Security Solutions Today

September / October 2019



HOMELAND AND BORDER SECURITY

Cover Story

The Advent of 'Border Automation 2.0'

Inside Look

Is 5G The Future Of Intruder Alarm Systems?

In Focus

Cloud-Native Security Unable To Provide Sufficient Coverage

Scan this to download the latest issue from our website

More Light, More Pixels, More Details

4MP Starlight+ provides more reliable monitoring experience



- 1/1.8’’ ultra-large 4MP sensor offers bright images with abundant details for highly reliable monitoring.
- Clear detail information such as human face enables higher probability and better accuracy for AI enabled analytics.
- Longer period with color view gathers more valid human, vehicle, and event evidence.
- 4MP Starlight+ flagship performance and high cost-efficiency with wider portfolio including PTZ, IP and HDCVI cameras.
- Built for critical areas and low light environments such as city streets, parking lots, airports and stations.

Recommended Models



SD8A440WA-HNF

4MP 40x Starlight+ IR PTZ AI Network Camera



IPC-HFW5442E-ZE

4MP Starlight+ AI Network Camera



IPC-HDBW5442R-ASE

4MP Starlight+ AI Network Camera



HAC-HDW2402T-A

4MP Starlight+ HDCVI Camera

ISO 9001:2000

DAHUA TECHNOLOGY SINGAPORE PTE. LTD.
Add: 62 Ubl Road 1 #06 -15 Oxley Biz Hub 2 Singapore 408734
Tel: + 65 6538 0952
Email: sales.sg@dahuatech.com
Facebook: @DahuaTechnologySpore

Safety & Security Asia 2019

The 18TH International Safety & Security Technology & Equipment Exhibition

1 - 3 October 2019

Halls B & C, Marina Bay Sands, Singapore

10,000sqm gross exhibition space • **250 exhibitors** from 20 countries • **9,000 trade professionals** from 40 countries

*Combined statistics across Architecture & Building Services 2019

Be a part of **Safety & Security Asia 2019** - the quality sourcing platform for excellent commercial security solutions. Showcase your latest technologies, innovations and related services in the safety and security arena in the most established and longest-running commercial security tradeshow in ASEAN!



JOIN SSA 2019 TODAY AND

Expand your business network and explore new opportunities
Stay updated on industry trends and developments
Maximise your marketing & publicity efforts

For booth enquiries, contact:
SSA@cems.com.sg or call
(65) 6278 8666
www.safetysecurityasia.com.sg

A Part Of
Architecture & Building Services 2019
Providing Solutions for Smart Nation Building

Organised By CEMS
Conference & Exhibition Management Services Pte. Ltd.

1 Maritime Square #09-43, HarbourFront Centre, Singapore 099253
info@cems.com.sg • (65) 6278 8666

IN THIS ISSUE



6 CALENDAR OF EVENTS

10 EDITOR'S NOTE

12 IN THE NEWS
- Updates From Asia and Beyond

29 COVER STORY
- Homeland Security: Real-Time Analytics in Flagging Risks
- Upgrading of Airports: An Analog System To A Scalable IP Security Surveillance Solution
- The Advent of 'Border Automation 2.0'
- Smart Borders: Increasing Security Without Sacrificing Mobility

40 CASE STUDY
- Safety in Sight: Video Surveillance Protects Cleveland

43 INSIDE LOOK
- Intelligent Video: Ensuring Substation Physical Security
- The Future of Warehouse Security and Efficiency
- Five Things You Didn't Know About Video Surveillance Data Storage
- Is 5G The Future Of Intruder Alarm Systems?
- Video Surveillance Storage: How Much Is Enough?
- Top 3 Cloud Security Trends For 2019
- How To Secure Cloud Apps: The Ultimate Guide
- Tailored And Secure IP Video Solution
- What is Zero Trust Security? And Why Should You Care
- Intrusion Market Trends: Where Do We Go From Here?

64 SECURITY FEATURES
- Dahua Technology Provides New Solution for Thefts from Boats at Yarmouth Harbour
- Senstar LM100 Hybrid Perimeter Intrusion Detection And Intelligent Lighting System
- Siemens Launches Speech-Based Alarms For Faster Evacuation
- Building Smart Autonomous Vehicles with Lidar Technology
- Netamo Unveils Its Smart Video Doorbell

71 IN FOCUS
- Homeland Security Market to Reach $418 Billion, Globally, by 2022
- Report Reveals Cloud-Native Security Are Rarely Robust And Unified Enough To Provide Sufficient Coverage
- Akamai Threat Research: Phishing and Credential Stuffing Attacks Remain Top Threat to Financial Services Organizations and Customers
- Thales Global Threat Report Reveals Digital Transformation Era Is Putting Organizations' Sensitive Data at Risk
- Gartner Says Security and Risk Management Leaders Must Leverage the Automation Continuum to Create New Value for Their Organizations
- Serious Zoom Security Flaw Could Let Websites Hijack Mac Cameras

COVER STORY 29
- How Digital Technology Is Changing Border Security Operations

You asked for it; **DELTA** made it.



The lighter weight DC-operated, M30 certified Delta DSC1500 portable beam barricade is now available. With a clear opening of 16 feet (4.8 m), the DSC1500 easily and temporarily secures locations where roads need closing down to one or two lanes, deters thefts from parking lots and protects anywhere a beam barricade is needed for short-term security.

Learn more about the DSC1500 and discover all of the security solutions offered by Delta at **www.deltascientific.com**.





For holding events, keep pedestrians and staff safe with Delta's full line of portable barricades and bollards. See them at www.deltascientific.com.

DELTA

Visit **www.deltascientific.com** for details and specifications.
GSA 47QSWA18D003B ▲ **1-661-575-1100** ▲ **info@deltascientific.com**

CONTACT

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

EDITOR
Esther Quek
(sst@tradelinkmedia.com.sg)

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

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

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

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

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

PLATINUM PARTNER
Security Solutions Today

alhua TECHNOLOGY



Images/Vectors Credit: Freepik.com / Unsplash.com / Pixabay.com
Designed by Fawzeeah Yamin

SECURITY SOLUTIONS TODAY
is published bi-monthly by
Trade Link Media Pte Ltd (Co. Reg. No.: 199204277K)
101 Lorong 23, Geylang,
#06-04, Prosper House, Singapore 388399
Tel: +65 6842 2580 Fax: +65 6842 2581
MCI (P) 084/05/2019 | ISSN 2345-7104 (Print)

Printed in Singapore by
Refine Printing Pte Ltd (L011/06/2019)

ANNUAL SUBSCRIPTION:

Surface Mail:

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

Airmail:

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

ADVERTISING SALES OFFICES

Head Office:
Trade Link Media Pte Ltd *(Co. Reg. No: 199204277K)*
101 Lorong 23, Geylang, #06-04, Prosper House,
Singapore 388399
Tel: +65 6842 2580 Fax: +65 6842 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

ISSN 2345-7104

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.

MicroEngine®

Integrated Security Systems

The Trusted Brand in Security Solutions

NO CLOUD
NO SUBSCRIPTION

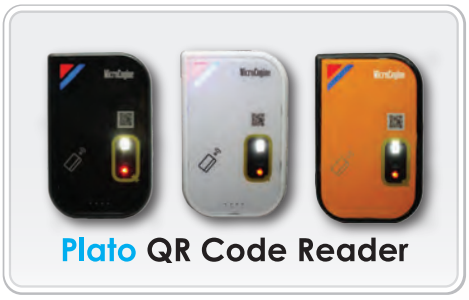
OnPremQR™

Mobile Identification System



- Innovative QR Code based security system
- On Premise mode, no Cloud subscription
- Better option for Non Cloud-Ready Offices
- Clone detection with Dynamic QR Code
- Higher security using AES128 Encryption
- Works with our Integrated Security System





Plato QR Code Reader

Available on the iPhone App Store

ANDROID APP ON Google play



1300-88-3925 or enquiry@microengine.net

www.microengine.net

DESIGNED BY MALAYSIAN
MADE IN MALAYSIA

REG No. 749921389

COMING SOON...

SEPTEMBER
GSX 2019

Date: 8 - 12 September 2019
Venue: Mccormick Place, Chicago, IL
Telephone: +1.888.887.8072, +1 972.349.7452
Website: www.gsx.org
Email: asis@asisonline.org

SEPTEMBER
WOSAS 2019

Date: 26 - 29 September 2019
Venue: World Trade Center Metro Manila, Philippines
Telephone: +632 656 9239
Website: www.wosas.ph
Email: inquire@worldbexevents.com

OCTOBER
Safety & Security Asia 2019

Date: 1 - 3 October 2019
Venue: Marina Bay Sands, Singapore
Telephone: +65 6278 8666
Website: www.safetysecurityasia.com.sg
Email: SSA@cems.com.sg

OCTOBER
Secutech Thailand 2019

Date: 28 - 31 October 2019
Venue: Bangkok, Thailand
Telephone: +886 2 8729 1099 ext. 215
Website: www.secutechthailand.com
Email: jason.cheng@newera.messefrankfurt.com

MAY
IFSEC International 2020

Date: 19 - 21 May 2020
Venue: ExCeL, London, UK
Telephone: +65 6780 4594
Website: www.ifsec.events/international/
Email: ifseccustomerservice@ubm.com

JUNE
IFSEC SEA 2020

Date: 23 - 25 Jun 2020
Venue: Malaysia International Trade and Exhibition Centre, Kuala Lumpur, Malaysia
Telephone: +60 3-9771 2688
Website: www.ifsec.events/kl/
Email: ifseccustomerservice@ubm.com

JULY
IFSEC Philippines 2020

Date: 22 - 24 July 2020
Venue: SMX Convention Center, Pasay City, Metro Manila, Philippines
Telephone: +63 2 581 1918
Website: www.ifsec.events/philippines/
Email: ifseccustomerservice@ubm.com



H5SL Camera Line

Value and Versatility, Combined

The H5SL camera features wide and long-range lens variants that are available in a variety of resolutions for clear and detailed imaging. It is one of our easiest-to-install cameras, providing you with a simple, flexible and cost-effective security solution.



Multiple Lens Options

Choose from various lens types, including a new long-range lens that allows you to see with more clarity at farther distances.

Audio Capabilities

Incorporate audio and configure input/output actions and alarms so that you can respond to events faster.

Ease of Installation

Simple and intuitive to install, with a modular design that easily snaps into the base of your choice, helping you to get up and running in minutes.

Patented Bandwidth Saving Technology

Our HDSM SmartCodec™ technology helps you save on both storage and network bandwidth, helping keep internet connectivity costs down.

avigilon.com/h5sl | asksales@avigilon.com

Product features and functionalities may not yet be available and, if and when available, may not be as depicted. Images have been simulated for illustrative purposes.
© 2019, Avigilon Corporation. All rights reserved. AVIGILON, the AVIGILON logo and HDSM SmartCodec are trademarks of Avigilon Corporation.

EDITOR'S NOTE

Dear esteemed reader,

With the recent spate of terror threats and civil unrest, countries have started strengthening their security at the borders as well as internally.

Conversations on the use of technology to create Smarter Borders have been in swing. Dan Newman, Lead Partner for Cloud Engineering, Deloitte Asia Pacific stresses the need for intelligent borders yet not sacrificing the mobility of it.

In this issue, we look at the advent of the second wave of border automation where risk assessment is championed to be the number one priority. Similarly, homeland security too underscores the need for real-time analytics especially in the work of intelligence.

This issue also features a case study of Cleveland, Ohio which sheds light on the importance of video surveillance in not only preventing crime but also enhancing citizen and infrastructure security throughout the city.

As much as the physical security of the country is important, cybersecurity needs to be strengthened as well. It is troubling to note that reports have revealed that cloud security rarely provide sufficient coverage. That is about to change, as Steve Cohen, Security Services Manager at Synopsys, divulges the ultimate guide on how to secure our cloud.

Happy reading!

Esther Quek

Editor

IFSEC INTERNATIONAL

informa markets



SAVE THE DATE

IFSEC International returns

19-21 May 2020, ExCeL London

Co-located with:

FIREX INTERNATIONAL

SAFETY & HEALTH EXPO

FACILITIES SHOW

Plus:

CTX COUNTER TERROR EXPO 19-21 May 2020 ExCeL London

FORENSICS EUROPE EXPO 19-21 May 2020 ExCeL London

AMBITION THE EPRR EXPO 19-21 May 2020 ExCeL London

AMAG Technology Expands Visitor Management Offering With New Symmetry™ GUEST Kiosks

AMAG Technology introduces its Symmetry™ GUEST visitor management family of interactive touch screen kiosks.

Symmetry GUEST improves the visitor experience by automating all processes associated with the lifecycle of a visitor, streamlining the journey through the reception area, enforcing compliance and reducing operating costs. Eliminate paper logbooks and create an audit trail to properly manage visitors. Kiosk setup is fast and easy as the software and hardware come pre-installed.

"End users will find Symmetry GUEST Kiosks improve visitor traffic flow and are a sleek and innovative addition to their lobbies, improving first impressions while mitigating risk," said AMAG Technology, Sr. Product Manager, Jim Murray.

The Symmetry GUEST Kiosks come in three main designs (Countertop, Slim Wall Mount and Freestanding) and two colours (white or black) with custom branding options to best meet your visitor check-in requirements and lobby décor. Countertop style kiosks provide options for either unfixed (portable) or fixed (secure) mounting to a receptionist desk



or check-in counter for easy access. Slim Wall Mount kiosks mount flush to the wall or glass and are perfect for small lobbies or large, such as busy areas where multiple units are needed to efficiently check-in a high volume of visitors. Freestanding kiosks come with or without cabinet and printer.

Custom branding options are available for all Symmetry GUEST Kiosks enabling organizations to place their visitor check-in messaging and logo on the kiosk for increased visitor engagement. SST

Avigilon Adds High Resolution Thermal Camera for Enhanced Perimeter Security

Avigilon Corporation announced that it will preview its upcoming high-resolution H4 Thermal camera at the International Fire and Security Exhibition and Conference (IFSEC 2019).

The new Avigilon H4 Thermal camera models will combine patented Avigilon technology with heat-sensing capabilities to improve perimeter security in areas with poor visibility, difficult lighting conditions and absolute darkness. The high-resolution H4 Thermal camera will enable users to see more accurately from longer distances, empowering customers with the information they need and helping ensure important details do not go unnoticed.





"We are introducing the high-resolution H4 Thermal camera to bring our customers longer-range detection in locations where environmental factors and lighting conditions are challenging," said Sergio Parise, senior vice president, Product Development at Avigilon. "With the ability to recognize threats with greater accuracy at longer distances under these conditions, this camera will provide an excellent video security solution for sites requiring perimeter protection."

The H4 Thermal camera is expected to launch globally in the third quarter of this year. SST

Part of the
ASEAN Super 8 Series

IFSEC SOUTHEAST ASIA

SECURITY • FIRE • SAFETY

23 - 25 JUNE 2020

MALAYSIA INTERNATIONAL TRADE AND EXHIBITION CENTRE (MITEC), KL



SECURITY IS CRITICAL
IFSEC IS ESSENTIAL

Organised By
informa markets | UBM

WWW.IFSECSEA.COM

@IFSECSEA #IFSECSEA IFSEC Southeast Asia

Surveillance Simplified With BCDVideo's Hyperconverged Solution

BCDVideo is a leading firm in enterprise-quality, purpose-built IP video storage solutions, and Scale Computing. It also a market leader in edge computing and hyperconverged solutions. BCDVideo recently announced, after a year of development, the certification of its new Hyperconverged Infrastructure for Video Surveillance (HCI-VS). It is underpinned by Scale's HC3 software, BCD218-HCI Series, built on a Dell OEM technology foundation, offers modularity and ease-of-use without sacrificing performance and quality.

Initial tests of the solution, configured with Genetec's Security Centre software, ran at throughput of 1800Mbps with ten video archiver virtual machines (VMs). BCDVideo expects final testing in the 2200-2400Mbps range. Its new Hyperconverged Infrastructure for Video Surveillance (HCI-VS) Series greatly simplifies the deployment, management, and maintenance of its infrastructure, saving the security integrator training costs, and most importantly, eliminating system downtime. The HCI-VS system installs at the project site within an hour and is a fully integrated cluster-wide resource. Deploying new Virtual Machines (VMs) can be achieved in minutes and everything is managed through a very easy-to-use web interface. The native high availability built into this all-in-one solution utilizes automation and self-healing to eliminate the complexities around deployment and ongoing management.

Said Jeff Ready, CEO and co-founder, Scale Computing. "The HCI-VS system, powered by Scale Computing combines the HC3 self-healing automation with BCDVideo's leading technology, giving customers a solution built to meet industry wide surveillance requirements while also simplifying the management and maintenance of their infrastructure". SST

SkyBiometry Updates Cloud-Based Face Detection and Recognition API with New Face Algorithm

SkyBiometry, a subsidiary of Neurotechnology, today announced the release of the new version of its face detection and recognition algorithm. Significant enhancements make the algorithm much more accurate and allow for a wider range of facial attributes in the detection process. The latest face detection algorithm locates many more faces in varied and difficult conditions and can detect multiple head rotation angles up to, and including, a full profile. Compared to the previous version, face recognition accuracy is five times higher when set at a low False Acceptance Rate. Other face processing algorithms within the API have also been updated, including more accurate facial-feature points detection, better face image quality estimation and improved face properties and emotion classifiers.

The new features made available in the latest version of the SkyBiometry facial algorithm were added and augmented based on customer feedback. Previous versions of the algorithm were able to determine such attributes as gender, age, smile (or not), glasses, dark glasses, lips (parted/sealed), eyes (open/closed), emotions (neutral, angry, disgusted, scared, happy, sad, surprised), roll, yaw, and facial feature points. Additions to the SkyBiometry algorithm can now establish whether a person is wearing a hat, has a beard or a moustache and determine race/ethnicity. Detected attributes may be used in a wide range of scenarios, from entertainment applications to advanced security and image moderation.

The latest facial recognition algorithms achieved high scores in NIST FRVT (2018) evaluations. SkyBiometry's face identification algorithm ranked among the six most accurate algorithms (out of 40 different vendors) in the largest test, a population of 12 million subjects, and ranked 3rd (out of 40) when face photos were taken up to 18 years after the initial enrolment photo. Another ongoing FRVT evaluation classifies the face verification algorithm to be ranked among the 15 most accurate algorithms (out of 82 different vendors) in the "wild" test, identifying faces culled from various real-world sources.

The SkyBiometry API can be used for face detection, recognition, grouping and attributes determination. It simplifies the process of identifying and cataloguing images for photographers and others who work with large photo databases. For example, it can be used to build a comprehensive system that searches through image databases to identify individuals in photos, eliminating a great deal of manual effort.

The API can also be applied in developing time and attendance software, using facial identification to speed up and automate the time entry process and ensure the accuracy of individuals who are clocking in and clocking out. It can be used as a simple, fast and secure form of identification for user authentication by face. And the SkyBiometry API can also be used in marketing and entertainment applications, for building interactive advertisements or mobile applications or to moderate pictures in social media and dating sites. SST

IFSEC PHILIPPINES

SECURITY • FIRE • SAFETY

22 – 24 JULY 2020

SMX CONVENTION CENTER
PASAY CITY, METRO MANILA



THE LEADING **SECURITY, FIRE** AND **SAFETY** EVENT IN PHILIPPINES

Organised By
informa markets | UBM

WWW.IFSECPHILIPPINES.COM

@IFSECPH #IFSECPHILIPPINES IFSECPHILIPPINES

Counter-terrorist Delta Barrier Stops Intruder at Naval Air Station Corpus Christi

The Delta MP5000 portable barrier from Delta Scientific, stopped a stolen Ford Edge crossover SUV at the North Gate of the Naval Air Station – Corpus Christi. The trespasser had driven across the base to escape but crashed into the Delta unit and erupted into flames. The driver was shot and killed.

Delta's totally self-contained MP5000 mobile deployable vehicle crash barriers carry a K8 rating (M40 ASTM rating), stopping 6400 kg vehicles traveling 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.



Delta MP5000 had been successful in preventing such security intrusions before. In 2018, six of the Associated Press (AP) top-10 football schools stayed one step ahead of terrorists and errant drivers on their campuses by identifying vulnerable areas and securing them within minutes with Delta MP5000 temporary, portable barriers. In many situations, such as at the air base, the temporary barriers provide more flexibilities than a permanent solution. SST

Smarter Security Introduces Fastlane® Turnstiles to Tackle Unauthorized Access via "Sidegating"

Smarter Security, the intelligent entrance controls company announced new optical technology that reduces the risk of "sidegating" when two people attempt unauthorized side-by-side entry through a turnstile.

Sidegating is a growing security issue as changing regulations and customer demands for increased pedestrian and wheelchair user comfort dictate the need for wider turnstiles. If a lane is wide enough to comfortably fit a wheelchair, it is also wide enough to fit two pedestrians side-by-side. Until now, turnstiles have been unable to detect this kind of behaviour, which leads to increased risk for unauthorized access and security breaches.

Smarter Security's Fastlane Glassgate 155 turnstiles feature new optical technology to prevent sidegating from happening. An intelligent infrared matrix powered by neural network algorithms senses who or what is going through the turnstile in real-time and makes thousands of calculations per second to determine if the entry should be authorized. The system can distinguish between people and objects to minimize nuisance alarms, and process unsurpassed throughputs of up to one person per second.

"Security teams must approach insider threats and collusion with a layered security strategy that starts at the front lobby. This innovative optical turnstile technology available in the Fastlane Glassgate 155 is the first of its kind to identify and alert when sidegating is occurring," said Jeff Brown, CEO of Smarter Security. "Our customers who need those wider lanes also need to have the confidence that only authorized people are coming into the building."

