Security Solutions Today

March / April 2019



HOPE OR HYPE?

Is AI a silver bullet for the security industry or is it just hype?

Cover Story

Can AI fight identity fraud?

Cover Story

AI is changing video and the industry will never be the same again

Inside Focus

Why mobile credential is more secure than card-based systems

Scan this to download the latest issue from our website



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

Recommended Models



IPC-HFW4239T-ASE
1080P Full-color Network Bullet Camera



IPC-HDBW4239R-ASE
1080P Full-color Network Dome Camera



HAC-HFW2249E-A-LED
1080P Full-color HDCVI Bullet Camera



HAC-HDW2249T-A-LED
1080P Full-color HDCVI Eyeball Camera

CE FC UL RoHS ISO 9001:2000

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

INTERPOL
WORLD 2019

www.interpol-world.com

ENGAGING CO-CREATION TO PREPARE FOR FUTURE SECURITY THREATS

2 - 4 July 2019

Sands Expo & Convention Centre • Singapore

www.interpol-world.com



Global Safety Today • Improving Security for Tomorrow • Forecasting and Planning for the Future

INTERPOL World is a global **co-creation** opportunity which engages the public and private sectors in dialogue and fosters collaboration to counter future security and policing challenges.

30 strategic **Co-creation Labs** to discuss the challenges and solutions for combating the crimes of the future

Exhibition that serves as a business and networking event for **250** manufacturers, distributors, and Research and Development organizations to offer innovative products and cutting-edge technologies

INTERPOL Working Groups
(by invitation only)
including the chief innovation officers group, artificial intelligence, drones and the Darknet and cryptocurrency group

Register for INTERPOL World 2019!

visitor@interpol-world.com

#INTERPOLWorld

EVENT OWNER
INTERPOL

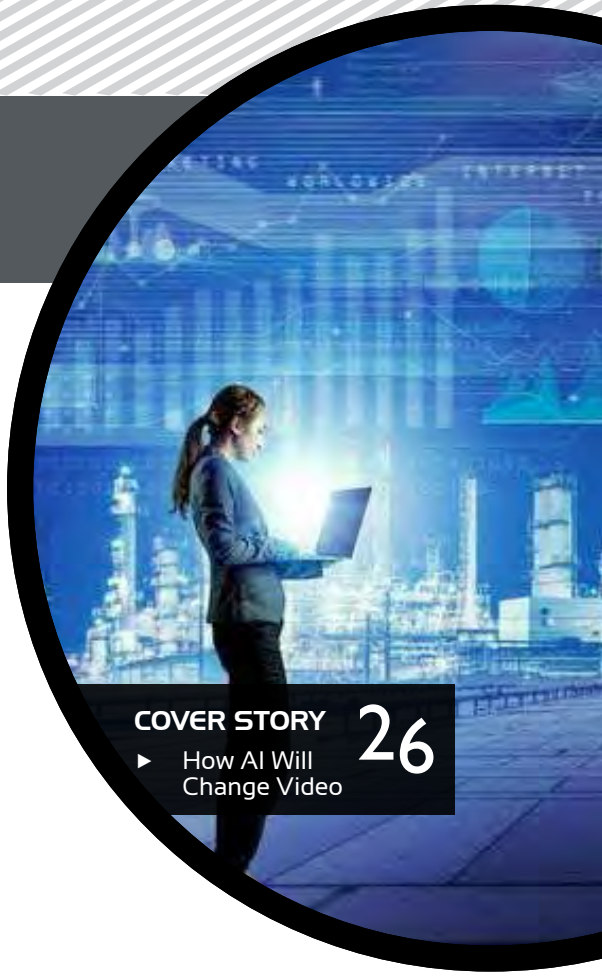
SUPPORTED BY
MINISTRY OF HOME AFFAIRS SINGAPORE
SINGAPORE EXHIBITION & CONVENTION BUREAU

INDUSTRY INSIGHTS BY
pwc

HELD IN
SG singapore Passion Made Possible

MANAGED BY
imp

IN THIS ISSUE



6 CALENDAR OF EVENTS

8 EDITOR'S NOTE

10 IN THE NEWS
Updates From Asia And Beyond

26 COVER STORY
- How To Use AI To Fight Identity Fraud
- US$12 Billion Intelligent Robot Market By 2023
- Fast-Growing Global Artificial Voice Box Market To Hit US$24 Billion By 2024
- Humans Vs Machines: AI And Machine Learning In Cybersecurity
- AI And The Cybersecurity Industry: Magic Bullet Or Hype?
- Artificial Intelligence In Cybersecurity: Beyond The Hype

44 CASE STUDY:
Keeping Patients Safe At NHS Facilities In England

46 INSIDE LOOK
- 2018 Global Smart Home Device Revenue Reached US$28 Billion
- Why Mobile Credential Is More Secure Than Card-Based Systems
- Video Verification Is Combating False Alarms
- 2018 Was The Year Of The Next-Gen Cyber Attack
- The Internet Without Passwords: Prediction Or Pip Dream?
- Cloud And Mobile Deployment The Weakest Links In Enterprise Networks
- Critical Infrastructure Security Spending To Hit US$125 Billion By 2023

59 IN FOCUS
- Mitsubishi Electric Develops Security Technology To Detect Attacks On Equipment Sensors
- A Safer, CLeaner London Borough WIth Dahua Video Cameras
- Dallmeier's Solution Halts Airport Terminal Closures
- Mitsubishi ELectric Develops Cyber Defence Technology For Connected Cars
- Trustonic Launches Service That Slashes Smartphone Thefts
- Full Integration Across Security, Safety And Site Management Systems At Dubai's Landmark Bluewater Island
- Neurotechnology's Palm Print Recognition Algorithm Emerged Top
- RFID DIsplay Readers With Expanded Features
- Smart Solutions For Casino Surveillance
- Three Australian Universities Roll Out SafeZone Protection On Campus And Beyond

74 SECURITY FEATURES
- Five Technology Trends for 2019

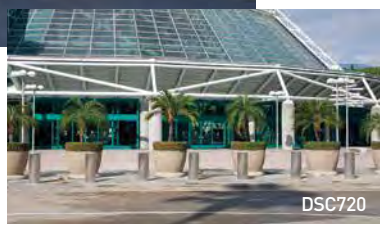
78 SHOW PREVIEW
- Preview The Dazzling Future In Hong Kong

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





MP5000



DSC720

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
Michelle Lee
(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

Designed by Siti Nur Aishah

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

Printed in Singapore by Refine Printing Pte Ltd

ANNUAL SUBSCRIPTION:

Surface Mail:	
Singapore	- S$45 (Reg No: M2-0108708-2 Incl. 7% GST)
Airmail:	
Malaysia/Brunei	- S$90
Asia	- S$140
Japan, Australia, New Zealand	- S$170
America/Europe	- S$170
Middle East	- S$170

ADVERTISING SALES OFFICES

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

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

xPortalNet HS

High Security System Software

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



Projects


Commercial / Complex


Factory


Condominium

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


Plato DesFire Reader



1300-88-3925 or enquiry@microengine.net

www.microengine.net


Our Office


Service Centre

GlobalGROUP ISO 9001 5965

REG No. 749921389

COMING SOON...

MARCH

IFSEC Southeast Asia 2019

Date: 19 - 21 March 2019
Venue: Malaysia International Trade And Exhibition Centre (MITEC), Kuala Lumpur, Malaysia
Organiser: UBM Malaysia
Telephone: +603 9771 2688
Website: www.ifsec.events/kl
Email: info-my@ubm.com

APRIL

ISC West 2019

Date: 9 - 12 April 2019
Venue: Sands Expo, Las Vegas, NV, USA
Organiser: Reed Exhibitions
Telephone: (800) 840-5602
Website: www.iscwest.com
Email: inquiry@isc.reedexpo.com

MAY

Secutech 2019

Date: 8 - 10 May 2019
Venue: Taipei Nangang Exhibition Center, Taipei, Taiwan
Organiser: Messe Frankfurt New Era Business Media Ltd, Taiwan Branch
Telephone: +886 2 8729 1099
Website: www.secutech.com
Email: services@secutech.com

JUNE

IFSEC Philippines 2019

Date: 13 - 15 June 2019
Venue: SMX Convention Centre, Pasay City, Metro Manila, Philippines
Organiser: UBM Exhibitions Philippines, Inc
Telephone: +63 2 551-7718 / 839-1306
Website: www.ifsecphilippines.com
Email: info-ph@ubm.com

JUNE

IFSEC International 2019

Date: 18 - 20 June 2019
Venue: ExCeL London, London, UK
Organiser: UBM plc
Telephone: +44 (0) 20 7921 5000
Website: www.ifsec.events/international/
Email: ifseccustomerservice@ubm.com

JUNE

BMAM Expo Asia 2019

Date: 27 - 29 June 2019
Venue: IMPACT Exhibition Center, Hall 6, Bangkok, Thailand
Organiser: IMPACT
Telephone: +66 8 6561 3344 / +66 2833 5111
Website: www.bmamexpoasia.com
Email: radcharinn@impact.co.th

JULY

INTERPOL World 2019

Date: 2 - 4 July 2019
Venue: Sands Expo and Convention Centre, Singapore
Organiser: INTERPOL
Telephone: +65 6389 6613
Website: www.interpol-world.com
Email: layeng.see@interpol-world.com

OCTOBER

Safety & Security Asia 2019

Date: 1 - 3 October 2019
Venue: Marina Bay Sands, Singapore
Organisers: Conference & Exhibition Management Services Pte Ltd
Telephone: +65 6278 8666
Website: www.safetysecurityasia.com.sg
Email: SSA@cems.com.sg

GOING UP?

POWER HAS REACHED **NEW LEVELS.**



ALTRONIX **EFLOW™** SERIES POWER SUPPLY/CHARGERS PROVIDE FASTER BATTERY CHARGING, FIRE ALARM DISCONNECT, OVER VOLTAGE AND BATTERY PROTECTION. **EFLOW™** LET'S YOU CONTROL AND MONITOR POWER REMOTELY OVER THE NETWORK, REPORT DIAGNOSTICS WITH **LINQ™**, OUR SMART POWER MANAGEMENT TECHNOLOGY WHICH REDUCES SYSTEM DOWNTIME, CREATING MORE RMR.

POWER THAT TRULY ELEVATES YOUR SECURITY.



Altronix eFLOW™

MADE IN THE U.S.A. ALTRONIX.COM LIFETIME WARRANTY

EDITOR'S NOTE



Dear esteemed reader,

Artificial intelligence is by far the most influential technology force affecting everything and everyone in the digital world. And it will change the face of the security industry.

Or will it? Could it be one big hype?

Industry experts take polar positions on this. In this issue, you will hear both standpoints – and some words of warning.

Nevertheless there is no question that AI will become a giant part of the security industry. In 2017, the AI in Security market was valued at US$3.92 billion. Over the next eight years, this market is expected to explode at a compound annual growth rate of 31.38% to reach US$ 34.81 billion by 2025 according to a research report by MarketsandMarkets.

The increased integration of IT into the daily activities of industries, governments, families and consumers, along with the rising sophistication levels of cyber attacks, has forced the enterprise industry to focus more on cybersecurity and to adopt AI in its security solutions, said MarketsandMarkets.

Research firm Infoholic Research reports the factors driving the growth of the North America market – the biggest market for AI in Security - as the increasingly stringent regulations imposed by governments on data privacy and security, increasing number of startups providing AI-based security tools, increasing security breaches and advanced persistent threats in this region. With malwares getting more intelligent by the day there is a need for counterattack using artificial intelligence and machine learning technology.

Both research firms agree that the Asia Pacific market will grow rapidly in the near future. Plainly the future is here already and it's everywhere – in your home, at your work and in your public spaces. And it will only get more so.

Michelle Lee

Editor

secutech

8 – 10 May 2019, Taipei, Taiwan
www.secutech.com



Bringing Asia's security, IoT & AI ecosystem together under a single roof

7 Smart solution pavilions

- Smart Retail
- Smart Hotel
- Smart Factory
- Smart Parking
- Smart Healthcare
- Smart Community
- Smart Transportation

7 Thematic zones

1. AI+Software Zone
2. RFID Applications Zone
3. LPWAN Applications Pavilion
4. Smart Lock Pavilion
5. Cybersecurity Pavilion
6. Police Equipment Zone
7. Smart Factory & Industrial Safety



MOBILITY powered by Secutech

- Asia's leading fair for Intelligent Transport Systems
- Showcasing solutions that range from smart road, smart railway, smart parking to fleet management

SMART BIoT SOLUTION powered by Secutech

- Asia's first event for the 'Smart Building Internet of Things'
- Focusing on four major applications: residential & community, hospitality, nursing facility and commercial building

fire & safety powered by Secutech

- Highlighting a full range of solutions from natural disaster monitoring, safe city, industrial safety to personal safety
- Advanced smart disaster prevention applications

info security powered by Secutech

- Revealing the latest cybersecurity solution for the IoT

messe frankfurt

Huawei Debuts AI Solutions For Government And Businesses At MWC 2019

For the first time, Huawei is dedicating a zone to governmental and enterprise customers at MWC 2019. Held in Barcelona at end February 2019, the GSMA Mobile World Congress (MWC) is the world's largest mobile industry exhibition.

The Chinese telecommunications equipment and consumer electronics maker will be introducing its latest AI applications in the smart city, finance and retail realms at the event.

Huawei will be launching several star enterprise business products including a high-end storage product for enterprises, the OceanStor Dorado all-flash storage. Featuring 7,000,565 SPC-1™ IOPS and 0.5 ms latency, the NVMe-based Dorado has been put into widespread commercial use by seven of the top 20 global banks.

Huawei will also be unveiling the industry's first wireless AP with data transfer speed of up to 10Gbps. The Huawei Wi-Fi 6 AP includes the industry's first application of 8x8 MU-MIMO, OFDMA, and 1024 QAM. Using Huawei's 3rd-generation smart antenna and SmartRadio technology, the bandwidth is quadruple that of current models, enabling five times the number of concurrent users. The coverage distance is 20% larger and the whole network capacity sees a 30% increase compared to current models. It enables high-speed access for multiple users, ideal for enterprises that require the application of the IoT.

Huawei is also debuting the industry's first data centre switch built for the AI era, the CloudEngine 16800. With an embedded AI chip, the CloudEngine 16800 uses the innovative iLossless algorithm to achieve an AI computing power of 100%, improving data storage IOPS by 30%. It provides the industry's highest density 48-port 400GE line card per slot, and its switching capacity is five times the current industry average. SST







IFSEC INTERNATIONAL

18-20 JUNE 2019
EXCEL LONDON UK

"40% MORE LEADS THIS YEAR THAN LAST. THE MEETINGS WITH VIPS HAVE BEEN SO BENEFICIAL, WITH QUALITY NAMES WHO ARE READY TO BUY, NOT JUST SPECULATE."
Managing Director, ZKTeco

SECURITY IS

CRITICAL

IFSEC IS ESSENTIAL

Position your brand at the centre of the critical security conversation. Be part of IFSEC 2019.

Unique in attracting the entire security buying chain, IFSEC 2019 is your world-class, integrated security summit. Influence the innovation dialogue with over 27,000 global security integrators, installers, distributors, consultants and end users from over 117 countries – all under one roof.

- **43,461 Leads were generated onsite at IFSEC in 2018 – an average of 123 per exhibitor**
- **34% of visitors had an annual purchasing budget of over £1,000,000**
- **Generate global business with quality buyers – Expand your business into high-growth markets around the world**

Find out more at: www.ifsec.events/international/exhibit

Industry's First Lithium Iron Phosphate Battery Chargers

Altronix, a leader in power and data transmission solutions for the professional security industry, has introduced the industry's first lithium iron phosphate battery charger. The optimised battery charger accommodates LiFePO4 batteries with significantly longer shelf life and much more efficient charge cycles compared with conventional sealed lead acid (SLA) batteries.



The optimised chargers can be found in Altronix's new series of NetWay Spectrum PoE+ Switches.

Altronix's NetWay Spectrum PoE+ Switches with LiFePO4 battery charging come with many advantages.

Superior performance and cost efficiencies are realised through a 10-year battery shelf life, over 5,000 charge cycles and the greatly reduced weight of the LiFePO4 batteries. In addition, the switches utilise a single LiFePO4 battery for PoE backup versus four SLA batteries, reducing service and maintenance.

"Our new Hardened PoE switches with optimised lithium iron phosphate battery chargers are truly a game changer for the industry. It presents a new and unique value proposition for installers and end-users, ensuring continuous system operation while greatly reducing service and maintenance costs," said Alan Forman, President of Altronix Corporation.

Altronix plans to extend this LiFePO4 backup feature to its other products in the near future. SST

Adder Launches World's First 4K Solution

Adder Technology, a global specialist in connectivity and IP KVM, debuted the world's first dual-head, high performance 4K IP KVM matrix over a single fiber with the launch of the ADDERLink™ INFINITY 4000 Series (ALIF4000).

The ALIF4000 will help businesses integrate 4K content into their everyday work quickly and efficiently.

Adoption of 4K technology continues to rise dramatically. It is predicted that the global 4K display market will be worth US$52 billion by 2020 (up by 188% compared to 2015). The projected growth of 4K technology, and the increasing demand for 4K content, means the launch of the ALIF4000 series is perfectly timed to support IP KVM users as they move to 4K environments.

The ALIF4000 delivers pixel-perfect picture quality, audio and USB to single or dual 4K screens over a single fiber link. At the same time, it supports mixed 1Gb and 10Gb networks and gives customers right-size technology with an opportunity to embrace 4K when they're ready.

Full compatibility with the existing INFINITY range means the ALIF4000 can be phased into an existing network without disruption, downtime or the costly need to rip and replace.

The ALIF4000 series simplifies the adoption and efficiency of 4K IP KVM by offering 4K, USB and audio all through a single fiber connection. This makes it the ideal solution for anyone looking to implement single or dual 4K screens into an IP KVM environment.

Adrian Dickens, managing director at Adder Technology, said, "Adder has delivered a product that enables our customers to add 4K to their workflow, at a time that is right for them, without enduring unnecessary costs." SST

IFSEC
PHILIPPINES

SECURITY • FIRE • SAFETY

13 - 15 JUNE 2019

SMX CONVENTION CENTRE
PASAY CITY, METRO MANILA

Organised By

UBM



THE LEADING
SECURITY, FIRE & SAFETY
EVENT IN THE PHILIPPINES

EMPOWERING THE PHILIPPINES TO BE THE SAFER NATION BY PROVIDING GLOBAL INNOVATION AND EXPERTISE TO THE EMERGING TRENDS AND SERVICES IN SECURITY, FIRE AND SAFETY MARKETS.

