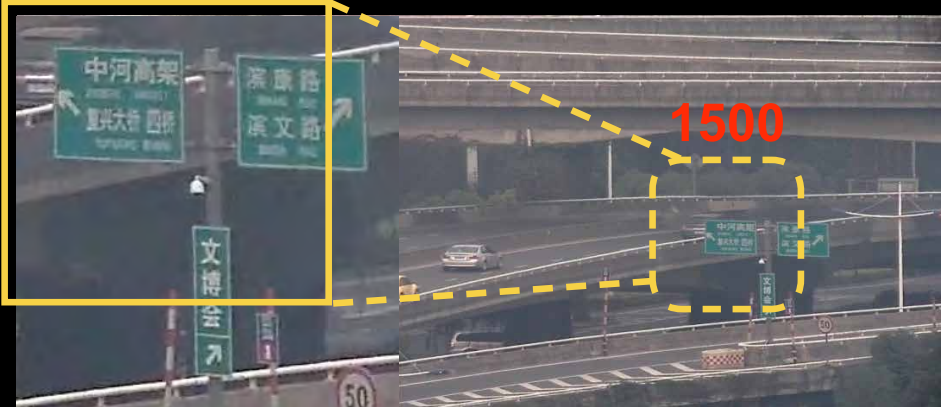
Dahua's new smart thermal network camera family includes thermal hybrid PTZ camera, hybrid speed dome camera, thermal bullet camera and thermal dome camera which all equipped with a variety of smart functions. The smart thermal cameras adopted top-notch sensor even detects tiny differences in temperature. This camera series can achieve higher detection accuracy and functions in complete darkness and adverse weather conditions. The cameras' combined intelligence, efficiency and high performance comprise of smart features such as smart detection, smart analyse, smart perception, smart tracking and smart control.

The smart thermal network cameras can determine the object temperature and the temperature distribution even on small and fast moving objects, with precision. These cameras are excellent for detecting water leaks behind a wall, a person hiding in the bushes at night or even identifying passengers with a fever passing through a checkpoint.

Dahua thermal hybrid network PTZ camera is a professional combination of a visual camera with integrated max 40x optical zoom lens and a thermal camera, perfectly synchronised in pan and tilt movements. The network camera can capture images in full scale without the need to step back or frame the shot. The thermal camera is suitable for both night-vision missions and precise thermographic surveys.



Left: Network camera, Right: Thermal camera



40x Optical Zoom Lens



IVS and Auto-Tracking



Hot Resource Detection and Alarm

The special lens focuses on the infrared light emitted by all of the objects in view and delivers several independent H.264 streams for different quality needs and bandwidth constraints simultaneously.

Dahua also provides software and accessories including smart PSS, NVR and DMSS to work together in order to meet the individual requirements of various industries such as transportation, energy, border and coastal surveillance and other special applications.



DAHUA SMART THERMAL NETWORK CAMERA FAMILY

Thermal Hybrid PTZ Camera PT8320/8620 (-T)



- Thermal resolution:640*512 or 336*256
- Lens optional:35/60/100mm
- Visible camera support 40X optical zoom
- Support IVS
- IP66-rated

Thermal Hybrid Dome Camera SD8320/8620 (-T)



- Thermal resolution:640*512 or 336*256
- Lens optional:25/35/50mm
- Visible camera support 30X optical zoom
- Support IVS
- IP66-rated

Thermal Bullet Camera BF5300/5600 (-T)



- Thermal resolution:640*512 or 336*256
- Lens optional:7/13/19/35mm
- Tri-mode output: IP/HDCVI/Analog
- Support IVS
- IP67-rated

Thermal Dome Camera SD5300/SD5600 (-T)



- Thermal resolution:640*512 or 336*256
- Lens optional: 13/19mm
- Tri-mode output: IP/HDCVI/Analog
- Support IVS
- IP66-rated

For more information, please visit www.dahuasecurity.com

Model: BioStation A2

By: **Suprema Inc.** | www.supremainc.com

Product Specifications:

- Class-leading powerful Quad Core CPU
- World's best matching performance
- Smooth graphics
- Quick response for users
- BioStation A2 carries massive 8GB memory
- Stores up to 500,000 users, 5,000,000 text logs and 50,000 image logs
- Live Finger Detection technology using proprietary optics and algorithm technology
- Distinguishes fake fingers made from various materials
- Secures maximum usability for users
- 5" IPS LCD touch screen provides wide viewing angles and easy operation with special reinforced glass screen for maximum screen visibility
- User-friendly material design inspired by Android
- Hairline pattern on front face for sleek and solid look
- Rose-gold colored rim finish blends in beautifully with any environment
- Extended versatility with built-in 2MP wide-angle camera that captures high resolution face captures through face detection for image logs
- Supports videophone, PoE and built-in WiFi
- RF card options to ensure versatility