Smarter Security's Fastlane brand of intelligent optical turnstiles and speed gates are favoured by end-users for their superior return on investment, and by architects for combining the depth of functionality with extensive customization options. The turnstiles are installed in thousands of iconic building lobbies, government buildings, corporate campuses and universities around the world. SST

secutech THAILAND

Concurrent with

fire & safety powered by Secutech Thailand

SMART Living powered by Secutech Thailand

info security powered by Secutech Thailand

smart city solution powered by Secutech Thailand

28 – 31 October 2019 • Bangkok, Thailand • www.secutechthailand.com

In collaboration with:
Digital Economy Promotion Agency depa

The largest security, fire and smart living & home and info security fair in Thailand reflects the growing smart city developments

Increase of smart cities can be seen across the country as Thailand 4.0 set its mark with development of various infrastructure projects with high investments across all verticals in the Eastern Economic Corridor (EEC). Secutech Thailand will be returning as the center for answering the demand of security, fire safety and smart living & home and info security technologies in smart cities.

2019 Show features

- 250+ Exhibitors
- 7,500+ sqm
- VIP 16+ Exclusive VIP tours

Top vertical projects in the EEC

- International airports
- High-speed rails
- Motorways
- Sea ports
- Hospitals
- Tourism
- Industrial factories

INTELLIGENT SECURITY

- Intelligent video & AI-enhanced surveillance
- Biometric identification
- Smart sensors & alarm
- Gate control

FIRE & SAFETY

- Active fire protection
- Passive fire protection
- Disaster prevention
- Efficient rescue
- Personal protection



SMART LIVING

- Intelligent homes
- Residential security & safety
- Elderly & home care

SMART CITY SOLUTION

- Environmental management
- Waste management
- Water management

INFO SECURITY

- IoT security
- Mobile security
- Cloud security
- Network & endpoint security
- Risk remediation

messe frankfurt

WORLDEX Group of Exhibition Companies

Organiser contact
Messe Frankfurt New Era Business Media Ltd
Jason Cheng I +886 2 8729 1099 ext. 215
jason.cheng@newera.messefrankfurt.com

Johnson Controls Announces VideoEdge Integration With EntraPass Go Mobile App



Johnson Controls is introducing the integration of the Tyco Kantech EntraPass go Mobile App with the Tyco American Dynamics VideoEdge software, enabling remote management of access control, video and intrusion tasks for seamless, on-the-go security system operation from a mobile device.

The American Dynamics VideoEdge integration with the EntraPass go Mobile App provides a single easy use interface for managing, responding and controlling aspects of your Video Management System infrastructure through the use of the EntraPass go Mobile App. Video management capabilities include the ability to view live video with PTZ control, video playback with manual search and the ability to view video linked to access and/or intrusion events.

With the EntraPass go Mobile App, users can manage and create cards, lock and unlock doors, view live video, arm and disarm intrusion partitions and request reports. This free app enables you to interact with your EntraPass security management system software from anywhere, without being tied to the EntraPass workstation.

The VideoEdge platform improves the efficiency of security personnel and daily business operations by creating powerful video management solutions allowing users to leverage high-performance video streaming, analytics and video intelligence.

EntraPass go Mobile App is available on Android and Apple devices. SST

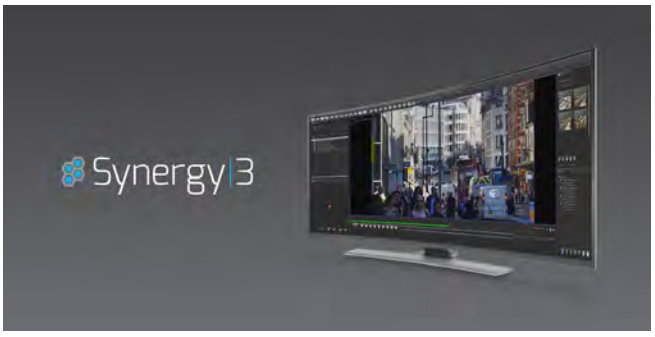
Mapping, Monitoring, and Managing Security Simplified with Synergy 3

Synectics has commenced the roll-out of Synergy 3 2019, the latest release of its command and control platform for demanding surveillance and security environments.

Introducing enhanced customizable mapping, camera management, and third-party integration capabilities, the feature-rich platform is the most customer-centric iteration of the software to date and aims to make the Synergy 3 experience more user-friendly.

The new release will be available across Synectics' key markets, spanning transport and infrastructure, oil and gas, high security, public space, and gaming.

Camera-related developments in the 2019 release also enable footage to be viewed in more intuitive ways. The de-warping functionality within Synergy 3 has been enhanced to provide an undistorted view of fisheye cameras, offering the ability to monitor live footage from multiple angles of the same camera for wide-area situational awareness. Furthermore, Synergy 3 now supports H.265 compression for all IP cameras



compliant with ONVIF Profile S.

Two notable developments in this respect are the introduction of quad view automation and the new clip mode functionality. The former refers to tailorable alerts that, if specific criteria are met, trigger quad layouts - allowing the simultaneous tracking of live action and investigation of recorded footage. Clip mode ensures that any footage viewed is automatically imported to a clip basket, for quick and easy transfer to the incident locker if verified as pertinent. SST



bathroom + kitchen today

Southeast Asia building
Sustainable Architecture • Interior Design • Landscaping

lighting today

• SOUTHEAST • ASIA •
CONSTRUCTION

Security Solutions Today

We reach out to various segments of the professional readers within the building, construction, security and lighting industries across Asia-Pacific region with our specialised publications in print and digital formats as well as on social media platforms.

Visit our website **www.tradelinkmedia.biz** for more information.

Scan to visit our website

TRADE LINK MEDIA PTE LTD

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

New IDIS Micro Dome Ideal For High End Settings

The new DC-C4212RX 2MP micro dome camera is the latest addition to the DirectIP® line up from IDIS, which is South Korea's largest in-country manufacturer of surveillance technology.

The compact design of the DC-C4212RX allows for faster and more convenient installation and is the perfect choice for retail and discrete security applications. It is the best choice for an understated, less noticeable installation. The neat aesthetics are ideal for applications where there is a need for unobtrusive surveillance but where comprehensive, high-performance video capture is paramount.



Measuring only Ø86 mm x 58 mm and weighing just 105 grams, the DC-C4212RX delivers advanced benefits within its lower profile and is the right choice for high-end locations such as jewellery shops and boutiques, as well as up-market restaurants and luxury hotels.

The DC-C4212RX offers all the key benefits that installers expect from IDIS DirectIP dome cameras, including the company's signature plug-and-play installation and configuration. The elimination of a pigtail cable allows faster and easier deployment.

The 3-axis mechanical lens enables rotation and easy angle adjustment, making it an important design feature for precise image capture, particularly when the camera needs to be discretely wall-mounted. The camera can also operate in a wide range of lighting conditions, delivering high performance live monitoring and playback.

Other key features include true wide dynamic range (WDR); IR LED illumination up to 15m with day and night ICR; dual codec H.264/H.265 performance; and easy, plug-and-play integration with IDIS VA in the Box. This cost-effective video analytics appliance delivers value-add business intelligence gained from heat mapping, people counting, queue management and comprehensive reporting. SST

Reliable, accurate weapon detection by Smiths Detection

Smiths Detection has added weapon detection to the innovative iCMORE family of smart and adaptable object recognition algorithms. It provides invaluable support for security operators, customs officers and other controlling authorities.

iCMORE is designed to identify threats and help combat the movement of unsafe, undeclared or illegal goods. Offering automatic detection of handguns, gun parts, flick and fixed-blade knives, the weapons module was developed for use in a range of applications such as aviation passenger checkpoints, critical infrastructure protection, prisons and customs. It is available for some of the scanners like the HI-SCAN 6040aTiX and HI-SCAN 6040-2is. Although an algorithm for other scanners has been developed and is now ready for customers to trial.

The weapons kit is offered as an option on new systems or as an upgrade. Potential threats are framed and shown on the main system screen in tandem with the images from the explosives detection scan. The supplementary function does not affect any regulatory certifications or approvals.

Deep learning is fundamental to artificial intelligence (AI) and Smiths Detection took this approach in developing the weapons algorithm – collaborating with customers to build a huge library of images from which the algorithm could 'learn'. However, conventional methodology may also be employed in future to create iCMORE modules for the detection of substances which do not present in consistent forms or shapes – such as drugs or currency.

The lithium battery detection is also available for some scanners. Other scanners will follow in due course for both the lithium battery and weapons module. The number of detectable items will continue to grow along with the range of systems offering the various algorithms. Following the introduction of lithium battery detection in 2018, weapon detection is the latest option to go live. SST

Western Digital Introduces Surveillance-Class Storage Solution

Western Digital® WD Purple® SC QD312 Extreme Endurance microSD™ card was developed for AI-enabled security cameras, smart video surveillance and advanced edge devices that capture and store video at higher bit rates than mainstream cameras.



With the migration to 4K and higher video resolutions, and the introduction of more smart cameras with built-in AI and improved local processing capabilities, surveillance cameras need to be able to store both video and raw data to facilitate these AI capabilities. As a result, storage with higher capacity, more intelligence and greater durability is increasingly required.

Expanding upon four generations of world-class industrial storage products, the Western Digital WD Purple SC QD312 Extreme Endurance microSD card addresses the tremendous growth of high-resolution security video with its rich feature set. The small form factor storage solution was created to meet the demands of extreme endurance, high capacity and challenging environments for the edge storage to confidently store high-quality video while reducing the need for frequent replacements.

Surveillance customers look to durable and reliable devices with intelligent monitoring to save time. The microSD card is equipped with the power of 3D NAND which ensures no-compromise, primary, on-camera storage for high bit-rate video and advanced functionality for some of the latest AI-enabled smart cameras. SST

LifeShield Enhances DIY Smart Home Security Offering with New HD Video Doorbell Camera

LifeShield, an ADT Company, is adding the LifeShield HD Video Doorbell to its lineup of easy to set up and professionally monitored smart home security products. The new Wi-Fi-connected HD video doorbell complements the brand's flexible "Build Your Own Set" package, making it easy to tailor a security system to your smart home needs.



The HD Video Doorbell was designed specifically for owners seeking increased visibility around their front doors.

The addition of the LifeShield HD Video Doorbell to our existing lineup makes LifeShield one of the most complete DIY home security systems on the market.

Key Features

The LifeShield HD Video Doorbell pairs directly with the LifeShield home security system, giving owners the freedom to record, store, and watch live and on-demand video.

Features include:

- Two-way audio support – the LifeShield mobile app and security touchpad can give visitors the impression someone is home, even if they are not.
- People detection technology – distinguishing between people and other objects, preventing unneeded notifications and recordings.
- Crystal clear 1080p HD resolution video, 170° wide lens and night vision.
- Notifications and video previews of the live event can be viewed on the LifeShield mobile app or security touchpad.

In addition, the new LifeShield HD Video Doorbell provides custom detection in specific zones. SST

Seagate Delivers Industry's First Enterprise-Ready Exos 16TB Hard Drive And Raises The Bar With IronWolf 16TB For NAS

Seagate Technology announced it has been actively shipping 16TB helium-based enterprise drives as part of the Exos® X16 family, delivering high performance and record capacity for hyperscale data centres to efficiently and cost-effectively manage ever-increasing amounts of data. The company also updated the IronWolf® and IronWolf Pro Network Attached Storage (NAS) drive lines with new 16TB capacity models.

Rising to unprecedented levels are the need for hyperscale, cloud and NAS storage solutions. A recent IDC whitepaper sponsored by Seagate predicts that the Global Datasphere - the amount of data created, captured or replicated across the globe – will grow from 33 zettabytes (ZB) in 2018 to 175 ZB by 2025. Seagate's Exos X16 hard drive delivers the highest storage density available with the field-proven reliability and continuous high performance to support a broad range of workload requirements and high-availability use cases.

Exos X16 HDD is the world's highest capacity 3.5-inch 7200 RPM drive designed to solve challenges by enabling hyperscale, datacentre, OEM and distribution channel businesses to maximize storage capacities, provide customer flexibility, and reduce complexity with uses in multiple workloads with increased I/O and enhanced caching capabilities. Seagate's new Exos X16 16TB drive delivers 33 percent more petabytes per rack compared to 12TB drives while maintaining the same small footprint for a reduced overall total cost of ownership. Exos X16 offers built-in data protection, including Seagate Secure™ Instant Secure Erase for safe, affordable, fast, and easy drive retirement.

Seagate continues to establish new benchmarks in speed and capacity with the additional announcement of IronWolf and IronWolf Pro 16TB drives, built for multi-user NAS environments and supporting workloads up to 300TB/year. IronWolf is the ideal drive for home and small office NAS systems that deliver performance, low noise and low power consumption, making it efficient for everyday use such as back up, remote access and file sharing. IronWolf Pro drives are robust for NAS that operate in creative pro and small-medium business environments that demand heavy workloads to support their data needs. SST

Vision-Box Achieves Top Ranking on latest NIST's Facial Recognition Vendor Test

Vision-Box, the global provider of biometric-based digital identity solutions and Seamless Travel Platforms, has submitted their facial recognition algorithm to tests by the US National Institute of Standards and Technology (NIST), outperforming other top competitors.

NIST provides an independent assessment of facial recognition technology for industry, governments and law enforcement agencies across the globe. The latest benchmark covering 109 algorithms from over 63 providers has ranked Vision-Box´s algorithm within the top 15. In particular, the performance in the live-to-live recognition test-set demonstrates it's a highly performant face recognition solution for usage in Seamless Traveller Programs.

Vision-Box FR™ facial recognition algorithm is based on state-of-the-art Artificial Intelligence and Deep Learning technologies, guaranteeing a continuous, fast and automated self-improving ability. The Vision-Box Research and Innovation team hosts a highly qualified and dedicated group of AI experts that continually seeks to improve the performance of its biometric capture, matching engines and related technologies. The focus is particularly on applications in the Aviation and Border Control sectors, in which the company has a dominant market position – Seamless Traveller Programs, contactless border control or simpler biometric boarding processes.

Vision-Box FR™ is part of the company's flagship Orchestra™ Seamless Traveller portfolio. It includes a cloud-ready Identity

continued on page 21

Management as a Service (IdMaaS) architecture that connects stakeholders, including Border Control Authorities, Airlines, and Airports. The goal is to optimize their biometrically enabled passenger process points that use advanced AI and IoT technology. This scalable solution securely enables a single biometric token for matching services beyond borders. Everybody wins, with a much more connected, user friendly, quicker and secure travel experience, that respects citizen's privacy and any legal frameworks.

Vision-Box FR™ is an integral part of Orchestra™ and shall be available to all its current and future customers, within the suite, as a native biometric service, providing a trusted digital identity, biometric recognition technology and a collaborative identity management platform accessible to various authorized stakeholders.

The current most advanced One iD program leveraging a single token system, such as Amsterdam-Schiphol, Dubai, Bangalore and Aruba, are considering the hundreds of passenger process-points, operating from curb to gate. This releases passengers from the printed paper or electronic document presentation hassles and reduces long queues, while transforming the whole journey into a digital, seamless and much safer travel experience.

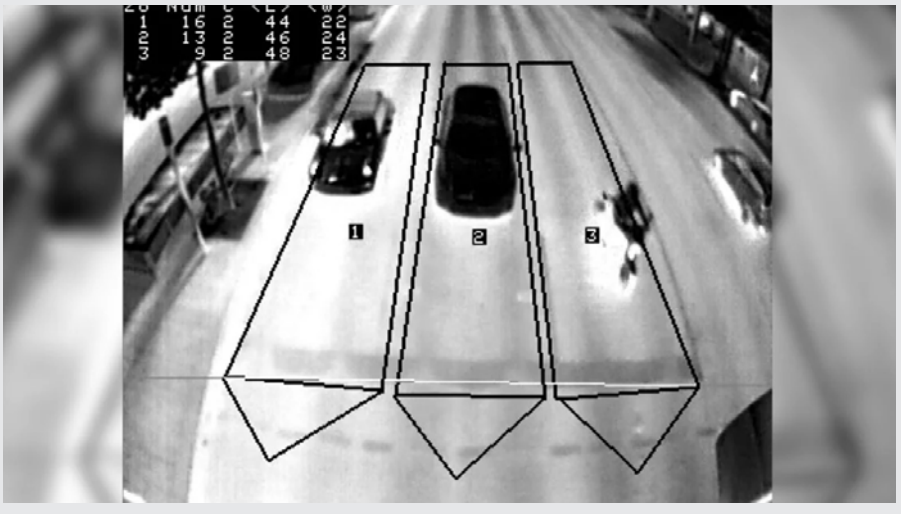
Just using a face and intuitively walking through the workflow at the control-points, like at check-in, baggage drop, security screening, border control, lounge access or boarding, the passengers' process will be handled in the background through Orchestra, simultaneously and together with all the other seamless travellers. The platform is connecting the travellers' journey at each process-point towards the airplane, while providing all the stakeholders with critical real-time information to plan, to collaborate and operate more efficiently. SST

TrafiData Intelligent Thermal Traffic Sensor Solution by FLIR provides Road Traffic Security



FLIR TrafiData intelligent thermal traffic sensor solution by FLIR Systems promises improved data collection capabilities. FLIR TrafiData is a unique offering in the Intelligent Transportation System (ITS) market with the ability to perform as both a data collection device and classification unit with the advantage of thermal and artificial intelligence (AI) technologies in a single, unified platform.

Using the combination of thermal imaging as well as AI to detect, track, classify, and communicate road traffic data over Wi-Fi, FLIR TrafiData is able to relay to security management a multitude of results: measuring real-time travel, differentiating and counting vehicles, cyclists, and pedestrians, and providing origin and destination insights. The massive data set is collected over the Acyclica by FLIR platform, a smart city data management platform, which is seamlessly accessed through FLIR's Cameleon ITS advanced transportation management software, or other compatible management software. The ability to capture this high-resolution, real-time data enables city planners and transportation managers to manage emerging traffic conditions, reducing congestion and enhancing road security.



Jim Cannon, President and CEO of FLIR Systems, stressed that by combining thermal camera with Acyclica's real-time analytics into a single device, TrafiData helps transportation and city planners gain access to ground-breaking data collection capabilities for smarter, safer cities. SST

Siqura Introduces The New 920 Series Cameras

The product line consists of three cameras which are called the BC920, the FD920 and the PD920. A fixed box camera, a fixed bubble dome camera and a pan-tilt-zoom bubbleless dome camera. Our R&D department has developed them specifically for the mobility / traffic market and the high-end surveillance market, where the cameras of this range will outperform their cameras.

Integrated SFP Slot: Greater Connectivity

The main feature is an SFP slot integrated into all three cameras. This provides for optimal connectivity because you no longer need a separate junction box to house additional equipment to convert the signal for transport over optical fiber cable to the control room. More importantly, safety and security are enhanced when using fiber, where 'eavesdropping' is made impossible. SFP ensures long-distance transmission without signal attenuation. With CAT5 ethernet the distance is limited to 100 meters. It is also possible to transmit the data on another wavelength than the standard, further increasing data safety.

Cyber Security

On top of the inherent secure connection by using fiber, the 920 series takes particularly care of cyber security. Common security features are implemented, such as strong passwords are promoted, unused ports are blocked, IEEE802.1x. After a limited number of failing logins, the camera will lock for a period of time. The 920 series can stream and can be controlled over a secured and encrypted connection, using HTTPS (SSL/TLS).

A Sharp Image Under All Lighting Conditions

Another feature, which has proven itself over the years, is the P Iris. The 'P' stands for 'precise' because the iris uses both the ability to automatically adjust like an auto iris and controls in the camera's software to create improved video clarity and depth of field. Ideal for recording in situations where the light is constantly changing.

Auto Back Focus Provides For Easy Installation

Back focus is the distance between the rear lens element and the image sensor (CMOS). Usually, this is adjusted manually. With Siqura's 920 Series this can be set remotely or even automatically. It is far easier to focus a megapixel camera than rely on BNC output to focus with the spot monitor. This also saves valuable time



of installation.

Wide Dynamic Range For Excellent Detailing

The BC920 and FD920 camera provide two modes for wide dynamic range. Single-image WDR using nonlinear gain in a single image. The second, dual-shutter WDR, which makes two different exposure settings to capture both darker and lighter areas with excellent details, much like HDR in the smartphone technology.

Servo Feedback Always Returns Camera To Original Position

The PD920 camera will always maintain its original position. When forced away from its original position – due to shocks, vibration or vandalism – the camera will return immediately. The pan and tilt motors are controlled by servo feedback, keeping track of the PTZ position at all times. No more drifting of the presets. SST

ShotSpotter® Missions™, an AI-driven Crime Forecasting Tool Updated

ShotSpotter, Inc., the leader in solutions that help law enforcement officials identify, locate and deter gun violence, announced an updated version of ShotSpotter® Missions™ – an AI-driven crime forecasting and patrol management software tool. Acquired from HunchLab in late 2018, today's product release represents ShotSpotter's first set of enhancements as it extends its penetration into this emerging category.

The new enhancement to ShotSpotter Missions enables current and future ShotSpotter gunshot detection customers to regularly and accurately update crime and gunfire forecasts so that law enforcement agencies can better plan patrol missions. Updates are scheduled to happen every 24 hours

continued on page 23

as gunfire events unfold and as patrol shifts consistently monitor ShotSpotter coverage areas across their city.

ShotSpotter Missions also includes a new report to help command staff better understand their patrol resources engagement. The new report shows which officers executed missions, and when, where, and what tactics the officers used during each mission. The report also includes the total available missions, total mission sessions, total minutes in mission, and number of officers on a shift. Agencies can then filter the data by date, time, area, and patrol or special task force units and then print or download into Excel.

Ralph A. Clark, ShotSpotter CEO and President said, "we believe we have the opportunity to redefine and grow the crime forecasting category with the help of our customers and make crime prevention software a valuable tool within law enforcement."