WWW.IFSECPHILIPPINES.COM

@IFSECPHILIPPINES #IFSECPHILIPPINES IFSECPHILIPPINES

Future-Facing Camera With A Focus On Detail

Bosch's belief in working smarter is fully expressed in the FLEXIDOME IP starlight 8000i fixed dome camera, which is developed to streamline the video security process and save up to 75% of camera set-up time.

The camera features built-in Intelligent Video Analytics, making it highly intuitive. It also elevates its importance beyond mere security. The setup of the video analytics is surprisingly straightforward; simply enter the camera height and the video analytics will calibrate itself via information provided by the built-in gyro sensor.

When image detail matters, the FLEXIDOME IP starlight 8000i delivers with frame rates of up to 60fps, which enables fast-moving objects to be easily captured. Even in extreme low-light situations, Bosch's starlight technology (together with 1080p, 6 megapixel, or the 4K Ultra HD resolution) provides exceptional detail. The High Dynamic Range compensates for areas with a high variance of dark and light.

The future-facing camera features remote commissioning. When used with the Project Assistant app, the pan, tilt, roll and zoom (PTRZ) function can set the field of view even beyond the initial setup. The camera is also water- and vandal-resistant and can operate at temperatures of -50 to +60°C.

When Intelligent Dynamic Noise Reduction and intelligent streaming are combined with H.265 video compression, they can reduce bitrate by up to 80%, and the addition of various software and hardware measures keeps vital video data secure. SST



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



IFSEC
SOUTHEAST ASIA
KUALA LUMPUR EDITION
SECURITY • FIRE • SAFETY

19 - 21 MARCH 2019

MALAYSIA INTERNATIONAL TRADE
AND EXHIBITION CENTRE (MITEC), KL

Part of the
Super 8 Series of Events
ASEAN SUPER 8

SECURITY IS
CRITICAL
IFSEC IS
ESSENTIAL



PRE-REGISTRATION IS NOW OPEN

Organised By
UBM

WWW.IFSEC.EVENTS/KL
WWW.SUPER8ASEAN.COM

@IFSECSEA #IFSECSEA IFSEC Southeast Asia

AXIS' New Pan-Tilt-Zoom Auto Tracking In Perimeter Defender

Axis Communications has launched a pan-tilt-zoom (PTZ) auto tracking application for its intrusion detection analytics AXIS Perimeter Defender.

With AXIS Perimeter Defender PTZ Autotracking, a fixed thermal or visual camera running AXIS Perimeter Defender is used to detect people and vehicles. When an alarm is triggered, the PTZ Autotracking application takes control of a PTZ camera to track and get closer views of alarm objects. Together one fixed camera works seamlessly with one PTZ camera to enhance perimeter protection.

This is how it works: the fixed camera sends the location data of the alarm objects to the PTZ camera. The PTZ camera then automatically adjusts the zoom level to keep in view the alarm objects, including new ones that appear in the fixed camera's detection zone. An operator can take manual control of the PTZ camera at any time, for instance after PTZ auto tracking comes to a halt when objects move out of the fixed camera's detection zone.

PTZ Autotracking offer several key benefits. The application



lets the fixed camera maintain detection coverage over a large area while the PTZ camera automatically zooms in to provide more details on alarm objects. This allows for the capture of fine details of alarm objects without compromising detection coverage. In addition, the PTZ camera is activated automatically and will automatically keep all alarm objects in view. Finally, just one management programme is needed to set up the analytics in a fixed camera and the PTZ auto tracking application in a PTZ camera.

The application is compatible with specific Axis PTZ cameras and allows one fixed camera to be paired with one PTZ camera. A separate license is needed for the application. PTZ Autotracking is available now in Europe and Israel and will be available in other regions at a later date. SST

Qognify Completes Acquisition, Becomes One of World's Largest VMS, Video Analytics and PSIM Companies

Qognify, a technology solution provider for physical security and enterprise incident management, has acquired the IP video management software (VMS) company On-Net Surveillance Systems (OnSSI), including the pioneer of IP video technology, SeeTec GmbH.

Qognify is backed by global investment firm Battery Ventures. With Qognify, OnSSI and SeeTec operating under one umbrella, the company is today one of the largest VMS, Video Analytics, PSIM and Critical Incident Management companies in the world.

Qognify's solutions includes video management, video and data analytics, and PSIM/ Situation Management solutions. OnSSI's Ocularis delivers robust cybersecurity protections for a range of applications including education, gaming, government, healthcare, manufacturing, public safety, transportation and utilities. SeeTec GmbH is one of the leading vendors of video management software in Europe.

Stated Steve Shine, CEO and President of Qognify, "Today, through our combined portfolio of award-winning and market-leading technologies, infrastructure and expertise, we expand our global presence, creating an entity capable of meeting the exacting requirements of mid-market and enterprise organisations anywhere in the world."

Qognify's VisionHub, NiceVision, FAST and Situator solutions are trusted by financial services companies, mass transit infrastructure, large international airports and seaports, as well as smart and safe city projects around the world. The OnSSI Ocularis and Cayuga VMS solutions are deployed across education, gaming, government, healthcare, logistics, manufacturing, retail, public safety, transportation and utilities organisations in more than 100 countries. SST

27-29 JUNE 19

IMPACT Exhibition Center, Hall 6, Bangkok, Thailand

BMAM EXPO ASIA 2019

THE BUILDING & FM EXPO



5,000 Sq.m.
Exhibition space

150
Exhibitors

4,000+
Qualified visitors

Book Your Stand
Now!

Contact: Ms. Radcharin Nuttayakul (Tucky)
M: +66 (0)8 6561-3344 T:+66 (0)2 833-5111 E: radcharinn@impact.co.th

Follow us on
BMAM Expo Asia

Organizer
IMPACT MUANG THONG THANI

World's First Intelligent Motor Locks

Security expert Abloy UK has launched what it describes as the world's first intelligent motor locks, the EL495 and EL595. The locks automatically diagnose the condition of its capacitors, so that when the lock reaches the end of its lifecycle it gives an audible warning for the lock to be replaced before it fails.

There are three variants of the EL495 and EL595 available, including a Fail Unlocked (FU) model, Fail Locked model (FL) and high security lock case with mechanical exit feature.

The Fail Unlocked (FU) model is designed for high security two-way access control doors. The Fail Locked model (FL) is for exceptional environments.

For both EL495 and EL595 the inside handle does not operate the lock; access control is required on both sides of the door to allow entrance or exit. However, the inside handle is electrically controlled allowing the handle to be operational when required, on activation of a fire alarm or other input.

The high security lock case features a mechanical exit feature, and in normal operation the lock is used with access control from outside and the handle on the inside always operational. There is no electronic handle control or diagnostics feature.



The locks are compliant to British Standards - EL495 is BS EN179 and BS EN1125 approved, and the EL595 is BS EN179 approved. The EL495 is for profile doors and EL595 is for solid doors. SST

Symantec Launches Automatic Fake Email Blocker

Each year protecting email becomes harder as attacks become more sophisticated. According to the FBI, Business Email Compromise (BEC) attacks grew 136% over the past two years, with reported attacks totalling US$12.5 billion. In particular, impersonation emails from trusted senders are a major threat to organisations.

Not only are email threats costly, but manually enforcing email authentication standards including SPF, DKIM or DMARC can be time consuming and requires highly technical resources to accurately identify third-party email senders without false positives that block important emails. To help enterprises combat BEC attacks, Symantec has launched Email Fraud Protection. The automated solution helps organisations block fraudulent emails from reaching enterprises, ensuring complete brand reputation and sender trust.

With the solution, email authentication standards are met by automatic monitoring of approved third-party senders. Email Fraud Protection integrates with Symantec Email Security to support email authentication standards and help block platform threats on-premises or in the cloud, such as spam, malware and phishing attacks. It can also integrate with Symantec Email Threat Isolation to minimise the risk



of spear phishing, credential theft, account takeover and ransomware attacks.

Email Fraud Protection saves businesses time and money by drastically reducing workload for IT departments and eliminating the need to manually manage email security configurations BEC attacks.

"It's not easy to find a solution that can stop email impersonation through DMARC, especially in a business world where you have multiple legitimate senders for a domain. Symantec Email Fraud Protection is that solution," said James Charlton, IT security manager at MS Amlin – Global Specialty Insurer and Reinsurer. SST

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

Showcase Of Automated Police Tools

Dallmeier, a leader in CCTV/IP video security technology, combined innovative camera equipment and modern software to showcase how video surveillance, observation and analysis can be conducted more efficiently at the European Police Congress held in Berlin in February.

In 3D Smart Viewing, Dallmeier combined new, ultra-high performance Panomera® 360 degree systems with other Panomera® models to enable incidents to be captured even when separated by great distances. With this combination, essential tasks like tracking objects between multiple cameras or activating the most favourably placed camera are performed semi-automatically. This makes it possible to use a minimum number of monitors to observe connected incidents.

Response teams can be further relieved of the burden of monitoring when the technology is combined with AI-based analysis systems. These systems serve to direct attention to significant events and to filter out irrelevant connections before human intervention or evaluation is required.

Dallmeier also presented software solutions for situational awareness. The modular solution allows response teams to receive real-time information from a central source via their mobile devices. This information may be static or moving images from camera systems or real-time map information.

With this solution, control centres can now direct response teams based on accurate information and optimal coordination with the control centre.

At football matches, for example, this solution allows security personnel to nap a suspicious individual in front of exit tunnels because these officers received photos and other information about the individual through their mobile devices in real time.

This system can be combined with the digital police file solution. This is an exceptionally flexible system where all data pertinent to an incident can be collected from various sources regardless of location and assigned to a digital incident file. Data from an enormous range of sources and media formats can be collected in this file and integrated electronically in subsequent investigation steps. The system can be configured flexibly and adapted for various procedures. It may also be used for traffic incidents and in many other situations where capture and further processing of investigation data is very labour- and cost-intensive. SST

Carbon Black Makes Replacing Legacy Antivirus Easier

Carbon Black's latest version of Cb Protection incorporates a new "File Delete" feature that allows customers to replace legacy antivirus (AV) without going through the compensating control process.

Cb Protection is the cybersecurity company's market-leading application control solution used by organisations to lock down servers and critical systems, prevent unwanted changes, and ensure continuous compliance with regulatory mandates, including Payment Card Industry Data Security Standard (PCI DSS).

Leveraging cloud-reputation services, IT-based trust policies and multiple



sources of threat intelligence from the Cb Predictive Security Cloud, Cb Protection ensures that only trusted and approved software is allowed to execute on an organisation's critical systems and endpoints. Cb Protection achieved a Security Effectiveness rating of 100% in an independent test conducted by NSS Labs in 2017.

With the 'File Delete' feature in Cb Protection 8.1, Carbon Black makes customers' lives easier by automating response measures protecting server workloads from compromise while also assuring compliance.

"It was a standout product to us. The effort required to install and maintain it appeared to be much lower than other products in its class," said Simon Turner, Head of IS Architecture at Kordia. SST

Samsung Galaxy Smartphones First In The World To Achieve FIDO Biometric Certification

Samsung S10 and S10+ smartphones are the first products to feature certification from the FIDO Alliance's new Biometric Component Certification Program. This certification validates that the new in-display fingerprint recognition system meets industry standards for user verification and detecting presentation (or "spoof") attacks.

Formed in 2012, the FIDO (Fast IDentity Online) Alliance is changing the nature of authentication with standards for simpler, stronger authentication that define an open, scalable, interoperable set of mechanisms that reduce reliance on passwords. FIDO Authentication is stronger, private and easier to use when authenticating to online services.

The FIDO Alliance developed the biometric certification programme to fill a gap in the market. In the past, biometric vendors had to repeatedly prove performance for each customer. This ability to test and certify a biometric system only once results in substantial time and cost savings for vendors and gives customers a standardised way to trust the biometric systems they are relying upon for fingerprint, iris, face and/or voice recognition.

The programme utilises accredited independent labs to certify that biometric subcomponents meet globally recognised performance standards for biometric recognition performance and Presentation Attack Detection (PAD).

"Protection of customers' data and privacy on our devices is of utmost importance to Samsung, which is why we went through the FIDO Biometric Component Certification Program," said Henry Jong-Hyeon Lee, SVP and Head of Mobile Security Technologies Group, IT & Mobile Communications Division, Samsung Electronics.

"The FIDO Alliance Biometric Component Certification Program fills an important gap in our industry as biometrics expand out of the enterprise and government marketplace into the mainstream consumer electronics marketplace," said Dr. Kevin Wilson of iBeta. "We are very pleased to be the first accredited lab to perform biometric certification assessments under this programme." SST



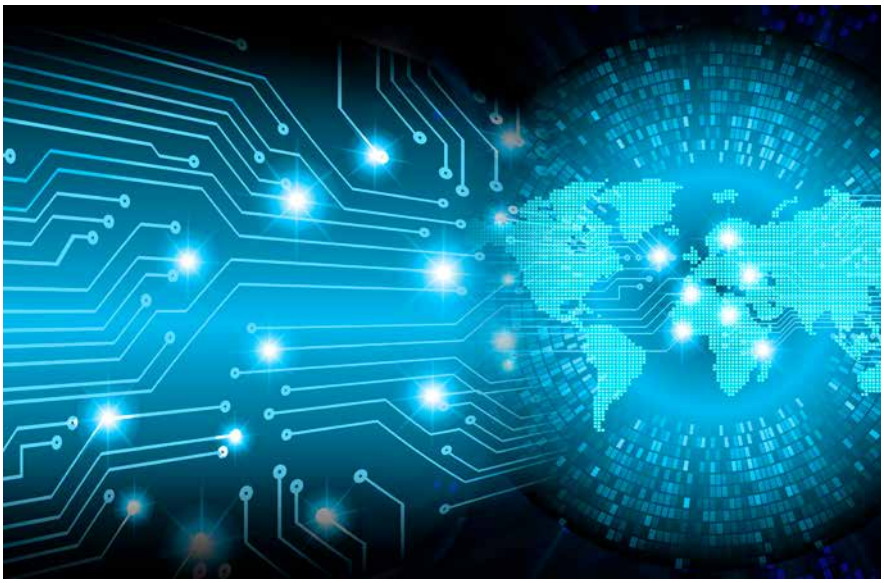
Android Now Fido2 Certified, Accelerating Global Migration Beyond Passwords

Android is now FIDO2 Certified, bringing simpler, stronger authentication capabilities to over a billion devices that use this platform every day.

With this, any compatible device running Android 7.0+ is now FIDO2 Certified out of the box or after an automated Google Play Services update. This gives users the ability to leverage their device's built-in fingerprint sensor and/or FIDO security keys for secure password-less access to websites and native applications that support the FIDO2 protocols.

Web and app developers can now add FIDO strong authentication to their Android apps and websites through a simple API call, to bring password-less, phishing-resistant security to a rapidly expanding base of end users who already have leading Android devices and/or will upgrade to new devices in the future. Mobile apps and websites can now leverage FIDO standards to provide a simpler and secure biometric login for users on over a billion devices supporting Android 7.0+.

The FIDO (Fast IDentity Online) Alliance was formed in July 2012 to address the lack of interoperability among strong authentication technologies and remedy the problems users face with creating and remembering multiple usernames and passwords. The FIDO Alliance certifies authentication devices like biometrics and/or security keys, clients and servers to verify that they comply with FIDO specifications including FIDO2 and meet certain security profiles. This ensures that web users can use their FIDO Certified device across all FIDO-enabled web services for a seamless experience.



"Google has long worked with the FIDO Alliance and W3C to standardise FIDO2 protocols, which give any application the ability to move beyond password authentication while offering protection against phishing attacks. Today's announcement of FIDO2 certification for Android helps move this initiative forward, giving our partners and developers a standardised way to access secure keystores across devices, both in market already as well as forthcoming models, in order to build convenient biometric controls for users," said Christiaan Brand, Product Manager, Google.

Already supported in market by leading web browsers Google Chrome, Microsoft Edge and Mozilla Firefox (with preview support by Apple Safari), FIDO2 is comprised of the World Wide Web Consortium's (W3C) Web Authentication specification and the corresponding Client to Authenticator Protocol (CTAP) from FIDO Alliance. Collectively, these standards enable users to more easily and securely login to online services with FIDO2-compliant devices such as fingerprint readers, cameras and/or FIDO security keys.

"FIDO2 was designed from day one to be implemented by platforms, with the ultimate goal of ubiquity across all the web browsers, devices and services we use every day. With this news from Google, the number of users with FIDO Authentication capabilities has grown dramatically and decisively," added Brett McDowell, Executive Director, FIDO Alliance.

FIDO2's simple user experiences are backed by strong cryptographic security that is transparent to the user and protects against phishing, man-in-the-middle and attacks using stolen credentials. FIDO2 support has been growing since the specifications were introduced last spring. In addition to browser and platform support, several FIDO2 Certified products have been announced to support implementation. SST

Anti-Drone Solution For Airports, Prisons And Military Bases



KNOX, MyDefence's anti-drone system that protects large areas against the threat of drones, is now available for commercial use at airports, prisons, critical infrastructure and military bases.

The system is a customisable end-to-end anti-drone solution with purpose-built RF sensors, drone radars and integrated EO/IR for visual tracking. To accomplish the most effective detect-and-defeat solution, KNOX utilises different sensor technologies, with each serving a purpose in detecting, locating, tracking and defeating a drone threat in the vicinity of the secured area.



For military customers, the solution features reactive smart jamming effectors. This next-generation jamming technology has the least impact on other radio communication. Other sensor technology includes purpose-built drone radars that track the location of drones as well as integrated EO/IR for visual tracking in real-time. The combination of sensor technologies complements each other to provide the best possible protection against unauthorised drones.

KNOX is designed for any scale of installation sites, from prison facilities to large international airports spanning miles across. The anti-drone solution will fortify and harden the perimeter against unauthorised drones in the airspace.