Model: S700e Fully Integrated IP Card Reader and Combined Controller

By: **CEM Systems** | www.cemsys.com

Product Specifications:

- Intelligent card reader and combined controller all housed within the same unit, no requirement for an additional intelligent control panel in the system design
- Contactless card presentation with the option to enable Personnel Identification Number (PIN) for two stage authentication
- Soft-touch capacitive keypad for dual authentication of card and associated PIN number
- Context sensitive function keys for selection and navigation
- Integral reading support for 13.56MHz smartcard and 125 kHz proximity technology
- Large reader database for off-line card verification and alarms
- Bright 2.4 inch graphical LCD display which is used to display a number of easy-to-read and simple to comprehend predefined messages
- Four analogue inputs to monitor door or alarm conditions
- Two changeover relay outputs to activate door strike or other equipment
- Weather-proof casing: IP65 rated & IK06 impact rating





Model: KeyWatcher® Touch

By: Morse Watchmans | www.morsewatchmans.com



Product Specifications:

- Contain security and notification upgrades and ease of use improvements that make the key management system even more flexible and useful in fulfilling the safety and security needs of resorts and casinos
- New security features protect the system from cyber breaches via the network
- With the firewall enabled, all incoming traffic is ignored unless it is on the specific ports the system requires for network and server communication
- The data between the KeyWatcher Touch and the KeyWatcher Touch Server can now be encrypted with AES256 technology with a pre-shared key that is definable on a site-by-site basis
- KeyWatcher Touch Server service can now run under a domain user account
- Windows authentication is supported for SQL, while server logins eliminate the need for the IT department to add SQL users to the SQL Server for the purpose of authentication
- The KeyPro™ III software import utility has been revamped to make it easier to use
- Day-to-day user conveniences have been upgraded including the ability to replace keys from TrueTouch™ key tracking software using the SmartKey reader
- All reports in TrueTouch now support being saved/viewed as a PDF, or saved as a CSV file
- A new notification that allows for users to be notified when an overdue key has been returned is also included, as well as notifications for dual and triple user removals/returns

Model: Myris

By: eyeLock | www.eyelock.com

Product Specifications:

- USB powered Iris Identity Authenticator
- Uses patented technology to convert individual iris characteristics to a unique code
- Provides unparalleled security
- Portable
- Lightweight and easy as looking into a mirror
- Can be used to quickly and easily enrol users for EyeLock's access control products or grant users access to corporate domain environments within seconds without username and password
- Administrators can set complex passwords and once myris is linked, they can forget them
- Can be used for enrolment, directory authentication or to secure workstations, high-value transactions, critical databases and information systems
- Hand-held operation
- Simple connection to PC via USB
- Easy iris capture for enrollment or authentication
- Secure communication and encryption (AES 256)





Model: MorphoFACE

By: Safran Identity and Security | www.morpho.com

Product Specifications:

- Smart face capture for ultimate in user experience
- ‘On-the-move’ face capture and identification
- Multi-cameras face capture for reliable 3D video tracking
- Non-intrusive & intuitive, requiring minimal user cooperation
- Robust to users’ behavior and profile
- Anti-spoofing capabilities
- High availability: 99.8%, 24/7
- High image quality and accuracy



The best in key management performance and value.

Our KeyWatcher systems are packed with features and capabilities, expertly engineered to protect, control and track your keys. We invented key management, and we just keep making it better for you.

Visit morsewatchmans.com to learn more



Product door not shown in image. Fingerprint reader optional.