The updated version of ShotSpotter Missions will be available August 1. Gunfire forecasts are only available when used in conjunction with ShotSpotter's gunfire detection service. ShotSpotter Missions is also available as a standalone solution to forecast many other crime types beyond gunfire. SST

Securing Critical Site Using Smart Camera's Thermal Detection and Colour Assessment

SightLogix, the technology leader for smart thermal cameras, introduced the SightSensor TC product line, which adds high-definition visible colour to thermal detection cameras.

The smart camera uses an ideal outdoor intrusion sensor – thermal video – to detect targets with high accuracy in darkness, rain, and snow. An integrated HD visible imager provides colour video assessment. With powerful onboard video processing, SightSensor TC analytics maximize the full dynamic range of the thermal imager to detect intruders with great accuracy. The camera also provides a clear, high-contrast thermal image that can be used for assessment. Both thermal and colour streams are viewable through a wide range of third-party VMS systems.

The camera's thermal and visible imagers are optically aligned to create a rapid, real-time assessment tool, unlike other dual-imager security cameras. With the red alarm box on both thermal and visible streams, users are able to attain comprehensive details about the intrusion and can make a quick and informed response.

There are economic benefits to SightSensor TC as well. Long-range and wide area detection means fewer cameras are needed to protect large



outdoor areas. And combining two imagers in one device means one camera on the pole instead of two, with a single network drop, one mounting bracket, and simpler installation overall. SST



Do you have news for us?

Good! Email us at sst@tradelinkmedia.com.sg



NEC Partners With C-DAC To Deploy Automated Fingerprint Identification System For Kerala State Police In India

NEC Corporation announced that NEC Technologies India (NECTI), has partnered with the Centre for Development of Advanced Computing (C-DAC) (Note 1) to deploy its industry-leading automated fingerprint identification system (AFIS) for the Kerala State Police in India. The new AFIS will be used by the Kerala State Police to match unknown fingerprints against a central database of known fingerprints for criminal investigation. More than 600 police/enforcement facilities across the state, including police stations and the district police headquarters, will have access to the system for verification and new registration of fingerprints.

This new system will help state police accelerate investigations more efficiently by providing a faster and more accurate fingerprint verification. The new system is able to enhance the quality of fragmented fingerprints captured at crime scenes and makes it possible to match the prints against the central database.

NEC's AFIS prides itself on its authentication accuracy and is a core technology of the company's portfolio of leading biometric solutions, "Bio-IDiom". With the implementation of a new fingerprint recognition infrastructure, NEC is committed to build safer and smarter cities in India. SST

NEC To Provide Customs Procedure System With Face Recognition For Six Major Airports In Japan

NEC Corporation announced in July, an order from Japan Customs, under the Ministry of Finance, for an electronic customs procedure system utilizing face recognition to be installed at the customs inspection areas of six major airports in Japan: New Chitose Airport, Narita International Airport, Haneda Airport, Chubu International Airport, Kansai International Airport and Fukuoka Airport.





This electronic customs procedure system utilizes NEC's face recognition technology and has already been put into operation at Narita International Airport Terminal 3 as of April 15 of this year. Japan Customs is now expanding this system throughout six major airports, which account for approximately 90% of the annual passengers entering Japan, aiming to commence operations from March 2020.

This system is designed to accelerate the customs procedures at leading airports, where NEC's face recognition technology can confirm travellers' identities when using the system's electronic declaration terminal and passing through exit gates. Moreover, NEC aims to further accelerate customs procedures by enabling baggage to be reported electronically through the use of smartphone applications.

Going forward, it is expected that the number of international visitors entering Japan will continue to rapidly grow. As part of this, NEC will utilize its cutting-edge biometric technologies to reduce the congestion of customs inspection areas and shorten waiting times.

About the Electronic Customs Procedure System

The electronic customs procedure system consists of customs declaration apps which simplify customs and declaration procedures for baggage, an electronic declaration terminal, and an exit gate that enables passengers to pass through using face recognition.

continued on page 25

The exit gate is equipped with NEC's AI engine "NeoFace", which is the core technology of NEC's biometric identification portfolio "Bio-Idiom" and has won the world's No.1 recognition accuracy. The system operates by taking a facial image at an electronic declaration terminal installed at the customs inspection area, this image is then matched with a facial image that is taken by a face recognition camera at an exit gate. Since the face of a person approaching an exit gate is continuously photographed, walk-through authentication is possible, without requiring travellers to stop. Smooth identification contributes to reducing the congestion of customs inspection areas and shortening travellers' waiting time.

Customs declaration apps and an electronic declaration terminal

Customs declaration apps and an electronic declaration terminal enable efficient and easy electronic declaration for customs inspections. Travellers enter the contents of their portable goods with customs declaration apps, obtain a QR code, and then read their passport and the QR code with an electronic declaration terminal installed in the customs inspection area. This is considered simpler and easier when compared to preparing conventional forms for the "Declaration of Personal Effects and Unaccompanied Articles".

In addition, during operation of the electronic declaration terminal, a traveller is photographed with a built-in camera and checked against their facial image embedded in the IC chip of their passport. The facial image taken at the terminal is only used for identification processes and is deleted in an appropriate manner after use. SST

Dahua Technology Launches New Series of XVR To Support Full-channel AT & AF PoC Cameras

Dahua Technology has launched a new series of digital video recorders comprising XVR5104H-X-4P, XVR5108H-X-8P and XVR5216AN-X-16P, boasting stronger functions while saving a significant portion of wiring and power cost. Transmitting of video/audio/power/data over one single coaxial cable would benefit Dahua's customers and end users with true plug & play.

The HDCVI PoC cameras come in two types: AT mode (maximum power consumption≤12W) and AF mode (maximum power consumption≤6W). The new series of recorders support full-channel Dahua AT & AF PoC camera access, regardless of different series and resolutions, with zoom or fixed lens. This is a remarkable improvement in compatibility comparing to their predecessors as well as other brands in the market. Meanwhile, the PoC technology makes it possible for back-end recorders to provide instant power, through the same coaxial cable, to PoC cameras, which is a more stable way of energy supply.

Another huge improvement worth noting concerns audio quality. Dahua Technology's -PoC products support broadcast-quality audio, which is far better than ordinary coaxial cable transmission. Moreover, the new back-end products are smart enough to automatically tell if it is a non-PoC camera



being connected to the system and decide whether to provide power or shut the power down in one specific channel, thus greater safety.

The beauty of coaxial cable power supply also lies in the much lower cost for users, since separate camera power supplies are no longer needed. Gone with front-end power sources is the complex work of wiring that can only be done manually. In areas where labor cost is infamously high, Dahua Technology's new series of XVRs are likely to reduce the cost by half or even more. SST

Surveon NVR GSe Pro 205/205T Series Simplifies and Secures File Sharing



Surveon, the professional surveillance and storage solution provider, launched NAS-SAN-NVR-Cloud multiple usage product under compact size and best C/P value – GSe Pro 205 / 205T. From 4 ch to 64 ch camera channel support, the variety alternatives could fulfil SMB and SOHO a single device to serve multiple usages, NAS (for file sharing), SAN (for data storage), NVR (for CCTV surveillance) and even Cloud gateway (upload data to cloud) when needed. All these business demands can be easily managed using GSe Pro 205 / 205T.

Meeting Small-Medium Enterprise's Requirements

- Single device fulfils both storage & 24/7 non-stop surveillance needs
- Enterprise Data Protection with RAID & Auto Cloud Backup Solution
- Easy cross-office file-sharing and collaboration with diverse storage
- Flexible cloud applications & storage capacity expansion for future

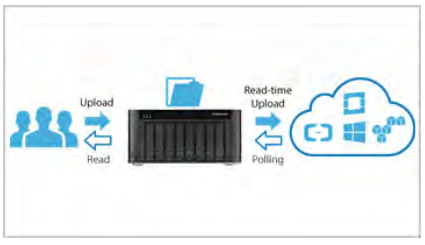
24/7 Effective Monitoring with Multi-stream Technology

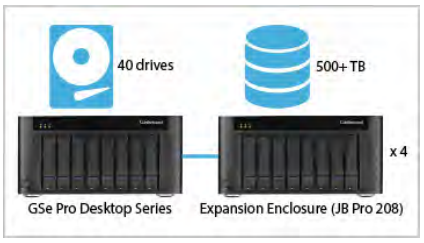
Real-time videos provide an intuitive interface while smart multi-stream technology allows users to effectively monitor and control multiple IP cameras. Users can monitor their property anytime, anywhere with just a web browser or a desktop client software.



Easy Cross-office File-sharing and Collaboration

GSe Pro 205/205T can sync business data with the cloud in real time, offering a perfect solution for cross-office file sharing and collaboration between the HQ and branch offices. By leveraging the cloud as a centralized





database, important data can be kept securely.

Highly Flexible Storage

To meet the ever-growing needs on data storage, the GSe Pro 205/205T supports up to 37 drives and more than 500 PB capacity with four expansion enclosures, ideal for storage-intensive applications such as video surveillance, data archiving, and much more.

Easy Maintenance with Versatile Host Interfaces

GSe Pro 205/205T comes with multiple host interfaces - FC 16Gb/s, FC 8Gb/s, FCoE 10Gb/s, iSCSI 10Gb/s, and iSCSI 1Gb/s - ensuring seamless compatibility with your IT infrastructure and applications. SST



Do you have news for us?
Good! Email us at sst@tradelinkmedia.com.sg



VIVOTEK Unveils Its First License Plate Recognition Camera



Taking video analytics to the next level, VIVOTEK, the global leading IP surveillance solution provider, has introduced a license plate recognition camera, the IB9387-LPR. Featuring built-in license plate recognition software and edge-computing capability without additional server, the IB9387-LPR can identify license plates from over 70 countries around the world. These and other features make it a powerful License Plate Recognition (LPR) system and a cost-effective all-in-one device applied for condominiums, parking access control and Stop & Go toll systems.

VIVOTEK's IB9387-LPR also offers efficient access control management through black & white lists and multi-site camera centralized maintenance. With a black & white list embedded inside the IB9387-LPR, the control barrier will open the gate when a white list vehicle is detected. On the other hand, a blacklisted vehicle will trigger an alarm and a notification will be sent to security staff. With VIVOTEK's IB9387-LPR, security staffs of parking lots with multiple entry points no longer need to upgrade system one after another. They can simply upload these lists to a single centralized LPR camera and all the other LPR cameras will download the master list, thus significantly reducing both installation time and maintenance efforts.

Thanks to its various Application Programming Interfaces (APIs), third-party systems such as parking management, toll collection, and weighbridge systems are able to receive live LPR images with specific country, state, date, time, and confidence level from IB9387-LPR. Finally, the sophisticated camera is safeguarded by Trend Micro IoT Security, providing proactive protection in cybersecurity. Combining recognition and management technology, VIVOTEK's IB9387-LPR offers an intelligent, scalable and highly secure standalone LPR system. SST

Airbus Introduces TH9 Tetra Radio To Middle East and Asian Market



Airbus' TH9 has now added 800MHz to its band portfolio of operation. The 800 MHz version was presented to the public during the opening day of Critical Communications World exhibition in Kuala Lumpur. It is now made available for public safety users in the Middle East and Asia.

The rugged yet powerful TH9 is a renowned Airbus Tetra radio for field use and specially designed for mission critical users such as police forces and security staff whom require rugged radios for their daily operations. This robust radio allows sharp, powerful and stable secure communication between users.

With the integration of a global navigation satellite system (GNSS) receiver supporting the Beidou positioning system, the TH9 is prepared for positioning technologies used in Asian markets. The enhanced global navigation satellite system allows users to benefit from accurate and autonomous geo-spatial positioning.

In addition to its already demonstrated success on 380-430 MHz band, Airbus' TH9 is now equally available for the 800 MHz band. The latter will allow the customers using this frequency band to benefit from the added value that the radio can bring to mission critical operations such as excellent radio performance, high audio quality, and long battery autonomy. SST

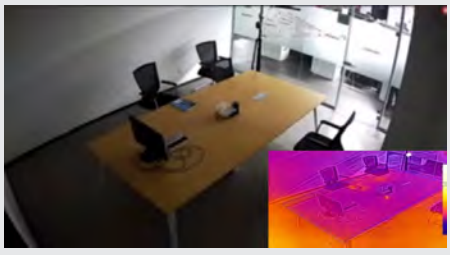
Hikvision Launches Thermal Bi-spectrum Deep Learning Turret Camera

Hikvision has released a new Thermal Bi-spectrum Deep Learning Turret Camera, which will bring enhanced capabilities of indoor fire detection, including an advanced temperature anomaly alarm and visual warning. This new cost-effective camera reduces the risks of fire and property loss.

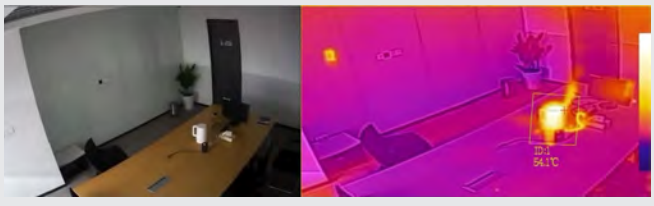
Bi-spectrum image technology

Hikvision's Thermal Bi-spectrum Deep Learning Turret Camera supports fire detection using high-quality internal hardware components to capture images using both visible light and infrared light, also called "bi-spectrum" image technology.

The bi-spectrum image technology creates a picture-in-picture preview and image fusion, which can capture what caused the alarm and help personnel to check the situation quickly. It monitors through only one channel, reducing bandwidth and simplifying the live preview procedure of switching channels between thermal and optical channels.



The bi-spectrum image fusion function also provides more image details under different environmental circumstances, making it easier to find hidden objects and document unusual events.



The camera's image processing technology combines multiple image processing techniques to create the best thermal imaging results. It also utilizes a "noise equivalent temperature difference" (NETD) of less than 40 mK (this is a measure for how well a thermal imaging detector distinguishes between minute differences in thermal radiation within an image). This means that the lower the temperature difference sensed by the camera, the smaller the value and the better the image.



Temperature anomaly alarm

This new thermal camera also features a reliable temperature anomaly alarm, which will trigger an alarm once the temperature goes higher than a user-set limit. This setting effectively improves the pre-warning capability before a fire occurs and can alert safety personnel to eliminate hidden dangers before the temperature reaches ignition or combustion.

In a practical application, it can help to detect smoking behaviours in the first place, especially for areas that are clearly prohibited from smoking like shopping malls or that are heavily banned like oil depots. Through effective alarms, staff can find and stop the person from smoking in time to reduce environmental pollution or fire damage caused by smoking.

Reduce false alarms with Deep Learning

In addition, the camera contains a built-in GPU for running the deep learning algorithm to effectively help indoor monitoring and detect illegal intrusion. Its intelligent video content analysis technology can help reduce false alarms by filtering out interference factors such as changes in lighting or movement of animals in the field of view. Only actual threats trigger alarms, making security measures vastly more efficient and preventing unwanted entry.

Equipped for double-duty – fire detection and intrusion detection – this camera is highly recommended for use in indoor fire detection and intrusion detection solutions, especially in application scenarios such as warehouses, museums, data centres, and banks. Wide viewing angle (up to 90 degrees) along with relatively small and well-designed camera housings make them easy to install and convenient to use. SST

How Digital Technology Is Changing Border Security Operations



►► **By: Ian Deacon,** Sales and Operations Director, Fotech

The last few years have seen extraordinary changes driven by the digital revolution. Some of the world's oldest industries and largest organisations have been revamped entirely as old legacy processes are swept away, and business models transformed.

The rate of change has been rapid and unprecedented. In face of such innovation, the only option is to evolve, adapt and try to keep pace with the progress or risk being left trailing in its wake.

There are very few, if any, industries left that have been unaffected by digital disruption and border security is no exception. While many physical operations still rely on secure fences, perimeter patrols and border officials – especially in remote regions – smart technology is fast becoming the most effective way for governments and organisations to ensure security.

Border management is a complex operational process which poses a unique set of challenges. Today, officials are faced with record volumes of traffic, from both trade and travel. They constantly have to monitor new and evolving security threats, keep abreast of legislative changes, deal with budgetary constraints, and manage a complex and variable mix of opportunities and risks.

In order to do this successfully, constant communication is required – all relevant agencies, departments and officials need to have access to accurate and up-to-date information, in real-time. But maintaining efficiency and integrity across the entire length of a border can be difficult to achieve as various teams are operating at different locations.



For border operations, the use of digital technology aids in the mapping out of the entire border which provides a continuous stream of information regarding the perimeter's security to all teams. This optimises management, increases co-operation between border personnel and enables better co-ordination between the governments of neighbouring countries.

One of the most advanced and state-of-the-art technologies that can be deployed to unite the various agencies and departments in border security operations is Distributed Acoustic Sensing (DAS). The technology converts a single fibre optic cable into a network of highly-sensitive, individual vibrational sensors.
The technology effectively provides an invisible 'smart barrier', detecting disturbances along its entire length. It enables operators to provide continuous monitoring 24/7, detect potential threats and direct operational responses in real-time.

When it comes to physical border security, smart technology looks set to revolutionise operations, providing officials with a far more complete picture of their operations than is currently available. By giving them access to intelligent and actionable insights, border agents will be better co-ordinated and in a stronger position to respond to potential threats in the shortest amount of time.

To find out more about Fotech's technology, visit: https://www.fotech.com SST

Homeland Security: Real-Time Analytics in Flagging Risks





►► **By: Claus Larsen,**
Global Director, Business Development, e-Government, Security & Alliances for the Public and Defense Sector

►► **By: Yannick Rolland,**
Head of Big Data for Mission Critical Systems, Atos

In the post Wikileaks era, you don't have to be working for an intelligence agency to have an understanding of the information that can be gathered about you. Terrorists, or potential terrorists, understand this better than most. They know they might be under surveillance; they know the data sources that are likely to be gathered and so they are learning to change their behaviour accordingly.

How Do Intelligence Agencies Stay A Step Ahead?

A vast amount of academic and intelligence studies has made clear that there is no single terrorist profile. Instead, intelligence agencies must look at various threat-related activities in order to assess not only the intent but also the capability, preparation and planning. We now need to understand "unknown behaviours" and use more complex behavioural indicators, particularly noticing any changes and concealment or deception activities.

Anticipating Future Threats

This requires a mixed behavioural and statistical approach to get the greatest depth of knowledge and to anticipate future events or actions. The key intelligence indicators are:

- Communications – cell phone use, movement, peer group etc
- Image –physical actions and interactions, movement through crowds etc
- Open source intelligence – social media interactions.

Looking at and triangulating all of these simultaneously can give you an indication of a person's risk even if single indicators are weak.

Unknown Behaviours and Unknown Target

As mentioned above, key indicators to flag are changes in behaviour and deception activities. Change could be seen in many different areas, for example they may have given up activities and hobbies especially if they are mainstream and against religious code. Conversely, have they stopped all suspicious activity and are they acting in a way to deceive or conceal behaviour such as joining activities or hobbies that are contrary to religious code? None of these activities alone can be indicators but put together you begin to get a view of suspect behaviour.

Unfortunately, we cannot always know what we are re looking for exactly. The ways of attack can change – only in the last few years have we seen vehicles used as weapons. This constant adaptation requires constant adaptation of indicators and flags.

Real-Time Necessity

This is where real-time analytics comes in and is hugely important to the work of intelligence agencies. A snap-shot view will not reveal anything but a real-time view – like a film, rather than a picture – will offer a dynamic flow of information enabling intelligence agencies to move targets continuously from one tier of risk to another. They may be able to recognize behaviours that relate to a series of events.

A number of behavioural studies have shown that the speed of mobilization to violence takes an average of 12 months. Monitoring a flow of behavioural indicators over time can therefore track progression from radicalisation to violence. Having real-time analytics in place and being able to flag key indicators along a path of progression can therefore serve as a good indication of a person's risk and threat level.

Human Intelligence and Intervention in Analytics

Analytics platforms that have been carefully established to flag certain behaviours or behavioural changes can alert intelligence agencies to potential risk but here is where human intelligence must come in. It is not possible to sacrifice this for technology; it must play a vital role in the process. A machine cannot understand a local culture or various anomalies that would be easy for a person to identify.

Machines and algorithms need constant updating and refining in order to learn and keep up with new trends and emerging behavioural identifiers. Post incident analysis must be gone through:

- What went wrong?
- What did we not see?
- Where were the signals?
- Where's the red flag

Those involved in illegal activities are highly imaginative when it comes to finding new ideas for achieving their ends and at hiding themselves within the population, which means that indicators that are important today may not be important tomorrow. SST

Upgrading of Airports: An Analog System To A Scalable IP Security Surveillance Solution



▸▸ **By: Sean Kennedy,** Content Manager, IndigoVision



Security Issues And Analog Hangovers

With the existing proprietary solution at the airport locked down to one manufacturer and littered with issues resulting in high maintenance and expansion costs, a new solution was required that would allow the airport to scale its surveillance solution in line with future expansion plans.

Not only was the existing surveillance solution analog and a proprietary, it wasn't intuitive and was difficult for operators to use. There were several "satellite" security installations scattered in the various terminal buildings that weren't viewable in the centralized Control Room which meant extra operators were required. The low-resolution analog cameras made it difficult to identify people during incidents and coupled with the lack of video coverage it gave operators poor situational awareness.

Reviewing past events with the existing VMS was difficult as playback wasn't synchronized and, without bookmarks, it was time-consuming to find important events. The combination of multiple terminal buildings and the Centralized Analog Architecture resulted in bottlenecks and latency issues as all processing must pass through the centralized server.

There was also no redundancy so if there was any failure in the system the Control Room would no longer have the capability to view live or recorded video. Additionally, as the system was locked down to one manufacturer and the whole system had to be hardwired to the centralized server, there were very expensive expansion costs.