The underlying modularity of the software suite handling inputs from the sensors allows for the anti-drone system to be integrated into a customer's existing security setup, without the need for a standalone system. The seamless integration into a customer's existing security setup results in less required operational training and for a more open platform that can accommodate current and future requirements of the customers. SST

Dahua Technology Safeguarded 2018 FINA World Swimming Championships

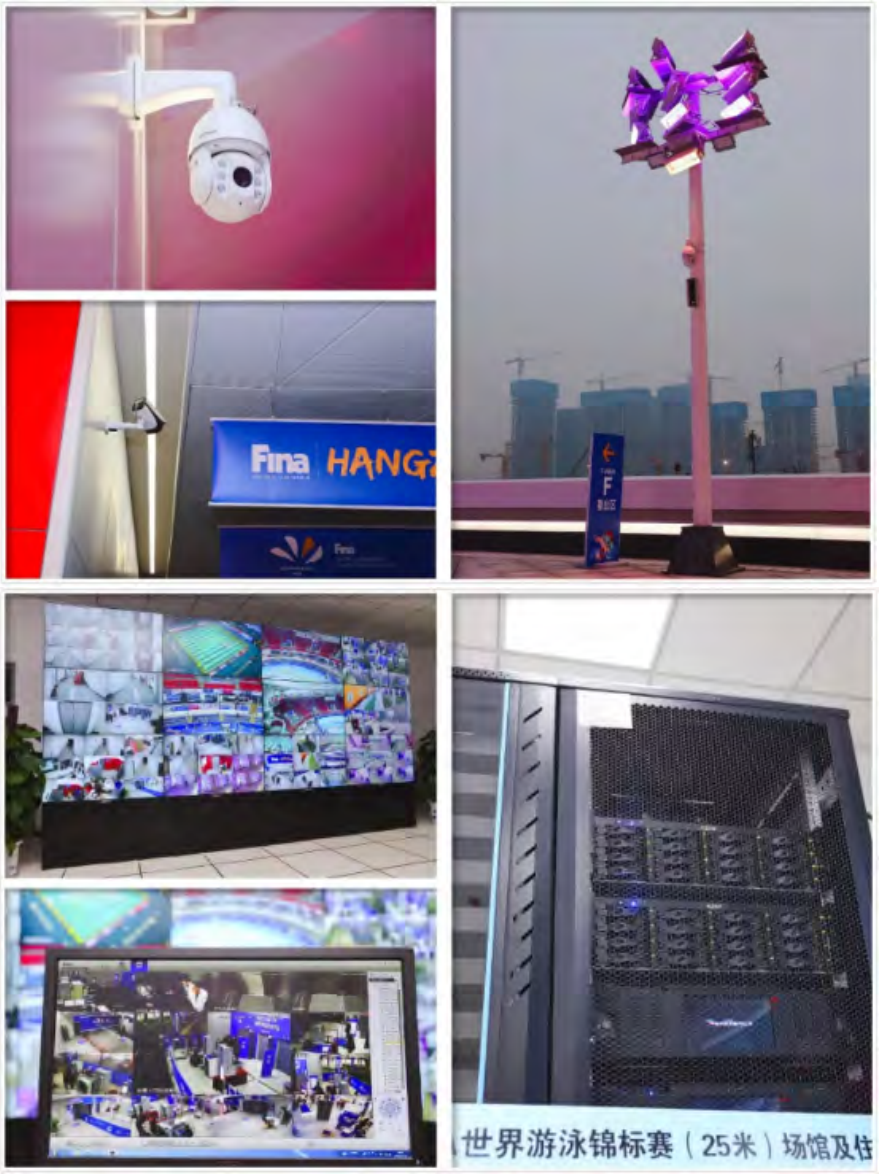
When 1,000 swimming stars from 178 countries came together for the 14th FINA World Swimming Championships held in Hangzhou, China, in December 2018, Dahua technology was used to ensure their safety.

The World Swimming Championships is one of the world's highest level swimming events. It is also the highest level individual international sporting event ever held in Hangzhou. Hence securing the venue is of paramount importance.

Intelligent HD PTZ cameras, fibre cameras, bullet cameras, domes, transmission and other intelligence equipment were deployed in the periphery areas surrounding the venue, important entrances and exits, various passages and commanding points in the venue and security commanding headquarters.

An intelligent security video management system turned the cameras inside and outside the stadium into "smart brains" to guarantee the safety of all at the event.

This ensured full security monitoring of every area, from the periphery to the Hangzhou Olympic and International Expo Center itself. SST



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



Trend Micro Moves Into New Regional Headquarters In Singapore

In January, global leader in cybersecurity solutions Trend Micro moved into a new 12,000-square-foot office space in Singapore.

The new office will serve as Trend Micro's headquarters for Asia Pacific, Middle East, and Africa (AMEA). Trend Micro is also setting up a SaaS endpoint security data centre in Singapore, strengthening data sovereignty for local customers.

Located in Suntec Tower Four, the office will house a team of cybersecurity professionals whose roles span technical, sales, research, operations, marketing, legal, HR, finance and support.

Singapore is chosen for its strong cybersecurity vision, wide-ranging influence across the region, business and cybersecurity hub status, proximity to Trend Micro's customers and diverse talent pool.

In addition, Trend Micro also unveiled new business initiatives for AMEA and Singapore.

The company is building a new managed detection and response security operations centre sitting out of the Singapore office. The centre will focus on helping customers monitor threat activity on a 24/7 basis across their endpoints and network, sweep for indicators of compromise and investigate the root cause of cyber attacks.



The company is also bringing its Certification Program in IT Security to Southeast Asia and Singapore. Participants will get hands-on training over two intensive months of immersive learning and leave with technical knowledge on the nuts and bolts of running a cybersecurity business. SST













HOW AI WILL CHANGE VIDEO



►► By Benjamin Low,
Vice President, Asia Pacific,
Milestone Systems

Video technology is evolving at a furious pace. And artificial intelligence (AI) and machine learning are the major drivers behind this.

Both AI and machine learning have enormous potential to transform video technology and how they will be used to fundamentally change the way we live, work and even shop.

One example will illustrate this. In 2018, Thailand's biggest convenience store chain 7-Eleven implemented facial recognition video technology in its 11,000 stores across Thailand. The technology is used to identify the chain's loyalty programme members, analyse in-store traffic, suggest purchases and even measure shoppers' emotion.

The chain is also using the technology to allow managers to single out loyalty programme members for promotions. Essentially, the chain views video as not merely a surveillance tool but also a marketing tool, a tool to better understand customers, a tool to improve staff efficiency and, potentially, a tool to customise shoppers' in-store experience.



In the healthcare industry, institutions are beginning to use video analytics to improve patient care. Videos for example, are being programmed to alert staff if a patient has gone too long without being checked, or to signal that a patient has fallen and needs assistance.

In almost every sector, AI-powered video technology is already being used to simplify everyday processes, from enabling easier security checks at the airport to allowing passengers to pay for purchases with a smile.

From here on, the tide will only rise, with the projection of one billion video cameras connected to artificial intelligence platforms by 2020[1].

Why AI Is So Potent Today: The Ability To Learn Deeply

AI is the ability of a machine or a computer programme to think, act and learn like humans. Previously limitations of hardware processing power means that machine learning – an application of AI – could only deploy shallow learning of very large data sets, which looks at data in just three dimensions.

With recent, significant advances in processing power of graphical processing units such as a new coding technique known as parallelisation, we can now utilise a deep learning approach where we can look at data in many more levels or dimensions. Hence the word "deep".

Software parallelisation is a coding technique for breaking a single problem into hundreds of smaller problems. The software can then run those 100 or 1,000 processes into 1,000 processing cores, instead of waiting for one core to process the data 1,000 times.

With parallelisation, there is a quantum leap forward in how fast we can solve a problem. Having the ability to solve problems faster allows us to go deeper with a problem and process larger, more complex data sets. As the world's data is set to grow tenfold by 2020[2], for businesses, being able to process data faster and deeper will become a defining factor in whether they can stay ahead of the business curve.

Bringing The Potential Of AI Augmentation To Life

One of the greatest application of AI and machine learning is in performing low-cognitive functions. AI-enabled devices and machines are able to master and perform tasks that humans cannot do very well. With proper aggregation of information, machines can be better at low-cognitive tasks and often deliver a better quality of service than humans.

For example, humans cannot sit and watch two or more video cameras simultaneously. Our attention span simply does not work that way. However, machines are extremely good and detailed at this. While we see objects, the machine sees the smallest finite details – that is, each and every single pixel. Within the pixel, the machine can see even more details: the shade of colours of that image.

By aggregating data and by allowing machines to automate responses and solutions, we can boost humans' interaction with their environment.

Here is one example. Imagine a

[1] Cloud-To-Edge Inference For Smarter Ai Cities, NVIDIA, 2018
[2] Data Age 2025: The Evolution of Data to Life-Critical, SeaGate, 2017

scenario where a law enforcement officer is viewing a large surveillance screen. Between the officer and the large screen is an additional clear screen which can also have video and data cast onto it. Finally, the officer is wearing smart glasses that can project information onto its lenses.

In a surveillance situation, a video feed can be shown on the main screen, while the screen in the medium distance will augment the main screen by appearing to layer extra visuals on top, for instance the face of a suspect. The smart glasses will then show detailed text data, for instance car licence plates or descriptions of suspects. The live video, augmented visuals and text data will work in concert. Data on the main viewing screen can even change to show information according to what the officer is seeing through his smart glasses' lens. While this may sound rather futuristic, it is actually possible today.

With AI, there will be massive advancements in how we review and utilise video and data.

The City of Hartford in Connecticut, United States of America, is a great case study of how technology can be turned into a force multiplier. Working in tandem with local law enforcement and partners BriefCam and Axis, Milestone Systems was able to enhance the City's C4 Crime Center and significantly upgrade the Hartford Police department's ability to prevent and effectively respond to incidents throughout the city.

The Crime Center features the Milestone XProtect Smart Wall, which has thirty 55-inch, 4K video monitors connected to a high-powered workstation, which runs the Milestone XProtect Smart Client on every screen. The Center is staffed almost round-the-clock by civilian crime analysts who monitor the 450 PTZ video network cameras from Axis Communications that are located throughout the city.

With this centre, instead of spending 30 hours doing low-cognitive, manual tasks such as freezing on a rooftop monitoring a drug house all day and night, the City of Hartford's officers now sit at their desk and within just a few minutes, know exactly where a drug house is by seeing an augmented reality of foot traffic over time.

With the enhanced system, officers can simply go into the data and extract the answer with precision and efficiency. Not only are many crimes now solvable, the video technology is





changing how police work will be done in the future.

An Intelligent Industrial Revolution

Having machines take over low-cognitive tasks will be a significant game changer for years to come.

Take Amazon. The online retail giant is applying this to its retail stores where the concept of a checkout is being replaced by customers simply walking out. By using data from smartphones, cameras, sensors, purchase histories and other data points, Amazon is making it possible for its customers to walk into a store, pick up what they need and walk out. Everything else is taken care of by machines. This type of thinking and tool creation is in its earliest infancy but will continue to address areas where value can be added to our lives.

In the book The Inevitable, author Kevin Keely says the next 10,000 startups will be based on finding applications for AI, similar to what happened with electrification during the second industrial revolution. The intelligent industrial revolution is beginning to happen all around us. It will be very disruptive within the security and surveillance industry. But it will also be insightful and liberating as it will free humans to perform higher cognitive processes. SST



HOW TO USE AI TO FIGHT IDENTITY FRAUD



▸▸ **By Glenn Larson,**
VP of Engineering, Acuant

It's no secret that identity fraud is a growing problem: A record 16.7 million US adults experienced identity fraud in 2017, marking an 8% increase from the year before, according to Javelin's 2018 Identity Fraud study.

The number of fraudulent transactions, massive data breaches and instances of identity theft continue to rise as hackers and fraudsters become more sophisticated.

AI Could Be The Solution To Identify Fraud

ID scanning solutions have various strengths; some simply scan an ID's barcode, whereas more robust software performs forensic and biometric tests to ensure that an ID is not forged. All of these ID scanning solutions can be strengthened considerably by applying artificial intelligence.

Artificial intelligence and its subsets of machine learning and deep learning make it possible to accurately process, verify and authenticate identities at scale. Here's how.

Scaling ID Authentication With Machine Learning

Identity documents, such as driver's licenses and passports, are scanned to test various elements of an ID, either on the premises or remotely using mobile devices. Some examples of authentication tests include confirmation of genuine microprint text and security threads, validation of special paper and ink, comparison between OCR and barcodes and magnetic strips, data validity tests, and biometrics or facial recognition to link the individual to the ID credential.

Using machine learning — or automation — creates a more efficient and accurate process compared to relying on an untrained human to look at the document. These solutions should contain an anonymous internal data collection mechanism capable of storing information about the operation and performance of the software. Then,

the data is automatically transmitted to the provider on a regular basis. This process — when automated — saves time and improves the quality of the result.

Why You're Only As Good As Your Data

There are thousands of forms of ID — passports, DHS "Trusted Traveler" cards (Global Entry, NEXUS, SENTRI, FAST), military IDs, permanent resident cards, border crossing cards — and obtaining significant quantities of each type to understand the variations, wear patterns and so on is a monumental task.

Effective ID authentication relies on the collection of metadata on the document recognition and authentication process. Instead of containing information about the document being processed, this metadata contains information about the processes that are run and the details and outcome of those processes. By analysing this information, the software trains itself to detect complex patterns and output a prediction/result. It optimises the performance of the software and library to improve the reliability of the document read and authentication processes.

Using machine learning to differentiate between good and bad IDs is extremely efficient. However, without supervision, the logic developed by the algorithm may exclude IDs that are not fraudulent. There are many reasons why an ID may not pass even though it is valid: wear and tear, other physical damage, manufacturing errors or defects, minor design changes or even variations in production depending on where and how the card was produced (central versus instant issue).

Most states now use central issuance but have the ability to instantly issue an ID in some situations, for VIPs for example. Given that IDs are often not printed in the same location by the same machine, there are often anomalies based on printing quality, misprints or unclear images. It is not uncommon for an entire batch of IDs to contain a manufacturing error.

In addition, a computer must be taught that IDs that are worn or damaged are still valid. Accessing a programme that allows the collection of operational and performance metrics for the software is useful for improving the recognition and authentication of documents supported by the document library of the provider.

A robust document library against which to compare captured IDs is vital; access to a comprehensive and regularly updated library cuts down the time that machines must process data on their own and maximises data extraction and authentication capabilities. Semi-supervised machine learning enables adjustment of the direction of the logic without interfering with the insights that authenticate documents or slowing down data processing.

Data Mining, Semi-Supervised Learning And Regression Analysis In The Feedback Loop

There are multiple models of ID authentication to choose from:

- Data mining: Examining large databases to turn raw data into useful information. For more efficiency, be sure to extract clean data to save time with this process.
- Semi-supervised learning: Relying on completely automated machine learning can result in "failing" documents for items that have experienced wear and tear or ones with document manufacturing errors.
- Regression analysis: This method continually tests and analyses the outcomes to improve the algorithm.

New data is fed into the algorithm to test outcomes. This process is often called the feedback loop. As new data is fed into the algorithm, the feedback loop tests that the outcomes are consistent and improving. The outcomes are then fed into the algorithm so that the software continues to learn and adjust.

When To Use Biometrics For Identity Management

Biometric identity verification methods implement biometrics, such as facial or voice recognition, to strengthen the identity verification process. Not only is it more passive for consumers (since it reduces the need to remember a password or enter PII information), but it's also a more stringent security protocol.

Biometric security solutions utilise deep learning to mimic the way human neurons process extremely difficult information, such as faces and language. With deep learning technology, the software provider can model large amounts of complex data, such as many images and faces.

Facial recognition technology utilises deep learning to learn to match the image on the ID to a person's face. Then the algorithm looks for certain patterns such as basic shapes (eyes, mouth, nose) and complex shapes (complete faces and distinctive shapes), and finally returns an output that indicates whether the image matches the ID's face or not.

Machines + Humans = The Highest Accuracy

Trained professionals using the software can step in to prevent bad customer experiences when the software flags a legitimate ID because it is damaged or worn. During the rare instances when the computer fails to identify what is wrong with an ID, the professional can apply an expert eye, determine what error occurred, and teach the computer how to spot the issue in the future.

The key is to quickly understand what data points are relevant to identifying a document as fraudulent versus results that are noise due to expected variations (wear, damage, manufacturing issues and so on). A human eye can do this much more effectively than a computer. This creates a different method of learning, where new information is being input to the learning model, so the model can improve. SST



US$12 BILLION INTELLIGENT ROBOT MARKET BY 2023



Artificially intelligent robots are among the most exciting fields in AI today. And the market is going to be huge by 2023.

According to Research And Markets, the AI robot market is expected to grow from US$3.49 billion in 2018 to US$12.36 billion by 2023, at a compound annual growth rate of 28.78% between 2018 and 2023.

The major driving factors of the AI robot market are the wide adoption of robots for private use like companionship and entertainment and the push from governments worldwide to develop modern technologies, the report detailed.

Among all technologies, machine learning is expected to hold the largest share of the AI robot market in the forecast period. Machine learning enables robots to analyse and learn from different working environment, thereby making the robots safer and efficient. This technology aids in creating accurate models that can guide future actions and rapidly identify patterns at a scale that was not achievable before.

Software is expected to hold a major share of the AI robots market in the forecast period. The software integrated into an AI system is responsible for carrying out complex operations and providing learning capabilities. The market for hardware is also expected to grow at a high rate in the same period.

Military and defence applications are expected to hold the largest share of the AI robot market in 2018. Increasing budgetary constraints, along with the decline in the recruitment of defence force personnel and equipment by countries in the Americas and Europe, necessitate the development of innovative and cost-effective robots to accomplish military missions. The market for stock management applications is expected to grow at the highest rate during the forecast period.

Among all regions, Asia Pacific is expected to hold the largest share of the AI robot market in 2018. In addition the market in this region is expected to grow at the highest rate during the forecast period. Countries such as China, Japan and South Korea contribute to the growth of the AI robot market in the region. The increasing adoption of deep learning and NLP technologies for retail and security applications is also driving the growth of the market in this region.

The two big factors holding down the AI robot market are the resistance against adopting new technologies and the lack of standardised laws to manage risks related to networked and autonomous robots.

By application, the market is segmented into:
- Military and Defence
- Personal Assistance and Caregiving
- Public Relations
- Education and Entertainment
- Research and Space Exploration
- Industrial
- Agriculture
- Healthcare Assistance
- Stock Management

The types of robots include:
- Service Robots
- Ground Robots
- Aerial Robots
- Underwater Robots
- Industrial Robots
- Traditional Industrial Robots
- Articulated Robots
- Scara Robots
- Parallel Robots
- Cartesian Robots
- Collaborative Industrial Robots

Products include software, hardware, AI solutions, AI platforms, processors, storage devices and network devices. SST



FAST-GROWING GLOBAL ARTIFICIAL VOICE BOX MARKET TO HIT US$24 BILLION BY 2024



Artificial intelligence in speech recognition is transforming voice recognition technology. The high level of accuracy achieved currently meant that speech technology is ready for the enterprise market, according to J Arnold and Associates analyst Jon Arnold.