Model: SekuFACE Biometric Face Recognition System

By: Eurotech | www.eurotech.com

Product Specifications:

- Privacy-compliant IP-based recognition system that detects human faces and processes them automatically
- Monitors the transit of people through checkpoints and access passages in restricted areas
- Option for cross controls with identification documents and badge devices
- Creates a biometric map in just 3 seconds
- Stores individuals' biometric tracks and pathways onto internal memory and remote database
- Built-in IR Illuminator makes sekuface suitable to operate under any light condition
- Face images are captured live with no need for triggering
- Average identification rate achieves 95%, providing extreme reliability
- Maximises security in targeted areas by mapping face image into an 86-measures biometric track
- Compliant with privacy regulation
- Intuitive web GUI for easy configuration of operating parameters
- Vision and communication features
- FPM (False Positive Matching) and FNM (False Negative Matching) levels
- Effortless management of white/black lists
- Statistical analysis of detections
- Data provided in CSV and highly optimised formats
- Securely stored in a remote FTP server
- Permits cross-checking between the biometric profiles and personal ID codes for diversified access security levels
- Several passages can be managed contemporarily
- People's pathways across hierarchic gates are traceable
- Biometric maps of individuals are deleted upon exiting restricted area
- Pathway record kept for time span definable by the GUI in accordance with privacy constraints for the installation
- High reliability access control system
- Compatibility with ICAO standard
- Biometric tracking over 86 facial measurements
- Crosscheck with identity document scanning
- Crosscheck with badge devices
- Military and Civilian Installations
- Access control in high-risk areas, e.g. Barracks and Courts
- Access control in residential areas
- Access control in private and public buildings such as hospitals, museums, airports, harbours, manufacturing plants, pharmaceutical and chemical plants, restricted access R&D departments
- Visitor management
- Security and surveillance Systems



Model: BI2002 Human Body Inspection System

By: Nuctech | www.nuctech.com

Product Specifications:

- Detects both metallic and non-metallic threats
- Detects contrabands concealed inside body and artificial limbs beneath clothes and in shoes
- Best proven and extra low dose x-ray transmission imaging technology
- Reduced X-ray radiation with diverse x-ray doses according to person's size and region of interest
- Unmatched imaging performance with advanced medical x-ray generator optimised for body screening
- High resolution detector technology
- Creative system structure design for scanning human body in static status
- Ergonomic
- Friendly user interface
- Full radiation protection design ensuring x-ray leakage from housing covers is close to natural background level
- No extra radiation protection structure, region or measurements required.
- Excellent reliability and maintainability
- Windows system based computer platform with strong networking capabilities
- Possible usage includes customs, airports, rail transportation stations, prisons and rare metal mines.



Model: Compass DA Full Body X-Ray Security Screening System

By: Adani Systems | www.adanisystems.com

Product Specifications:

- Combines two-in-one - integrated access control and effective
- Detects wide range of organic and inorganic objects concealed in bags, under clothing or hidden in the anatomical cavities
- Can be easily integrated into existing entrance infrastructure and most access control systems.
- Suitable uses include VIP facilities, military bases, critical infrastructure sites
- Intergration flexibility
- Radiation safety
- High throughput rate
- COMPASS SV/DV/LT functionality
- Selective scanning of visitors and staff
- Opportunity to hold a suspect inside the booth
- Low percentage of false alerts
- Remote operation
- Bulletproof construction option
- Integrated 2 way communication and internal CCTV option



- Integration with Biometric Access Control and other access control cards
- Door lock system
- Unique function of stealth scan from up-down
- Multiple scan dose settings
- Anti-vandalism glass or metal panels
- Color scheme can be adjusted according to building design





Model: HAC-HFW2401E Water-Proof HDCVI IR-Bullet Camera

By: Dahua Technology | www.dahuasecurity.com



Product Specifications:

- 1/3" 4 MP CMOS
- 25/30 fps at 4 MP, 25/30 fps at 1080p, 25/30/50/60 fps at 720p
- High speed, long distance real-time transmission
- HD and SD dual output
- WDR (120dB), day/night (ICR), AWB, AGC, BLC, 3DNR
- IP67, DC12V



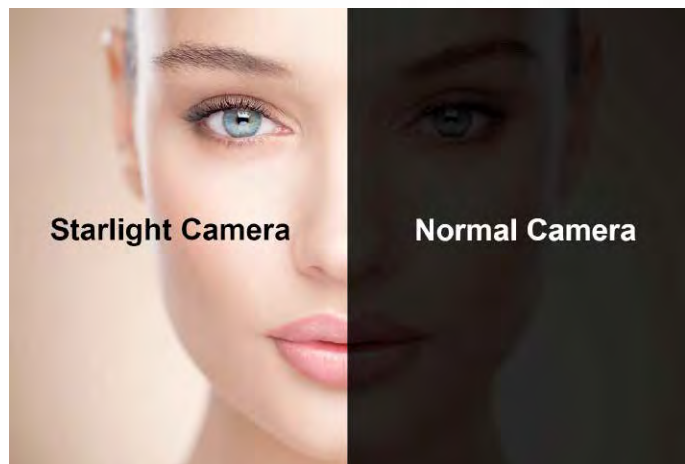
Model: NZ3-T133 3MP Starlight 33x High Speed Dome IP Camera