Addressing Security And Scalability Concerns

The required solution had multiple requirements to ensure that the existing issues were resolved and that the solution could scale with the planned expansion.

With expansion planned to facilitate growing passenger numbers, an open IP based solution was specified to replace the existing analog solution to improve situational awareness, provide scalability and integrate with a number of other systems operating in the airport.

The architecture needed to limit bottlenecks, reduce latency issues, provide redundancy advantages and be scalable to allow for multiple new terminal buildings to be connected with ease.

New HD cameras were specified to improve image quality and coverage with a Video Wall required in order to view and manage the increase in video streams in the centralized Control Room. New large capacity NVR's were also specified to cope with the increase in camera streams and an extra NVR for redundancy and failover.

Distributed Architecture Helped Exceed Requirements

A solution with Distributed Architecture was chosen as it solved multiple issues with the existing solution and facilitated future expansion without the need for a centralized server.

Distributed Architecture allows data to be kept close to where it is produced or needed. When cameras, surveillance workstations, NVRs, alarm servers, integration gateways all participate in a Distributed Architecture, data bottlenecks are minimized as all processing doesn't need to pass through a centralized server. Distributed Architecture provides a truly unlimited and scalable solution that can easily accommodate the largest airports in the world.

It also minimized the existing bottlenecks, reduced latency, and provided higher availability and faster access to data. It also allowed all "satellite" security installations to be viewed in the centralized Control Room enhancing situational awareness. New HD cameras were installed and due to the scalability of Distributed Architecture, future cameras can easily be connected when needed. Furthermore, the scalability of Distributed Architecture enabled the airport to build new terminal buildings and connect with ease to the security solution when ready.

Lowering Total Cost of Ownership (TCO)

Distributed Architecture enables planned future expansion as it can support thousands of cameras, workstations and NVR's dramatically reducing the Total Cost of Ownership (TCO). The scalability of such allows the airport to continue with planned expansion and add a single camera/NVR or a whole new terminal when needed.

Learn more about network scalability and how to implement a scalable architecture by signing up to IndigoVision's upcoming CPD certified course "Essentials for Modern Network Scalability" at https://www.indigovision.com/essentials-for-modern-network-scalability/ SST

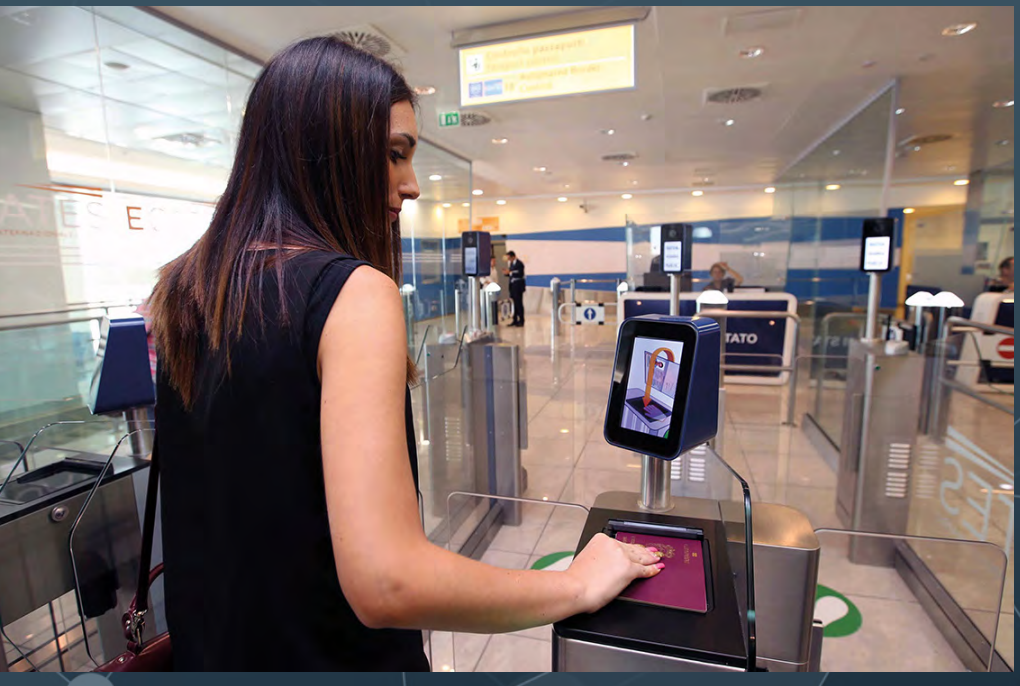
The Advent of 'Border Automation 2.0'



►► **By: Kier-co Gerritsen,**
Business Development Director,
SITA Border Management Portfolio

The first wave of border automation was e-Gates. But we now need to examine what the second wave can deliver – for governments and their stakeholders; port and airport operators, airlines and transport providers, and, of course, passengers themselves.

That's why the focus would be placed on what we call 'Border Automation 2.0.' What we're already seeing is a distinct shift towards 'automated risk assessment' and 'automated targeting'. This could form a vital part of the second wave of border automation.



Analyzing And Risk-Assessing Data

SITA, is already pretty well known for our ability to move passenger data securely between airlines, airports and governments. What SITA perhaps is less well known for, in some circles, is the ability to analyze and risk-assess that data.

Aid is given to governments create an 'automated risk assessment' capability, by being smart about how data is linked together. That includes e-passport data, Advance Passenger Information (and its interactive iAPI form, Passenger Name Record data) and biometrics.

Such an approach enables robust risk assessments to be conducted before the passenger travels, and certainly before they arrive in a country. It creates populations of pre-cleared travellers, and pre-load border systems, including e-Gates with verified identities of passengers who've been risk-assessed. These passengers will now benefit from a fast track experience when they arrive at the border.

Is There A Danger Automation Could Be Misused?

No single system or process is 100% secure. That's why the importance of taking a layered approach to improving border security, using a combination of people, processes and technology is advocated.

The reality is there's enough time to automate checks and risk assessments well before a passenger arrives in a country. It's a question of making sure the right data is available in the right place at the right time. And then making sure related business processes, such as issuing an electronic visa or travel authorization, are aligned to provide a complete picture of each passenger and the risk they pose.

In the future, we may have 'automated identity verification' using a variety of self-service options, including kiosks, mobile apps and, of course, e-Gates. And technology, particularly data analytics augmented by machine learning, will automatically identify suspicious patterns of behaviour and automatically select passengers for secondary screening – i.e. those security needs to talk to when they arrive at the border.

A More Seamless Future At The Border

In years to come, automated arrivals processes will be less visible and more seamless, resulting in passengers arriving in a country and walking non-stop from the aircraft gate to the baggage hall and out to the kerb. There will, of course, always be opportunities for law enforcement and other government stakeholders to intervene during the arrivals process.

There is a possibility that self-service kiosks are more likely to have a future than eGates. Today, self-service kiosks for the border are typically located in restricted (and supervised) areas of a port or airport. Tomorrow, they could be in unsupervised locations in hotel lobbies, conference centers or shopping malls.

What will be important is the integrity of the business process and the ability to build an 'identity picture' having verified passenger data and identity information, no matter where the kiosk is located. This 'identity picture' can be re-used multiple times for many other steps in the passenger journey.



What About Border Automation And The European Entry/Exit System?

The European Entry Exit System (EES) paves the way for that all-important second wave of border automation. When deployed in about two years' time, it will transform the border control process.

Currently, every non-EU passenger, known as a Third Country National (TCN), must be processed by a Border Control Officer and have their passport physically stamped upon arrival. But Europe faces a challenge in mitigating the risk of irregular migration, typically in the form of non-EU nationals lawfully arriving in Europe but then overstaying.

From 2021 onwards, once EES is operational with every EU Member State connected to it, it will no longer be necessary to physically stamp the passports of TCNs. Stamping will be digitized. Every arriving passenger will have their information, including biometrics, recorded in a central system. This will be complemented by the date, time and location of their arrival. Records stored in the central system will be accessible to all EU Member States.

So, when a passenger arrives in Country X and departs from Country Y, data can be reconciled, and records updated to indicate a passenger has left the EU. Conversely, when a passenger does not leave Europe, an automated process will update their record and share relevant information to assist in locating the passenger.

What's important here is to perform a variety of checks on other key systems, such as the Schengen Information System (SIS) and the European Asylum Database (EURODAC), and combine identity data with flight data, booking information, arrival dates and times etc.

Delivering The Second Wave Of Border Automation

What has been learnt from managing borders in dozens of countries, including the Middle East and our work with US Customs & Border Protection (CBP). That is the what is necessary to bring to the government customers looking to automate key functions at the border, no matter whether that be land, sea or air.

This blog was first published on www.sita.aero SST

Smart Borders: Increasing Security Without Sacrificing Mobility



►► **By: Dan Newman,**
Lead Partner for Cloud Engineering,
Deloitte Asia Pacific

Our borders have been transformed from a static line on a map to an ecosystem for shared decision making and real-time collaboration that empower government and industry to work together to create safer, more standard and cost-effective perimeters. Border security and management is a broad term encompassing a vast range of national security, economic, and socio-political functions.

An increased focus on the physical security of goods and people moving across borders in response to 9/11 and an overall global emphasis on counterterrorism has caused a systemic shift in the border security landscape. The evolving international economic and security environment signals a need for increased intelligence cooperation. Governments seeking to encourage the success of their citizens and businesses should consider new and innovative measures to mitigate the impact of two converging issues, namely heightened security and the exponential increase in the flow of populations and goods.

How can a government provide enhanced security while at the same time facilitating the rapid and efficient movement of goods and people? There needs to be an implementation of a variety of organizational restructuring, technological investments, and bilateral cooperative agreements in an attempt to bolster security without compromising economic progress. These approaches have produced varying results and a wealth of lessons learned. Upon examination of these efforts, four solution areas have emerged that deserve special consideration when constructing a long-term vision for border security and management:

Make a Safer Border by Employing Risk Based Decision-Making

As a first step, establishing common assessment criteria and mutual guidelines for identifying, segmenting, and addressing risk is necessary in order for agencies to reach agreement on high priority risk areas and drive risk-based resource allocation. In this setting, integrated risk assessments prioritize emerging vulnerabilities and enhance individual and shared border security efforts. Early success stories have come out of co-habitation of intelligence or fusion centers.



Many of these centers use automated technology platforms and solutions to support information sharing and have helped address threats early by bringing leads to an appropriate law enforcement resolution. Shifting to a risk-based approach that deploys the most effective inspection and scanning technologies to detect and prevent the entry of hazardous materials, goods, and terrorist weapons is another important component. Policy changes can include advanced screening programs which determine that containers that pose a potential risk for terrorism are identified and inspected at foreign ports before they are placed on vessels destined for their designated country.

The technologies that enable this type of screening include mobile Non-Intrusive Inspection (NII) which detect, and interdict weapons, narcotics, currency, and other contraband hidden in commercial shipments; large-scale x-ray and gamma-ray imaging systems, radiation detection technology; portable and handheld devices. "Green Lanes" have also been deployed which accelerate the flow of legitimate goods for low risk cargo at ports of entry and trusted traveler programs which work similarly but for individuals.

Yet, these risk assessments can only be effective if they are supported by ample information sharing between agencies and governments, particularly as it relates to travelers' biographic information, good content information and risk profiles.

Improve Standardization by Normalizing Data Requirements and Partnering Across Border

The standardization of data requirements significantly increases the efficiency and effectiveness of information sharing within and between governments and industry alike. In order to standardize data effectively, governments should first begin to utilize a shared risk model across its security agencies, to promote information sharing within its own borders. A clear, common risk model can improve communication between law enforcement arms, improving performance and coordination across multiple areas of border security.

However, in order to implement collaborative border management, partner governments must also standardize the types of information collected, and the processes for doing so. Efforts to unify data requirements are most effective when governments are capturing and using the same type of information to drive decision making at the border. This element is especially impactful for those in the law enforcement community. By sharing information collected about passengers and cargo, participating governments and industry stakeholders can streamline individual data-collection efforts and strengthen overall security and efficiency through the use of consistent and accessible data.

A potent example of neighboring countries partnering to increase the mobility of their citizens is in the Schengen area. The Schengen states are a group of 26 European countries that have abolished passport and immigration controls at their common, internal borders, while simultaneously tightening common external border to ensure the security of those living or traveling in the Schengen area. Central to this cooperation are the "Schengen rules" that establish the legal framework for collaboration that are best embodied in two information sharing systems.

The Visa Information System (VIS) allows the Schengen States to exchange visa data, while the Schengen Information System (SIS) allows for exchanges of data on risk groups and goods, including suspected criminals, people who may not have the right to enter or stay in the EU, missing persons and stolen, misappropriated or lost property. Continuous improvements to the existing information sharing systems as well as the legal framework have been imperative for the Schengen States.

Increase Cost Savings by Consolidating Government Functions at the Border

Many countries have moved beyond

existing concepts of collaborative border management to actually consolidating around functions. By streamlining and fortifying border security operations, multiple countries have consolidated governmental agencies and related border functions to allow agencies that were once separate to pursue the security of the border in tandem with trade and immigration. In this paradigm, border security becomes an integrated way of addressing national security, community protection, biosecurity, trade and immigration issues concurrently. Not only can this improve the oversight of security issues related to the flow of goods and people, but it also enables a critical holistic view of operations and opportunities to streamline inefficient trade and travel security procedures.

For these reasons, in 2003, the United States stood up the Customs and Border Protection Agency (CBP) as the centralized agency within the Department of Homeland Security charged with managing border security as well as facilitating immigration and trade.

But consolidation also has its challenges. Once agencies and departments are combined, the overall mission can become very large and unwieldy. The UK's recent creation of three distinct but closely connected functions out of what was the UK Border Agency (UKBA) illustrates the need to balance the benefits of integration with the retention of a clear focus and mission. As the scope of border security continues to evolve to include a focus on immigration, commerce, and consumer protection, consolidation will play an even greater role, especially as governments seek to incorporate leading practices related to technology use and cross-border agreements.

Innovation at the Border by Enabling the Ecosystem to Bring Commercial and Community Solutions

A critical step to improving the flow of trade and travelers is simple cooperation and leveraging the capabilities of non-government players for innovative ways to shore up key infrastructure. To that end, there is a critical need for strong public-private partnerships (PPP) in order to help secure the border.

IATA sets standards for airport checkpoints and is currently working to streamline security measures for both passengers and cargo. IATA efforts to improve security screening of cargo include Consignment Security Declarations, which provide a standardized audit trail for cargo along the entire supply chain; Advance Electronic Information, which facilitates the risk assessment process by customs authorities; and Secure Freight, an air cargo security project that aims to ensure freight is protected from unlawful interference.

IATA has also created programs to standardize key passenger information that is shared with governments and works to promote use of those standards internationally. Its "checkpoint of the future" working group seeks to address overall passenger flow and security, acknowledging that today's processes are unsustainable in light of anticipated growth in air travel.

Conclusion

Despite unique challenges and varying approaches, border security specialists share a vision for Smart Borders. With a goal of facilitating the movement of goods and people across borders, the ideal global solution will strive to be safe, standardized, and cost effective. And for each of these components there are two primary stakeholder groups that should be addressed: industry and government.

The vision of a seamless border is designed to create a business model for the processing of people and goods that is agile enough to accommodate projected large increases in volume. The concept should deliver an experience characterized by the smooth movement of legitimate cargo, travelers, and industry stakeholders while enabling targeted interventions against illicit and threatening activity.

Leveraging leading practices is a key feature in developing a vision for smarter borders. The countries referenced in this report have pursued a variety of policies in their efforts to alleviate border congestion while at the same time staying ever vigilant on national security. Each has a unique perspective and can point to successes via programs that incorporate new technologies and innovative thinking. Bi-lateral agreements are also critical and promote a more seamless flow of goods and people across borders. But this issue affects more than those countries that sit physically next to each other on a map. The overarching need for a global border management solution is one shared by all countries. SST



SAFETY IN SIGHT: VIDEO SURVEILLANCE PROTECTS CLEVELAND



Cleveland, Ohio wanted to strengthen its efforts to prevent crime and enhance citizen and infrastructure security throughout the city. The city of Cleveland is officially home to about a half million residents and its population swells to about 750,000 on workdays, and around a million on certain weekends. The city is the business, entertainment, healthcare, education and sports hub for Cuyahoga County and Northern Ohio. To increase protection of critical infrastructure and institutions, the city worked with the Department of Homeland Security to help fund a high-speed wireless video network with a dual purpose: to guard against national security threats and to help prevent crime and provide enhanced citizen safety.

Video Surveillance Network to Monitor and Protect

The city deployed a pilot program using a Motorola Solutions wireless mesh video surveillance network to monitor and protect the downtown area. The Cleveland Department of Public Safety has always been committed to being on the leading edge of technology and a few years ago created the Cleveland Shared Security Surveillance (CS3) program. The goal of the program is to provide officers and first responders with a shared security presence and enhanced officer awareness through a high-speed wireless mesh network with video surveillance cameras. As the city's first initiative, a pilot video surveillance system of nine cameras were positioned around the Public Square area in the heart of downtown Cleveland which then expanded to the CS3 initiative.

The successful pilot program has resulted in the ongoing expansion of video security throughout the city. From the initial Public Square pilot, Cleveland's wireless video surveillance network has continued to evolve and grow. With funding through Homeland Security and other federal organizations, the city and Motorola Solutions have deployed a continually expanding network throughout the city. Today, the city itself has 25 cameras and a growing number of cameras provided by local organizations and businesses that are tying into the network.

Coverage is expanding to the port area, the west side market and the arena district, and soon, the network will be extended deeper into the neighbourhoods around the city. With the cameras in place and clearly visible, the system enables citizens and visitors alike to feel a greater sense of safety and security.

Increasing Officer Awareness with Help of Video Security

The St. Patrick's Day Parade is one of the city of Cleveland's most popular annual events. More than half a million people come downtown to join the party, making security a significant



challenge. "To monitor activities and provide security for all those folks is very difficult, especially on foot," says Mike McGrath, Cleveland's Chief of Police. "That's where video surveillance comes in. The cameras allow officers to monitor activities in real time so they can quickly identify potential threats and respond faster and better."

Security Cameras Stream Real-Time Information to Police

The city's video surveillance planning began a few years ago with the creation of the Cleveland Shared Security (CS3) program. The CS3 program is a public-private partnership that allows security cameras to stream real-time information back to a police command vehicle, Emergency Operations Centre (EOC) and to a dispatch centre. Cleveland's cameras can tilt, pan and zoom in on a particular area to follow the activities of an ongoing situation or help predict a dangerous situation before it happens. Square one for the program was a nine-camera pilot deployment around the downtown Public Square area which has proven to be highly successful. Motorola Solutions' Integration Services played a key role in the City of Cleveland's video surveillance project, resulting in an excellent model for planning future video solutions. Starting with a small build out of a wireless network system, the project has evolved into a phased in approach of an ever-growing system with increased capability and functionality including the CS3 public private partnership.



Better Situational Awareness for First Responders

"The day-to-day value the camera system delivers is two-fold," says Larry Jones II, CS3 Project manager. "There's better situational awareness for first responders and that leads to increased safety—and a heightened sense of security—for our citizens and visitors." The city is incorporating some of the cameras into its CAD (Computer Aided Dispatch) system. "We want to focus on getting our video into the dispatch centre where it can help police, fire and EMS as they arrive on a scene," continues Jones II. "We want a dispatcher to be able to say, 'those guys just ran to the west, one's in blue, the other's in red.'" Video solutions also allow an emergency responder in distress to press an emergency button on his or her radio that triggers an alarm at the dispatch centre. The Video Solutions system then identifies neighbouring cameras and directs them to the responder's coordinates.

A Network Growth Spurt

Not surprisingly, the Video Solutions system is growing quickly. "The system has been successful from a number of perspectives," says Martin Flask, director of Public Safety. "As a result, community groups and elected council people want us to expand surveillance throughout all the neighbourhoods of the city of Cleveland."

The city is expanding coverage to its port area, the west side market and along the lakefront where facilities such as the Rock 'n Roll Hall of Fame, Browns Stadium and Jacobs Field are located. In addition to extending the network geographically,



the city and a number of other public and private organizations are also expanding by adding cameras. "One of the great things about having an infrastructure in place," adds Jones II, "is that as private entities add cameras of their own, we can tie those cameras into the system." As the number of cameras grows, the surveillance network is increasingly being used to not only discourage crimes, but to help solve them. Explains Flask, "It's also provided important forensic evidence that helps our police to solve some crimes that would not potentially have been solvable had the surveillance system not been there."

Mobile Video Security for Areas without Video Cameras

Cleveland also has the capability of providing video security in areas that don't yet have video cameras deployed. "If we don't have coverage in an area, we would deploy our command bus," says Quenton Cantionez, Public Safety Systems Manager. "We have cameras on the command bus, including one on the boom, as well as portable cameras on tripods. We deploy the unit to a location, and we can provide live monitoring and, with point-to-point line-of-sight connectivity, send a video feed to one of our towers." If there's no line of sight connectivity, personnel can record video on the bus for evidentiary purposes. Video can also be sent to the city's Emergency Operations Centre in emergency situations.

Force Multiplier

The Video Solutions network also acts as a force multiplier. "In today's culture where we have this flash mob mentality," says Chief McGrath, "for us to be able to use the video feed to observe these people in downtown Cleveland, and then relay that intelligence information to the officers on the street, is very, very important. Video security has definitely supplemented our workforce." Adds Cantionez, "The overall benefit of having the video security network is to have eyes in places when you don't have eyes available."

Motorola Solutions' Video Solutions system allows first responders to view live, real-time, 24/7 visuals of their communities. They have immediate access to view commercial districts, neighbourhoods, high-risk areas, crowded public events, dangerous intersections, public transit vehicles, and municipal buildings when they're not physically on the scene. Live mobile video streaming from the scene back to the command center or eventually to hand-held devices – such as Motorola Solutions' LEX L11– enhances coordination of efforts from all officers and response teams.