Google's technology for artificial intelligence in speech recognition, for example, achieved 95% accuracy, according to venture capital firm Kleiner Perkins Caufield & Byers.

This growing accuracy of speech and voice recognition and the inflated demand for multifactor authentication are two factors driving the rapid growth of the global voice box market.

According to market research and consulting firm. Market Research Engine, the market is expected to exceed more than US$24 billion by 2024 at a compound annual growth rate of 19% between 2018 and 2024.

The other major factors driving this growth are growing demand for voice authentication in mobile banking applications and growth in voice control based smart assistive devices in consumer and enterprise vertical.

Market Research Engine highlighted that the greatest opportunities for the market lie in development of speech and voice recognition software for micro-linguistics and local languages, and the application of speech and voice recognition in service robotics.

However, the market is held back by the inaccuracy of speech and voice recognition systems in noisy and harsh working environments and oligopoly in the development of speech and voice recognition technology.

The lack of a standardised platform for the development of customised speech and voice recognition software products is another barrier. SST

HUMANS VS MACHINES: AI AND MACHINE LEARNING IN CYBERSECURITY







▸▸ By Estelle Chiu, Customer Success Manager, Horangi Cyber Security

Artificial Intelligence is fronting a new techno-tsunami that is transforming the way we live and work.

"Historically, an antivirus researcher might see 10,000 viruses in a career. Today there are over 700,000 per day," said Ryan Permeh, Chief Scientist at Cylance. Could AI be the solution to solving the big data problem, and bridging the widening workforce gap in the cybersecurity industry?

Intelligent machines now have the power to make observations, understand requests, reason, draw data correlations and derive conclusions. Not only can AI help effectively detect anomalies and tackle manpower shortage, but it can also support rapid incident response operations against zero-day threats.

According to research by Cylance, 62% of security experts believe that there will be an increase in AI-powered cyber attacks in the near future. Bad actors could significantly develop their phishing attacks by using AI to circumvent machine learning based phishing detection systems. In an experiment by Cyxtera, two attackers were able to use AI to improve their phishing attack effectiveness from 0.69% to 20.9%, and 4.91% to 36.28%, respectively. AI may be used as an intelligent cyber weapon to counter these attacks.

Is AI the answer to patching all the flaws in our security systems? Is it making IT professionals redundant? Beyond the hype, any future-proof business must consider the applications and implications of this incoming wave.

The Power Of Machine Learning

Traditionally, cybersecurity has relied on rules-based or signature-based pattern matching. Detecting anomalies instinctively, with real-time data, is actually a method that's been around for years to detect spam in our inbox. Similarly, with antivirus, researchers at antivirus companies find malware and generate signatures that can be used to check files on an endpoint to see if they match a signature of known malware. The system must know what it is looking for in order to find something. This means that one can only detect malware that is known and that matches a virus definition or signature.

With AI, instead of relying on code signatures, machines can analyse the behaviour of the programme and use machine learning to find a match, where that behaviour is predictive of malicious code. These algorithms are able to predict security trends and identify behaviours and data patterns, picking up on suspicious activity that has never been encountered before, also known as "zero-day" malware. A simple analogy is when you introduce a cat to a little child



who has never seen a cat before. Without explaining what is a cat, you expose the child to a few different cat breeds and this supervised training process helps the child learn.

Soon enough, the child will be able to start recognising an animal never seen before as a cat. AI self-learns through capturing, processing and classifying huge chunks of data at one time. Once new malicious trends have occurred, the machine will automatically pick up the threat. It will also keep constantly up to date with current fraud trends so that it is able to stop the next breach from happening.

Ability To Detect And Predict New, Complex Threats

Conventional technology is past-centric and depends heavily on known attackers and attacks. This means blind spots when it comes to detecting abnormal events in new-age attacks. This limitation of older defence technologies is now being surmounted via machine learning.

With machine learning, any privileged activity within an internal network can be traced, and any sudden or significant spike in privileged access activity can be tracked and examined as to whether it is generated by an insider threat. If an attack is successfully detected, the machine will reinforce the validity of the actions and become more sensitive to detecting similar future patterns. With larger amounts of data and examples, machines can better learn and adapt to spotting anomalies more quickly and accurately. This is especially useful as cyber attacks are becoming increasingly sophisticated, and hackers are coming up with new and innovative approaches that older security technologies would be slow to detect.

Ease Burden On Cybersecurity Personnel

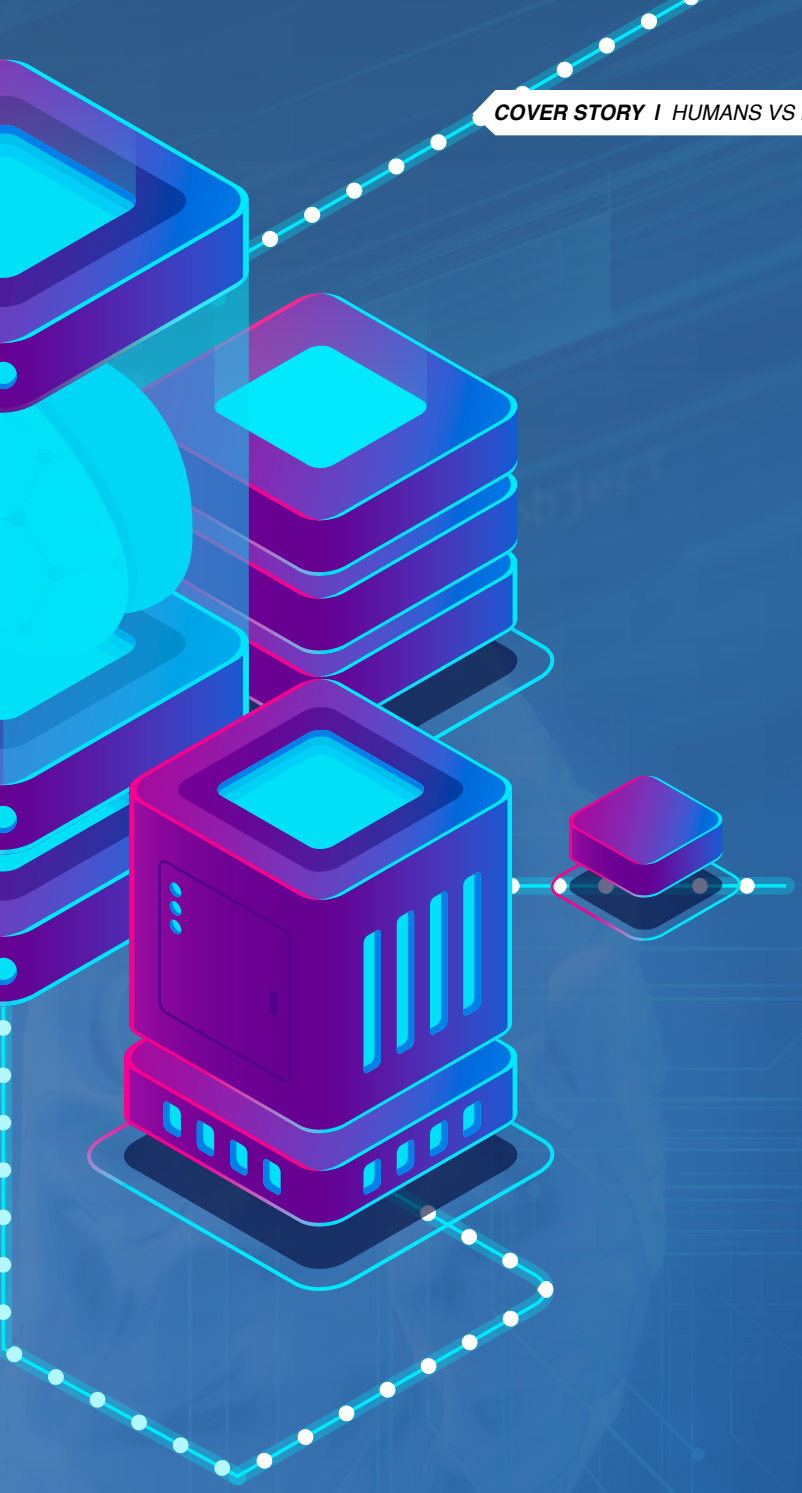
Machine learning is most effective as a tool when it has access to a large pool of data to learn and analyse from. With machine learning, organisations can apply predictive analytics to reduce attack surfaces.

In contrast, humans find it difficult to cope with high volumes of data. The sheer number of security alerts that appear daily can be very overwhelming for the security team. As substantial quantities of security data are being generated and transferred over networks every day, it becomes progressively difficult for cybersecurity experts to monitor and identify attack elements rapidly and reliably.

This is where AI comes in handy.

AI is able to monitor and make sense of the copious data. Machine learning can help cybersecurity personnel respond to scenarios that they have not specifically encountered before, replacing the laborious process of human analysis. Automating threat detection and response helps lighten the load of cybersecurity professionals and can aid the detection of threats more efficiently than other software-driven methods.

AI and machine learning also assist IT security professionals in achieving good cyber hygiene and enforce robust cybersecurity practices.



With AI, cybersecurity becomes less about the incessant hunting down of malicious activity, and more about continuous prevention, prediction and improvement. It could potentially solve the widening talent gap in the cybersecurity industry.

Limitations Of AI And Machine Learning

One of the greatest challenges in the adoption of AI technology is the quality of deployment.

For a machine learning engine to perform well, it must retrieve the right data, extract the correct features and cast the appropriate angle on those features. This requires good training by the humans running the engine.

If trained poorly, the engine will make inaccurate predictions. Models are only as good as the data that is fed in. Companies who only perform end-point detection will likely miss out on the benefits of AI as they lack the data required to leverage on AI.

Seeking Human-Machine Symbiosis

"Cyber attacks aren't a statistical phenomenon. There is a human attacker behind these threats. We have a living and breathing adversary on the other side of the internet coming up with new methodologies daily," said Kevin Lee, Executive Chairman of Horangi Cyber Security.

Many cybersecurity experts have bold opinions as to whether machines should be responsible for managing something as complicated as cybersecurity. According to the Institute of Electrical and Electronics Engineers, responsibility for decisions should still be made by the humans of the organisation. Refusing to take ownership of the machine's actions and pushing the liability onto machines is foolish and could create a regulatory and public backlash.

Only a human can understand the business context of why an attacker might be after a piece of information and what his motivations are.

Machine learning is an effective tool against both known and unknown malware, as it can identify and understand malicious activity when applied properly. However, it should not be the only solution. "The combination of human and machine is superior to machine alone or human alone," said Lee.

Ultimately, the future requirements of cybersecurity are an interplay of advances in technology, legal and human factors and mathematically verified trust. Effective cybersecurity should be about striking a balance between humans and machines. Humans make sense of data by ensuring machine-suggested actions have business value too. Humans add business, legal and commercial elements to decision making, while machines have the capacity and speed to analyse and interpret big chunks of data. Both human intelligence and artificial intelligence must work symbiotically for optimal results. This is the way towards a comprehensive solution that protects against the full spectrum of threats facing today's businesses. SST

AI AND THE CYBERSECURITY INDUSTRY: MAGIC BULLET OR HYPE?





▸▸ By Boris Cipot,
Senior Security Engineer,
Synopsys Software Integrity Group

Today many companies are using new artificial intelligence (AI) solutions to combat cyber attacks. Keeping this emerging tech reality in mind, the million-dollar question becomes: Will AI slay the beast?

Unfortunately, AI isn't going to be the magical solution to resolve all vulnerabilities. Not just yet anyway.

Many companies are working to implement AI algorithms to automate threat detection and response. And this is a good thing! However, it's important to also understand that automation and AI are two entirely different things.

Automation is rule based. It is often referred to as machine learning. AI, on the other hand, is when a software is trained to learn and adapt based on data received. The fact that a software is able to adapt to changes, especially in a landscape as quickly changing as the cyber threat landscape, is very promising. However, AI is still at a very immature stage of development.

AI's promise of bringing cognition to the realm of software has been exciting tech enthusiasts for many years. The fact remains however that it is still software. And as we should all know by now, software (particularly web-based software) is vulnerable.

The future, however, is bright.

Interactive application security testing (IAST) solutions, such as Seeker by Synopsys, allow software developers (including those developing web-based AI applications) to perform security testing during functional testing. Seeker helps organisations identify and manage security risks associated with vulnerabilities discovered in running web applications using dynamic testing techniques. It uses software instrumentation techniques to monitor an application to detect vulnerabilities. This technology is very compatible with the future of AI.

Importance Of Software Security In AI

Software security is always an important part of any product, whether the product is in the development stage or in the usage stage. AI is no exception.

If you consider all the possible applications (health, automotive, robotics) of AI, the importance of software security for the development of AI applications is at a really high level and should be of high concern throughout the application's life cycle.

Just imagine if someone were to take control of your AI device or software and give you false answers. Or think about an even simpler scenario: an attacker who is able to control the input information that your AI needs to process — the input information that the AI will act on. For example, an attacker who is able to control the sensorics input of the surroundings in a car. Getting wrong information as input would lead to wrong decisions, which can potentially endanger lives.

There are more examples in which a breach could make an AI application not only not useful but also dangerous. Bottom line: the development and usage of AI must be absolutely secure.

AI: Does It Make Our Life Better Or Worse?

AI is nothing new. We have been living with it and its implications for several years now. It has been improving and the computation hardware advances have made it possible to have even more AI applications in our lives.

There is no doubt that AI brings a great many benefits into our lives. It allows us to achieve advances in medicine. When deployed in common applications, it supports lifestyle goals and can boost the quality of life. Take a language translator for example. Thanks to AI, this type of application can translate your native language into that of another language — in real time.

But there are also concerns. The dark side of AI is that it can be used also to do bad in the cybersecurity world. It is good that we have concerns about how AI can impact our lives. This pushes us to be more cautious and try to find mechanisms that will avoid catastrophes in respect to AI's decisions and actions. In the end, I am positive that AI will make our lives better.

How Will AI Evolve in the Near Future?

AI in industry applications is nothing new. The drive to greater automation is always there. What AI offers is to make manufacturing and production processes safer and more efficient.

Increasingly, we are seeing great advances in home robotics, whether they serve as robot companions, robot pets, or smart devices like refrigerators and cleaners. They are becoming increasingly common in households.

What's interesting is the AI push in the direction of do-it-yourself (DIY) processes. 3D printing, for example, has been adopted by many tinkerers who like to make creations in the comfort of their own home. 3D has become incredibly easy to use in the last few years and its adoption rate has risen accordingly. Combine this with the easy development of software for microcircuits such as Arduino or Raspberry PI and I think we will see many more people making AI applications and devices at home, from robotic appliances to smart clothing. SST

ARTIFICIAL INTELLIGENCE IN CYBERSECURITY: BEYOND THE HYPE



►► **By Matthew Bennett,** Vice President and Managing Director, Asia Pacific & Japan, Carbon Black



Artificial Intelligence (AI) and Machine Learning's (ML) roles in preventing cyber attacks have been met with both hope and scepticism. They have been marketed as game-changing technologies though doubts still persist, especially when used in siloes. In a survey by Carbon Black, 74% of the respondents said that AI-driven cybersecurity solutions are still flawed, while 70% believe that attackers can bypass ML-driven security technologies[1].

Despite the hype around AI, it is not an all-encompassing solution to all our cybersecurity challenges. There is still a long way to go before we can fully rely on them. That said, these technologies can still bring tremendous value to cybersecurity teams as long as organisations are cognisant of the risk-benefit trade-offs and can strategically plug the gaps to build a robust cybersecurity programme capable of tackling today's sophisticated threat landscape.

Timely Intervention

The most obvious benefit of AI is its ability to sift through significant amounts of data – a process that used to take days or weeks is now completed within minutes or hours. It is also an incredible resource for highlighting non-obvious relationships in big data that might escape the human eye. This translates to exceptional real-time intel that enables cybersecurity teams to respond to and mitigate potential threats in a timely manner, thus preventing or minimising costly damages.

Thailand, for example, is using AI to monitor network traffic and conduct big data analyses to detect suspicious user behaviour[2]. According to a government spokesperson, AI can help to protect the country's burgeoning digital economy by alerting them of malicious activities as soon as possible.

The caveat here is that cybersecurity responses must still come from a human. One of the most commonly cited flaws of AI is that it is incapable of mimicking the cognitive thinking that humans possess. Simply put, AI should be harnessed for detection and threat hunting; decision making and response activations should be performed by the cybersecurity team.

Mind The Gap

Another challenge that global cybersecurity teams are facing is the shortage of cybersecurity professionals. The Cyber Security Agency of Singapore announced that Singapore is set to face a potential talent shortage of up to 3,400 cybersecurity professionals in 2020[3]. While many higher education institutions are building cybersecurity programmes and awareness of the need for skilled professionals has never been higher, the skills gap is not something that can be bridged overnight.

In the interim, teams can leverage AI-driven systems' ability to learn behaviour patterns of its own team members. By offloading these predictable and routine tasks, the scarce security expertise can be allocated for more strategic activities including investigations and cyber forensics.

Yet, there is much to be cautious about, and one must understand that technology will not be able to fully replace skilled professionals. No matter how quick or efficient it may seem, AI is ultimately programmed and trained by humans. AI-driven security will only work as well as it's been taught to; and it takes continuous experimentation, close human supervision, and swift troubleshooting to be made effective.

Beyond The Hype

AI has the potential to significantly boost APAC's cybersecurity capabilities, but organisations must ensure that these technologies are employed as an addition to modern information security programmes, and not a replacement.

AI can assist, augment and empower human decision making for swifter and more accurate responses. However, without the full aptitude of human cognition, AI cannot be exclusively relied upon as a sole protection.

Full AI adoption is going to take a while; 87% of researchers Carbon Black surveyed believe it will be years before we can trust AI to lead cybersecurity decisions[1]. In moving towards that goal, APAC organisations should secure a firm foundation. Educating employees with the appropriate knowledge and skills, such as good security postures and security hygiene, is a great start. Beyond that, empowering security teams with the tools they need to proactively hunt threats will go a long way in keeping attackers at bay. SST

[1] Carbon Black, research report, Beyond the Hype – Security experts weigh in on Artificial Intelligence, Machine Learning, and non-malware attacks
[2] Digital Government Development Agency of Thailand, interview, How Thailand is using AI for cybersecurity
[3] A.T. Kearney, research report, Cybersecurity in ASEAN: An Urgent Call to Action



Keeping Patients Safe At NHS Facilities In England

Video technology from IDIS has been chosen by Southern Health NHS Foundation Trust for a comprehensive upgrade across their facilities in Hampshire, England. In one of the largest projects of its kind, the new system will improve safeguarding at a number of sites for patients requiring specialised mental health care in a secure setting.