By: WAMA | www.wamatech.co



Product Specifications:

- Uses Sony CMOS image sensors that incorporate the STARVIS technology
- Back-illuminated pixel technology developed by Sony features sensitivity of 2000mV or more per 1µm².
- High picture quality in visible light and near infrared light regions
- Advancement in CMOS sensor technology for high quality videos even when recorded in very low light environments
- Sony 1/2.8" 2.1MP STARVIS sensor
- H.265 / H.264 / M-JPEG dual streams
- Built-in video analytic functions
- Motorised vari-focal lens
- Micro SD slot for recording
- Enhancements: D-WDR, 3D NR, defogging
- ONVIF (Profile S)
- High speed dome IP camera with 3MP resolutions
- Starlight sensitivity with 33x optical zoom
- Long IR range of 150m with adaptive illumination angle
- Suitable for outdoor and long distance surveillance



Model: Reolink Keen

By: Reolink Digital Technology Co., Ltd | www.reolink.com

Product Specifications:

- World's First Battery-Powered, Wireless Pan-tilt Security Camera
- Battery-powered wireless camera
- Can be used in any indoor space
- Can be mounted to the wall from the ceiling or placed inconspicuously on a shelf
- Sets up in seconds
- Gives 1080p HD view of entire space
- Gives user control of everything right from smartphone via intuitive app
- Comes with a remote motion sensor and night vision capability
- Stays connected with dynamic two-way audio



Do you have products for us?
Good! Email us at sss@tradelinkmedia.com.sg





Model: UV-AHDDX614~UV-AHDDH614 Intrusion Detection Smart Illumination Camera

By: Unique Vision | www.unique-cctv.com

Product Specifications:

- Intrusion Detection AHD Camera with PIR Sensor and White Light and Infrared Combo Led
- 1pcs High Power IR Array Leds, 2pcs White Light Leds, Smart Illumination controlled by PIR motion sensor
- IR leds are on, the white leds are off during the night in the absence of human intrusion producing a black and white image
- White lights turn on when there is human intrusion and the image turns to color
- PIR motion sensor on camera front, below the camera lens
- Motion sensor detects movement of human sized objects when in view of the camera lens.
- Clearer, advanced bright color separation, signal filtering, 3D noise reduction technology
- Higher image resolution
- Better image reductibility
- Longer Transmission with Coaxial transmission common 75-3 cable up to 500 meters
- Zero Delay,Front-end data without coding compression to the back-end, real-time, high fidelity
- Compatible with ordinary D1/960 h and analog peripherals (distributors, matrix, etc.)
- Easy Operation,Support OSD menu design
- Cheap Price and High Quality
- High integration AHD front-end chip prices
- Third party open standards, compatible with AHD from other manufacturers products
- 720P/960P/1080P, Metal Housing, IP66 Waterproof



Security Solutions Today is now on issue!
issuu.com/securitysolutionstoday



Model: E.L.I.T.E.™ Model EL230

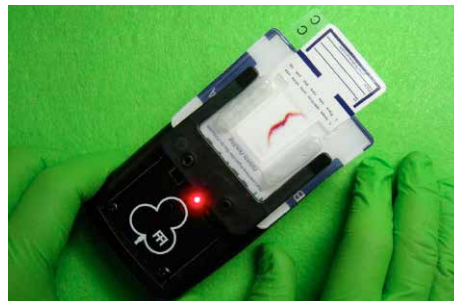
By: APP Systems | www.appsystems.com.sg

Product Specifications:

- Detects all of the peroxide-based explosives (TATP, MEKP, HMTD, etc.) in one simple, self-contained disposable device
- Detects chlorate and bromate mixtures
- Measures suspect particles and vapours
- Detects trace amounts of peroxide-based explosives from roughly 500 nanograms and hydrogen peroxide solutions above roughly 30% concentration without contact with suspect liquid (Concentration is much lower when in contact with the liquid)
- Distinguishes the peroxides from chlorates/bromates by a colour differentiation
- Pen-like design to minimise the likelihood of injury to a user's fingers in case of detonation

Example Scenario 1:

- During a routine search, a bottle with an



unknown fluid is found

- The EL230 tip turns blue when held over the open mouth of the bottle (without touching the liquid)
- This indicates that the liquid is a highly concentrated solution of hydrogen peroxide