An Ounce of Prevention

"The most important aspect of the camera system, for me personally, is the preventive component," says Chief McGrath. The city feels strongly that simply the visible presence of the cameras is a safety benefit. Cameras are mounted in plain sight on fixed utility poles and other structures. The city wants residents, visitors and especially those who come into town with another agenda to know that they're there. "We have blue strobe lights on the top of them," McGrath continues. "So when you're walking through our downtown neighbourhood, especially at night-time, you'll see these blue strobe lights all over the place. That's a blanket of security I don't think you can put a price tag on."

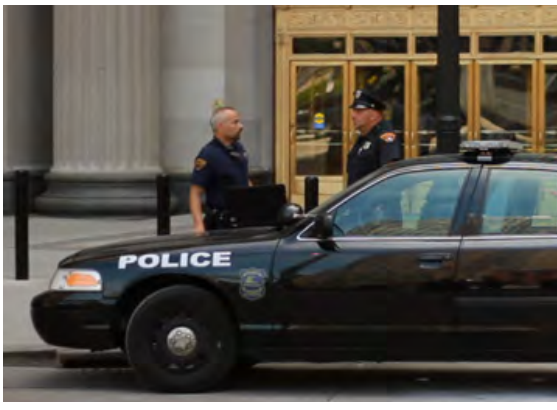
Partnerships and Funding

The city of Cleveland was able to obtain funding for the Video Solutions project through a variety of grants. "As part of our grant application, we identified critical infrastructure here in the city that could be targets of some type of national threat," explains Chief McGrath. Funding from the Department of Homeland Security and other federal organizations has allowed for CS3 to support 25 city owned cameras and dozens of other cameras owned by local organizations, businesses and other public safety agencies. The result is a partnership in which national and local security programs converge and overlap, and the city has been able to use its federal funding to maximum advantage.

In mission critical public safety networks, vendor partnership is all-important. The working relationship between the city of Cleveland and Motorola Solutions has been ongoing and successful both in terms of technology and equipment and of service. "Overall, Motorola Solutions' responsiveness has been excellent, in my opinion," says Cantionez. "They've been there for the design phase, implementation, go live, and troubleshooting. Motorola Solutions has been like our crutch, in a sense." Others on the team agree. "Our partnership with Motorola Solutions has been very good, especially during implementation," says Chief McGrath. "Any request we had, they responded to. If something wasn't working, they were up on their ladders making it right for us. Vendor partnership and service are very important, especially in law enforcement."

Positive Feedback

Citizen and business reaction to the Video Solutions system has been very positive. Cleveland's Video Solutions system is protecting both property and lives relative to any national homeland security threat, and at the same time is helping the community reduce crime and increase safety. SST



Intelligent Video: Ensuring Substation Physical Security

►► By: PureTech Systems

The power grid is a modern engineering marvel, providing us widely available and affordable energy for not only our day to day lives, but also highly critical infrastructure elements for which we rely on personally, and as an economy.

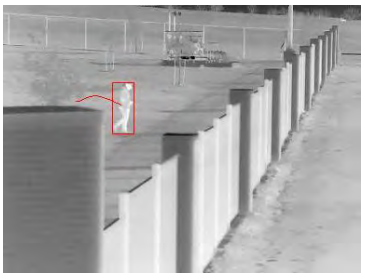
However, our reliance on the grid also makes it highly susceptible to adverse events, including physical attacks. All parts of the grid can become victims of malicious events, but substations are particularly vulnerable due to their role in power distribution and the nature of their equipment. The challenge power utilities worldwide are facing is finding an affordable solution, which can help detect, deter and facilitate an informed response to a substation security event. Fortunately, there are many solutions to help power utilities address these security concerns, one effective choice is the use of intelligent video.

An Affordable Solution

Intelligent video, or video analytics, is a popular choice for the protection of critical facilities given its ability to detect, provide instant visual confirmation of the event and subsequent event forensics. The capability of this technology is increasing at a rapid rate, while decreases in hardware cost make such solutions affordable for owners or operators of critical bulk-power system sites. Such a system consists of fixed cameras, pan-tilt-zoom (PTZ) cameras, a



deterrence device and data communication capability.



Detecting Targets Entering Perimeters

Perimeter designs can vary based on the vulnerabilities identified, aspects of the site, budget, etc. In most cases, substations can benefit from a simple camera-following" design, which includes surveillance of a potential breach at the fence line, as well as, the ability for early detection for some distance beyond the physical perimeter. Each camera is responsible for covering the blind spot of the adjacent camera. That camera is then responsible for covering the blind spot of the next camera, and this pairing continues around the perimeter until the final camera covers the blind spot of the first. This type of coverage design is very effective and affordable for locations with well-defined perimeters, such as substations.

Using this layout, the video feed from the fixed cameras are then enabled with video analytics algorithms to alert when predefined conditions are met. This is done by inputting the video signal into a server, edge device or NVR, located at the site, or remote to the location.

Intelligent video technology provides for very specific alarm criteria, which in addition to only alarming when a target enters in a specific region, can also discriminate, or classify, by the type of target: human, vehicle, etc. Furthermore, the alarm can be restricted by specific actions taken by the target, such as loitering in an area, dropping or throwing an object, more than one target entering with a valid badge swipe (tailgating) or even the speed at which a target is entering an area. This level of discrimination provides the ability to address very specific vulnerabilities, as well as, avoid nuisance targets, such as wildlife, debris or moving vegetation.

Assessing and Identifying Targets

Another key feature with significant value to substation protection is the geospatial aspects available with some video analytic solutions. This capability maps each pixel of video to its real-world latitude, longitude and elevation. The target is further assessed, including the actual location, the real size of the target, the real speed and the current track. It also affords the opportunity to provide a real-time display of this information to the security operator through an easy to understand map-based user interface.

Another key assessment aspect of this substation protection scheme is the use of autonomous PTZ cameras. These are typically placed at the corners of the perimeter where they can service detections from multiple fixed cameras. As previously mentioned, geospatial video analytics, provide the benefit of knowing the exact map-based location of the target. Knowing the location of the target is extremely valuable to the security officer, but it is also the basis for a feature known as "slew to cue," whereby PTZ cameras armed with video intelligence can be automatically steered to the same location for instant confirmation of the target. In most cases, "slew to cue" functionality also includes an "intelligent zoom" feature, which uses the target size information from the alarm, the PTZ camera location and the target location to adjust the zoom level of the PTZ for an instant view of the target that can provide identification details (clothing colour, car type, etc) without the need for the operator to further adjust the zoom.

At most installations, you'll see landscaped islands at the entrance drives which regulate vehicular access. If allowed to drive into the complex, you will cross over vehicle control barriers and bollards at the entrances. Indeed, all exits at the end of all drives are controlled with barriers, which pop from the ground when needed. You'll see similar barriers and bollards at refineries, distribution centres and headquarters offices of petrochemical and hydrocarbon companies, literally around the world.

Responding to Threats

Once a target is detected and confirmed, a security approach leveraging the use of intelligent video can continue with a coordinated response to the event. When video analytics is applied to pan-tilt-zoom cameras, it can automatically follow a defined target, freeing the operator to take other actions, such as coordinating with law enforcement officials. This feature, referred to as camera auto follow or PTZ following, can be automatically engaged as the result of a detection



event, or subsequent to a slew to cue action. The system will continue to follow the target until it reaches a pre-defined system time-out, the operator takes manual control, or the camera can no longer view the target. The system can then provide the resulting PTZ video as a component of the detection alarm, for a more complete understanding of the intrusion for the operator to review.

Deterring Intrusions

When the system has detected the target, classified its type and verified it has met alarm conditions. As part of the alarm it has also included dynamic indication of its location on a map, autonomously steered a PTZ to the target to allow for gathering of more detailed target information and a PTZ has locked on and is now following the target without any required user interaction. Total elapsed time to this point in the security response is typically less than 5 seconds.

This level of automated response addresses many vulnerabilities typically identified as part of a CIP-014 security assessment, but with minimal extra cost, it can be extended to help with the aspect of deterrence. Deterrence is often realized as a fence, physical barriers or access-controlled gates. These are physical items and should certainly be included in a substation security plan.

However, another form of deterrence, which can be enabled using intelligent video is the idea of audio talk down. This is the use of live or pre-recorded audio, which is activated upon an intrusion to deter the intruder. Different from a general alarm warning audio, audio talk down uses information about the location of the intruder and their actions to select appropriate pre-recorded audio to deter the intruder. Worse case, the understanding that they are being actively monitored may hasten their plan.

Coordinate Communication back to Command and Control

A common concern when deploying such a system is the amount of bandwidth required. Substations are almost always unmanned, which means the intrusion information must have a means to get communicated back to the main monitoring location. From a design aspect, this is typically the case, but it is important to know that it is not a requirement in order to gain security benefits from a video-based system. The system described in this article has the capability to detect, assess, respond and deter without any communication back to a main command and control. Alarms, events and system actions can be logged and stored remotely for review later.

Utilities will want to be notified and react in real time. In these cases, video systems can adjust to the available bandwidth – from a low bandwidth situation where a textual alarm is provided with an image of the detection, to a high bandwidth installation where feeds from multiple cameras can be monitored and controlled in real time.

In each case, complete alarm information, including meta data, images and video can be readily available to the security operations centre, which can then take action based on their security response plan, including contacting and coordinating this alarm data with local law enforcement through web-based access or mobile phones.

Article courtesy of PureTech Systems.
https://www.puretechsystems.com/ SST

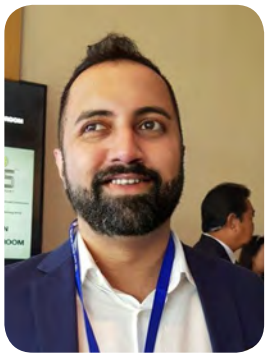
Security Solutions Today

sst.tradelinkmedia.biz

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

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

The Future of Warehouse Security and Efficiency



▸▸ **Mohammed Muneer Khan,**
Principal Consultant,
StrozTech

As recent as a decade ago, warehouses were often seen as a separate entity in the overall supply chain. They were merely used for the storage of merchandise, a holding place before the goods are transported to their final destination. Today, businesses are progressively discovering the advantages of moving towards integrating the modern day warehouse into the greater supply chain as they see the benefits of having an enhanced inventory management – a greater loss prevention and theft protection. Not only that, security solutions integrated into the supply chain can keep businesses competitive and increase their operational efficiency.

Real Time Inventory Visibility

Radio-Frequency Identification (RFID) is one such technology solution that has been increasingly integrated throughout the supply chain for both security and inventory tracking. An RFID tag consists of a tiny microchip with an in-built aerial which contains information on the particular item and is typically fixed to a product or its packaging.

RFID can then be used to identify and track items within the warehouse and beyond. It is able to provide real time inventory updates. Through having greater awareness of inventory, businesses can then reduce products going out of stock. This results in increased overall conversion and, in the end, overall customer satisfaction.

RFID tags communicate with readers, which can be fixed or handheld. Through placing fixed readers in different locations within a warehouse, it is then possible to track the movement of goods, even when numerous products are located on a single pallet.

By 'source tagging' during the manufacturing process, complete accuracy on shipment orders can be achieved. This ensures the exact number of items received aligns with those ordered. It also means that merchandise arrives in stores with security labels already in place, which can be deactivated at point of sale, saving the retailer both time and employee resources.

A Clearer View of Warehouse Activity

By combining RFID technology with CCTV solutions, it is possible to provide proof to customers and logistics companies that goods were received or shipped, providing assurances for both parties and complete transparency throughout the supply chain. This can also aid in disputes such as insurance claims when products are lost, misplaced or damaged.

We all know that warehouses can be enormous sprawling maze of aisles, pallets and storage racks. This means a comprehensive CCTV surveillance solution is necessary in order to achieve complete surveillance. By mounting High-Definition Megapixel CCTV on existing IP networks, businesses can reduce initial installation costs and have more versatile camera placement, thereby greatly improving coverage of otherwise "blind spots". HD CCTV is increasingly being deployed in warehouses as it provides superior discernible detail, greatly improving facial recognition ability.

Improved detail can mean that post-event analysis can be conducted with greater efficiency; enabling investigators to analyse and process data more accurately in the event of any criminal activity or prosecution. Through electronic timestamps when searching archived data, police and security staff are then able to hone in on the relevant footage far faster than with analogue recordings.

Warehouse Access Control for People and Vehicles

To physically control the flow of vehicles to and from the site, access control to the site perimeter should be



achieved through barriers, bollards and ramps. The choice of vehicular access control solution should be based on the amount of traffic expected, with access often needed for HGVs or forklifts in addition to staff and contractors. Access control should not inconvenience or slow down authorised access for vehicles. To achieve this, RFID can once again be used for contactless access control. Automatic Number Plate Recognition (ANPR) is another alternative that can make this a smooth and seamless process.

In order to prohibit access to the warehouse from unauthorised persons, access control such as biometrics (fingerprint or retina scanners), smartcards or passwords can be implemented to control their movement within the warehouse. By integrating with employee time and attendance systems, these access control systems can offer added benefits such as providing additional analytics, salary tabulation and cost savings to the business.

An Integrated Approach to Warehouse Security

For any business, we know that the operational and commercial success is dependent on being able to mitigate security risks. This is particularly the case in warehouses. After all, highly valuable stock is an attractive prospect for criminals. However, RFID technology and CCTV should not be used simply for reducing theft and loss. Instead it can also be utilised for greater operational awareness.

Operators are therefore increasingly turning to an integrated security solution to achieve this. A Physical Security Information Management (PSIM) platform can bring together these otherwise disparate solutions, simplifying the command and control. By seamlessly bringing together Access Control, CCTV, RFID, Intruder detection and Fire systems, security operators can have an at-a-glance snapshot of all operations, enhancing their situational awareness and increasing their ability to react not just to any security infringements but also operational errors.

The future of the supply chain should begin with the warehouse. Through the implementation of the technology solutions discussed and also the tailoring them to the needs and specifications of the warehouse building and site, businesses are able to reap not just improved security but greater efficiency throughout the supply chain.

Article courtesy of StrozTech.
https://www.stroztech.com/ SST

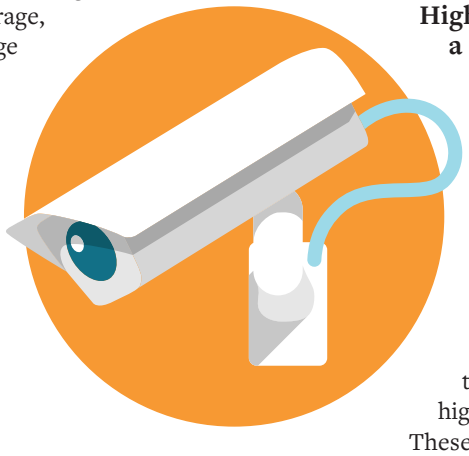
Five Things You Didn't Know About Video Surveillance Data Storage

▸▸ **By: Julie Fagan,** Solutions Marketing Manager, NetApp

When most decision makers think about a new video surveillance solution, they typically think only about video cameras and video management software. However, that's a mistake because video storage often exceeds 30% of the cost of the entire solution. With the improvements in the effectiveness of video surveillance, such as more high-definition cameras and longer retention times, many businesses and government agencies have had unpleasant surprises when their video storage bills arrive.

Because video is unstructured data, to be cost-effective, it requires special storage. Not knowing about this requirement for special storage, many businesses go with file-based storage solutions or cloud storage for all their video. They don't realize how much more expensive it will be in the long run.

Key takeaway: Not all storage is created equal, especially when it comes to video. Neglecting to do a thorough evaluation of your options at the start of a video surveillance project can result in raking up huge bills.



Reliability

Reliability is important, especially when losing video files can mean losing evidence of a critical situation in the making. For police departments, it might mean that key evidence from a body-worn camera is lost. In a court setting, that lost evidence might have been crucial to show the situation from the point of view of the officer.

Other storage companies might claim 99.999% reliability, but if the fine print is read, you will learn that when things break, the video might be stored, but at a lower resolution. And the diminished quality might continue for an extended period while the system rebuilds itself or re-indexes itself when failed disks have been replaced.

Lower quality might not sound like a big issue, but what if the footage is from a body-worn camera and is needed to back up a police officer's testimony? The degraded resolution that's caused by a problem with the storage solution can result in a video that doesn't show the accurate important details to catch the perpetrator. It is important that surveillance footages need to be stored reliably in the highest resolution and with the highest quality possible from your cameras.

High Performance and High Density in a Small Footprint

High performance and high density are important because there is a need to be able to store video at the fastest possible rates from the largest number of cameras.

For example, surveillance storage system's video streaming bandwidth must be high enough to support and to sustain write capabilities for multiple high-resolution feeds across the network. These bandwidth requirements can be daunting. Just as high-definition video requires much more capacity when it's stored, it also demands far more bandwidth when it's ingested into the storage system. On top of that, it must simultaneously support multiple high-resolution streams. That support can mean recording hundreds of parallel video streams, consuming huge amounts of bandwidth.

Surveillance environment that requires 24/7 video monitoring, the bandwidth utilization would be even higher. Depending on the number, duration, and actual resolution of the incoming video streams, the storage system might struggle to

keep up, significantly increasing the risk of dropped frames. Video evidence often plays a critical role in civil and criminal proceedings, the loss of key video images can have devastating financial and legal consequences.

More than just bandwidth, there is also need for enough storage space. Video surveillance solutions are deployed in a wide range of environments and are often installed in confined locations with little available floor space. Storage arrays that might present an acceptable footprint in conventional data centres are simply too bulky and inefficient for use in the cramped control rooms that confront many security professionals. These space limitations make the need for superior bandwidth in a space-efficient array significant.

Easy-to-Use, Easy-to-Secure Systems

The ease in operation is a plus point as well so lesser time would be spent on learning how to use and maintain your video storage. Storage solutions should be simple and intuitive, yet you want to feel confident that video files would not be compromised. A complex, scale-out file-system storage deployment that is finicky and that requires a trained and dedicated person to keep it running is undesirable.

Scalability

Adding more cameras, switching to higher-definition cameras, and responding to longer retention requirements equates to the need for additional storage. Many security and IT professionals don't realize their need for scalability, and often they purchase cheap, file-based storage instead of the enterprise-level block storage, like NetApp® E-Series, that they really need. So, unfortunately, as their organization grows, they either must start from scratch or must bear the accelerating costs of adding onto their "inexpensive" initial storage investment

Low Cost of Ownership

Most security professionals are unaware that there's a huge range in total ownership costs between the different video storage options. File-based systems, which are not optimal for storing video, can easily be 22% more costly than simple, reliable block-based storage systems. This is because block-based storage with its inherent flexibility and versatility and is preferred by leading Video Management System providers.

Many security professionals also fall for the lure of cloud-based storage without realizing how much costlier it will be. Many police departments have had to put their entire body-worn camera program on hold after they discovered that they couldn't afford the cloud storage costs that are associated with their solution. By simply going to a hybrid cloud or to an on-premises block storage solution, they can get their program going again, but not without the significant additional costs of breaking contracts and rearchitecting their solution. SST



Is 5G The Future Of Intruder Alarm Systems?



►► **By: Anna Sliwon,**
Security Analyst,
IHS Markit

The shutdown of the 2G network in the United States in 2017 had a ripple effect on the market for intruder alarms, mostly affecting the sales of control panels and communicator modules. With many traditional systems using 2G or public switched telephone networks (PSTN) as alarm signal communication paths ahead of the shutdown, the impending mobile network re-farming required upgrades to intruder alarm signalling modules. The increased rates of equipment replacements in the immediate run up to the shutdown date resulted in a much smaller replacement market in subsequent years. In fact, according to the latest IHS Markit research on the global intruder alarms market, shipments of control panels sold to the United States market will experience a compound annual decline of 4.9 percent from 2017 through 2022.

Advances in Communication Technologies

Advances in telecommunications technologies are making intruder alarm systems more versatile, by increasing the speed and stability of communications between the sensors, control panels and alarm receiving centers. However, the rate of adoption of the latest communication technologies in the intruder alarm industry has been quite slow.

While 4G connectivity has been available since 2009, 4G communicators were not used frequently with intruder alarm systems until recently. Pockets of data sent from traditional intrusion systems are small, requiring little bandwidth for transmission, but as more devices – especially video cameras – are added to intruder alarm systems, the demands on alarm and signal transmission capacity will also grow. With the promise of 5G offering much higher speeds and connection stability, the technology could open the opportunities for more product and system innovation.

The Role of 5G

Traditional intruder alarm systems have relied on PSTN and General Packet Radio Services (GPRS) communication for signal transmission. With the heightened demand for signal transmission capacity, due to increasing use of video cameras with security systems and the growing number of sensors installed in an average system, an alternative communication path was required: internet-protocol (IP) communication performed that role. While this protocol has been implemented in a vast number of systems around the world, IP connectivity depends on the strength and stability of the internet network supplied to the home or the building. These can be compromised in a number of ways, which is why IP is often used as a back-up communication channel to the primary GPRS channel.

In the world of Internet of Things (IoT) for both residential and commercial applications, devices equipped with 5G-capable chipsets can





offer superior battery life and much lower power consumption in wired systems. This functionality is crucial to reducing overall system maintenance costs, increasing their longevity and guaranteeing signal transmission stability that is far superior to existing technologies. In residential systems, the benefits of longer battery life and improved transmission capability could enable live video verification of intruder alarms on a wider scale. In commercial systems, 5G connectivity could support deployment of smart buildings that aim to improve the environmental footprint of commercial buildings, while delivering the benefits of automation.