IDIS is the largest video surveillance manufacturer in South Korea with more than two million recorders installed worldwide and over 16.5 million cameras utilising IDIS technology.

Gaps In Coverage Plugged

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

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

This was a major issue because staff at Ravenswood House are caring for vulnerable people and if an incident occurs, it's vital that the establishment can quickly access recordings that show exactly what happened. Delays in investigations can result in interrupted care delivery and costly disruption, hence delays must be minimised.

Because of the sensitive nature of the care being provided, the vulnerability of patients and the risks to staff, it was essential that the video solution not only must be network secure but can also be relied on to capture scenes in close detail in all lighting conditions. Southern Health wanted a fully managed system that links all their sites onto their local LAN without

the risk of system hacking, which is a key NHS consideration in selecting any IP CCTV solution.

The IDIS equipment was identified as the best for the project following a full proof-of-concept comparison, with equipment set up onsite to demonstrate picture quality and ease of use. Compared to a previously installed IP video system, which comprised a mix of equipment from different manufacturers, the IDIS setup offers lower cost of ownership due to ease of use and simple installation and maintenance combined with industry-leading warranty.

IDIS is also fully network tested and approved, which means it is secure enough to be linked to the wider NHS network at any point in the future, giving NHS the option of centralised monitoring and control.

Another advantage is that the IDIS 12MP fisheye cameras allow all events to be captured automatically without the need for operators to focus in on an incident. Recordings from the new cameras deliver a 360-degree view of any given area without any blind spots. Just as importantly, the system is easy to use, and the footage can be accessed quickly. The fisheye units offer a choice of six de-warping view modes and ensure night-time IR viewing at up to 15 metres.



Completed by security integrator ISD Tech, the Ravenswood House rollout saw the installation of almost one hundred 12MP vandal-resistant IR Fisheye cameras as well as full HD IR domes, DirectIP® H.265 4K recorders, PoE switches and full-HD monitors.

The new system also overcomes a particular loophole at Ravenswood House: in some areas motion-sensor activated lighting was not sensitive to very slow movement. As the previous system did not have IR capability, this meant the system could not capture images. This increased the vulnerability of both patients and staff. However the built-in IR capability in the IDIS fisheyes enables the capture of crisp, clear images even in darkness.



The new solution also features IDIS's Smart Failover technology which protects against loss of footage due to potential fault conditions, including network instability, network failure, storage failure, recorder hardware failure and power supply failure.

IDIS and ISD Tech worked particularly closely to ensure the phase one installation went smoothly, said Nicky Stokes, ISD Tech's Managing Director. "Our engineers had to be very sensitive and careful working on this project because of the nature of the site and the needs of the patients. Everything went smoothly; IDIS equipment really is 'plug and play', which made our job much faster."

With phase one completed, full rollout of IDIS technology at other Southern Health NHS Foundation Trust sites will continue through 2019. SST

2018 Global Smart Home Device Revenue Reached US$28 Billion



▸▸ **By Blake Kozak,**
Principal Analyst, Smart Home and Security Technology, IHS Markit

Worth US$18 billion in 2017, the global smart home market is forecast to reach US$28 billion in 2018.

Leading the growth in this market are connected appliances, smart speakers and connected lighting. The global installed base of these products totalled 361 million devices in 2017, which means the penetration rate for smart home devices was 9% of broadband households globally in 2017.



The installed base of smart home devices is expected to expand to about 560 million devices by the end of this year.

Although still a bourgeoning market, the smart home is no longer just for hobbyists or techies, and device manufacturers and service providers are looking to take these technologies to the masses. They will accomplish this by focusing on what customers know and understand, which includes video cameras, smart speakers, thermostats and home gateways.

Video Surveillance

Video surveillance for the smart home can become a gateway for other connected devices in the home in two ways. First, the average consumer already understands the value of security cameras better than he understands connected lighting or other devices, which can be perceived as novelty purchases. As such, the learning curve for consumers is less steep. Second, adding video security in the home is a sign of consumer trust, signalling their tacit acceptance of the possible loss of privacy that comes with the installation of smart, connected



> ***Leading the growth in this market are connected appliances, smart speakers and connected lighting. The global installed base of these products totalled 361 million devices in 2017, which means the penetration rate for smart home devices was 9% of broadband households globally in 2017.***

devices. Smart home video surveillance will also stimulate consumer curiosity and willingness to learn about smart home technology, inevitably leading to greater adoption.

Smart Speakers

More than 22 smart speakers have been launched so far in 2018. And more than 56 companies are either already offering a smart speaker or planning to offer one in 2019. Furthermore, smart speakers are now being embraced by some of the top players in audio, such as Bang & Olufsen, Harman, Bose and Sonos – all of which have already launched, or plan to launch, smart speakers by the end of this year. Other companies are also getting more involved in smart speakers, such as Netgear, Deutsche Telekom, Samsung, Facebook, Insignia (Best Buy) and Motorola. The Microsoft Cortana smart speaker and another new entry from Nokia are also rumoured to be set for release in 2019.

Routers And Gateways From Service Providers

Routers and gateways with embedded voice assistants and smart home radio-frequency technology will gain more traction in 2019. Deutsche Telekom made progress this year with its Speedport Smart router – soon to be into its third generation with smart home features enabled - and Comcast launched its xFi Advanced Gateway with smart home capabilities for its gigabit broadband subscribers. However adoption of these service-provider gateways continues to be pushed out, because the time to market can be long and rollouts are often limited at the start. As a result, IHS Markit expects that this year and next year there will be a major influx of service providers announcing limited releases of routers with smart home functions. SST

Why Mobile Credential Is More Secure Than Card-Based Systems



▸▸ **By Scott Lindley,** General Manager, Farpointe Data

In recent years, integrators and customers have focused on ensuring that their card-based access control systems are secure.

To give businesses extra incentive to address cybersecurity threats, the Federal Trade Commission these days holds the business community responsible for failing to implement good cybersecurity practices and has proceeded to file lawsuits against those that don't. The Federal Trade Commission filed a lawsuit against D-Link and its U.S. subsidiary, for instance, alleging that its inadequate safeguards on its wireless routers and IP cameras left them vulnerable to hackers.

Even as companies are learning how to protect card-based systems, along comes mobile access credentials and their companion readers that use smartphones instead of cards as the vehicle for carrying identification information.

Mobile Credentials: A Rising Tide

Gartner suggests that by next year, 20% of organisations will use mobile credentials for physical access in place of traditional ID cards. Let's rephrase that last sentence. In less than nine months, one-fifth of all organisations will use the smartphone as the focal point of their electronic access control systems. Not proximity. Not smart cards. Phones!

Smartphone Credentials Are Inherently More Secure

While many companies perceive that they are safer with a card, in my opinion, mobile access can be a far more secure option.

Why are smartphone credentials more secure? To start, the smartphone credential is a multi-factor solution.

Access control authenticates you by scrutinising three things. It:

- recognises something you have (RFID tag/card/key),
- recognises something you know (PIN) or
- recognises something you are (biometrics).

Your smartphone will have all three of the above authentication parameters. This makes smartphone credential, by definition, a multi-factor solution. Your mobile credentials remain protected behind a smartphone's security parameters such as biometrics and PINs. Once a biometric, PIN or password is entered to access the phone, the user automatically sets up a 2-factor access control verification - what you know and what you have or what you have and a second form of what you have.

In addition, you can't access the credential without having access to the phone. If the phone doesn't work, the credential doesn't work. The credential operates just like any other app on the phone. The phone must be "on and unlocked". These two factors – availability and built-in multi-factor security verification – are why organisations want to use smartphones in their upcoming electronic access control implementations.

Plus, once a mobile credential is installed on a smartphone, it cannot be reinstalled on another smartphone. Think of a soft credential



as being securely linked to a specific smartphone. If a smartphone is lost, damaged or stolen, the process should be the same as for a card. It should be immediately deactivated in the access control management software, with a new credential issued as a replacement.

Leading smartphone readers additionally use AES encryption when transferring data. Since the Certified Common Criteria EAS5+ Computer Interface Standard provides increased hardware cybersecurity, these readers resist skimming, eavesdropping and replay attacks.

When the new mobile system leverages the Security Industry Association's (SIA) Open Supervised Device Protocol (OSDP), it also will interface easily with control panels or other security management systems, fostering interoperability among security devices.

Likewise, new soft systems do not require the disclosure of any sensitive



end user personal data. Activating newer systems simply requires the phone number of the smartphone.

A special word of caution here. Many legacy systems require the use of backend portal accounts. In addition to being rich caches of sensitive end user data, a target of hackers, these portals can include hidden fees. What are these annual fees? Are they fixed through the life of the system? And who's responsible for paying? It is best to simply avoid these types of systems.

Smartphone Credentials Can Do Much More

Plus smartphones offer many more features to be leveraged. What are these features? They include biometric capture and comparison as well as an array of communication capabilities from cellular and Wi-Fi to Bluetooth LE and NFC.

Anything a card credential can do can be replicated by a smartphone credential. However, smartphone credentials can exploit new technologies in a way not possible with cards.

As Suzi Abell of 3xLOGIC wrote in the September 14, 2018 issue of SIA newsletter, "a credential – supporting two-way communication with active notification capabilities – can be leveraged to send automated or ad-hoc notifications to users. Add location services and geo-fencing capability, and you can send notifications only to those people who are within a specific geographic area. And you can further target those notifications to specific people."

She suggests, "Stop treating a smartphone like a legacy credential; no one should ever 'badge' a phone at a reader. By using location services, administrators will define how near to the door a person must be to request access. A mobile app that functions as the user's credential and provides two-way communications with a central monitoring station will also provide a path for two-way emergency communications. For example, an employee leaving the building at the end of the shift on the way to her car can quickly and easily ask for assistance or notify security of a potential issue remotely via the mobile device in her hand."

Lower Installation Costs With New-Generation Smartphone-Based Implementations

Newer solutions provide an easier way to distribute credentials with features that allow the user to register their handset only once and need no other portal accounts, activation features or hidden fees. Users don't need to fill out several different forms.

Some older mobile systems force the user to register themselves and their integrators for every application. Door access – register. Parking access – register again. Data access – register again, with each registration requiring the disclosure of sensitive personal information.

By removing these intrusive information disclosures, these new solutions also get rid of privacy concerns that have been slowing down adoption of this technology. All that is needed to activate the credential is simply the phone number of the smartphone. When mobile credentials are sold from OEM to integrator to end user, it avoids setting up multiple accounts and eliminates sensitive personal information from being available for hacking.

Bluetooth or NFC?

Bottom line: both Bluetooth and NFC credentials are safer than hard credentials. However, read range difference makes a difference between the two.

There are advantages to a closer read range. NFC eliminates any chances of the smartphone unknowingly getting read as can happen with a longer read range. There are also applications where multiple access readers are installed very near to one another due to many doors being close to each other. One reader could open multiple doors simultaneously. The shorter read range or tap of an NFC-enabled device would remove such problems. However, it must also be understood that Bluetooth-enabled readers can provide various read ranges, including tap range.

There are advantages to a longer reader range capability. Since NFC readers have such a short and limited read range, they must be mounted on the unsecure side of the door. This exposure breeds problems. In contrast, Bluetooth readers can be mounted on the secure side of doors and kept protected out of sight.

Also, you don't want hackers listening in on your Bluetooth transmissions, replaying them and getting into your building. So make very sure that the system is immunised against such replays. That's simple to do. Your manufacturer will show you which system will be best for your application. Research shows that Bluetooth-enabled smartphones are continuing to expand in use to the point where those that are not Bluetooth-enabled are already the exceptions. There is no doubt that Bluetooth-enabled smartphones are going to be a major force in physical and logical access control.

Scott Lindley is a veteran of the contactless card access control industry. SST

Video Verification Is Combating False Alarms





►► By Anna Sliwon,
Security Analyst, IHS Markit

In 2017, nearly 23% of residential intruder alarm systems - including professionally installed systems, connected do-it-yourself (DIY) systems and multiple-system operator systems - were sold globally with some form of video verification. This penetration is forecast to increase to nearly 32% by 2022.

Why the growing popularity of video verification? To a large extent, it's because video verification solves the problem of false alarms.

False alarms are a major problem plaguing the intruder alarm and remote monitoring services industry. Between 90% and 95% of alarms reported to the central monitoring stations turn out to be false. These false reports cost service providers, who must send out a response team to verify each and every alarm. It also strains local police resources and could even increase the financial burden on end users, depending on local alarm response regulations and potential fines.

Video verification reduces false alarms by offering an undisputed remote confirmation of the nature of the alarm in the shortest possible time. This helps speed up the operator's response process. Video images can be transferred in real time to the operator, so it can be assessed almost immediately and a response team or police forces sent without delay.

The Role Of DIY, Smart Homes And Consumer Video

The popularity of video verification solutions is boosted by trends in the DIY security, smart home and consumer video market.

DIY: Consumer video cameras today are typically high-resolution internet-protocol (IP) cameras that allow users to check on their home and review footage of past events at their convenience. This can be done by viewing videos via a dedicated intruder alarm mobile phone application.

Smart home: Smart home/building automation systems are becoming more popular with end users in all sectors. Cameras are usually advertised alongside smart plugs or smart lights, which gives users an extra level of control over what is happening in the house. Some cameras also offer smoke detection features that support traditional smoke detectors, while providing surveillance of self-monitoring and verification to users. With alarm monitoring stations increasingly offering smart home monitoring services, the video verification market will receive a boost from this side of the industry.

Consumer video: The number of consumer video devices available on the market is growing rapidly, providing a much broader choice of solutions at various price points. End users can add an IP camera to their home systems and enjoy low-cost self-monitoring and self-verification functionality.

Benefits To Installers, Dealers And Remote Monitoring Stations

Many central monitoring stations now offer video verification for an extra fee added to their basic monitoring services. For service providers, adding video verification to the monitoring package reduces the likelihood the subscriber will cancel the contract or choose another provider offering more comprehensive services.

Video verification can also benefit installers and dealers that want to offer a broader range of services to their customers. Cloud hosting and support for video self-monitoring delivers greater value to end users. Installers may also find themselves closer to their customers compared to remote monitoring companies.



This makes it easier for installers to increase customer awareness about new offerings. In any case, partnerships between installers and remote monitoring stations can increase revenue per user and provide a more stable annual income. Subscriptions generated by installers could offset normal attrition rates experienced by remote monitoring companies.

Barriers To Broad Adoption

There are three main barriers to broad adoption of video verification.

Cost: Even though the benefits of including video verification with intruder alarm systems are clear, many end users – particularly those in the residential sector – may struggle to afford video devices. Passive infra-red (PIR) camera detectors can be three times more expensive than PIR detectors that are not video based.

Privacy and cybersecurity: Residential users have grave concern about privacy issues surrounding video verification and video cameras. The main worry is that a hacker will use the device to watch and listen in on the private lives of residents. There have been media reports of attackers successfully compromising consumer video IP cameras. This kind of reports can delay the decision to buy video-based devices. Another concern is that alarm-monitoring operators could be watching residents in their homes, outside of the authorised time. Providers of video verification solutions must make sure their systems are designed with privacy protections built into the system setup, giving the user the ability to restrict access to video devices whenever they want to.

The trend towards self-monitoring: The increasing availability of consumer video devices and DIY security systems that incorporate video products into the offering has led to the emergence of self-monitoring and self-video verification. Such systems usually come pre-configured to handle video files, which makes adding a consumer video camera much easier and lowers the barriers to adoption related to the complexity of the system setup. SST

2018 Was The Year Of The Next-Gen Cyber Attack



2016 may have been The Year of the Fileless Attack and 2017 may have been The Year of Ransomware but 2018 was The Year of the Next-Gen Cyber Attack, according to endpoint security provider Carbon Black.

The year saw several high-profile, global-scale cyber attacks. In 2018 billions of personal records were stolen in 2018, unearthed in breaches that successfully targeted household names in government, technology, healthcare, travel and hospitality.
In Singapore, the greatest data breach to date took place in 2018 with the SingHealth attack, with personal data of 1.5 million patients compromised.

Constant Onslaught Of Attacks

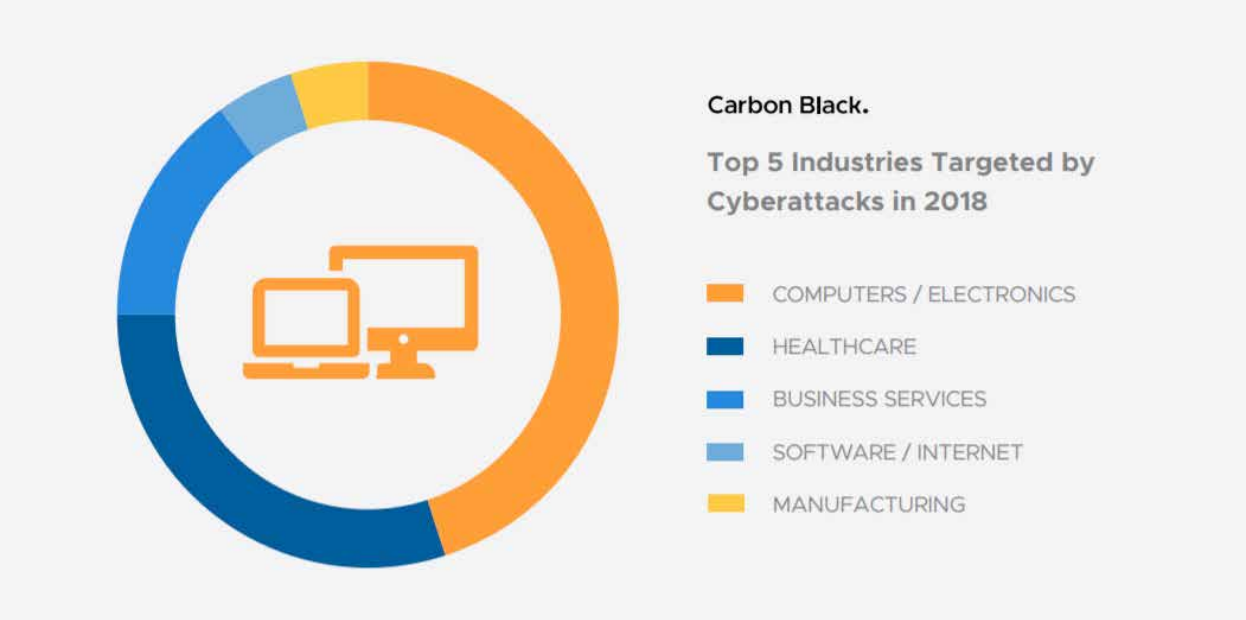
Throughout 2018, the average endpoint protected by Carbon Black was assaulted by two cyber attacks a month. This means that an organisation with 10,000 endpoints would have seen more than 660 attempted cyber attacks per day.