Example Scenario 2:

- When taking down a suspected meth lab, officers discover a white powder scattered on a table
- The EL230 tip turns blue after being touched against one of the particles
- This indicates a positive for peroxide-based explosives

Model: HandyRam™ Series

By: Field Forensics | www.fieldforensics.com

Product Specifications:

- Pocket-sized
- Laser-based
- Identifies controlled drugs, explosive materials, pharmaceutical ingredients and wide range of unknown substances
- Point-and-shoot capability
- Quick and safe vial-measurement receptacle
- Smallest system on the market today but powerful and has features that larger systems
- Rapid Laser Spin (RLS™) for safety when analysing sensitive materials
- RLS™ feature rapidly scans laser across the sample surface eliminating intense hot-spots and reducing possible burning of sample materials
- Operates for up to 11 hours with only two AA batteries

- Compatible with PC
- Includes PEAK software to upload spectra or create libraries for downloading to the HandyRam™

Applications:

- Forensics Analysis, including Narcotics
- Bioscience and Biomedical Diagnostics
- Biotoxins Analysis and Identification
- Chemical Warfare Agent Detection
- Pharmaceutical Material Analysis
- Polymer and Chemical Analysis
- Environmental Science
- Explosives Detection
- Petroleum Analysis
- Food and Agriculture





Model: S700e Fully Integrated IP Card Reader and Combined Controller

By: CEM Systems | www.cemsys.com



Product Specifications:

- At 3Gbps IndigoVision achieves twice the data recording rate of our nearest rivals
- There is up to 1.5PB storage in a single NVR, a security industry first
- IndigoVision's NVRs have been designed and injected with Distributed Network Architecture (DNA) to allow for easy expansion of system
- They also contain IndigoVision's innovative SMART guard technology that introduces five layers of security to protect data
- 5 layers include: Cybersecurity, Digital Watermarking, NVR Failover, RAID resilience and Fault Monitoring
- The latest NVR-AS 4000 designs on the Large Enterprise, Enterprise and Compact appliances have fantastic performance and throughput
- The Large Enterprise NVR-AS 4000s can record up to 600 security cameras per NVR
- They have a massive 3Gbps of throughput and up to 1.5PB of storage
- Enterprise NVR-AS 4000 is available in both Windows and Linux OS and can record up to 200 cameras
- It now has doubled the performance of the nearest rival with 2Gbps of throughput and up to 112TB of storage
- The Compact NVR-AS 4000s are perfect for sites with up to 20 cameras and ideal for distributed multi-site recording
- Increased storage options of 1TB, 3TB and 4TB provide more freedom of choice for those wanting a small but powerful appliance
- All NVRs are plug and play ready and come with IndigoVision's flexible system design that allows for mixing and matching to build a customised solution



SOUTHEAST ASIA **building**
SUSTAINABLE ARCHITECTURE • INTERIOR DESIGN • LANDSCAPING

Asia-Pacific's leading source of information for professionals interested in the technique and technology of quality architectural, interior and landscaping design.

bathroom + kitchen today

A regional trade magazine designed to reach a progressive, diverse and dynamic audience of the bathroom, kitchen and ceramic industries.

• S O U T H E A S T • A S I A •
CONSTRUCTION

Features civil and structural projects in the region and all over the world, the latest in construction equipment, materials, technology and industry news.



With a solid network of designers, installers, specifiers and rental specialists in the lighting, audio, and visual solutions industries, LAVA has what it takes to place your brand in the spotlight.

Security Solutions Today

Showcasing products in categories that include access control, CCTV/surveillance systems, integrated security systems, detection and alarm systems, fire extinguishing systems and passive fire protection.

lighting today

A publication that aims to promote lighting's purpose as an integral part of realising a quality built environment, emphasising the importance of the role of professional lighting designers in the total design process.



Scan to visit our website

TRADE LINK MEDIA PTE LTD

101 Lorong 23 Geylang #06-04 Prosper House Singapore 388399 T: (65) 6842 2580 F: (65) 6745 9517
W: www.tradelinkmedia.com.sg E: info@tradelinkmedia.com.sg



A GLIMPSE INTO THE NEXT FRONTIER OF AIRPORT SECURITY

The year is 2022. You arrive at the airport after an exhausting flight. The last thing you desire is another four hours of going through strenuous airport checks. The thought however only lingers on your mind briefly as you are reminded that times have changed since you last travelled and we are now living in a brave new world where technology advances by the minute. You step into the security kiosk where you answer a series of questions addressed to you by a friendly face on a screen that greets you much like a friend would. The cheerful disposition of the avatar is somewhat comforting as opposed to the intimidating airport security staff of yesteryears.