5G could accompany cloud technologies in enabling real interconnected environments and to leverage big data. While the cloud has enabled the processing of large data sets from a variety of building and home systems, 5G could greatly speed up the transmission between systems, while improving connection stability. These benefits are particularly important to high-security applications where the costs of unsent or delayed signals could be very high.

Too Early to Tell?

5G is still at a very early adoption and deployment stage. Current global coverage of the 4G network is not universal, as certain countries only have partial coverage. This lack of 4G coverage reduces the popularity of this frequency for alarm communication, since the service offered by 5G-ready equipment may not work.

Significantly higher deployment costs on a national level may lead to postponement of country-wide rollouts, which will make investment in 5G technologies for intrusion systems riskier for manufacturers that do not prioritize 5G in their home markets. International markets may instead offer an opportunity.

5G technology is only beginning to roll out in certain countries, and its full potential has yet to be realized. Any IoT device or a security system equipped with 5G-capable chipsets will likely see a steep price increase, before the technology can become mainstream, like 3G and 4G. For end-users to accept a significant price increase, the comparable functionalities offered by these systems would have to be significantly higher than those currently offered. In the residential sector, these offerings might only resonate with more savvy users of intruder alarm – primarily those who are interested in advanced ultra-smart home security systems. In commercial systems, 5G benefits may be more readily realized in smart buildings that integrate intruder alarm systems with other building systems, or with high-security applications.

5G provides a more capable alternative to 3G and 4G communication paths, particularly for feature-rich systems that integrate video devices. Higher resolution cameras require better bandwidth, before they can send sizeable images through the network. However, transfer of large amounts of data through cellular networks is likely to result in higher data costs to system owners.

The volume of data transferred through 5G networks will be enormous, which has strengthened existing concerns about the cybersecurity of big data and the potential for misuse or breaches.

Opportunity Versus Need

5G could be the technology that offers the best of all available communication technologies to the security industry. However, the regulations covering intrusion systems in many countries require dual-path communication for ultimate confidence in a system's ability to send out alerts of intrusion. In other systems, IP communication has already met the demand for alternatives to cellular technologies. The ultimate test for 5G in intruder alarm systems will be around the question of whether 5G is necessary to accomplish what modern and future intruder alarm systems are capable of. However, embracing the opportunity for innovation, which 5G can offer, could help make future intrusion systems more efficient and capable.

Intruder Alarms & Monitoring Services Database

This study provides an assessment of the intruder alarm and monitoring market, including significant trends over the next five years. The report provides detailed estimates of market revenue and shipments from 2016, with a base year of 2017, and forecasts through 2022. It also estimates the market share of major suppliers in each product category. SST

Video Surveillance Storage: How Much Is Enough?

While digital video surveillance systems offer an embarrassment of riches compared to their analog ancestors, they still require thoughtful design and deployment to ensure maximum cost-effectiveness. Among the various criteria that impact surveillance network video recorder (NVR) system value, storage capacity can be particularly significant and easily misunderstood.

- Higher image resolution
- More active cameras
- Longer archival periods
- Intelligent video recognition

Abundant storage capacity is a fundamental enabler of such capabilities, and it is here that some video surveillance deployments can go amiss. In an effort to minimize costs, some NVR systems may utilize multiple low-cost, low-capacity hard disk drives (HDDs) to meet their storage requirements. On its surface, this approach appears to be a viable option to reduce storage expenditures.

In conventional computing environments, hard drive capacity is typically viewed only in quantitative terms; how much data can the storage system hold? But in the context of NVR solutions, drive capacity plays a key role in determining both the quantity and quality of data that the system can store.

Because 24×7 video streams are the very lifeblood of NVR systems, to deliver superior performance and efficiency in a given security environment, these systems must have sufficient storage capacity to address three fundamental video parameters:
Quantity—the number and time duration of the video streams
Quality—the image quality of the video streams, expressed in terms of frame resolution (for example, 1280×1024 pixels) and frames per second (fps)
Archiving—the length of time the video streams will be stored.

Video Balancing Act

Once the specific balance of video data quantity, quality and archiving required for a given security application is determined, it's easy to estimate the amount of storage capacity a NVR system must include. Simply go to one of the video surveillance storage matrix tables to select the table row that lists the frame resolution and fps needed for each 24×7 video stream, then read across to find the nearest desired archival period (shown in days) and the corresponding drive capacity required for each individual stream.

Note: Table 1 reflects MPEG-4 compression, while Table 2 reflects the H.264 encoding; results will vary depending on video compression formats and specific video recording applications used.

The tables show the enormous variation in the hard drives recording capacity based on a 24×7 video streams resolution and frames per second. Also refer to our Surveillance Storage Calculator that takes in account additional variables like video quality,



NTSC: Recording Variable: 10fps			Surveillance Hard Drive Capacity					
			1TB	2TB	3TB	4TB	5TB	6TB
176 x 120	Low Quality	# Days	694	1388	2082	2776	3470	4164
352 x 240		# Days	266	532	798	1064	1330	1596
704 x 480		# Days	86	172	258	344	430	516
1280 x 1024	High Quality	# Days	26	52	78	104	130	156

NTSC: Recording Variable: 20fps			Surveillance Hard Drive Capacity					
			1TB	2TB	3TB	4TB	5TB	6TB
176 x 120	Low Quality	# Days	346	692	1038	1384	1730	2076
352 x 240		# Days	132	264	396	528	660	792
704 x 480		# Days	42	84	126	168	210	252
1280 x 1024	High Quality	# Days	12	24	36	48	60	72

NTSC: Recording Variable: 30fps			Surveillance Hard Drive Capacity					
			1TB	2TB	3TB	4TB	5TB	6TB
176 x 120	Low Quality	# Days	230	460	690	920	1150	1380
352 x 240		# Days	88	176	264	352	440	528
704 x 480		# Days	28	56	84	112	140	168
1280 x 1024	High Quality	# Days	8	16	24	32	40	48

Table 1. Video Surveillance Storage Matrix (assumes MPEG-4 encoding)

NTSC: Recording Variable: 10fps			Surveillance Hard Drive Capacity					
			1TB	2TB	3TB	4TB	5TB	6TB
176 x 120	Low Quality	# Days	1080	2160	3240	4320	5400	6480
352 x 240		# Days	414	828	1242	1656	2070	2484
704 x 480		# Days	134	268	402	536	670	804
1280 x 1024	High Quality	# Days	40	80	120	160	200	240

NTSC: Recording Variable: 20fps			Surveillance Hard Drive Capacity					
			1TB	2TB	3TB	4TB	5TB	6TB
176 x 120	Low Quality	# Days	540	1080	1620	2160	2700	3240
352 x 240		# Days	206	412	618	824	1030	1236
704 x 480		# Days	66	132	198	264	330	396
1280 x 1024	High Quality	# Days	20	40	60	80	100	120

NTSC: Recording Variable: 30fps			Surveillance Hard Drive Capacity					
			1TB	2TB	3TB	4TB	5TB	6TB
176 x 120	Low Quality	# Days	360	720	1080	1440	1800	2160
352 x 240		# Days	138	276	414	552	690	828
704 x 480		# Days	44	88	132	176	220	264
1280 x 1024	High Quality	# Days	14	28	42	56	70	84

Table 2. Video Surveillance Storage Matrix (assumes H.264 encoding)

compression type and number of operational hours per day. With so many security applications entailing dozens of cameras and 24×7 video streams, it soon becomes apparent that a typical NVR systems storage requirements can easily reach beyond +10TB.

In the following three examples, the varying video profiles of different security environments (and the storage capacities they require) are compared.

Example A: Extended Archiving

There are many businesses (point-of-sale and retail, restaurants, banks, and so forth) where high-resolution, full-motion 24×7 video streams are simply overkill. Typically employing a modest number of fixed cameras to record customer activity, NVR solutions in these environments are able to employ lower image resolution and fewer frames per second while still delivering sufficient video detail for subsequent review as needed.

When the quality of an NVR systems 24×7 video streams can be relatively low, the benefits of greater HDD capacity come from enabling longer archival storage. Archive periods can be economically extended from a select number of days to months, or even years; indeed, continuous video signal at 10fps/352×240 resolution can be streamed onto a 6TB drive for 1596 days with MPEG-4 compression and an astounding 2484 days with H.264 encoding (refer to Table 1 and Table 2).



Example B: Enhanced Quality

Environments with more stringent security requirements (for example, schools, public buildings and airports) rely on 24×7 video streams with higher resolution and more frames per second to better identify suspicious persons and activity. Coupled with broader camera deployment, the enhanced video quality of such streams gives security personnel a more detailed, comprehensive view of the areas under surveillance.

Not surprisingly, the higher resolution and frame rates of such 24×7 video streams can significantly increase the capacity requirements of the SDVR system. As shown in Table 1, just one continuous video stream at 20fps/704×480 image resolution can fill a 1TB drive in only 42 days with MPEG-4 compression. Table 2 shows how H.264 encoding extends video storage in this scenario to 66 days. Multiply that by the dozens of 24×7 video streams that such NVR systems typically employ, and the need for massive storage capacity quickly becomes clear.

Example C: Intelligent Video

Designed for maximum-security surveillance environments, intelligent video takes full advantage of the exceptional detail found in high-resolution, full-motion (30fps) 24×7 video streams to recognize visual patterns. The best-known use of this technology is facial recognition; intelligent software analyzes objects, behaviors and even, in some cases, faces in stored surveillance footage, comparing the video to known risks that the system is trained to identify. When a match is found, the application automatically notifies security personnel for follow-up investigation.

These high-resolution, full-motion 24×7 video streams deliver superlative visual quality, but do so at a price; they consume vast quantities of storage capacity. The tables show the voracious nature of such streams. Using MPEG-4 compression, a single continuous stream at 30fps/1280×1024 resolution fully exhausts the capacity of a 6TB drive in just 48 days, while H.264 encoding delivers approximately 84 days of the same quality video. If AI data is collected simultaneously alongside the video, this will also incrementally increase storage usage and should be accounted for.

Conclusion

Boasting an unprecedented blend of visual detail and storage capacity, network video recorder systems are spearheading a new era of surveillance effectiveness and flexibility. Purpose-built surveillance drives are key enablers of this revolution, storing enormous quantities of video data at remarkably low cost per GB. The result is surveillance systems that can seamlessly accommodate the unique image quality and extended archival needs of modern security environments.

Article courtesy of Seagate: https://www.seagate.com/sg/en/tech-insights/how-much-video-surveillance-storage-is-enough-master-ti/

Seagate's Surveillance storage calculator: https://www.seagate.com/sg/en/video-storage-calculator/ SST

Top 3 Cloud Security Trends For 2019

►► By: Synopsys Software Integrity Group

As 2019 hits the halfway mark, the top three cloud security trends from previous years continue. In fact, they've grown. A survey of the 400,000 members of the Cybersecurity Insiders information security community explored what's top of mind for these predominantly senior-level managers in IT security and IT operations:

- The top cloud security concern is data loss and leakage (64% of respondents).
- The most challenging part of cloud compliance is monitoring for new vulnerabilities in cloud services (43%).
- The biggest barrier to cloud adoption is data security, loss, and leakage risks (29%).

Public Cloud Security, Confidence, and Concerns

Top cloud providers AWS, Microsoft Azure, and Google Cloud should take note: Cloud security is a huge concern for cyber security professionals. The vast majority, as revealed in the 2019 Cloud Security Report, are moderately to extremely concerned. And they have every reason to be, faced with an upward trend in cloud security incidents, including high-profile data breaches, and the OWASP Top 10 now including a category for components known to be vulnerable.



Paradoxically, most respondents also reported being at least moderately confident in their organization's own cloud security posture. It's hard to reconcile this level of confidence with the challenges listed in the report. Do cyber security professionals think the problems trending in cloud security only apply to the other guys?

The top cloud security concern is data loss and leakage (64%), followed closely by data privacy and confidentiality (62%). But cyber security professionals have other cloud security issues on their minds too. Compliance, accidental credentials exposure, and data control are also high on the list of trending cloud security concerns.

Challenges of Cloud Compliance

Ask anyone who has ever had to deal with software standards compliance for HIPAA, PCI DSS, GDPR, or other rules and regulations concerning software security or data privacy. They're likely to tell you that monitoring for new vulnerabilities is one of their greatest challenges. Likewise, the 2019 Cloud Security Report notes that monitoring for new vulnerabilities in cloud services is trending as the No. 1 cloud compliance challenge (43%). Following closely are surviving audits and risk assessments and monitoring for ongoing compliance.

Another cloud security trend relates to the inexorable migration of applications to the cloud. Specifically, organizations think it's important to maintain continuous compliance when transitioning on-premises workloads in containers or virtual machines (VMs) to the cloud. Only 5% of cyber security professionals disagreed.

Barriers to Cloud Adoption

Regarding barriers to cloud adoption, the current trend doesn't present itself as one specific security obstacle, or even two. Cyber security professionals profess that data security, loss, and leakage risks are the top impediment to cloud adoption (29%). But an almost equal number of respondents mentioned general security risks (28%), and budget issues, compliance, and staffing were close behind. SST

How To Secure Cloud Apps: The Ultimate Guide



▸▸ **By: Steve Cohen,**
Security Services Manager,
Synopsys Integrity Group

The advantages of the cloud are well-documented yet concerns about security remain the primary reason more organisations haven't completely adopted it. When surveyed, security professionals say that their biggest security concerns about public clouds are:

- Assessment and management of security and compliance risks
- Misconfiguration of the cloud platform
- Unauthorised access
- Unsecure interfaces and APIs

Public cloud providers like Amazon Web Services (AWS) have revolutionized the way organizations build, deploy, and operate their applications. But in migrating to the cloud, to ensure the security of their software, firms need to adapt to this new development landscape and its associated security risks.

So how should development teams approach application security in the cloud? In short, organisations must manage risk by injecting security at the velocity of development. They must extend testing for security vulnerabilities beyond the applications themselves to the underlying infrastructure stack; bottom line organisations must more tightly integrate security testing within development workflows.

Overall, cloud security translates to three key areas:

1. Development teams want to minimize security risk by utilizing baseline security controls that can guide them in building or deploying cloud applications.
2. DevOps teams want to ensure that containers are secure and are composed of secure open source software in every layer.
3. Compliance and Security Auditors want to accelerate cloud infrastructure deployments with environments that meet regulatory and compliance requirements, all while supporting the needs of development teams.

Gartner notes that in the near future, at least 95% of cloud security failures will be the customer's fault. This is in part because of the shared responsibility model, which can be thought of as a line in the sand where a cloud service provider's (CSP) responsibility for security and compliance ends and the customer's begins.

The first step in securing your cloud apps is to know what your responsibilities are.



Image by: Freepik.com



Understand Your Role in Securing Your Infrastructure

Once you understand your security obligations relative to your cloud model, you should examine the underlying infrastructure of your cloud deployment for weaknesses. Determine if cloud security controls are configured securely. An architect with an understanding of security controls and frameworks can perform a cloud architecture risk analysis to help you design a system that lowers your risk of a security breach. And a skilled security expert can perform threat modelling to model real-life scenarios with annual business logic testing to help you address those vulnerabilities.

These are the best practices for securing your cloud architecture:

1. Keep IT up-to-date with current cloud security practices.
2. Utilize infrastructure as code to establish secure reference architectures with baseline security controls to address security, compliance, and regulatory requirements.
3. Always implement a least privilege access control model to prevent unexpected access to your cloud resources.
4. Implement security in containerized and microservice based environments.
5. Use your software security tools and the security features of your CSP.

Prepare Your Applications For The Jump

The tight coupling of complex customer-cloud interactions with an application means that security implications vary widely from platform to platform and from app to app. Chances are your legacy applications and workloads were not built with the cloud in mind. When you move to the cloud, your organisation is exposed to new classes of vulnerabilities you might not have considered.

Even if you're developing cloud-native applications, it's critical that you keep performing these standard AppSec activities:

- Static application security testing (SAST) analyses source code to identify vulnerabilities during development.
- Software composition analysis (SCA) detects third-party open source components in source code and binaries.
- Interactive application security testing (IAST) performs runtime code analysis through instrumentation during QA and functional testing.
- Dynamic application security testing (DAST) allows you to conduct penetration testing in running applications.

Maintain A Strong Cloud Security Posture

Organizations must understand the distributed nature of modern systems, start with and maintain secure builds, and begin to practice the principle of least privilege, especially when it comes to the application workloads within the cloud. Automation and orchestration will help organisations build fast and deliver continuously, but they can make managing security a challenge. Using cloud security controls effectively and building security into the continuous integration (CI) pipeline in your cloud development environment gives you the visibility, agility, and speed you need for fast, continuous delivery. As you continue to use the cloud, you must focus on developing a mature cloud software security approach. SST

Tailored And Secure IP Video Solution



▸▸ By: Christian Jourdan,
Video Security Expert,
Konica Minolta Business Solutions Deutschland GmbH

Companies often install video systems without being aware of their impact on the corporate network. This is because a camera with a high resolution produces a very large amount of data. If the corporate network is not designed for this, performance or stability problems can quickly occur because the performance is insufficient. At the latest when several video cameras are integrated, the existing network often reaches its limits.

What are my goals?

For this reason, companies should first consider very carefully what goals they are pursuing with the integration of security cameras. Do I really need high-resolution images that can be used later in court, to identify a license plate, or to automatically control access to the company premises? Or is a lower image resolution completely sufficient to provide the necessary information with sufficient quality under the ambient and lighting conditions both day and night? In such an application, an IP camera with a resolution of 4K would be overkill.

Video solution is part of the overall system

At the same time, organizations must be aware that an IP video system is part of the overall system and must be integrated into the corporate network, especially if the information generated is to be used within the production systems. Therefore, before integrating a video solution, it should be checked whether the productive network is designed for the implementation, including the associated new specific requirements. Otherwise, a parallel network must be set up that ensures both network separation and the required performance.

Protecting Video Infrastructure From Unwanted Access

All video systems must also be installed in such a way as to not be in the direct access area of outsiders. Otherwise it would be easy for criminals to switch the camera off or




Image by: Freepik.com

manipulate it. The same of course applies to digital remote access. Therefore, the video systems should have integrated backup and configuration tools. This includes end-to-end data encryption during transmission. Video data is often inadequately protected. Especially low-cost systems usually have no basic protection or serious security gaps in their operating system. As a result, cybercriminals are able to penetrate the Local Area Network (LAN) with simple means and access data. This can have far-reaching consequences. This allows the cameras to be deactivated or other settings to be made via remote control. This endangers all users working in the corporate network. In addition, the devices themselves can be compromised and made part of a botnet, as in the case of Mirai or IoTroop.

GDPR-Compliant Data Storage

When setting up video security, data protection aspects must also be taken into account. Which areas should and may be monitored? How long is data stored? Who has access to the data? The General Data Protection Regulation (GDPR) provides very clear rules for action here. Companies are required to delete data that is no longer relevant. This archiving process can be automatically controlled with a high-quality IP video solution. As soon as a previously defined point in time is reached, the recordings are then automatically overwritten. At the same time, organizations must protect all data by assigning individual access rights. For example, the gatekeeper only needs access to live images, while other employees also need access to archived recordings.

Specialized IT Service Providers Deliver Tailor-Made Solutions

Since there are many aspects to creating and implementing the right concept, companies should seek the support of specialized IT service providers such as Konica Minolta. They use consulting workshops to show their customers the options offered by IP video systems. In addition, they work with them to develop operational requirements and acceptance criteria, as well as an appropriate concept.

Such specialists take over all necessary operational tasks as well as maintenance and ensure the video security system's continuous availability. With custom-fit cameras, integrated backup and configuration tools and some basic security measures, companies ensure that they reliably get exactly the images they need. And at the same time, they reduce the attack surface for hackers. SST

What is Zero Trust Security? And Why Should You Care

▸▸ **By: Dana Katz,** Product Marketing Manager, Security Platforms, Check Point Software Technologies

Today, workers no longer have to set foot in the office building to come to work. Advancements in technology have expanded what is now classifies as "the office," with companies able to interface through mobile devices and cloud software regardless of where their employees are located.

However, these developments pose a cybersecurity dilemma. The security perimeter is no longer confined to the walls of an office building. Valuable business data transfers continuously between SaaS applications, IaaS, data centers, remote users, IoT devices, and more. Which means cyber-criminals have access to wider attack surfaces and more points of entry than ever before. As evidence, in 2018, 34% of cyber-attacks were perpetrated by insiders.



To complicate matters even more, once these cyber-criminals are inside one's business' perimeter, they seek and steal valuable and sensitive data for months before being detected. In fact, in most cases, it takes six months to detect a data breach.

Alarmingly, most incumbent security infrastructures are generationally outdated and dangerously behind the level of attacks they must protect against. Clearly, it's time for a new security paradigm.

The Zero Trust Security Approach

Across the industry, security professionals are shifting to a Zero Trust Security state-of-mind: No device, user, workload or system should be trusted by default, regardless the location in which it is operating from, neither inside or outside the security perimeter.

The Forrester Zero Trust Extended Security Model

Zero Trust is more than just a concept. The Zero Trust Extended Security model, introduced by Forrester analysts, offers seven key principles of implementation that organisations should focus on when moving toward a Zero Trust security model. Implementing these principles enable the adoption of a security posture of "Default Deny" where systems are hardened and isolated until a level of trust is established.

These principles are:

Zero Trust Networks

When moving toward Zero Trust Security, it is crucial to "Divide and Rule" one's network. Identifying the valuable assets and defining "Micro-segments" around them create multiple junctions and inspection points that block malicious or unauthorised lateral movement, so that in the event of a breach, the threat is easily contained and isolated.

Zero Trust Workloads

Securing workloads, particularly those who are running in the public cloud, is essential since these cloud assets (e.g., containers, functions, and VMs) are vulnerable and attractive targets to malicious actors.

Zero Trust Data

Zero Trust is all about protecting the data while it is shared continuously between workstations, mobile devices,

Zero Trust is all about protecting the data while it is shared continuously between workstations, mobile devices, application servers, databases, SaaS applications, and across the corporate and public networks.

application servers, databases, SaaS applications, and across the corporate and public networks.

Zero Trust People

With 81% of data breaches involving stolen credentials, it is clear that username and passwords no longer prove the identity of a user. Identities are easily compromised, so access control to one's valuable assets must be strengthened.

Zero Trust Devices

With 70% of breaches involving compromised devices, every device connected to one's network should be treated as a threat vector, whether it's a workstation, a mobile, or an IoT/OT device. Security teams must be able to secure every device on their network and isolate it if compromised.

Visibility and Analytics

One can't protect what can't be seen or understood. A Zero Trust Security model continually monitors, logs, correlates, and analyses every activity across one's network.

Automation and Orchestration

A Zero Trust Security architecture must automatically integrate with the organisation's broader IT environment to enable speed and agility, improved incident response, policy accuracy, and task delegations. SST



Intrusion Market Trends: Where Do We Go From Here?



▸▸ **By: Ross Wilks,**
Head of Marketing
Communications, Vanderbilt

For many organizations across the world, intrusion alarms and detection are at the center of their focus for establishing a comprehensive security plan. And the numbers support this: The European perimeter intrusion detection systems market alone is set to see growth at a rate of 15.7 percent annually through 2024, due in part to the growing demand for video surveillance, remote access via the cloud and wireless technology to help enhance security systems.

Additionally, Global Market Insights reported a hike from $3 billion in 2018 to $8 billion by 2025 in the intrusion detection/prevention system market, attributed to the growth in IT data breaches and security threats, rising demand for enterprise mobility and stringent regulations established by government to safeguard data.

As demand grows, manufacturers are tasked with developing products and solutions that meet a wide number of needs within the physical security market. But there are significant trends in the intrusion prevention/detection market that persist and are emerging today across the globe:

Trend 1: The Cloud

Perhaps the biggest trend across the security industry — and especially for intrusion — is the increased adoption of cloud-based systems as a means to achieve comprehensive and flexible protection for an organization. The benefits speak for themselves: remote alarm management, more connectivity and a greater ability for operators to streamline security operations. A number of manufacturers now offer cloud-based Security-as-a-Service solutions that give end users flexibility and interconnectivity. More and more investments are being made not only in cloud-based intrusion, but also access control, following the demand these companies are seeing in the market today for these kinds of solutions.

Trend 2: Product to Service Focus

While a continuing trend, the security industry is seeing a big shift away from manufacturers being solely product-focused to being able to offer solutions that support customers working as a service-based company. And there are many businesses moving in that direction. This encompasses the idea that today's organizations want more long-term partnerships rather than "one-and-done" purchases with no real value in continuing the relationship. Some might argue that security in general has typically been more service-based, but this trend is really taking off as one of the major developments in recent years.

Trend 3: Increased Connectivity

Within intrusion and beyond, there's certainly a trend toward all devices becoming smarter, interoperable and interconnected, and the industry can look toward the focus on the Internet of Things (IoT) as the source. Customers demand the ability for their intrusion detection system to work seamlessly with and talk to their access control, fire detection and video management systems in an effort to implement an integrated security solution. Customers who are looking to do more with their systems are demanding this level of connectivity to maximize the investment being made. This trend is set to continue as more and more integrations are made possible from various manufacturers and systems.

Trend 4: More Communication

With increased levels of connectivity comes the demand by customers to enhance communications across devices and teams. There are a number of new wireless initiatives being made across the industry that are designed to bring two-way communication to the forefront through a cloud-based system that utilizes the same interface but can be programmed either onsite or remotely. This will be a powerful tool for installers that has already begun to roll out, but will have additional functionality introduced in the coming year. It is part of a



The Internet has remarkably revolutionized the way technology is used, allowing us to create an extension of systems and processes that once required a plugged-in setup to our mobile devices. The ability to remotely manage and monitor a facility is paramount to the kind of flexibility that end users want today, combining ease of use, efficient response abilities and centralization to deliver higher levels of situational awareness.

concerted effort to push as much information out as possible, including more support from installers and dealers for end users, more videos that provide guidance for usage and setup, and the integration of our products through web-based training.

Trend 5: Remote Management and Monitoring

The Internet has remarkably revolutionized the way technology is used, allowing us to create an extension of systems and processes that once required a plugged-in setup to our mobile devices. The ability to remotely manage and monitor a facility is paramount to the kind of flexibility that end users want today, combining ease of use, efficient response abilities and centralization to deliver higher levels of situational awareness. For example, any time an intrusion alarm goes off, remote monitoring and management make it possible to investigate the alarm from anywhere, any device and at any time. This makes response times faster, allowing greater protection for facilities.

From the cloud to interconnectivity and increasing communication to service focus, demand for intrusion solutions that deliver more for customers is rising. As the physical security industry continues to grow across the globe, security professionals must look toward the future to build comprehensive security solutions to keep their organizations safe from rising threats. Through continued innovation and research, along with the goal to achieve higher levels of interconnectivity, this will be made possible. SST

Dahua Technology Provides New Solution for Thefts from Boats at Yarmouth Harbour



The Yarmouth Harbour in the Isle of Wight consists of a large marina, docks for the Wightlink Ferry terminal, and pontoons and boat moorings upstream.

Following a number of thefts from boats and boat fires in neighbouring harbours, a new solution – including a thermal imaging capability – was specified. The previous system that was installed was becoming outdated, with poor picture quality and cabling issues. Thus, a video surveillance system with around 40 IP and thermal cameras from Dahua Technology was installed at the harbour.

Thermal and Lighting Sensitive Technology

The Dahua cameras come in various forms, they are a mix of thermal bullets, IR bullets, Ultra PTZs, IR domes and fisheye cameras. The thermal cameras are especially suited for wide area outdoor video surveillance and are especially ideal for the large, water-based environments at the harbour. The cameras feature Vox uncooled thermal sensor technology and high thermal sensitivity at less than 40mK, enabling them to capture more image details and temperature fluctuations. With a built-in fire detection functionality, the cameras provide an extremely sensitive fire alarm system.

The IR bullet cameras feature highly efficient H.265 encoding technology, PoE and IR illumination at up to 50 metres, as well as a wide dynamic range, providing vivid images even in the most intense contrast lighting conditions and delivering powerful day or night surveillance in a compact package.

Images Communicated to Control Room

Images are transmitted wirelessly back to a control room at the main harbour office. In the event that the control room is not staffed, Yarmouth Harbour can nominate individuals to receive alerts and images on their tablets and smartphones via the Dahua surveillance app.

Not only is the surveillance security of the harbour itself covered, the system also covers the adjacent Yarmouth pier, a Grade II listed structure said to be the longest wooden pier in the UK and recently refurbished. Automatic people-counting technology has been incorporated into the cameras at the pier's entrance to monitor numbers on the pier as a health and safety measure.

Benefits of the Camera

"The new surveillance system has transformed our ability to monitor the harbour for the safety and security of our customers, staff and the visiting public," said Dave Rice of Yarmouth Harbour Commissioners. He also notes that the HD picture quality allows the capturing of the perpetrators' faces, which is incomparable to the with the previous cameras. The system has also proved straightforward to use. SST



Senstar LM100 Hybrid Perimeter Intrusion Detection And Intelligent Lighting System

Combining two key security functions in one cutting-edge product, the Senstar LM100 acts as a powerful deterrent against intruders, detecting and illuminating them at the fence line while alerting a security management system (SMS).

The Senstar LM100 provides localized, uniform, configurable lighting along the fence line and is the only security lighting system on the market with dimming capabilities. It can be set at any lighting level required – from 1%, providing enough of a slight glow at the luminaire's head to let intruders know a system is in place, to 100%.

Optimized for security cameras, uniform light coverage allows cameras to operate with a higher dynamic range, ensuring objects and people are illuminated while avoiding the generation of dark silhouettes in front of bright backgrounds. This high color rendering (CRI) index maximizes camera performance, providing clearer images of the intrusion attempt and allowing security personnel at the monitoring station to better assess the situation and initiate an appropriate response.

While the lighting acts as an initial deterrent, if an intruder persists and an attempt to cut, climb or otherwise break through the fence is detected, the closest luminaire brightens to its alarm level lighting and/or strobes while an alert is sent to the security management system. The intruder knows immediately they have been detected and that their exact location is known by security and others in the vicinity.

By combining lighting, sensing and communication technology, the Senstar LM100 system can be used to alert security systems of impending threats while mitigating false environmental triggers on a system level.

Senstar has been a leader in perimeter security for close to 40 years, serving a variety of markets including corrections, energy and industrial, military, oil and gas, transportation, and manufacturing and logistics. With intelligent video management, video analytics, access control, and innovative perimeter intrusion detection systems, Senstar offers a comprehensive suite of proven, integrated technologies that reduce complexity, improve performance and unify support. SST

SIEMENS LAUNCHES SPEECH-BASED ALARMS FOR FASTER EVACUATION





Siemens Smart Infrastructure has launched new ceiling- and wall-mounted alarm devices. The expanded portfolio includes both acoustic and optical alarm devices in accordance with European Standards EN 54-3 / EN 54-23 and EN 54-17. One highlight of the expanded portfolio are the voice sounders with built-in voice messages because they improve the reaction time to alarms.

The new products address evolving market developments for close integration of voice alarms with fire protection systems. Experience has shown that in the case of a fire or another dangerous situation, a simple alarm tone is often not observed but instead misinterpreted as a false alarm or as a drill. As a result, the persons who need to be warned either don't react or react belatedly. Speech-based alarms keep evacuation times as short as possible and minimize the risk to people.



The sounders feature 16 integrated tone patterns and three different sound levels (Min/Mid/Max), with the highest sound pressure being 99 dBA. The voice sounders have the same features as the sounders, but in addition contain messages that can be emitted in two languages along with an attention tone. In total, 15 languages are available in five pre-defined message categories: fire evacuation, emergency evacuation, alert, test and all-clear.

The tone and voice messages are compliant with EN 54-3 and synchronized in an audible area and across all loops of a panel. Voice messaging, especially if it is in two languages, improves the reaction time, particularly for people who are not familiar with the building. Beyond the standard offering, the portfolio includes customized devices where any languages, message categories and tones can be incorporated.

The optical alarm devices feature three beacon settings in accordance with EN 54-23, which can be tailored to different room sizes and detector coverage areas. They have an extra setting that supports the use of the device with supplementary optical indication to save power. In addition, they are designed for use in system extensions and modernizations. All devices are addressable, loop-powered, and available with red and white LEDs.



To improve evacuation performance, a shorter pulse length with higher illumination is built into the beacons because studies have shown that this combination increases awareness in the case of an alarm. Beacons with these features are especially valuable in areas with loud ambient noises where acoustic signals are easy to miss. In addition, they help reach people who are hearing-impaired, wearing ear protection or using headphones.

Going a step further, Siemens increases the reliability of its alarm devices through daily disturbance-free self-tests of the electrical circuit, loudspeaker and light source. Very low levels of sound and light are emitted during testing so as not to disturb occupants. On a system level, the fire control panel can silently activate all alarm devices. The test results show if the power is sufficient for each alarm device, or if there is an overload or a wiring problem on the loop.

Following the standard for all Siemens fire safety peripherals, the alarm devices have an outstanding recovery time in compliance with EN 54-17. In case of a short circuit on the loop, the integrated line separator ensures that the alarm devices continue to work under any condition. SST

BUILDING SMART AUTONOMOUS VEHICLES WITH LIDAR TECHNOLOGY







Velodyne Lidar, Inc. and Idriverplus are one of the first companies in China to launch the commercialization of driverless technology and realize mass production, is using Velodyne's ground-breaking lidar sensors in a range of autonomous driving products. Velodyne has strategically teamed with Idriverplus to help Idriverplus with its efforts for mass production of commercial autonomous vehicles, which include street cleaners, passenger cars, and logistics vehicles.

The lidar sensors are being used in all Idriverplus self-driving vehicles, providing rich computer perception data that allows real-time object and free space detection needed for safe navigation and reliable operation.

"We have a vision for the future that autonomous driving is not only a means of transportation, but also a necessity of life," said Idriverplus CEO Dr. Zhang Dezhao. Lidar is indispensable in our development of autonomous driving technology as it ensures that the that the car is performing and stable while accurately addressing the necessary requirements.

> **"WE HAVE A VISION FOR THE FUTURE THAT AUTONOMOUS DRIVING IS NOT ONLY A MEANS OF TRANSPORTATION, BUT ALSO A NECESSITY OF LIFE."**
> - Dr. Zhang Dezhao

The Idriverplus street cleaning vehicle, called Viggo, is an unmanned, purely electric solution to intelligently sweep roads. During the cleaning process, Viggo can automatically track and avoid obstacles with stable and reliable performance and monitor real-time vehicle information. More than 100 units are in operation in universities, factories, parks, an amusement park and city streets with deployments in Beijing, Tianjin, Shanghai, Hebei, Zhejiang, Henan, Hunan and other provinces and cities. Idriverplus also has strategic cooperation partnerships in Singapore, Dubai, Malaysia, and other areas in Asia.

Idriverplus is developing two commercial autonomous car solutions. An SAE Level 4 vehicle that provides autonomous driving in closed parks and some public roads, and an advanced driver assistance system (ADAS) solution for automatic parking (AVP) and highway follow-up (HWP). Its product applies self-driving technology to the logistics industry, providing a safer and better distribution experience. The driverless vehicles have accumulated test mileage exceeding 400,000 kilometres, far surpassing other domestic autonomous vehicle manufacturers.

Idriverplus is trailblazing the commercialization of driverless technology in China. It proves how Velodyne intelligent lidar sensors are enabling companies to place autonomous vehicles on the road today. They are transforming multiple service sectors by creating powerful autonomous driving solutions. SST

Netamo Unveils Its Smart Video Doorbell

With the Smart Video Doorbell, the user knows who is ringing their doorbell at any moment. The user can see the visitor on their smartphone and speak to them and respond immediately when when they are not at home. The Netatmo Smart Video Doorbell also immediately alerts the user if it detects people loitering around the house. It is the first doorbell compatible with Apple HomeKit that can be controlled using the Apple Home app or by voice using Siri.

"The Smart Video Doorbell is the best response to the growing need for solutions to secure the home entrance," says Fred Potter founder and CEO of Netatmo. As with the other products the Smart Video Doorbell is in compliance with essential principles to guarantee the best smart home experience possible; it is a useful and reliable product, which ensures the users' data protection.

Netatmo's Smart Video Doorbell won an award in the "Home Appliance" category at the prestigious CES 2019 Innovation Awards.

Respond to Visitors from Anywhere

With the smart doorbell, the user knows who has come to see them, wherever they are. When a visitor rings the doorbell, the user receives a video call on their smartphone and sees the visitor. They can choose to speak to them – or not – and immediately respond remotely from their smartphone whether they are at home, in the office or on the other side of the world.

The user can thus tell the delivery person where to leave a package when they are at the office, turn away salespeople without having to open the door, or welcome guests while preparing dinner.

Enhanced Security Outside the Home

Netamo's Smart Video Doorbell protects the home from intruders and helps the user feel safe in the event of an y suspected activity. Thanks to the people detection, the user knows in real time if someone is lurking around the front of their home. A precise "Person Detected" notification is received on their smartphone and a video of the event is recorded.

Using the built-in microphone and speaker, the user can speak to the intruder to deter them from approaching their home.

For added protection, the Security app alerts the user immediately on their smartphone when someone attempts to deactivate the doorbell or remove it from the wall.

Fully Customisable Smart Notifications

The smart doorbell settings can be fully customised. The user can switch off notifications and recordings according to their preferences. They can decide whether the doorbell sends them a notification and records a video when someone is detected.

The user can also set specific alert zones, for example around the main path. The smart doorbell then only notifies the user when something occurs in these zones.

Exceptional Image Quality for Protection Day and Night

The smart doorbell has a 1080p Full HD camera with a large 160-degree wide angle lens giving optimum video quality. The camera's HDR function adjusts to sudden changes in light and allows the user to clearly see what is happening in front of their home whatever the lighting conditions. This means that visitors' faces will be clear even against the sunlight.

The home would also be protected day and night using infrared night vision. The user can always see the visitor at their door, even in total darkness.

Easy Installation

It is easy and quick to install and does not require professional help. It simply replaces an existing doorbell and connects to the home Wi-Fi. It requires a wired doorbell to work. The smart doorbell is compatible with all electrical installations, from 8-24 volts up to 230 volts.

The user can access the Netatmo Security app on their smartphone, tablet, PC/Mac or Apple Watch. Through the app, the user can access all functionalities of the smart doorbell: specific notifications, access to livestream, call and event history, recording and storage of HD videos.

The Smart Video Doorbell comes with video storage. They are saved locally on an internal micro-SD card and can be automatically transferred and archived on the user's Dropbox account or personal FTP server. In order to ensure a secured transmission of data to the user's smartphone, the smart doorbell uses end-to-end encryption, guaranteeing the highest level of protection. SST



Homeland Security Market to Reach $418 Billion, Globally, by 2022

The Homeland Security Market research report published by Allied Market Research. Homeland security market is expected to garner $418 billion by 2022, registering a CAGR of 5.9% from 2016 to 2022. The cyber security segment is expected to dominate the global market throughout the forecast period. North America is expected to be the leading contributor to the global revenue during the forecast period.

Growing instance of terrorist attacks, wars between neighbouring countries, domestic wars due to political unrest, communism, riots, and others have fostered the adoption of homeland security solutions. In addition, increasing number of natural as well as man-made disasters including earthquakes, floods, cyclones, fire, industrial hazards, rail accidents, plane crash, and others are expected to drive the market. However, lack of awareness and high installation cost of technological advanced products and services of homeland security restrict the market growth. The development of technologically enhanced products, such as unmanned vehicles and terahertz radiation (T-ray) for detecting chemical composition of objects, robots for automation, executing human tasks, and others would provide numerous opportunities for the growth and development of the homeland security market.

> *"The homeland security market in Asia-Pacific region is projected to grow at significant rate during the forecast period, owing to increasing number terrorist activities, territorial wars, political unrest, protests, and government inclination towards police modernization in countries including India, Japan, China, and Sri Lanka."*
>
> *– Puja Mourya, Research Analyst, Aerospace & Defense*

In 2015, cyber security accounted for the maximum revenue share in the overall homeland security market, due to increasing threat of cyber terrorism, cybercrime, and internet fraud. Increasing trend of bring-your-own-device (BYOD), Internet of Things (IoT), web deployment, trends, cloud services, and big data analytics that need enhanced security provide huge growth opportunities to the cyber security market. In addition, the critical infrastructure segment is



presently the fastest growing segment, and is projected to grow at a CAGR 7.2% during the forecast period, owing to proactive government initiatives for protecting critical infrastructures in areas such as telecommunication, power plants, oil & gas, defence, financial & security services, manufacturing, and others.

North America accounted for majority of the global market share in 2015 and is expected to maintain its dominance during the forecast period due to heavy investment by government organizations in homeland security in the region.

Key findings of the Homeland Security Market

- In 2015, cyber security segment dominated the overall homeland security market in terms of revenue and is projected to grow at a CAGR of 4.3% during the forecast period.
- Critical infrastructure security segment is projected to grow at the highest CAGR of over 7% during the analysis period.
- Public end user segment is projected to generate the highest revenue in the market during the forecast period.
- In 2015, North America generated the highest revenue among all regions in the global homeland security market.
- Asia-Pacific is expected to grow at a CAGR of 7.2% from 2016 to 2022.

IBM Corporation, Lockheed Martin Corporation, General Dynamics Corporation, and Northrop Grumman Corporation are some of the prominent players in the market. Market players have focused on product launch and partnership for expansion in the market. For instance, in June 2016, IBM partnered with the GW Center for Cyber and Homeland Security, an organization for research and analysis on homeland security, counterterrorism, and cyber security issues in the U.S. IBM would help the latter to prepare its homeland security strategy. SST

Report Reveals Cloud-Native Security Are Rarely Robust And Unified Enough To Provide Sufficient Coverage

The Cloud Threat Report 2019 by Darktrace reveals case studies of cloud-based attacks identified by cyber AI which discusses the ability for cloud-native security to provide sufficient coverage.



A Double-Edged Sword

From small businesses seeking to cut costs to corporate innovation centres launching digital transformation projects, the large-scale journey to the cloud has fundamentally reshaped the digital business and the traditional paradigm of the network perimeter. As this perimeter dissolves, hybrid and multi-cloud infrastructure has become a part of the furniture of an increasingly diverse digital enterprise, empowering organizations to push the upper limits of innovation while expanding the attack surface at an alarming rate.

This trend of course represents the double-edged sword of the digital age, and the security challenges that business leaders must face on their journey to the cloud are difficult to overstate. The 'cloud' itself encompasses a wide range of systems and services, and a single security team can often be responsible for securing cloud workloads across AWS and Azure, email communications in Office 365, customer data in Salesforce, file sharing via Dropbox, and virtualized servers in traditional on-premise data centres.

Cloud-Native Security An Unfamiliar Territory

This complex patchwork of cloud-based platforms often fuels efficiency, flexibility, and innovation at the cost of a coherent and tractable security strategy. The cloud in all its various forms is unfamiliar territory for traditional security teams, and prior tools and practices are often too slow, siloed, or not even applicable to defend hybrid and multi-cloud environments against advanced attacks.

And while many cloud-native security solutions can often help with compliance and log-based analytics, they are rarely robust and unified enough to provide sufficient coverage – both because they continue to encourage a "stove-pipe" approach to security, and because they rely on rules, signatures, or prior assumptions and therefore fail to detect novel threats and subtle insiders before they have time to escalate into a crisis.