Across the Carbon Black customer footprint (totalling approximately 15,000,000 global endpoints) this means there were, on average, one million attempted cyber attacks per day.



Credit: Carbon Black

The top five industries targeted by cyber attacks in 2018 according to Carbon Black's global threat data were: computers/electronics, healthcare, business services, software/internet and manufacturing.



Credit: Carbon Black

In 2018, China and Russia were responsible for nearly half of all cyber attacks. Of 113 investigations conducted in the third quarter, 47 stemmed from those two countries alone.



Credit: Carbon Black

Carbon Black evaluated open-source reporting and dark web marketplaces to identify and quantify the largest threats posed from cryptocurrency-related crimes and found almost US$1.8 billion in losses from cryptocurrency-related thefts throughout 2018. The Singapore Police Force's Mid-Year Crime Statistics for January to June 2017 reported over US$40 million in victim losses from total internet crime in Singapore alone. Common attack methods included the Emotet banking trojan, Monero cryptomining attacks and ransomware that leverages open-source tools. Carbon Black projects that 2019 will be a year where endpoint visibility becomes more paramount than ever as attackers continue to evolve and global tensions increase. SST

The Internet Without Passwords: Prediction Or Pipe Dream?



►► **By Andrew Shikiar,**
Chief Marketing Officer
FIDO Alliance

Nobody likes using passwords. Users find them inconvenient and difficult to remember and companies are increasingly finding them inadequate for their security needs. Despite this, the username-password combination has remained the go-to authentication method for decades.

The ability of passwords to keep cybercriminals at bay is poor at best. A Verizon Data Breach Investigations Report revealed that 81% of major data breaches are traced back to a single compromised identity.

The resulting cost is tremendous. A Frost and Sullivan study last year, showed that the economic loss in Asia Pacific due to cybersecurity incidents can hit a staggering US$1.745 trillion, more than 7% of the region's total GDP! The root of the problem lies in the fact that older authentication systems are based on a shared secrets model, where the user's credentials are known by both sides of the transaction. Typically, users are required to have complex, unique passwords for each account that feature a mix of numbers and letters. However, an average user today has over 90 online accounts, and this makes it impractical to continue using this model.

In the meantime, as online services build their consumer base, user credentials (both usernames and passwords) are typically stored in a central data server or location. A single successful breach can allow cybercriminals to gain access to millions of username-password pairs, which are then resold on the Dark Web. This leads to credential stuffing, which has quietly become a major plague to businesses worldwide – with upwards of 80% of attempted e-commerce site log-ins being stuffing attempts.

As many consumers reuse passwords, the stuffing success rate ranges around 2%, which is costing businesses dearly (US$5 billion in the United States alone in 2017 according to Shape Security).

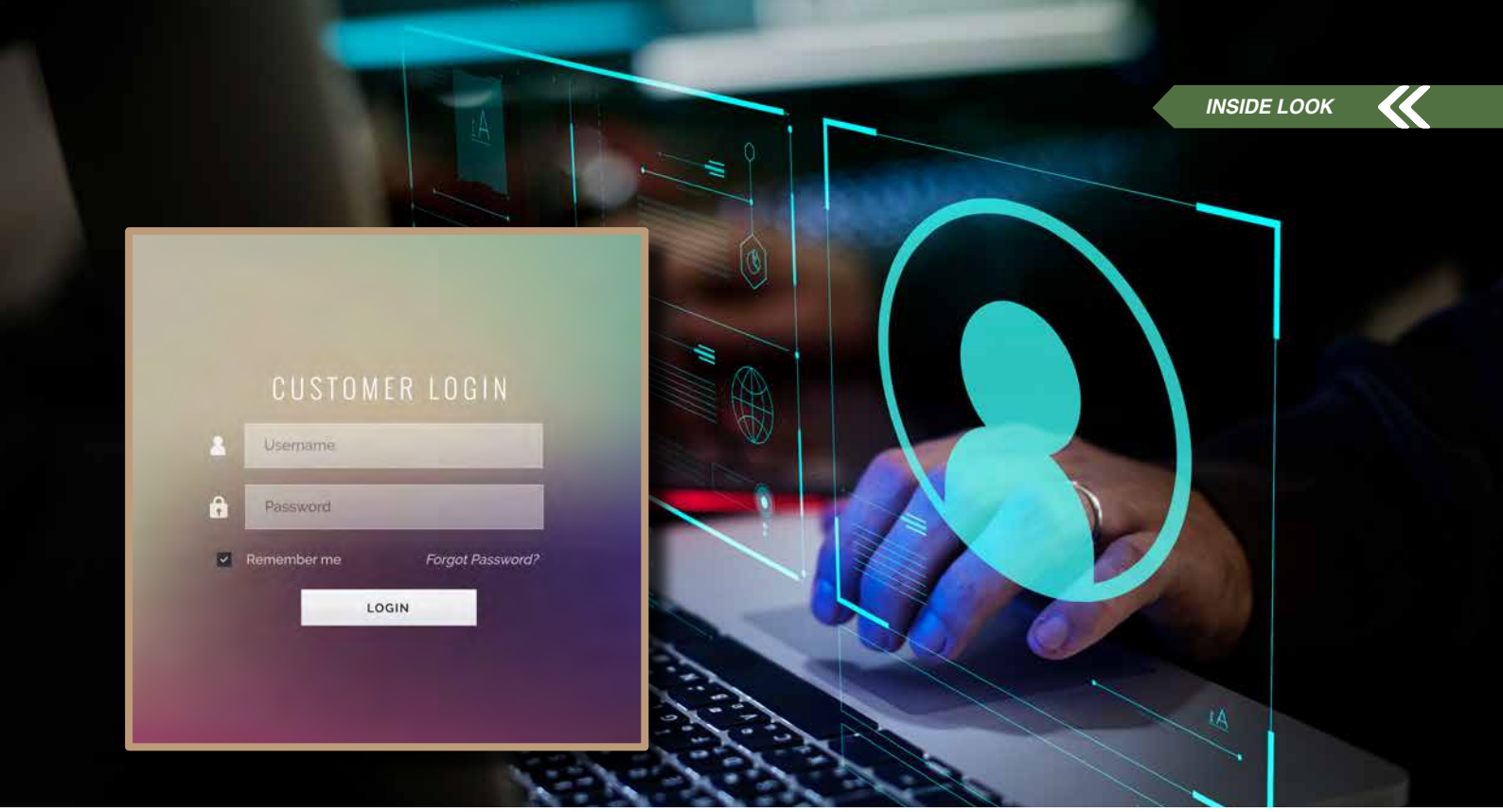
Hence, the cycle of data breaches continues.

The shared secret problem is not new, and the industry has posited several approaches over the years to resolve the issue. The most prevalent is the use of one-time passwords (or OTPs) to provide a second factor of authentication (2FA).

Closer to home, Singapore has mandated the use of OTPs for all sensitive e-government transactions since July 2016, and most essential government e-services now require 2FA. Additionally, banks here are legally obliged to implement 2FA at login.

This second layer of authentication, with a one-time password delivered in conjunction with dedicated OTP devices, mobile apps or via SMS, has certainly strengthened security, but at the cost of simplicity and user experience – which is awkward at best, forcing users to juggle devices and/or toggle between apps. And OTPs are still shared secrets (albeit with shorter longevity) that are susceptible to replay





attacks via spear-phishing and other means - which leads to account takeovers.

Clearly passwords are a failed methodology, and OTPs present significant usability challenges while not adequately mitigating security risks. Just as we do not use Windows 95 or dial-up modems anymore, it is time for us to upgrade our authentication processes.

But is an Internet without passwords really possible?

Enter The FIDO Alliance

Established in 2013, FIDO (Fast Identity Online) Alliance is a non-profit group comprised of technology industry partners working together to establish standards for strong authentication. FIDO is the industry's answer to the world's password problem, with leading companies spanning borders and industries collectively focused on creating open standards and an ecosystem of supporting products and programmes that enable simpler and stronger user authentication.

Core to the FIDO approach is the introduction of the concept of the FIDO Authenticator, which is a secure part of a device where user authentication credentials are stored as private keys unique to each service or log-in. These keys are established at point of account registration, at which point the service provider stores a corresponding public key on its server.

When the user returns to the site or app, he first verifies himself through a simple gesture such as swiping a finger, entering a PIN, speaking into a microphone, inserting a second–factor device or pressing a button. A challenge/response dialogue takes place behind the scenes that matches the private and public keys that also includes critical metadata about both the authenticator and the website or app that is entirely unique – thereby eliminating the threat of phishing or account takeover.

Keeping the private key resident to the device brings added privacy benefits as the consumer is always in possession of his authentication data. This localised authentication is well aligned with regulations in Europe such as revised Payment Services Directive and General Data Protection Regulation. It also addresses common users' fears associated with misuse of their biometric credentials -- which are well founded as the theft of biometrics from centralised repositories could cause irreparable harm as it is impossible to revoke one's fingerprint or iris scan.

FIDO's approach also does away with the requirement to store credentials in a centralised repository -- which both changes the threat landscape for would-be hackers and begins to de-risk the authentication process for the service provider by limiting their downstream exposure in the event of a data breach.

By utilising public key cryptography techniques, smart devices can be used to provide stronger authentication without burdening users.

Passwords still prevail today for restricting access to and protecting data and information. This outdated approach creates risk for consumers and businesses alike, and in doing so threatens the integrity of the connected economy.

Fortunately, leading companies from all corners of the world have rallied together in industry bodies such as the FIDO Alliance to create industry-wide solutions that will modernise the user authentication process.

FIDO's approach to authentication allows organisations to better protect data and information while, at the same time, enhance user experience and reducing friction.

A world without passwords is finally in the making. SST

Cloud And Mobile Deployment The Weakest Links In Enterprise Networks

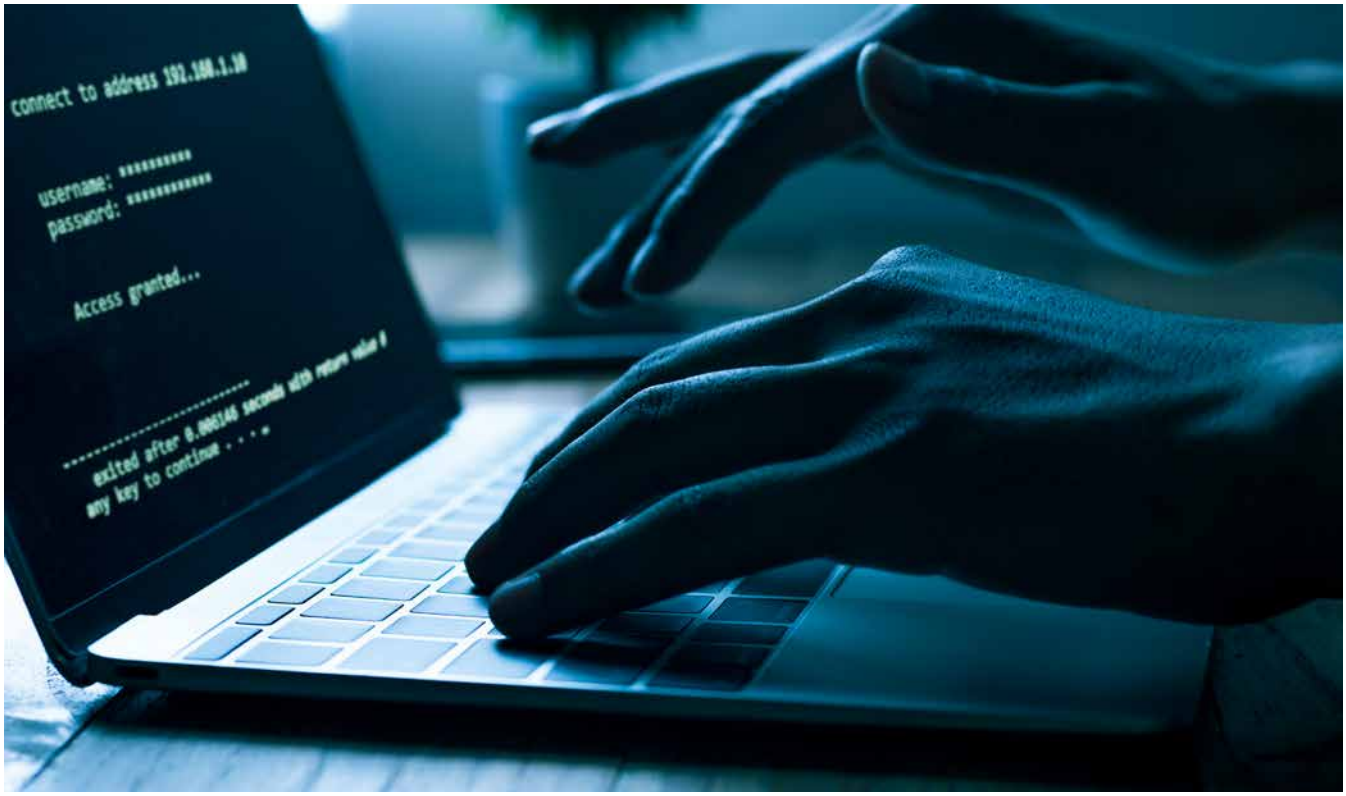
Check Point Software Technologies' 2019 Security Report pinpoints cloud and mobile deployments as the weakest links in enterprise networks.

Nearly one in five organisations experienced a cloud security incident in 2018, detailed the report. Check Point is a provider of cyber security solutions globally.

Threat actors are increasingly targeting the weakest, least protected points in an organisation's IT infrastructure and those points are public cloud and mobile deployments.

The report highlighted that:

- 18% of organisations globally had a cloud security incident in the past year. The most common incident types were data leaks and breaches, account hijacks and malware infections.
- IT professionals rated the biggest threat as misconfiguration of cloud platforms leading to data loss or breaches (cited by 62%). This was followed by unauthorised access to cloud resources (55%); insecure interfaces and APIs (50%); and hijacking of accounts





or data traffic (47%).

- 30% of IT professionals still consider security to be the responsibility of the cloud service provider. This is contrary to recommendations that cloud security should adopt the mutual responsibility model, in which security is shared by both the cloud provider and the customer.
- 59% of IT professionals do not use mobile threat defences. A majority of organisations have not deployed mobile security solutions capable of detecting leading threats including mobile malware, fake or malicious apps, man-in-the-middle attacks and system vulnerabilities.
- Only 9% of IT professionals consider threats on mobile a significant security risk, yet malware can propagate from unprotected mobile devices to organisations' cloud- or on-premise networks, exploiting this weak link in enterprise security defences.



"The third instalment of our 2019 Security Report shows just how vulnerable organisations are to attacks targeting their cloud and mobile estates, because there is a lack of awareness of the threats they face and how to mitigate them. As nearly 20% of organisations have experienced a cloud incident in the past year, it's clear that criminals are looking to exploit these security gaps," said Zohar Alon, Head of Cloud Product Line, Check Point Software Technologies.

Check Point's 2019 Security Report is based on data from Check Point's ThreatCloud intelligence; from Check Point's research investigations over the last 12 months; and on a brand new survey of IT professionals and C-level executives that assesses their preparedness for today's threats. SST

Critical Infrastructure Security Spending To Hit US$125 Billion By 2023

Critical infrastructures are radically transforming on an unprecedented scale, boosted by a rapid adoption of 'smart' operational technologies. Cybersecurity is a growing part of that evolution.

Market-foresight advisory firm ABI Research forecasts security spending for the protection of critical infrastructures will hit US$125 billion globally by 2023 in its Critical Infrastructure Security report.

Currently, defence contractors (Lockheed Martin, BAE Systems, Harris, Northrop Grumman), industrial OEMs (Honeywell, Siemens, Airbus, Rockwell, Boeing), technology leaders (IBM, Amazon, Microsoft, Verizon) and energy companies (Shell, Total, Exxon) are the big security spenders.

Three primary drivers are pushing better digital security in sectors such as utilities, transport, and healthcare. The drivers are: digital transformation and increased connectivity of operational technologies; democratisation of cyber attacks targeting critical infrastructure and a maturing market for industrial and IoT security.

"Connected OT has enabled optimisation and greater efficiency for decades-old legacy systems, cutting costs and vastly improving operations for operators," said Michela Menting, Research Director at ABI Research. "But it has also introduced new vulnerabilities and opened new threat vectors to previously air-gapped technologies."

The first specialised attacks against industrial control systems are now over a decade old, and the attack tools and methods are accessible to even the most common cyber criminals. Fortunately the cybersecurity industry has been working to address that security gap between IT and OT. As a result, security solutions for industrial control systems and IoT have been fast maturing, rendering them more widely available and affordable.

"Security budgets have increased significantly, which is encouraging news for those sectors that have long lagged in digital security," Menting explained.

However, these positive developments are pitched against several obstacles plaguing critical infrastructures: a macro-focus slowdown by governments regarding national cybersecurity strategies especially in the U.S. and the E.U., continued resistance to cybersecurity regulation and sectoral information sharing, and cyber threat fatigue leading to general apathy regarding cybersecurity by the private sector.

Many stakeholders view cybersecurity as a check-the-box exercise for one-time spending rather than investing on a continuous basis. "Consequently, while current security spending levels are significantly higher compared to just a few years ago, there is still significant room for further investment, both from an awareness and an implementation perspective," Menting concluded. SST





Mitsubishi Electric Develops Security Technology To Detect Attacks On Equipment Sensors

Mitsubishi Electric Corporation has developed what is believed to be world's first attack algorithm for sensors used in drones, cars, production equipment and more. The technology detects measurement-data inconsistencies by embedding a proprietary algorithm in sensor fusion algorithms, which combine multiple sensors for measurements used in manufacturing.

Sensor-based automatic control is becoming increasingly common in everyday applications such as drones, in-vehicle devices and production facilities, raising the need for cybersecurity countermeasures. Sensor fusion algorithms, which combine multiple sensors for measurement, were thought to offer attack resistance as well as high-accuracy measurements, but due to the complexity of algorithms and the difficulty of creating an evaluation environment, it had not been proven that the algorithms were actually resistant to attacks nor under what conditions attacks could succeed relatively easily.

Recognising the potential of using the internal calculations of sensor fusion algorithms, Mitsubishi Electric Corporation exploited these calculations in a novel embeddable attack-detection algorithm. Malicious attacks are detected on the basis of inconsistencies between measurements from various sensors such as compasses, gyros and accelerometers used for the automatic control of drones. The algorithm does not compromise computation speed because it exploits intermediate values calculated by the sensor fusion algorithm.

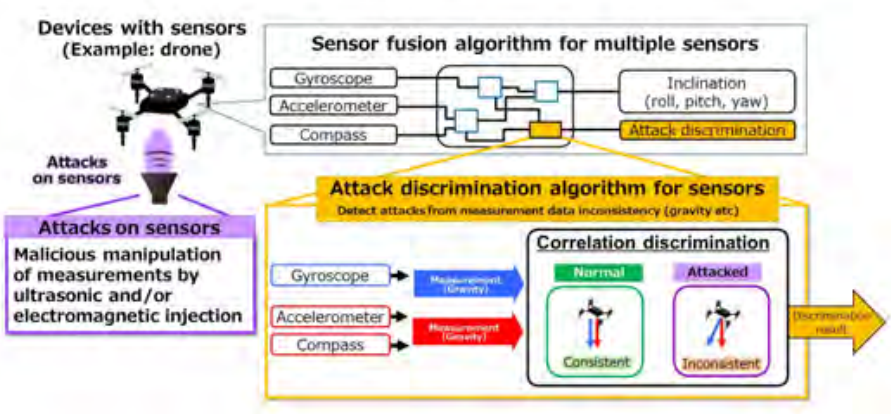
Mitsubishi Electric also created an advanced evaluation environment that applies abnormal signals individually to each sensor, such as a drone's compass, gyro and accelerometer, as well as simultaneously to multiple sensors. Using this environment, Mitsubishi Electric confirmed significant differences between disturbances caused by natural physical phenomena and measurement inconsistencies caused by malicious cyber attacks.

Mitsubishi Electric's algorithm detects malicious attacks based on more than 42% inconsistency in measurement data. In the case of ultrasonic attacks on drones, for example, the Earth's magnetism or gravity is calculated in two ways using intermediate values in the sensor fusion algorithm, and any difference between the two results is treated as an inconsistency.

The new algorithm can be implemented at low cost as additional software in existing sensor signal processing circuits without the need to add or modify hardware. The accuracy of sensor measurements is not compromised.

The company aims to commercialise the technology from the year 2020 onwards. SST

Application example using a drone





A Safer, Cleaner London Borough With Dahua Video Cameras

Council staff and police of a large London borough can now scrutinise street footage more effectively and gather more compelling evidence with the installation of over 1,000 high-definition cameras from Dahua across the borough. Dahua Technology is a leading solution provider in the global video surveillance industry.

The Dahua cameras – along with NVRs, XVRs and control and viewing equipment – cover around 80 council properties, including libraries, parks, golf courses and housing estates, using some 110 wireless microwave radios spread across an area of 25 square miles.

The system was installed to meet several goals. They include making the borough safe and clean; reducing anti-social behaviour, drug and alcohol misuse and providing reassurance to the public; identifying people who commit offences and gathering evidence of vandalism, littering, illegal dumping and unlicensed street trading for prosecutions; and providing support during public events and to the emergency services.

The mainly wireless video surveillance system, designed and installed by the DSSL Group, replaces a legacy analogue CCTV system. The 20-year-old legacy system was becoming unreliable, providing poor quality images and making it harder to comply with data protection legislation.

The system consists of 4K HD cameras. These cameras provide greater coverage with vastly improved image quality and four times the resolution of 1080p cameras. The Dahua cameras are a mix of PTZ, bullet and turret cameras for extended IR performance. They feature vandal-resistant housing and provide great image quality in full colour during the day, while at night, the cameras switch over automatically to night-vision mode.

The cameras are set up in both built-up and semi-rural areas. Most cameras are linked to a dedicated council control room, but around 150 of them are viewed locally using a Dahua keyboard and mouse control and other viewing equipment. Some of the cameras are set up for ANPR, which is used to monitor vehicles and auto-track people using facial recognition technology. These units are used to monitor people entering and leaving local council housing estates.

The upgraded control room, furnished by Intech Solutions, features 13 43-inch and 12 22-inch video screens. The control room uses a Genetec Security Center video management system to manage and control all images and alerts, with a 200TB server to process and store video material.

With the new system, the local police now enjoy clearer and sharper images – both live and recorded – for accurate



identification of suspects, wider coverage per camera, easier image sharing and viewing of images by authorised staff and powerful search and analytics tools. The new system, part of a £1.65 million investment by the council, generates savings of around £50,000 a year in leased line fibre costs alone.

Plans for future development of the system include ANPR in town centres, remote video door entry and the addition of 30 mobile CCTV cameras.

The entire 1,000-plus camera system was designed, installed and commissioned by DSSL within 12 months.

"This has been a great and demanding project to work on, not least because of the sheer number of cameras installed across a wide area of operation," said Aaron Stephens, Works Director at DSSL Group. "The high performance and intelligent features of the cameras have helped create an effective and responsive surveillance system for the borough. The integration of the Dahua cameras to the newly modernised control room has allowed the council to provide the added security of 24/7 HD coverage of a huge area, enabling local police to use the system in their daily operations. Images from the system have already successfully been used in court to secure convictions." SST





Dallmeier's Solution Halts Airport Terminal Closures

The problem is familiar to airport operators: Unauthorised individual enters the security area. Attempts to intercept the straying individual fail. Result: Threat of potential terminal closure.

These situations occur for example when passengers go back to the airside from the land side after passing through customs or wander between "clean" and "unclean" zones inside the security area. The task of detecting and intercepting these strays quickly and resolving the situation places enormous strain on personnel resources, and not infrequently is unsuccessful.

The consequence: The threat of partial or even complete terminal closures with the associated enormous costs.

Video security equipment manufacturer Dallmeier now offers a solution to this with a system based on 3D real-time location tracking, innovative video technology and mobile response team control for reliable and significantly faster incident investigation and slashing of operating cost by as much as 50%.

The Dallmeier solution combines the patented Panomera camera technology with 3D sensors and a software package that provides functions for detecting individuals, real-time positioning and automatic "wrong direction" detection.

When an individual in the monitored area moves in the wrong direction, he is detected by 3D real-time positioning. He is "captured" as an object in the positioning system and tracked seamlessly from then on.

The response team automatically receives an alert, a portrait photo of the intruder and an overview image updated once every second on team members' mobile devices. In the bottom half of the screen, real-time information about the



person's position and direction of movement is displayed on the building map.

The control centre has the same map view and image information of the events and is thus able to coordinate the activities of the response team. At the same time, the team members can switch between recordings on their mobile devices using simple swiping gestures, so they always know exactly where the individual they are looking for is located. In this way, the stray can be found immediately and the critical situation resolved much faster.

Besides speeding up investigation of threat situations, the Dallmeier solution also offers cost savings. Whereas previously a dedicated 24/7 presence was needed for every security checkpoint and passageway throughout the airport, with the Dallmeier solution, security for the corresponding areas can be automated.

Since the control centre and response teams have a much better overview of the situation and cooperation is optimised, the teams only have to intervene when an alert is issued. This enables savings of up to 50% of total operating costs. In effect, the solution pays for itself quickly. SST



Mitsubishi Electric Develops Cyber Defence Technology for Connected Cars

Mitsubishi Electric Corporation has developed a multi-layered defence technology that protects connected vehicles from cyber attacks by strengthening their head unit's defence capabilities.

The technology will enable more secure vehicle systems in vehicles that are equipped for connection to external networks.

Vehicles with communication functions provide connections to the internet and/or mobile devices such as smartphones. This makes these vehicles vulnerable to cyber attacks and even malicious remote control in extreme cases.

Mitsubishi Electric's new multi-layered defence technology prevents cyber attacks through a variety of robust security features, including an intrusion detection system without high-load processing and a secure-boot technology that quickly verifies software integrity during the boot process.

It achieves robust security by strengthening the security functions of the automotive head unit, the vehicle's main link with the internet. The developed technology is adapted from multi-layered defence technology originally developed for critical infrastructure such as systems for electric power, natural gas, water, chemicals and petroleum, as well as for vehicle systems, while requiring only limited machine resources.

The technology detects cyber attacks targeting the control of the vehicle and the automotive head unit. Load processing is reduced through a focus on attack activities.



The Fast Secure Boot technology enables faster and more secure boots that verify the integrity of the vehicle's software embedded in the automotive head unit. The technology requires less than 10% of the time for a normal boot-up sequence compared with conventional technology. SST



Trustonic Launches Service That Slashes Smartphone Thefts

Mobile cyber security software vendor Trustonic has launched its new Asset Lifecycle Protection Service (ALPS) that provides mobile network operators with protection from smartphone thefts.

ALPS slashes theft and fraud of smartphones by combining mobile device and app protection expertise with unique integration into the smartphone manufacturing ecosystem.

Developed in collaboration with some of the largest operators in North America, this robust solution can be deployed rapidly and scaled across device ranges spanning multiple OEMs. With ALPS, mobile network operators can now eliminate smartphone theft, fraud and trafficking, allowing them to safeguard their device investments, protect revenue and drive additional profit contribution.

Smartphone Crime Is Destroying Profits For Mobile Network Operators

A global crime wave of stolen, fraudulently obtained and sold-but-not-activated smartphones is costing operators billions of dollars in lost revenue annually, not to mention the loyalty of defrauded customers and the safety of employees. Device theft and fraud range from 5% to 25% of shipments. Operators report a 200% year-on-year increase in armed robberies at retail stores.

Protecting Revenue Throughout A Smartphone's Lifecycle

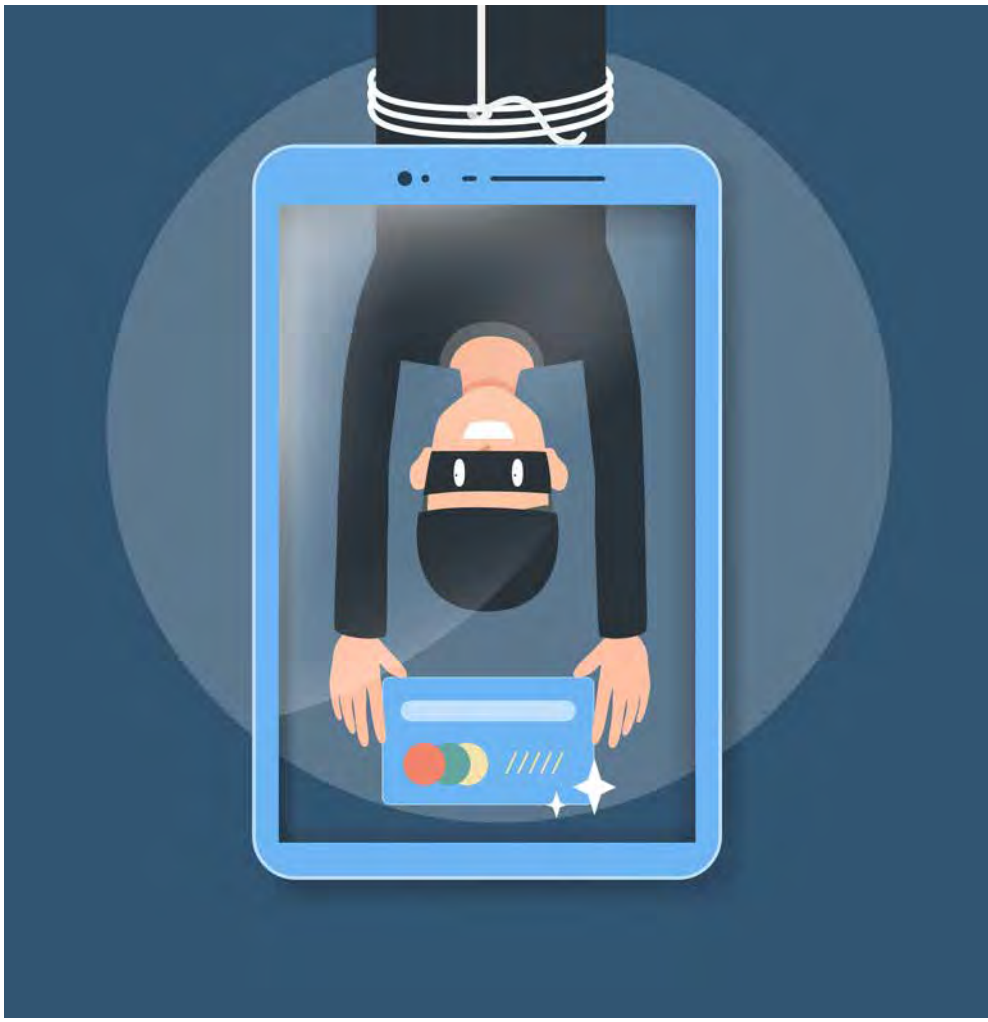
Existing manual unlock codes are easy to overcome, expensive to administer and offer a poor experience to subscribers. ALPS automates the process through an easy-to-use app installed during manufacture that offers good user experience.

ALPS helps operators to solve a range of challenges by establishing a Root of

Trust, meaning fraudulently obtained devices cannot be unlocked or reused.

ALPS offers:

- **Supply chain security.** ALPS protects smartphones by locking them from the moment they are produced. This safeguards smartphones at every stage of the device lifecycle as it makes them worthless if stolen or fraudulently obtained.
- **Protection of subsidised, financed and leased devices.** ALPS prevents the use and resale of devices when installment payments are not made. Once a subsidised plan is paid in full the subscriber can request for the smartphone to be unlocked. Similarly, when a lease agreement ends, the device can be locked if not returned.
- **Companion device protection.** ALPS protects companion devices like tablets, wearables and multi-device family bundles that mobile network operators often use as incentives. If the subscriber stops paying the plan, the main device and all companion devices can be simultaneously locked.





- **Warranty and insurance fraud prevention.** With ALPS, devices can be locked once a claim has been made by the customer, removing the incentive to fraudulently sell the device.
- **Device recall.** For consumer safety, devices are sometimes recalled. ALPS allows operators to lock devices and prevent continued use or re-sale after the recall has been issued.
- **Customer device unlock.** After a customer completes his contract, he can request to unlock his device.

Said Ben Cade, CEO of Trustonic, "We are empowering operators to take control in their fight against fraud, theft and device trafficking. This not only solves a billion-dollar problem for the industry, it also adds a significant contribution to their bottom line performance."

ALPS is now available globally. SST



Full Integration Across Security, Safety And Site Management Systems At Dubai's Landmark Bluewaters Island

For the region's newest tourism hotspot, Bluewaters Island in Dubai, the management wanted an efficient way to integrate all security, safety and building management functions into one easy operating system, with particular emphasis on a solution that would be efficient to use, inexpensive to maintain and robust going forwards.

For Bluewaters' management, the answer was Maxxess eFusion technology. Maxxess is a U.S.-based global corporation specialising in security management solutions and innovative technologies.

Bluewaters opened in November 2018 and is expected to attract more than 3 million visitors every year. The US$1.6bn project comprises four luxury residential complexes, a landmark Caesars Palace hotel, a shopping mall and the world's largest observation wheel, Ain Dubai, as its centrepiece.

The eFusion security management platform was chosen instead of a more costly or complex conventional PSIM



solution because it uses versatile, open-technology software. eFusion offers the advantages of a modular, building block approach and allowing maximum freedom to integrate, customise and adapt to future needs.

The eFusion platform at Bluewaters includes full integration with an ASSA ABLOY Hospitality system. It allows a unified system approach, with a single enrolment protocol for both front- and back-of-house access. The solution enables centralised management of room safes, mini bars and cupboards, and for control of all alarm transactions.

eFusion's integration with the Zenitel Stantaphone IP Intercom System ensures that video and transaction data is called up automatically in the Bluewaters control room as soon as any user presses a call button. For maximum efficiency, the system allows the operator to unlock doors and communicate with the user remotely, with full activity logs kept for audit.

With easy integration to the SeeTec Video Management System, eFusion also allows seamless control of all cameras. In addition, cameras are linked to the door access system, with video pop-up triggered by pre-defined events. The solution also gives the operators complete PTZ control, playback and video functionality.

"Thanks to its compatibility with leading surveillance, intruder, access and fire detection systems, eFusion proved to be a highly efficient integration technology for the Bluewater project," said Mr Henry Azoury, Senior Security Design and Engineering Manager at Omnix International.

ID badging and building management systems are also fully integrated, allowing easy operation and control of a wide range of functions including heating, ventilation and air conditioning.

"There is no need to switch between different management systems and the eFusion platform is easy to work with, allowing full benefit from integration with individual systems," said Lee Copland, Managing Director EMEA, Maxxess. SST







Neurotechnology's Palm Print Recognition Algorithm Emerged Top

The palm print matching engine of MegaMatcher SDK emerged the most accurate overall and fastest among the five most accurate matchers at FVC-onGoing in February.

FVC-onGoing is a web-based automated evaluation system for recognition algorithms. Tests are carried out on a set of sequestered datasets and the algorithms are evaluated using strongly supervised approaches to maximise trustworthiness.

Because of its complexity, palm print template matching requires much more computational time than single or multiple fingerprint matching.

MegaMatcher SDK is developed by Neurotechnology, a provider of deep learning-based solutions, robotics and high-precision biometric identification technologies.

Palm Print, part of Neurotechnology's MegaMatcher SDK, was ranked the most accurate for both full and partial palm prints, the fastest partial palm print matcher and the fastest full-print matcher out of the five most accurate matchers. Neurotechnology's algorithm also has the smallest template size overall, both in full palm print and partial (lower) palm print datasets. It is suitable for both 1-to-1 (verification) and 1-to-many (identification) applications.

"Our expertise in fingerprint recognition technologies carries over to palm print matching," said Dr. Justas Kranauskas, head of the biometric research department for Neurotechnology. "Though the palm print is a larger, more detailed recognition task, our experience in this field allows us to bring the most accurate, highest efficiency application available to the palm print recognition market."

Neurotechnology's palm print matching engine is included in MegaMatcher Standard and Extended SDKs. Now available from Neurotechnology and distributors worldwide. SST



RFID Display Readers With Expanded Features

RFID technology pioneer Idesco's newest RFID display readers offer novel uses for identification systems.

The screen allows personalised messages to be displayed to a user after the user has been identified. In turn, the user may respond to the system via the reader's key-enhanced keypad. This translates to two-way, user-to-system communication that supports a wider variety of services and dynamic, personalised processes, including simple self-service payment.

For users, this combination of a display with an RFID reader enhances value and convenience when it comes to self-service and cashless payment. Additionally, RFID is reliable, convenient, easily managed centrally and highly cost effective. Since transponders usually cost less than a euro, a lost transponder can be easily and quickly removed from a system and/or replaced.

Finnish firm Vidamin Oy has already begun deploying Idesco's newest keypad display readers in its application solutions. Vidamin Oy offers solutions used in logistics, industry, environmental technology, parking and freight deliveries. Vidamin plans to deploy Idesco's RFID display readers in locations as diverse as car wash stations, parking halls, unstaffed waste recycling stations and electric car charging stations.

Vidamin Oy's PlatformX system interfaces seamlessly with Idesco 8 CD 2.0 D Pin readers via the open technology two-way communication protocol, OSDP v2, to support interactivity,



allowing the firm to offer easy-to-use, versatile, added-value services.

These services include:

- Personalised, welcoming messages with vital time-sensitive information (such as reservations and meetings)
- Allowing users to track in real time their restricted visits/uses. Users limited to a finite number of visits/uses are kept up-to-date on their remaining quota via reader's display.
- Keeping time-restricted visitors up to date on the remaining duration of their access rights
- Confirmations of accepted payments via payment applications
- Selecting specific access function via display such as choosing a specific door to open
- Enhancing customer experience with direct, convenient customer service contact via display SST



Smart Solutions For Casino Surveillance

Many casino operators struggle with undetected fraud and theft, high operating costs and inefficient, manual processes. The Smart Casino Solutions from CCTV/IP solutions manufacturer Dallmeier claims to be an answer to this problem.

By combining video technology and Artificial Intelligence (AI), for example, Casino Automation Technology (CAT) protects against fraud. The first gaming automation system that is live in a productive environment, CAT uses AI technologies and standard Full HD IP cameras to gather data. With this, CAT is able to offer a wide variety of insights and automate core gaming processes. The system recognises chips and cards, provides real-time





information about bet position and bet value, game pace and float value, to name just a few key functions. This allows for accurate player rating, highly increased game pace and much more effective protection from fraud. CAT is available for Baccarat and Blackjack, which previously were difficult to integrate into data processing and analysis processes because of their analogue nature.

In addition, Smart Casino Solutions is also said to reduce the cost of surveillance.

Classic surveillance and CCTV play a major role in casinos: Large areas have to be monitored to protect guests, players, employees and the casino's inventory. With the new 360-degree version of the patented Panomera multifocal sensor system, casino operators can cover much larger areas with the same number of operators while at the same time significantly



improving overall security due to high resolution, 360-degree view of the overall scene. In case of an incident, operators can zoom into scenes using a PTZ camera without losing the overall picture. Also, multiple operators can zoom in at the same time to resolve complex scenarios. All this reduces the cost of video security infrastructure enormously, leading to significantly lower Total Cost of Ownership.

Smart Casino Solutions was showcased at ICE London 2019 in February. SST



Three Australian Universities Roll Out SafeZone Protection On Campus And Beyond

Three Australian universities have introduced SafeZone® technology in a drive to improve safety, increase their security teams' capabilities and provide better care for students and staff.

The three universities are the University of Tasmania (UTAS), the University of Southern Queensland (USQ) and the University of the Sunshine Coast (USC). Together they have more than 75,000 students and staff working in 33 campuses and associated facilities across four Australian states.

With this latest rollout, 30% of Australian universities are now using SafeZone, affirming CriticalArc's lead in safety and security management solution in the Australian market.

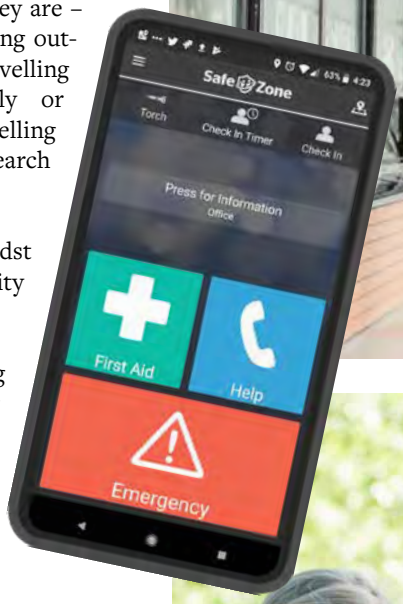
SafeZone is a security solution from CriticalArc that puts individuals directly in touch with response teams at universities, hospitals, government departments and other large organisations. The solution makes it easy for them to use their mobile phones to request help, trigger an emergency response, receive rapid notifications in the event of emergencies and benefit from a wide range of customer-care services.

The technology also lets students and staff share their

situation with response team members by checking in when working alone outside hours or in higher risk environments such as laboratories and workshops.

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





The move comes amidst growing safety and security concerns.

Preventing crime, managing public safety and handling emergencies are still the top concerns of university security teams, but universities are also seeking to address issues that are increasingly important. This includes improving support around mental well-being, tackling sexual harassment and making campuses inclusive environments where everyone can feel safe and welcome.

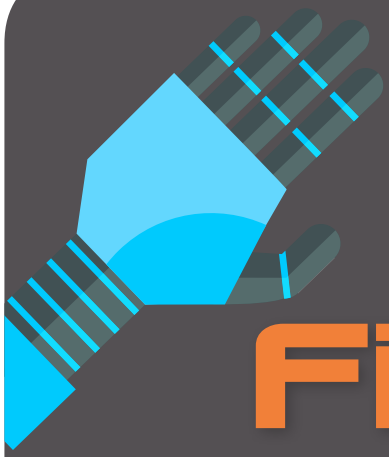


With its global reach combined with its ability to precisely locate vulnerable individuals, SafeZone is helping universities around the world to better meet their duty of care obligations, said Darren Chalmers-Stevens, CriticalArc, Managing Director.

"SafeZone offers all the functions that university teams want, in one easy package. It is not only helping them to deliver better care, it is letting them demonstrate this fact in an accountable way."

Currently SafeZone serves the needs of 1.5 million students and staff at more than 500 locations across the world. SST





Five Technology Trends for 2019





►► **By Hu Yoshida,** Vice President and Global Chief Technology Officer of Hitachi Vantara

2018 was a year when digital transformation entered maturity and most companies committed to transforming their companies; strategies were laid out and resources were allocated to adopting public cloud, agile methodologies and devops, RESTful APIs, containers, analytics and machine learning.

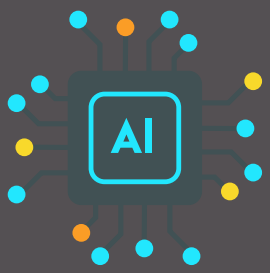
But what will be the big technology trends this year? Here are five trends for 2019 that I would like to call out.

Trend 1. Companies Will Shift from Data Generating to Data Powered

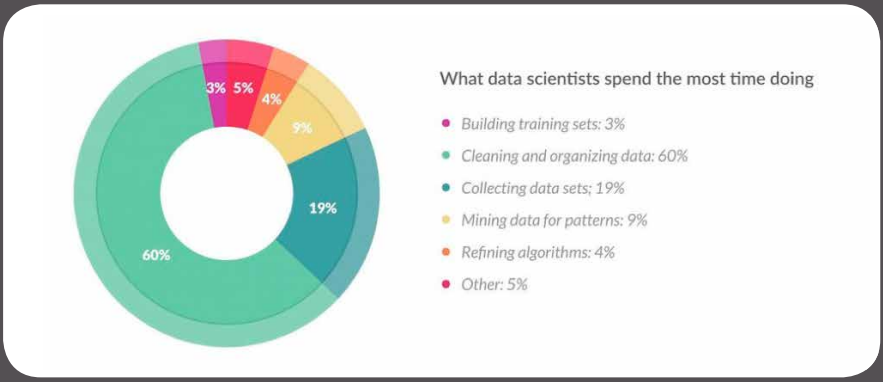
A 2017 Harvard Business Review article on data strategy noted, "Cross-industry studies show that on average, less than half of an organisation's structured data is actively used in making decisions — and less than 1% of its unstructured data is analysed or used at all."

Deployments of large data hubs have only resulted in more data silos that are not easily understood, related or shared. The new focus will be on understanding the meaning of the data as well as the technologies that are applied to the data so that data engineers can move and transform the essential data needed to power the organisation. More focus will be on the operational aspects of data rather than the fundamentals of capturing, storing and protecting data. Meta data will be key and companies will look to object-based storage systems to create a data fabric as a foundation for building large-scale flow-based data systems.

Trend 2: AI and Machine Learning Will Unleash the Power of Data to Drive Business Decisions



AI and machine learning technologies can glean insights from unstructured data, connect the dots between disparate data points, and recognise and correlate patterns in data such as facial recognition. AI and machine learning are becoming widely adopted in home appliances, automobiles, plant automation and smart cities. However, from a business perspective, AI and machine learning has been more difficult to implement as data sources are often disparate and fragmented and much of the information generated by businesses has little or no formal structure. While a wealth of knowledge can be gleaned from business data to increase revenue, respond to emerging trends, improve operational efficiency and optimise marketing to create a competitive advantage, the requirement for manual data cleansing prior to analysis is a major roadblock. A 2016 Forbes article published a survey of data scientists that showed that they spent most of their time (80%) on massaging data rather than mining or modelling data.



One needs also to understand that data scientists do not work in isolation. They must team up with engineers and analysts to train, tune, test and deploy predictive models. Building an AI or machine learning model is not a one-time effort. Model accuracy degrades over time and monitoring and switching models can be quite cumbersome.

Organisations will be looking for orchestration capabilities to streamline the machine learning workflow and enable smooth team collaboration.

Trend 3: Increasing Data Requirements Will Push Companies to the Edge with Data

Enterprise boundaries are extending to the edge – where both data and users reside, and multiple clouds converge. While the majority of the IoT products, services and platforms are supported by cloud-computing platforms, the increasing high volume of data, low latency and QoS requirements is driving the need for mobile cloud computing where more of the data processing is done on the edge. Public clouds will provide the connection between edge and core data centres creating the need for a hybrid cloud approach based on open REST or S3 App integration. Edge computing will be less of a trend and more of a necessity as companies seek to cut costs and reduce network usage.



Trend 4: Data Centres Will Become Automated

The role of the data centre has now changed from being an infrastructure provider to a provider of the right service at the right time and the right price. Workloads are becoming increasingly distributed, with applications running in public and private clouds as well as in traditional enterprise data centres. Applications are becoming more modular, leveraging containers and microservices as well as virtualisation and bare metal.

As more data is generated, there will be a corresponding growth in demand for storage space efficiency. Enterprises need to make the most of information technology — to engage with customers in real time, maximise return on IT investments and improve operational efficiency. Accomplishing this requires a deep understanding of what is happening in their data centres in order to predict and get ahead of trends, as well as the ability to automate action so staff are free to focus on strategic endeavours. A data centre is like an IoT microcosm; every device and software package has sensor or log and is ripe for the application of artificial intelligence (AI), machine learning and automation to enable people to focus on the business and not on infrastructure.

Automation must be based on a shared/open API architecture that allows companies to simplify transmission of data across a suite of management tools & and third-party tools. Everything companies have must be API-based so that they can draw information in from other sources to create a more intelligent solution.

Trend 5: Corporate Data Responsibility Becomes a Priority

The implementation of GDPR in 2018 has focused attention on data privacy and required companies to make major investments on compliance. All international companies that are GDPR compliant now have a data protection officer in an enterprise security leadership role.

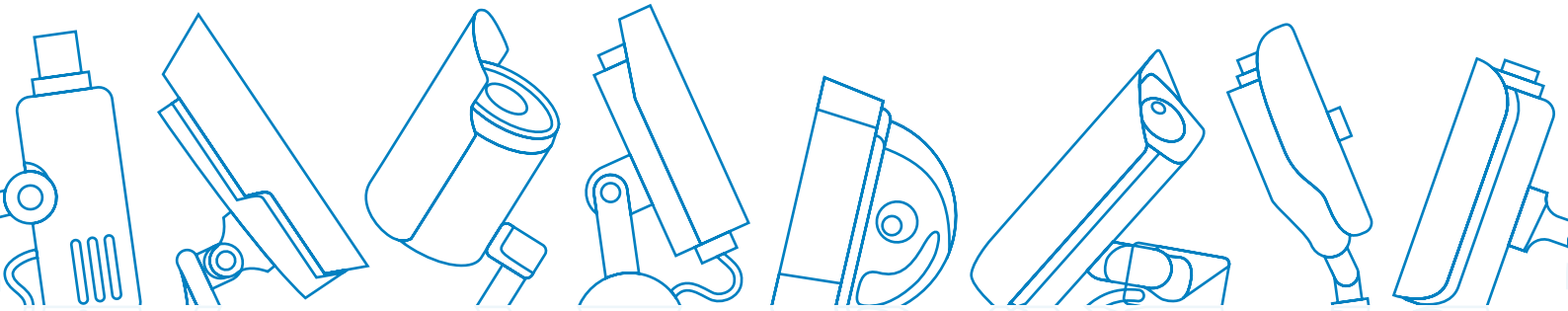
Big Data systems and analytics are becoming a centre of gravity as businesses realise the power of data to increase business growth and better understand their customers and markets. The most powerful companies in the world are those who understand how to use the power of data. However with great power comes great responsibilities.

IT must provide the tools and processes to understand data and ensure that the use of that data is done responsibly.

The views expressed in this article are the author's own and do not reflect the views of Hitachi or Hitachi Vantara

SST

Our tribute to **Safety & Security...**



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

Visit **www.tradecardsglobal.com** to sign up for a new account and your organisation listing. Input "**SECURETRIBUTE**" as promo code before proceeding to payment page. The promo code is valid until 31 December 2019.

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

TRADECARDS GLOBAL

Supporting mobile version of:

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

GET IT ON Google Play

Download on the App Store

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: _____

HKTDC International ICT Expo
HKTDC Hong Kong Electronics Fair (Spring Edition)
13-16 April 2019
Hong Kong Convention & Exhibition Centre

Preview The Dazzling Future In Hong Kong

Ground-breaking technologies and solutions will be showcased under one roof in Hong Kong this April, allowing visitors to fully experience the revolution happening in every aspect of work, life and play in the near future.

Running concurrently with the Hong Kong Electronics Fair (Spring Edition), International ICT Expo 2019 will be a stunning showcase of tomorrow, painting a bold future filled with mind-boggling smart city solutions, fascinating smart business solutions and state-of-the-art smart devices.

Organised by the Hong Kong Trade Development Council (HKTDC), the expo is Hong Kong's leading event for cutting-edge smart city solutions and ICT technologies across all sectors. The 2018 edition attracted over 32,000 buyers and featured over 600 top-tier exhibitors. Among these buyers, 58% were international buyers, underlining the fact that Hong Kong is a regional hub for ICT.

The theme for ICT Expo 2019 is Smart City. Smart Living. Exhibitors will showcase a range of smart city solutions including Smart Economy, Smart Environment, Smart Government, Smart Living, Smart Mobility and Smart People.

The Office of Government Chief IT Office will mount the Smart Government Pavilion and present projects on HK smart city development at the Zone. The So French So Innovative Pavilion will showcase smart city solutions designed by French corporates, SMEs and startups. Microsoft, SenseTime, NEC, Xiaoi Robot, Hong Kong Airport Authority, local R&D centres, Science Park, Cyberport and Smart City Consortium as well as groups coming from Canada, India and Hangzhou, Guangdong and Qingdao in China will share their various smart city solutions and applications at the Expo.







The other highlighted zones are Digital Infrastructure, Digital Marketing and e-Commerce, Enterprise Solutions, Home-grown Innovations, Retail Technologies, Smart Devices and Accessories and Startup.

Throughout the four days of the expo, participants will experience daily events curated to the revolving themes of AIoT - Next-Gen Connectivity, Data as Currency of the Future, Smart Living Powered by Technologies and Reinventing Business with Smart Solutions.

Admission is free for business visitors aged 18 or above.

Visit Web: ictexpo.hktdc.com/ex/13 Wap: hktdc.com/wap/ict/T119 for more information SST



PLATINUM PARTNER

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

GOLD PARTNERS

Robert Bosch	Singapore	+65 6258 5511	enquiry.apr@sg.bosch.com	www.boschsecurity.com	OBC
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

Altronix	U.S.A.	+1 718 567 8181	info@altronix.com	www.altronix.com	7

See us at following upcoming events!

Event	Date	City	Country	Website	Page
IFSEC Southeast Asia 2019	19 – 21 Mar 2019	Kuala Lumpur	Malaysia	www.ifsec.events/kl	15
ISC West 2019	10 – 12 Apr 2019	Las Vegas	United States of America	www.iscwest.com	IBC
Secutech 2019	8 – 10 May 2019	Taipei	Taiwan	www.secutech.com	9
IFSEC International 2019	18 – 20 Jun 2019	London	United Kingdom	www.ifsec.events/international	11
IFSEC Philippines 2019	13 – 15 Jun 2019	Manila	Philippines	www.ifsec.events/philippines	13
BMAM Expo Asia 2019	27 – 29 Jun 2019	Bangkok	Thailand	www.bmamexpoasia.com	17
INTERPOL World 2019	2 – 4 July 2019	Singapore	Singapore	www.interpol-world.com	1
Safety & Security Asia 2019	1 – 3 Oct 2019	Singapore	Singapore	www.safetysecurityasia.com.sg	19

REGISTER TODAY!

ISC WEST
INTERNATIONAL SECURITY CONFERENCE & EXPOSITION

PREMIER SPONSOR
SIA
SECURITY INDUSTRY ASSOCIATION

APR 9-12 2019

Sands Expo | Las Vegas
www.ISCWest.com

Discover the industry's latest products, technologies & solutions

Network with 20,000+ Physical, IoT and IT Security Buyers

Direct access to 1,000+ leading exhibitors & brands

85+ SIA Education@ISC Sessions



COMPREHENSIVE SECURITY FOR A SAFER, CONNECTED WORLD

FEATURING:

CONNECTED SECURITY EXPO @ ISC WEST & UNMANNED SECURITY EXPO @ ISC WEST

WWW.ISCWEST19.COM/SST

BOSCH
Invented for life

Secure operations 24/7 to see all the details, all the time with Bosch FLEXIDOME IP starlight 8000i.

With quick installation plus wireless and remote commissioning, camera adjustments can be corrected whenever needed plus up to 4k Ultra HD resolutions and starlight technology so you can see all the details all the time.

Find out more at **boschsecurity.com**