If you believed this to be a scene from *Battlestar Galactica* or a science fiction movie, you are mistaken as the scenario above could be coming to airports near you within the next few years.

Welcome to the wondrous world of robotic detection!

Meet AVATAR, who is also known as Automated Virtual Agent for Truth Assessment in Real Time. This brainchild of San Diego State University management information systems Professor Aaron Elkins and his team, is the epitome of science fiction meets real life. Films like *Minority Report* have espoused ideas on the implementation of robotics in law enforcement and security for years and it is about time that life imitates art. AVATAR understands the subtleties in human behaviour and uses this to detect suspicious signals in travellers. While questions on objectivity and

accuracy will inevitably be raised about this technology, its creators believe AVATAR can eventually assist agents in screening for potential terrorists and other criminals.

Currently being tested at the Canadian Border Services Agency, AVATAR was created in 2012 and since then has been constantly developed with additional sensors, the ability to analyse more data and even speak multiple languages. The friendly face of AVATAR greets travellers politely as it enquires about their purpose for travel. Throughout the duration of the interview, the machine detects changes in the eyes, voice, gestures and posture to determine potential risk. Questions include 'Do you have produce in your luggage?' and 'Are you carrying any weapons with you?'. Eye-detection software and motion and pressure sensors will be used to differentiate untruthful responses from honest answers.

The technology behind AVATAR has been developed continuously to include a plethora of biometrics such as iris scanners, fingerprints and facial recognition along with cameras, microphones and eye trackers to measure the pupil size of the responding travellers. AVATAR's creators are confident in its ability to greatly reduce the time taken to go through security checks hence catering to the needs of travellers while efficiently screening for dangerous individuals.

AVATAR could possibly be the quintessential security agent of the future. To decipher the complexities of human behaviour, it will ask a standard set of legally

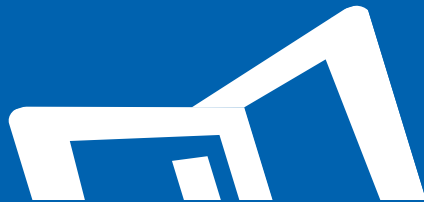
binding questions, observe behavioural anomalies and provide emotional information for border officials to act upon.

AVATAR creators are currently in discussions with government bodies and private companies about incorporating it into a myriad of industries such as law enforcement, border crossing and even human resources. While reactions from the industry have been mixed, European border and security officials have expressed positive views about AVATAR.

Perhaps what sets AVATAR apart from similar technology available today is its evolutionary human features such as its intelligence and personality which can be altered to be either more pleasant or aggressive depending on the situation. All in all, it is truly fascinating how technology inspired profoundly by human nature may soon become a tool that is vital to the protection of humans. Welcome to the future of security technology!

SST





Launching Soon.



Will be available on





Milestone America

12th Milestone Integration Platform Symposium (MIPS)
W Marriott San Antonio Hill Country Resort & Spa
San Antonio, Texas, 13- 16 February 2017

Milestone America's Partner Event Promotes Open Platform Community Initiatives

Technology innovations and business performance are recognized, latest integrations exhibited, future visions defined.

Background created by Harryants - Freepik.com

Milestone Systems, the open platform company in IP video management software (VMS), held its 12th Milestone Integration Platform Symposium (MIPS) in February 2017 in San Antonio, Texas. The prestigious event attracted over 500 attendees. The event served as an open platform community function engaging hundreds of channel and alliance partners, customers, media people, Milestone experts and management. Milestone business activities and product innovations were shared with over 60 solution partners showcasing their integrated offerings and services.

This year's event theme 'Together We Make the World See the Future' reflected a newly clarified company purpose emphasising community focus for the combined solution power of the Milestone open platform and its partners. Event goers were also treated to a futuristic feature when the CEO and President Lars Thinggaard appeared virtually as the audience put on VR headsets immersing them in the picturesque landmarks of Denmark that served to inspire them with a peek into the future.

Chief Sales & Marketing Officer at Milestone Mr. Kenneth Hune Petersen expressed that the co-creation of value is unique to Milestone's open platform community.