Still worse, the lack of visibility and control that security teams face in this area – together with the new and unfamiliar mindset required by the agility and speed of the cloud – also renders it an attractive target for cyber-criminals, who invariably seek to generate maximum profits while remaining sufficiently low profile to avoid attention from law enforcement. Cloud security is not where it needs it be, and cyber-criminals know this better than anyone.

Yet in many ways, organizations today need more than just cloud security – they need enterprise-wide security, and a unified solution that can operate at the speed of digital business, adapt to future threats, and correlate the subtle hallmarks of an advanced attack as it broadens its presence within a network.

Insider Threat in the Cloud

Unlike external threat actors, malicious insiders are often uniquely positioned to evade traditional controls given their privileged access and intimate

knowledge of the network. Whether these controls rely on binary detection logic or merely monitor the perimeter, a disaffected employee can often easily bypass static defences in the cloud and exfiltrate or manipulate critical data without triggering suspicion.

Cloud Misconfiguration

Configuring security controls in hybrid and multi-cloud environments is often an overwhelming and complex process, as native and third-party solutions in this area are often diverse, unfamiliar, and incompatible across platforms. This complexity, together with the unprecedented speed and agility of the cloud, has often led to critical misconfigurations that expose the business to attack.

Email Spoof Resulting in Network Infiltration

A malicious email spoof involves registering a seemingly legitimate domain that closely resembles that of a trusted contact or service, such that an attacker can trick an unsuspecting recipient and infiltrate a network with ease. More often than not, the attacker will seek to impersonate a high-level executive and make an urgent request, hoping that the employee will comply before spotting the forged sender address. For years this method has allowed attackers to evade traditional controls, as a newly registered domain would not only trick a recipient but also bypass solutions that rely on blacklists.

Compromised Credential Leaked

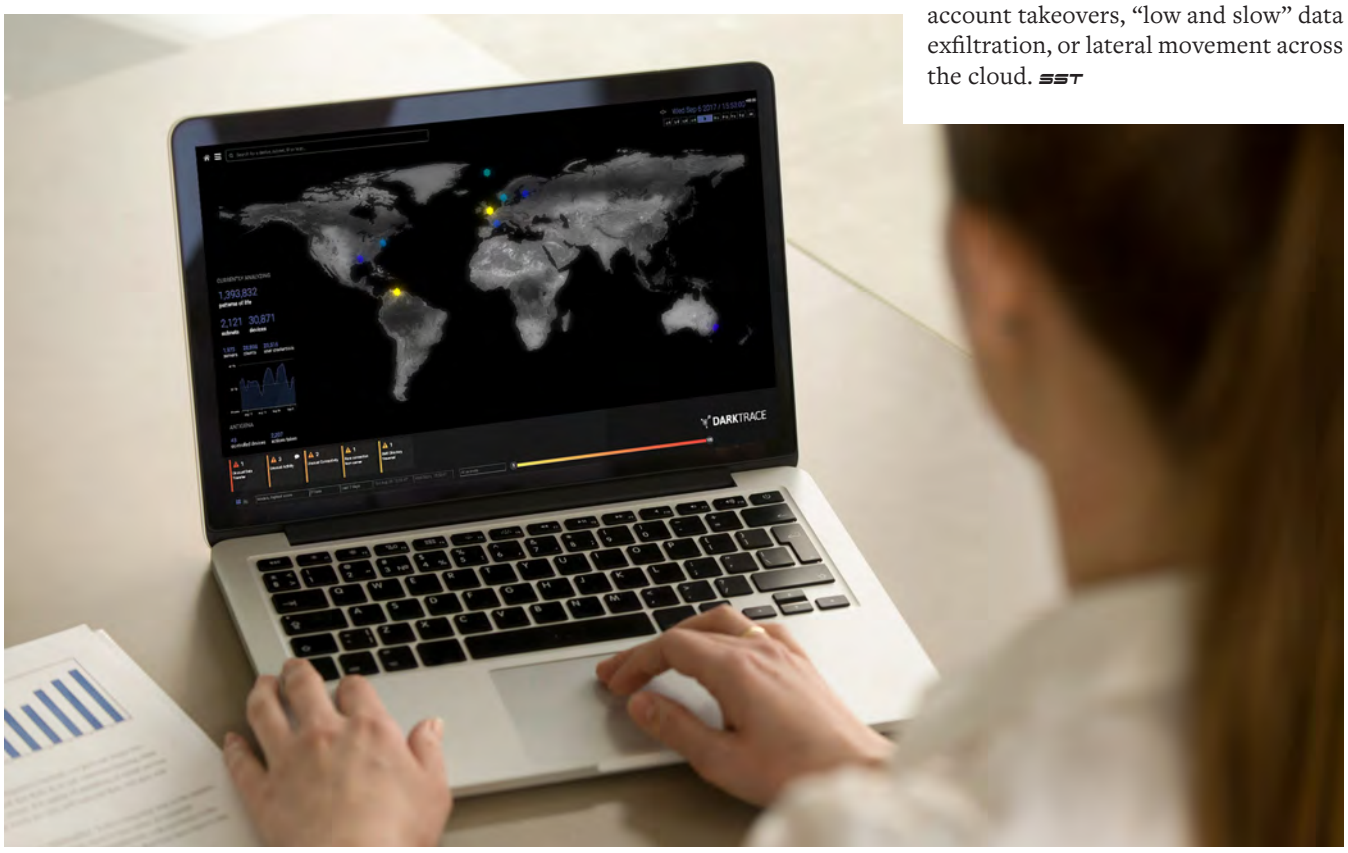
Advanced cyber-criminals can steal corporate account credentials in a variety of ways, from social engineering attacks to "smart" malware that combs through traffic and ephemeral cloud assets in search of passwords. And with stolen data readily available to buy and sell on the Dark Web, the frequency and severity of credential theft is increasing year on year.

The Solution

Powered by artificial intelligence, Darktrace's Enterprise Immune System fills these critical gaps with a unique self-learning approach that detects and responds to cloud-based attacks that others miss.

The solution works by learning the normal "pattern of life" for every user, device, and container across hybrid and multi-cloud environments, without defining 'benign' or 'malicious' in advance. By continuously analysing the behaviour of everyone and everything in the business, the self-learning AI can uniquely correlate the weak and subtle signals of an advanced attack as it emerges in disparate corners of the network.

And while pre-programmed point solutions can certainly complement this approach, the Enterprise Immune System is the only proven solution to stop the full range of cyber-threats in the cloud, from malicious insiders and external attacks, through to critical misconfigurations that can expose the business to future compromise – whether they originate from targeted spear phishing campaigns, corporate account takeovers, "low and slow" data exfiltration, or lateral movement across the cloud. SST



Akamai Threat Research: Phishing and Credential Stuffing Attacks Remain Top Threat to Financial Services Organizations and Customers

Newly released data from Akamai's 2019 State of the Internet / Security Financial Services Attack Economy Report has found that 50% of all unique organizations impacted by observed phishing domains were from the financial services sector. The data shows that, in addition to unique phishing attempts, adversaries also leveraged credential stuffing attacks to the tune of 3.5 billion attempts during an 18-month period, putting the personal data and banking information of financial services customers at risk.



Financial Services Targeted

The report indicates that between December 2, 2018 and May 4, 2019, nearly 200,000 (197,524 to be exact) phishing domains were discovered, and of those domains, 66% targeted consumers directly. When taking the phishing domains targeting consumers only into consideration, 50% of those targeted companies in the financial services industry.

There has been a steady rise in credential stuffing attacks over the past year, fed in part by a growth in phishing attacks against consumers. Martin McKeay, Security Researcher at Akamai and Editorial Director of the State of the Internet / Security Report asserts that, "criminals supplement existing stolen credential data through phishing, and then one way they make money is by hijacking accounts or reselling the lists they create. We're seeing a whole economy developing to target financial services organizations and their consumers."

Processing Ill Gotten Gains Through "Bank Drops"

Once criminals have succeeded in their schemes, they need to process their ill-gotten data and funds. One method of dealing with this situation centers on 'bank drops' – packages of data that can be used to fraudulently open accounts at a given financial institution.

Bank drops will typically include a person's stolen identity – often called 'fullz' by criminals online, including name, address, date of birth, Social Security details, driver's license information, and credit score. Secure access to the fraudulent accounts comes via remote desktop servers, which are matched to the geographic location of the bank and the 'fullz'.

Recycling Old Attack Methods

Financial institutions continue to investigate the ways in which criminals are opening these drop accounts, and are working diligently to stay ahead of the curve. What most businesses don't realize, however, is that criminals are recycling old attack methods.

The findings revealed that 94% of

observed attacks against the financial services sector came from one of four methods: SQL Injection (SQLi), Local File Inclusion (LFI), Cross-Site Scripting (XSS), and OGNL Java Injection (which accounted for more than 8 million attempts during this reporting period). OGNL Java Injection, made famous due to the Apache Struts vulnerability, continues to be used by attackers, years after patches have been issued.

In the financial services industry, criminals have also started launching DDoS attacks as a distraction to conduct credential stuffing attacks or to exploit a web-based vulnerability. Over the course of 18 months, Akamai uncovered more than 800 DDoS attacks against the financial services industry alone.

Financial Institutions and Their Weak Points

Attackers are targeting financial services organizations at their weak points: the consumer, web applications and availability, because that's what works. Businesses are becoming better at detecting and defending against these attacks, but point defences are bound to fail. It requires being able to detect, analyze, and defend against an intelligent criminal who's using multiple different types of tools for a business to protect its customers.

The criminal economy thrives, in part, because they target the financial services industry. By targeting banks for example, criminals attempt to steal sensitive data, and then turn around and use that same data to open fake accounts and lines of credit. It's a continuous cycle of crime. There is a deep level of irony in the fact that criminals are targeting the very industry they need to survive. While financial institutions are becoming better at detecting these attacks, adversaries continue to find success with old tricks, and that's a problem. SST

> *"Criminals supplement existing stolen credential data through phishing, and then one way they make money is by hijacking accounts or reselling the lists they create. We're seeing a whole economy developing to target financial services organizations and their consumers."*
>
> *- Martin McKeay, Security Researcher at Akamai and Editorial Director of the State of the Internet*



Thales Global Threat Report Reveals Digital Transformation Era Is Putting Organizations' Sensitive Data at Risk

Thales, a leader in critical information systems, cybersecurity and data security, announces that the rush to digital transformation is putting sensitive data at risk for organizations worldwide according to its 2019 Thales Data Threat Report – Global Edition with research and analysis from IDC.

As organizations embrace new technologies, such as multi-cloud deployments, they are struggling to implement proper data security. With cloud complexities and the demand for digitally transformative technologies increasing, they outpace security needs.

Sensitive Data is Everywhere

Ninety-seven percent of the survey respondents reported their organization was already underway with some level of digital transformation and, with that, confirmed they are using and exposing sensitive data within these environments. Aggressive digital transformers are most at risk for data breaches, but alarmingly, the study finds that less than a third of respondents (only 30%) are using encryption within these environments.

The study also found a few key areas where encryption adoption and usage are above average: IoT (42%), containers (47%) and big data (45%).

The Reality of Multi-Cloud Risk

As companies move to the cloud or multi-cloud environments as part of their digital transformation journey, protecting their sensitive data is becoming increasingly complex. Nine out of 10 respondents are using, or will be using, some type of cloud environment, and 44% rated complexity of that environment as a perceived barrier to implementing proper data security measures. In fact, this complexity is ahead of staff needs, budget restraints and securing organizational buy-in.



Despite Increase in Data Breaches Enterprises Still Not Investing in Protection

Globally, 60% of organizations say they have been breached at some point in their history, with 30% experiencing a breach within the past year alone. In a year where breaches regularly appear in headlines, the U.S. had the highest number of breaches in the last three years (65%) as well as in the last year (36%).

The bottom line is that whatever technologies an organization deploys to make digital transformation happen, the easy and timely access to data puts this data at risk internally and externally. The majority of organizations, 86%, feel vulnerable to data threats. Unfortunately, this does not always translate into security best practices as evidenced by the less than 30% of respondents using encryption as part of their digital transformation strategy.

No Organisation is Immune

The research shows that no organization is immune from data security threats and, in fact, it is found that the most sophisticated organizations are more likely to indicate that they have experienced a data security breach.

This trend is consistent no matter how we define the sophistication of the audience: those who are spending more on IT security, those for whom data security is a larger portion of their security budget, or those who are further along in their digital transformation journey.

Implementing and Supporting Mandates

Data security is vitally important. Organizations need to take a fresh look at how they implement a data security and encryption strategy in support of their transition to the cloud and meeting regulatory and compliance mandates. The attacks and breaches have now reached a point where almost every organization has been breached. As data breaches continue to be widespread and commonplace, enterprises around the globe can have to secure their digital transformation in the face of these ongoing threats. SST

Gartner Says Security and Risk Management Leaders Must Leverage the Automation Continuum to Create New Value for Their Organizations

Leveraging the automation continuum is security and risk management leaders' latest imperative in creating and preserving value at their organization, according to Gartner, Inc.

Katell Thielemann, research vice president at Gartner, explained that the automation continuum emerging in the security and risk landscape is one where new mindsets, practices and technologies are converging to unlock new capabilities. Using automation in areas of identity, data, and new products and services development were identified as three critical areas for the security and risk enterprise.

"We are no longer asking the singular question of how we're managing risk and providing security to our organization. We're now being asked how we're helping the enterprise realize more value while assessing and managing risk, security and even safety. The best way to bring value to your organizations today is to leverage automation," said Ms. Thielemann.

Automation is All Around Us

Automation is already all around us — and it is starting to impact the security and risk world in two ways:

1. As an enabler to the security and risk function itself
2. As new security frontiers that need to be acknowledged and understood

Automation follows a continuum of sophistication and complexity, and can use a number of techniques, either



stand-alone or in combination. For example, robotic process automation currently works best in task-centric environments, but process automation is evolving to increasingly powerful bots, and eventually to autonomous process orchestration.

By 2021, 17% of the average organization's revenue will be devoted to digital business initiatives, and by 2022, content creators will produce more than 30% of their digital content with the aid of AI content-generation techniques.

What this means to security and risk management professionals is that our organizations are likely building solutions and making technology-related choices often without realizing the risk implications of what they are doing.

Balancing Emerging Technologies and People

Automation is just the beginning. Emerging technologies will change everything and impact security and risk directly. Our reliance on data is ever increasing, yet it poses one of the largest privacy risks to organizations. In the next two years, half of large industrial companies will use some emerging form of digital twins, which will also need to be secured.

The demands of these emerging technologies and digital transformation introduce new talent challenges for the security function, altering how organizations expect security to be delivered.

Digital transformation demands that security staff play a wider range of roles, from strategic consultants to threat profilers to product managers, which in turn require new skills and competencies. It's already impossible to fill all the existing vacancies.

Mission-Critical Areas in Automation

The three mission-critical areas in today's enterprises are automation in identity, data and new products or services development:

- Identity is the foundation for all other security controls, especially as the business increasingly moves to cloud environments. Identity decisions should always remain within the organization's control, whether it is about humans or machines.
- Data is what organizations now depend on for virtually every transaction, and it needs to be shared as much as it needs to be protected.
- New products and services developed as emerging technologies gain a stronghold, prompting organizations to adapt and push the envelope. SST

Serious Zoom Security Flaw Could Let Websites Hijack Mac Cameras



►► **By: Boris Cipot,**
Senior Security Engineer,
Synopsys Software Integrity Group

All software has the potential to be vulnerable. However, a company that provides proprietary software might not be able to fix vulnerabilities immediately. The good thing is that once researchers disclose a vulnerability, they usually try to also offer a mitigation procedure or give users possible ways to mitigate the issue until a fix has been found. Nevertheless, users should monitor the software they're using (operating systems, applications and their extensions), patch them when needed and mitigate any vulnerabilities disclosed.

Recently, a security flaw reported in Zoom video conferencing software allows any website to turn on your Mac computer camera remotely without permission — even if the application had been uninstalled previously. The vulnerability was reported, but the Zoom team has yet to offer a proper security patch, putting over 4 million users at risk.

How Serious Is The Threat?

Every security vulnerability brings threats and they should be treated as highly risky. This vulnerability however brings with it another level of risk for those who were just using Zoom as an invitee into a Zoom session. Imagine a scenario where a company decided to use Zoom as a meeting provider, its employees are doing all the necessary things to monitor the application and mitigate its vulnerabilities.

Although the company does not usually use Zoom and it just happened that the company was invited in a Zoom session, it has the risk or the vulnerability also on its devices yet not even aware this risk exists. This means that the company is now a potential target for someone who wants to use this vulnerability as well – in this case to lower the performance of a machine or join a call with the camera activated without the user's permission which is a substantial privacy intrusion.

How Easy Is It For An Attacker To Exploit This Issue?

The attacker does not need to have the user's permission to join a Zoom call. This means that the vulnerability is easy to exploit. Utilizing this attack vector, any web page could interact with the local web server and abuse the vulnerability. That being said, the vulnerability would be triggered if the target were to visit a site that abuses the vulnerability. Even if this is a scenario that will most probably not happen, think about phishing attacks.

As said, the vulnerability is on the user's Mac already if the user used Zoom as a participant in a call. An attacker could theoretically carry out phishing attacks, create spam or other attack strategies where the user would need to click a link. Potential victims are lured to such a page and attackers could join them in a call without the user's knowledge.

What Can Organisations Do To Mitigate Their Exposure To This Threat?

A good mitigation procedure is to disable the ability for Zoom to switch on the user's camera automatically when joining a call. The user can do this in the Zoom settings by selecting the option "Turn off my video when joining a meeting" or by using the Terminal. Also shut down the local Zoom web server that is running on the user's Mac and prevent it being run again after the update. It is also important to monitor Zoom for any notifications on patches and fixes for this vulnerability. SST

Subscription Form

Fax your order today
+65 6842 2581

(Please tick in the boxes)

Southeast Asia Building

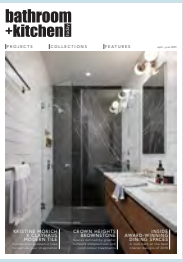


SINCE 1974

☐ 1 year (6 issues)

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

Bathroom + Kitchen Today



SINCE 2001

☐ 1 year (4 issues)

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

Southeast Asia Construction



SINCE 1994

☐ 1 year (6 issues)

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

Lighting Today



SINCE 2002

☐ 1 year (4 issues)

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

Security Solutions Today



SINCE 1992

☐ 1 year (6 issues)

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

IMPORTANT

Please commence my subscription in

_____ (month/year)

Personal Particulars

NAME: _____

POSITION: _____

COMPANY: _____

ADDRESS: _____

_____

TEL: _____ FAX: _____

E-MAIL: _____

Professionals (choose one):

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

☐ Property Manager ☐ Manufacturer/Supplier ☐ Engineer ☐ Others

☐ I am sending a cheque/bank draft payable to:

Trade Link Media Pte Ltd, 101 Lorong 23, Geylang, #06-04, Prosper House, Singapore 388399

RCB Registration no: 199204277K * GST inclusive (GST Reg. No: M2-0108708-2)

☐ Please charge my credit card (circle one): Amex / Diner's Club

Card Number: _____ Expiry Date: _____

Name of Card Holder: _____ Signature: _____

PLATINUM PARTNER

Dahua Technology	Singapore	+65 6538 0952	sales.sg@dahuatech.com	www.dahuasecurity.com	IFC

GOLD PARTNERS

Microengine Technology	Malaysia	+603 7957 2008	enquiry@microengine.net	www.microengine.net	5
Delta Scientific	U.S.A.	+1 661 575 1100	info@DeltaScientific.com	deltascientific.com	3

SILVER PARTNER

Avigilon	U.S.A.	+1 888 281 5182	asksales@avigilon.com	www.avigilon.com	7

See us at following upcoming events!

Event	Date	City	Country	Website	Page
GSX 2019	8 –12 Sept 2019	Chicago, IL	U.S.A	www.gsx.org	OBC
WOSAS 2019	26 –29 Sept 2019	Manila	Philippines	www.wosas.ph	IBC
Safety & Security Asia 2019	1 – 3 Oct 2019	Singapore	Singapore	www.safetysecurityasia.com.sg	1
Secutech Thailand 2019	28 – 31 Oct 2019	Bangkok	Thailand	www.secutechthailand.com	15
IFSEC International 2020	19 – 21 May 2020	London	United Kingdom	www.ifsec.events/international/	9
IFSEC SEA 2020	23 – 25 Jun 2020	Kuala Lumpur	Malaysia	www.ifsec.events/kl/	11
IFSEC Philippines 2020	22 – 24 July 2020	Manila	Philippines	www.ifsec.events/philippines/	13

ADMISSION IS FREE!

WORLDBEX SERVICES INTERNATIONAL

WOSAS

WORLD OF SAFETY AND SECURITY EXPO



Experience the Assurance

SEPTEMBER 26 – 29, 2019

10:00 AM TO 8:00 PM

WORLD TRADE CENTER METRO MANILA

REGISTER ONLINE NOW AT WOSAS.PH

SUPPORTED BY

Security Solutions Today

+ 632 656 9239

inquire@worldbexevents.com

GSX
GLOBAL SECURITY EXCHANGE

FORMERLY ASIS ANNUAL SEMINAR & EXHIBITS

8-12 SEPTEMBER 2019
McCORMICK PLACE | CHICAGO, IL

GSX.ORG | #GSX19



A Smarter EXCHANGE

GSX provides an invaluable opportunity to explore countless topics ranging from AI to VR, IoT security to insider threats, and robotics to radicalization—each delivering valuable, actionable takeaways to help shape your strategy—today and in the future.

20,000 registered attendees

110+ countries

300+ education sessions

Up to **30 CPEs**

2 X learning theaters in the Exhibit Hall

1 Global Exchange

See full education lineup by reviewing our conference brochure or go to ***GSX.org/SST***