Petersen presented the three pillars of the new Milestone community initiatives that begun in 2016 with more being planned in the future. The Milestone Marketplace will start with new developments for the Milestone Store. The Solution Finder is also evolving into the Solution Portal and the Developers Forum is expanding.

The afternoon was devoted to touring the Community Innovation Lab where Milestone Solution and Technology Partners demonstrated the latest innovations in the industry. After more VR fun watching introductions for the exhibit sections, the groups led by Milestone managers viewed feedback walls in each category throughout the hall which truly proved to be a journey inspiring brainstorming.

On the second day, Milestone VP America's Tim Palmquist gave his keynote speech that elaborated on his topic from the previous year's MIPS event - End to End is a Dead End; The Road to the Future is Open. He questioned if the glory days are indeed over for the surveillance market



TRADE CONNECTION

Home page announcements for added business opportunities.
Register now, contact:

Tel: (65) 6842 2580 Fax: (65) 6842 2581 / 6745 9517
E-mail : info@tradelinkmedia.com.sg



- RFID Electronic Key Management System
- Guard Tour System
- Vehicle Access Control System
- Contactless Smartcard System
- Biometrics Verification System
- Multi - Technology Card Reader



WE THINK SECURITY

Blk 28 Kallang Place #06-12/14
Singapore 339158
Tel: (65) 6741 5200
Fax: (65) 6741 6200
RCB No: 19880111W
Email: info@coselec.com.sg
www.coselec.com.sg

This space could be yours for

US\$				Color
1x	3x	6x	9x	12x
500	440	380	320	260

S\$				Color
1x	3x	6x	9x	12x
775	682	589	496	403



SOUTHEAST ASIA CONSTRUCTION

Features civil and structural projects in the region and all over the world, the latest in construction equipment, materials, technology and industry news.



Showcasing products in categories that include access control, CCTV/surveillance systems, integrated security systems, detection and alarm systems, fire extinguishing systems and passive fire protection.



With a solid network of designers, installers, specifiers and rental specialists in the lighting, audio, and visual solutions industries, LAVA has what it takes to place your brand in the spotlight.

SOUTHEAST ASIA building

Asia-Pacific's leading source of information for professionals interested in the technique and technology of quality architectural, interior and landscaping design.



A regional trade magazine designed to reach a progressive, diverse and dynamic audience of the bathroom, kitchen and ceramic industries.



A publication that aims to promote lighting's purpose as an integral part of realising a quality built environment, emphasising the importance of the role of professional lighting designers in the total design process.



Scan to visit our website

TRADE LINK MEDIA PTE LTD

101 Lorong 23 Geylang #06-04 Prosper House Singapore 388399 T: (65) 6842 2580 F: (65) 6745 9517
W: www.tradelinkmedia.com.sg E: info@tradelinkmedia.com.sg



and recommended a more realistic look at today's maturing IP market, which is experiencing a natural consolidation and product price wars amongst other competitive factors.

"It's no longer fast growth and 'easy money' like the early phases in a technology lifecycle, so new business models must be developed to encompass the next market disruptions that will come. Milestone's open platform community offers a framework to succeed – together – leveraging each other's innovations,"

said Palmquist.



Mike Sherwood, Milestone Director of Technical Operations, Americas, spoke on "The Engine of Innovation" stating that the best companies understand that it takes more than just one company alone to really succeed.

DELL VP Ron Pugh also took to the stage to talk about the digitisation of everything in modern life of today and how the Internet of Things (IoT) can unlock the potential of the unconnected by bridging IT and Operational Technology (OT). Milestone Partner NMS presented the breakthrough SpotterRF compact radar surveillance integration with XProtect VMS that gives aerial and ground views for perimeter protection.



Phoenix Sky Harbor International Airport shared knowledge gained from growing their systems on the Milestone open platform, including RFID readers that manage taxi traffic, a Unified Command Vehicle with six cameras and a Mobile Camera Trailer with solar power. Jamie Ritchie said that the airport is building for capacity with a focus on multi-purpose solutions. He expressed his excitement about the open platform, which would unlock many possibilities in the unknown future that lays ahead.

Breakout sessions in the afternoon had parallel Technology and Business Tracks covering such topics as developments in the XProtect platform, advances in technology evolving the business model and cloud solutions that work with currently available technology.

Advisory Board Gives Direction

In early 2016 Milestone created a new global Advisory Board with the first of several groups focused on advanced products. Others were formed to focus on the Business Ready portfolio, overall Business Strategy and the Developers Forum. Each group has members representing the spectrum of stakeholder roles such as end users, partners and Milestone staff. Monthly questionnaires have been sent along with the annual global partner survey and quarterly meetings have been held.

Milestone CTO Bjorn Eilertsen stated that the feedback from the community is essential to setting the direction in the organisation's product development. He added that there is a big opportunity for high-performing, platform-centric products with strong connectivity. According to Mr. Eilertsen, the shift from product to platform thinking applies to both software and hardware offerings and is initially addressed in the XProtect 2017 R1 release.





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

Lighting Audio Visual Asia

SINCE 2013

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

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: _____



Recognizing Achievements and Innovation

The awards were presented on the final evening of the event to the following organisations:

- Anixter: Distribution Partner of the Year (Americas)
- Wesco: Distribution Partner of the Year (USA)
- Southwest Microwave: Solution Partner of the Year
- Quantum Corporation: Technology Partner of the Year
- Differential Networks/ Spotter RF/ NMS: MIP Integration of the Year
- Convergent Technologies (Seattle, WA): Installation of the Year
- Brady Integrated Security: Education Partner of the Year
- Convergent Technologies (Houston, TX): Retail Partner of the Year
- Tactical Micro/Benchmark Electronics: Transportation Partner of the Year
- Tech Systems: Healthcare Partner of the Year
- Stone Security: City Surveillance Partner of the Year
- App-Techs Corporation: Regional Partner of the Year AND Government Partner of the Year
- Prosecur Technologia (Argentina): Regional Partner of the Year
- Presidio: National Partner of the Year
- Bosch: Camera Partner of the Year, Americas
- Axis Communications: Supported Camera #6,000 in Milestone Device Pack release 9.0

The first-ever Milestone Community Kickstarter Contest Winner of awards valued at \$50,000 was Parking Spotter.

Milestone Systems will be hosting MIPS Community events in Macao at end of February and in early May in Dubai. Other Milestone events will also be held regionally throughout the year.

*For more information, please visit: www.milestonesys.com **ESST***

ADVERTISERS' INDEX

COMNET EUROPE	5	MICROENGINE TECHNOLOGY	7
CPSE 2017	17	MORSE WATCHMANS	81
DELTA SCIENTIFIC	1	ROBERT BOSCH	3
GIGA-TMS	33	SAFETY & SECURITY ASIA 2017	IBC
IFSEC INT'L SHOW 2017	OBC	SECUTECH THAILAND 2017	15
IFSEC PHILIPPINES 2017	13	TRADE CONNECTION	93
IFSEC SOUTHEAST ASIA 2017	11	ZHEJIANG DAHUA	IFC
INTERPOL WORLD 2017	9		



SAFETY & SECURITY ASIA 2017 SINGAPORE

in conjunction with



Security Industry Conference 2017

www.sic.sg

THE 16TH INTERNATIONAL SAFETY & SECURITY TECHNOLOGY & EQUIPMENT EXHIBITION

4 - 6 OCTOBER 2017 HALLS B & C MARINA BAY SANDS SINGAPORE

Enhance your productivity through smart security solutions!

Safety & Security Asia 2017 is the quality sourcing platform for excellent commercial security solutions through an extensive array of technologies, innovations and related services in the safety and security arena. It is the most established event in the ASEAN region, as well as the longest running trade show which places focus on providing informative and strategic processes and issues related to the safety and security market of Southeast Asia.

Don't miss out on this opportunity to connect with key members of the industry through this exciting exhibition held in conjunction with the Security Industry Conference 2017!

For the latest updates, visit www.safetysecurityasia.com.sg

Book your premium location today!
ssa@cems.com.sg • (65) 6278 8666

Event Projections*



*Combined statistics from Architecture & Building Services 2017

Organised By



Host



Supporting Organisations



SIC 2017 Organiser



Event Highlight



Concurrent Events





IFSEC International

SECURING PEOPLE, PROPERTY & ASSETS

20-22 JUNE 2017 EXCEL LONDON UK



Over 10,000 security products to test & trial

- Find your perfect solution from over 600 leading security suppliers
- Pre-book 1-2-1 meetings with the suppliers you want to work with
- Discover future trends with free education seminars & discussion panels
- Grow your network with over 27,000 other security professionals
- Get discounted air travel & accommodation exclusively for IFSEC visitors

REGISTER TO GET YOUR **FREE** BADGE TODAY AT IFSEC.EVENTS

Supported by:



Your badge also gives you entry to:

