JULY / AUGUST 2020

SECURITY SOLUTIONS TODAY

INTELLIGENT ROBOTICS

The road toward self-learning machines

Manufacturing Feature

How Smarter Tech Is Shaking Up Manufacturing

Video Analytics Feature

Video's Critical Role In The Modern World

In Focus

The Growing Malware Threat In The Face Of Remote Workers

ASEAN SUPER 8

International ICW Construction Week

IFSEC

SOUTHEAST ASIA

SECURITY • FIRE • SAFETY

NEW DATES

15 - 17 JUNE 2021

MALAYSIA INTERNATIONAL TRADE
AND EXHIBITION CENTRE (MITEC), KL

SECURITY
IS CRITICAL
IFSEC
IS ESSENTIAL

IFSEC SOUTHEAST ASIA DIGITAL MARKETING SOLUTIONS

Go digital and maximize your online presence

- **Lead Generation E-Newsletter**
- **Newsletter Leaderboard**
- **IFSEC Cyber Hub**
- **Webinar**

Scan Here
To Download
Media Kit

FACTS AND FIGURES

expected **6,000** trade visitors

expected **170** participating companies from more than **10** countries

4,000sqm of exhibition space

expected **250** onsite business matching meetings

expected **10** group pavilions

Organised by
informa markets

WWW.IFSECSEA.COM | WWW.SUPER8ASEAN.COM

IFSEC Southeast Asia   IFSEC Southeast Asia

IN THIS ISSUE

tradelinkmedia.biz

SECURITY SOLUTIONS TODAY

Choose Magazine · Free Signup

OUR LATEST ISSUE

May-Jun 2020

ASSOCIATE PUBLISHER
Eric Ooi
EDITOR
JoAnn Chia

Security Solutions Today (SST), published bi-monthly since 1992, is one of the leading security trade publications in Asia. The magazine features industry news, market / technological updates, case studies / application stories on projects, product showcases for new and current security products / devices in available in the market, and security trade show previews and reviews. We feature latest technologies in Access Control, Video / CCTV Surveillance & Storage Systems, Intrusion/ Alarm Detection, Integrated Security Systems, Security Communication

All · Projects · Case Studies · Products & Technologies · Others · Industry Links · Magazines

LATEST

Office 365 Phishing Campaign Exploits Samsung, Adobe And Oxford Servers
Jun 28 2020

Office 365 Phishing Campaign Exploits…
Jun 28 2020

UK-US Data Deal Puts Brexit Data Adequacy Pa…
Jun 19 2020

Businesses Face Cybersecurity Risk Due …
Jun 14 2020

Identiv Develops NFC-Enabled Body Temperat…
Jun 07 2020

NEWS

COVID-19: How CIOs can prepare for business…
May 22 2020

Government Tells Social Media Companies They Mu…
May 15 2020

NCSC Tackles Unconscious Bias In Security Terminology
May 08 2020

Cyberattacks On Banks Seen Spiking, Says Carbon Black
Apr 30 2020

Application Performance For Remote Workers Becomes…
Apr 24 2020

Zoom User Credentials For sale On Dark Web
Apr 17 2020

SPONSORS

Microengine
P1000I PoE Controller

UPCOMING EVENTS

IFSEC International 2020
London, United Kingdom
FROM Sep 08,2020 10:00
TO Sep 10,2020 16:00

ASEAN Super 8
Kuala Lumpur, Malaysi
FROM Oct 20,2020 10:
TO Oct 22,2020 16:00

IFSEC Southeast Asia 2
Kuala Lumpur, Malay
FROM Oct 20,2020 10:
TO Oct 22,2020 17:00

sst.tradelinkmedia.biz

Visit our website for the latest information

News In The Industry · Upcoming Exhibitions · Download Magazine Issues

SECURITY SOLUTIONS TODAY
UNRAVELING UNMANNED AERIAL VEHICLES
Regulating the growing applications of drone technology
KEEPING EVENTS SAFE
SAFE CITIES, THE SMART WAY

CONTACT

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

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

EDITOR
CJ Chia
(sst@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)

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

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.

JULY / AUGUST 2020
SECURITY SOLUTIONS TODAY
AI
INTELLIGENT ROBOTICS
The road toward self-learning machines
Manufacturing Feature
How Smarter Tech Is Shaking Up Manufacturing
Video Analytics Feature
Video's Critical Role In The Modern World
In Focus
The Growing Malware Threat In The Face Of Remote Workers

Images Credit: Freepik.com

Designed by Fawzeeah Yamin

SECURITY SOLUTIONS TODAY
is published bi-monthly by
Trade Link Media Pte Ltd (Co. Reg. No.: 199204277K)
101 Lorong 23, Geylang,
#06-04, Prosper House, Singapore 388399
Tel: +65 6842 2580 Fax: +65 6842 2581
MCI (P) 056/05/2020
ISSN 2345-7104 (Print) | ISSN 2345-7112 (E-periodical)

ANNUAL SUBSCRIPTION:

Surface Mail:	
Singapore	- S$60 (Reg No: M2-0108708-2 Incl. 7% GST)
Airmail:	
Malaysia/Brunei	- S$105
Asia	- S$155
Japan, Australia, New Zealand	- S$185
America/Europe	- S$185
Middle East	- S$185

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

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

ISSN 2345-7104
9 772345 710005

COMING SOON

AUG
01 – 06
2020

Black Hat USA
Las Vegas, USA
+1 866 203 8081 https://www.blackhat.com/us-20/
blackhatregistration@ubm.com

AUG
20 – 22
2020

Secutech Vietnam 2020
Ho Chi Minh City, Vietnam
+886 2 8729 1099, +84 4 3936 5566 www.secutechvietnam.tw.messefrankfurt.com
stvn@newera.messefrankfurt.com, project1@vietfair.vn

SEP
21 – 25
2020

Global Security Exchange 2020
Atlanta, USA
+1 888 887 8072, +1 972 349 7452 www.gsx.org
asis@asisonline.org

OCT
5 – 6
2020

Cyber Security Asia Malaysia
Kuala Lumpur, Malaysia
+603 22606500 https://cybersecurityasia.tech/
admin@thomvell.com, karen@thomvell.com

OCT
5 – 8
2020

ISC West 2020
Las Vegas, USA
203 840 5602 www.iscwest.com
www.iscwest.com/Forms/Customer-Service-Form/

MAY
18 – 20
2021

IFSEC International 2021
London, UK
+44 (0)20 7069 5000 https://www.ifsec.events/international/
ifseccustomerservice@ubm.com

JUN
15 – 17
2021

IFSEC Southeast Asia 2021
Kuala Lumpur, Malaysia
+60 3-0771 2688 www.ifsec.events/kl/
ifseccustomerservice@ubm.com

JUL
21 – 23
2021

IFSEC Philippines 2021
Manila, Philippines
+63 2 551 7718 www.ifsec.events/philippines/
www.ifsec.events/philippines/eform/submit/contact

Dear readers,

Technology and how it interacts with the world around it is getting smarter. The development of smart devices that we can use in our daily lives is in part a result of the desire to add convenience and remove the need to be totally involved in mundane tasks. But beyond smart technology which allows the automation of simple tasks, lies a more intelligent future—one where machines can actively learn and improve, with minimal input from humans.

In this issue, we look into Artificial Intelligence (AI), technology which is very much still in its infancy. It is already clear that the pursuit of intelligent robots is an inevitable wave of change that we must ride, or risk redundancy. There has already been success found in machines with limited intelligence—AI machines able to replicate specific elements of intellectual ability. Other research projects end in failure, but these failures are simply necessary steps that take researchers closer to future success.

AI is already a reality beyond the boundaries of a laboratory. In the field of security, robots which use AI to more efficiently patrol and monitor areas are growing in demand. Of course, the technology is still expensive to implement, and has many shortcomings which we hope future iterations will address. Still, it's undeniable that much progress has been made in the field of AI, and the possibilities in how this will influence the security industry are truly exciting to consider.

We also explore how smarter solutions are shaking things up in the Manufacturing and Warehousing industries, which have come a long way from its roots of being heavily reliant on manpower. These days, smart technology makes manufacturing and tracking stored products easier, and organisations are better able to reallocate valuable manpower to more complex tasks.

The issue also looks at how video management software and analytical solutions have evolved to meet changing needs, even being identified as a critical part of managing the COVID-19 pandemic. Cybersecurity and especially malware protection is also in focus, a topic that is especially relevant with the increase of remote workers introducing more security gaps into organisational networks.

As the world returns to a new normal, security professionals are finding interesting ways to apply technology to keep people and networks safer even amidst a pandemic. It is this innovative spirit which opens the doors to the continuous growth of the security industry, and there are many lessons to be learnt from our industry partners who lead the way.

Safe reading!

CJ Chia

Editor

HACKERS EARN RECORD-BREAKING US$100 MILLION ON HACKERONE

HackerOne, the number one hacker-powered security platform, announced that hackers have earned US$100 Million in bug bounties by hacking for good on the HackerOne platform. A bounty—or a bug bounty— a monetary award given to a hacker who finds and reports a valid security weakness to an organisation so it can be safely resolved. With nearly half of bounty earnings awarded in the past year alone, this record-breaking milestone showcases how the world's largest hacker community is addressing the growing security needs of our increasingly interconnected society.

From US$30,000 paid to hackers across the globe in October 2013—the first month of bounty payments on HackerOne—to US$5.9 million paid to hackers in April 2020, working with hackers has proven to be both a powerful way to pinpoint vulnerabilities across digital assets and more than just a past-time. It's a career.

"We started out as a couple hackers in the Netherlands with a crazy belief that hackers like us could make organisations safer and do it more efficiently and cost-effectively than traditional approaches," explained HackerOne co-founders Jobert Abma and Michiel Prins in their blog post about the milestone. "US$100 Million in bounties later, maybe this idea isn't so crazy after all. Thank you to all the hackers who have made the internet safer one vulnerability at a time. Hacking is here for good, for the good of all of us."

The positive power of a growing community of ethical hackers pools our defences against data breaches, reduces cybercrime, protects privacy, and restores trust in our digital society. Highlights from this journey to US$100M include:

- 84: The number of new hackers that sign up to the platform every hour
- US$6,000: The amount of bounties paid out on the platform every hour
- 214%: Year-over-year hacker-powered security growth in the federal government
- 85.6%: The year over year growth in total bounty payments, with 17.5% increase since February when COVID-19 was declared a pandemic.
- 343%: The increase in signups over the past year on Hacker101 — HackerOne's free online classes for aspiring hackers.
- 38%: The increase in average weekly new registrants for Hacker101 since February, when COVID-19 was declared a pandemic.
- Over 170,000: The number of vulnerabilities hackers have uncovered in nearly 2,000 customer programs

"We are building a community able to test and vet every piece of our digital connected civilisation," said HackerOne CEO Marten Mickos. "US$100 Million is a number that attracts the best hackers, providing companies and governments unmatched ROI, significantly reducing the risk of data breach. We have arrived at the point in history where you are ignorant and negligent if you do not have a way to receive useful input from ethical hackers. In this new world of ever-evolving threats, the only way to get ahead is to get transparent. Openness, not secrecy, is the way forward."

Back in 2017, Mickos predicted the community of hackers on HackerOne would grow to one million strong and would have earned US$100 Million in bounties by the end of 2020. With over three quarters of a million individuals signed up to hack for good, we're well on our way to exceeding these expectations. Mickos shared the following predictions for the future:

- The HackerOne community produces outstanding security experts to fill the talent gap in the industry. Within the next 15 years, we expect to have produced over 500 Chief Information Security Officers (CISOs) out of our hacker ranks. These skilled and motivated people will help reduce cyber risk in key commercial enterprises and government agencies.

- Hackers will earn US$1 billion in bug bounties within five years on HackerOne. "Some of my favourite highlights are absolutely the interactions with the people on the other side, and reactions to some of the bugs I've found," reflected elite hacker Frans Rosen. "When the CISO of a company calls me up in the middle of the night to understand the severity and panics when he realises the impact. When I build a little game to show the impact of a bug and the company responds with "this is the best game ever, we've played it all day in the office." On live hacking events, when you submit a really critical bug and the team of the company fills the room afterwards to understand exactly what happened. I live for the reactions since I understand myself how I would feel to get the same kind of report myself."

Every minute of every day, hackers and companies across the globe come together to enhance security. Businesses are constantly seeking to grow: expanding into new markets, shipping new products and services, adding customers, releasing mobile offerings, processing new forms of payment, increasing web assets, and so on. And every time they do, they add a new layer to their attack surface.

By partnering with willing organisations, trusted hackers are an extension of any security team and earn up to 36% more than they would as a software engineer in their home country. For companies, working with the largest, most active community of hackers allows them to be proactive about their security strategy in an efficient and cost effective way.

"Our first priority at Dropbox is the safety of our customers' data, and we've looked to the global security research community on HackerOne to validate the security of our platform continuously," said Justin Berman, Head of Security at Dropbox. "We have an industry-leading vulnerability disclosure program that protects ethical researchers and partnered with HackerOne to include sensitive vendors in the scope of our bug bounty program to help protect our entire ecosystem. Our hope is that bug bounty programs like ours continue to spearhead a culture of collaboration and transparency that benefits cybersecurity as a whole." ■

CITY OF AUSTIN PARTNERS WITH NTT TO ACCELERATE SMART CITY TECHNOLOGIES

The City of Austin and NTT Corporation (NTT) announced their intention to partner on an Accelerate Smart pilot project that will use new technologies to analyse traffic patterns, ease congestion and support community planning in Austin.

NTT's Accelerate Smart data platform, as well as modular data centre infrastructure for edge deployments, will monitor traffic-related issues downtown using Internet of Things (IoT) devices deployed at the intersections of Cesar Chavez Street and Trinity Street and Neches Street and 8th Street. The smart city project will collect traffic-related and mobility data through vehicle counting and classification, as well as wrong way vehicle occurrences, to provide real-time notifications and better inform how to implement appropriate solutions to fit traffic patterns.

"We are piloting NTT because these solutions have the potential to help Austin digitally transform how people move safely through the city. By better understanding the data and causal effects of problems we see in challenging areas, we can develop effective solutions that meet the community's needs," said Jason JonMichael, Assistant Director of Smart Mobility, Austin Transportation. "Evaluating data is key to reaching our Vision Zero goal of eliminating fatalities and serious injuries on Austin roadways. Smart technologies like this one will help us prioritise improvements to make our streets safer."

Using IoT, NTT will deliver the City real-time alerts and traffic statistics that improve predictions and outcomes for the City of Austin. The Accelerate Smart service will collect and detect data, including vehicle counts and occurrences of wrong-way driving, to enable the City to make informed recommendations for effective transportation planning aligned with the Vision Zero initiatives.

The pilot program is designed to provide automated deployment and operation of necessary information and communications technology (ICT) resources from devices and networks to the cloud. This will allow the City to focus on improving traffic conditions through analysis and process data more efficiently without worrying about deployment and optimisation issues.

"For the City of Austin, traffic management is a critical component to minimise the challenges of rapid, significant growth," said Akira Shimada, Senior Executive Vice President, NTT. "Our Accelerate Smart solution will help the City of Austin in their pursuit of pedestrian safety goals and position them for continued innovation to improve the lives of residents and visitors."

NTT's Accelerate Smart solution was developed as a joint initiative across NTT's global operating companies. It uses a secure, distributed network as a platform solution built on NTT's innovative Cognitive Foundation™ architecture, and also incorporates hyperconverged infrastructure and IoT gateways, as well as virtualisation software hosting predictive analytics applications.

Following the initial pilot, the City of Austin and NTT plan to evaluate the viability of extending the pilot and potentially adding locations.■

ENTERPRISE CLOUDS HAMMERED BY CYBER ATTACKS DURING PANDEMIC

A steady stream of attacks on enterprise clouds during the first couple of months of 2020 has become a flood since the start of the COVID-19 coronavirus pandemic, with external attacks spiking by more than 600% in the space of a few weeks.

That is according to new statistics produced by cyber security firm McAfee using data drawn from 30 million users of its Mvision Cloud service. The Cloud adoption and risk report – work-from-home edition highlights what McAfee describes as "significant" and "potentially long-lasting" trends as the usage of cloud services, often accessed via unmanaged devices, spikes during lockdown.

It said such trends emphasised the need for security delivery models to change fundamentally, and urgently, particularly in industries such as financial services and manufacturing, which more usually rely on on-premise applications, networking and security, as well as the education sector.

"The move to widespread remote working has required many industries to adopt new cloud services in order to maintain staff communication and collaboration during such a challenging time," said Nigel Hawthorn, data privacy expert for cloud security at McAfee. "However, it is important to recognise the increased threat from cyber criminals who see opportunity in cloud services that are not managed securely.

"Cloud and data security should be absolutely front and centre in informing any enterprise's cyber security approach – even more so when they are increasingly reliant on the cloud. Without ascertaining where sensitive data resides or how it is used and shared, it is simply impossible for organisations to have an accurate picture of their security posture and where any vulnerabilities may be."

Hawthorn said it was crucial for organisations to recognise their role within the shared responsibility model, making everyone accountable for cyber security, from enterprise IT teams, to managed service providers accessing their networks, down to individual employees.

"When managed correctly, cloud is the most secure place to do business and an incredible driver of business growth, innovation and resiliency," he said. "Collaboration, strong data governance and regular staff training are the keys to making this a reality."

The report highlighted that cloud-based unified communications and collaboration tools, such as Cisco WebEx, Microsoft Teams and Zoom, as well as Microsoft Office 365, were particularly at risk from attacks – which most often take the form of large-scale attempts to access accounts using stolen credentials.

McAfee also observed that the level of insider threat to cloud environments remained largely constant during the survey period, suggesting that working from home has not had a negative influence on employee loyalty. But Rajiv Gupta, SVP of cloud security at McAfee, said the risk of threat actors targeting the cloud far outweighs any risk introduced by changes in employee behaviour.

"Mitigating this risk requires cloud-native security solutions that can detect and prevent external attacks and data loss from the cloud and from the use of unmanaged devices," he said. "Cloud-native security has to be deployed and managed remotely and can't add any friction to employees whose work from home is essential to the health of their organisation."

McAfee urged organisations to re-evaluate their security postures as a matter of urgency to protect against attack.

Some basic steps towards this could include: adopting a "cloud-first" thought process, shifting focus away from on-premise security; reconsidering network set-ups, as remote working reduces the ability for hub-and-spoke networking models to work effectively – direct connections through the cloud are more appropriate now; and consolidating and reducing complexity, with an eye on service interoperability. ■

ARCULES APPOINTS MICHAEL HYGILD AS DIRECTOR OF SALES, EMEA

Arcules, a leading provider of integrated cloud-based security services, announced that it has appointed Michael Hygild as Director of Sales, EMEA, effective July 1, 2020. The addition of Hygild to the Arcules leadership team will help to accelerate the company's current momentum and ignite its next phase of growth. In his new role, Hygild will be responsible for leading strategic sales initiatives, including channel programs, within Europe. Hygild joins Arcules from Hikvision where he managed the Hikvision Europe - Nordic business unit, focusing on rapidly expanding the company's reach and growth strategies in its early stage. During his tenure, Hygild drove the development and successful execution of sales and business development initiatives to significantly expand the reach and use of the company's solutions. He was recently selected as one of four finalists for Sales Excellence of the Year by Business Denmark and TACK International, awarded to sales leaders who have achieved high levels of sales expertise and execution across Denmark.

"Michael brings a wealth of knowledge, energy and experience to Arcules, including first-hand insight into the complexities and challenges our customers face in building the next evolution of video surveillance and security infrastructures," said Nigel Waterton, Chief Revenue Officer, Arcules. "As we expand our sales organisation, Michael's ability to go deep into markets, navigate executive and committee sales, and create exponential growth will be essential for the next phase of our expansion. The success we are having in the market has allowed us to attract someone of Michael's calibre who represents an ideal fit to help lead our sales initiatives."

In his nearly 20 years of experience, Hygild has managed sales teams and general business operations in the video surveillance market and played a pivotal role in expanding the adoption of IP cameras for a wide range of businesses. He was also instrumental in developing a security department for a European IT distributor, offering significant experience driving business from all points in the supply chain. As Director of Sales — EMEA for Arcules, he will help expand and grow the company's go-to-market strategy while identifying new revenue streams for the delivery of cloud-based services designed specifically for video surveillance and security use cases.

"Arcules' ability to deliver cloud services that are simple, scalable and secure are unlike anything else in the industry," said Michael. "As we continue to see more and more organisations embrace the cloud for its ease of usability and utmost reliability, I'm excited to be helping them experience the true potential of the cloud and address the changing needs of the modern business." ■

ADVANCED ENERGY'S TREK INTRODUCES INNOVATIVE NEW ELECTROSTATIC VOLTAGE SENSOR

Advanced Energy (Nasdaq: AEIS) announced the new Trek Model 875 Electrostatic Voltage Sensor is now available. Unlike other electrostatic voltage sensors on the market today, the Model 875 can perform electrostatic monitoring without touching the product being measured and is insensitive to distance (within the specified range).

These unique capabilities enable Model 875 to monitor electrostatic charge in a continuously moving production process, for the manufacturing of many products including semiconductor devices, flat panel displays, textiles, packaging, electrophotography, pharmaceuticals and electronics – processes in which electrostatic charge build-up can disrupt the production process or cause significant damage in the product being manufactured.

"Electrostatic charge is difficult to measure, and Advanced Energy has perfected the process with the Trek Model 875, which builds on our existing market leadership of 'field nulling' electrostatic voltmeters," said Elisabeth Pederson, general manager, Advanced Energy's Trek product group. "Customers that manufacture products in a moving production process will use various techniques to mitigate the build-up of harmful electrostatic charge. The Model 875 continuously measures the process, providing a real time monitoring of charge build up. This allows the manufacturer to take swift action to significantly reduce the risk of field failure and process issues."

Model 875 features several other competitive advantages. It is unique in being packaged in an industry standard 35mm width DIN rail enclosure, which makes it easy to integrate with any manufacturing line. Further, Advanced Energy's renowned probe design automatically helps to alleviate particle contamination on the sensor through continuous motion of it's chopper stabilised operation enabling it to maintain high accuracy and speed. Model 875 has a measurement range of +-500VDC or Peak AC, a speed of response of < 25mS, and an accuracy of +/- 0.5 percent of full-scale. ■

YESWEHACK ENSURES THE CONTINUOUS SECURITY OF FRANCE'S COVID-19 CONTACT TRACING APP

YesWeHack, a global bug bounty leader with a strong APAC presence, today announced the launch of a dedicated vulnerability detection programme for StopCOVID, France's official app in the fight against the spread of COVID-19. Developed by a consortium of public and private actors, the application aims to ensure reliable contact tracing as France progressively loosens the country-wide lockdown. Following a recommendation from France's national cybersecurity agency, the StopCOVID project team has opted for the highest possible transparency and security for the app users. YesWeHack's community of ethical hackers will aim to identify every potential weakness in the app. Those vulnerabilities are reported directly to the StopCOVID project team.

With this innovative security approach, the StopCOVID project team underlines the importance of information security and data protection in the fight against COVID-19. France is also the first country to secure its contact tracing app through bug bounty.

The security audit of the StopCOVID contact tracing app in France starts today as a private bug bounty programme with 20 ethical hackers selected from the YesWeHack community. The app is to be launched in June. By debuting the bug bounty before the app's official release, the consortium ensures StopCOVID will provide the best possible security to its end users. Once the app is released, the bug bounty programme will go public---the vulnerability hunt will open to all ethical hackers, thus harnessing the combined efforts and insights of YesWeHack's 15,000-plus strong community.

Every vulnerability will be reported through YesWeHack directly to the StopCOVID project team. Each report contains both the specific detail of the vulnerability and suggestions for remediation to speed up fixing.
By mobilising the YesWeHack ethical hacker community, swarm intelligence and continuous security audit strive to ensure an optimal security level for France's contact tracing app. A proven, turnkey approach befitting all types of organisations in their aspiration to repel brazen cyber criminals, bug bounty continues to revolutionise Information Security.

YesWeHack is a long-standing partner of government agencies, including the French Ministry of Defence, the Direction interministérielle du numérique, France's digital transformation agency, and Cybermalveillance.gouv.fr, the French platform for prevention and assistance to victims of cyberattacks. Also, Europe's Bug Bounty leader brings together companies from around the world that seek to improve the security of their digital assets thanks to ethical hackers. Those receive a bounty (a reward) for security flaws they identify.

The development of the StopCOVID contact tracing app is carried out free of charge by all parties involved. Thus, YesWeHack will bear the cost of the bounties to be awarded. "As a critical part of the our country's toolset against COVID-19, it is vital that our data is safe from cyberthreats. We are proud to be able to contribute to reinforce security in the current exceptional situation," says Guillaume Vassault-Houlière, CEO and co-founder of YesWeHack. ■

DELL EMC ISILON FILE STORAGE FLOATS INTO GOOGLE PUBLIC CLOUD

Dell EMC spun out a flurry of cloud initiatives to bolster one of the few areas where its products lag competing storage vendors.

The infrastructure vendor teamed with Google to make its Dell EMC Isilon OneFS file system available for scale-out analytics in the Google Cloud Platform (GCP). Dell EMC said Google cloud customers can scale up to 50 petabytes of Isilon file storage in a single namespace, with no required application changes.

The managed NAS offering uses Google compute to run software instantiations of Isilon OneFS. The service is part of Dell Technologies Cloud, an umbrella branding for Dell EMC's cloud options. This is Google's second major foray into file system storage within the last year. It acquired startup Elastifile, whose scale-out system is integrated in Google Cloud Filestore.

Dell Technologies Cloud hybrid cloud infrastructure enhancements also include native Kubernetes integration in VMware vSphere, along with more flexible compute and storage options.

Dell EMC allows customers to tier local file storage to all three public cloud providers via its Isilon CloudPools, but the Google partnership is its first effort at writing OneFS specifically for cloud-native workloads. AWS has the largest market share of the public cloud market, followed by Microsoft Azure and Google Cloud Platform.

Dell did not address if it plans similar integrations with AWS or Microsoft Azure, but it represents a likely path, especially as enterprises deploy multiple hybrid clouds. File pioneer NetApp started offering cloud-based versions of its OnTap operating system several years ago, while all-flash specialist Pure Storage recently added file services to its block-based FlashArray flagship array. Hewlett Packard Enterprise also sells file services in the cloud on ProLiant servers through an OEM deal with Qumulo, whose founders helped to engineer the original Isilon NAS code.

"Dell has to continue to execute on this strategy with the other major cloud providers. This can't be a one-and-done [with Google]. We'll need to see more improvements from Dell in the next six to 12 months to show they are able to bring their file storage technologies to the cloud," said Matt Eastwood, a senior vice president of enterprise infrastructure at IDC.

Although Dell and Google publicly acknowledged a beta version in 2018, the formal OneFS cloud launch comes a little more than one year after Thomas Kurian took over as CEO at Google Cloud Platform. An interesting twist would be noteworthy if Kurian's arrival helped spur the Dell product development: George Kurian, his twin brother, and CEO at NetApp, has said Dell is "years behind" NetApp's Data Fabric strategy.

Brian Payne, a Dell EMC vice president, said enterprises have struggled to run traditional file systems that fully exploit Google's fast compute services for analysing large data sets. Enterprises can purchase the cloud version of Dell EMC Isilon OneFS with the required compute services in the Google Compute Platform portal.

"We found that customers are using Google to run their AI engines or data services, and we paired with Google to help them process and store very large content files in Isilon," Payne said.

Dell's strategy has evolved on how to unify is hybrid cloud offerings with public cloud technologies, although its ownership of VMware provides assets supported by Dell EMC storage competitors.

Dell Technologies Cloud integrates VMware Cloud Foundation (VCF) and Dell EMC VxRail hyper-converged infrastructure as a combined stack to run workload domains, software-defined storage, software-defined networking and virtualised compute. Customers can buy Dell Technologies Cloud and manage it locally or as an on-demand service.

VMware Cloud Foundation 4.0 includes native Kubernetes integration that allows container orchestration to be managed in vSphere. The Kubernetes piece is part of Project Pacific, the code name for a major redesign of the vSphere control plane. Payne said it allows cloud-native workloads to run directly on the Dell Technologies Cloud platform, with Dell handling lifecycle management.

Dell Technologies On Demand offers the same services as a consumption license. Payne said Dell's new entry requirement is a minimum of four nodes, down from eight nodes, and users can scale capacity across multiple racks.

The Dell Technologies Cloud binge includes updates to Dell EMC SD-WAN software-defined networking, based on the VeloCloud technology VMware acquired in 2017. Dell also added support for Dell EMC PowerProtect Cyber Recovery data protection to VMware Cloud, which uses Dell EMC storage to extend private IaaS deployments to public clouds. ■

TEXAS TAKES SECOND RANSOMWARE HIT

The Texas Department of Transportation (TxDOT) has been hit by ransomware just days after the state's judiciary system suffered the same fate.

According to a May 15 message posted on Twitter by TxDOT, the attack struck on May 14, when a threat actor gained unauthorised access to the department's computer network.

The network was shut down as soon as the attack was detected in an effort to contain the threat and prevent any further unauthorised access.

TxDOT executive director James Bass said in the statement: "We want every Texan to rest assured that we are doing everything we can to swiftly address this issue. We also are working to ensure critical operations continue during this interruption."

Federal law enforcement was informed of the attack, and TxDOT said that no mercy will be shown to whomever is found to be responsible for it.

Bass said: "TxDOT is working closely with the FBI to find the individual(s) responsible and prosecute them to the fullest extent of the law." TxDOT oversees all air, road, and railway transportation in the state. At time of publication, the department's website was back up and running.

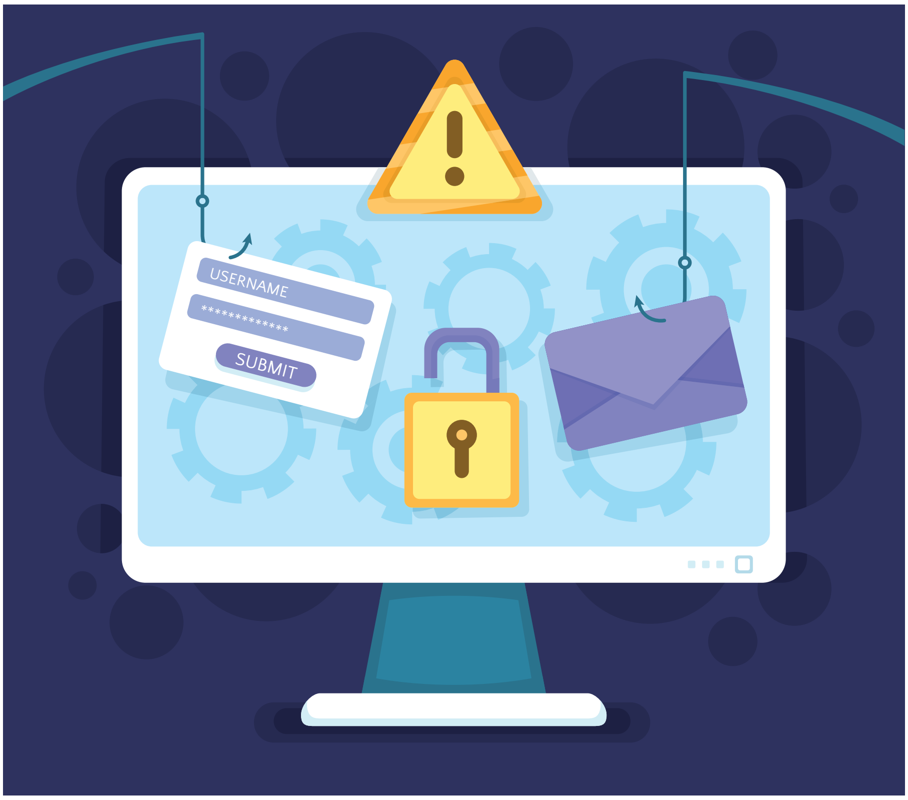
News of the TxDOT attack comes days after a ransomware attack hit the state's judicial agencies and appellate courts on May 8. As a result of the incident, access to case management systems was lost and court offices were unable to connect to the internet.

With the usual channels disabled by cyber-criminals, staff were reduced to using social media to announce legal rulings. The first attack was identified by the Office of Court Administration (OCA). No information as to whether the two attacks were linked in any way has been forthcoming.

Neither the OCA nor TxDOT shared any information regarding what, if any, data had been encrypted or stolen. Similarly, neither ransomware target has disclosed any details of a ransom demand.

Texas is fast becoming a hotspot for cyber-attacks. In 2019, ransomware was used to target 22 local governments across the Lone Star State in a single attack. The collective ransom demand for the coordinated assault was $2.5m. ■

EASYJET SAYS DETAILS OF NINE MILLION CUSTOMERS ACCESSED IN DATA BREACH



easyJet has revealed that the personal data of approximately nine million of its customers has been accessed following a "highly sophisticated" cyber-attack on its system. This includes credit card details of a small subset of these customers (2208), with the airline confirming it has already taken action to contact and offer support to those individuals.

For the rest of the customers affected, email addresses and travel details were accessed. Easyjet said these customers will be contacted in the next few days to and the company will "advise them of protective steps to minimise any risk of potential phishing."

The company took immediate steps to manage the incident once it was aware of the attack and closed off the unauthorised access. It also stated that it has notified the National Cyber Security Centre and the Information Commissioner's Office (ICO) of the breach. The firm has not given any details on the nature of the breach.

There is currently no evidence that the information accessed has been misused; however, the airline is urging its customers to stay alert to any unsolicited communications and to be "cautious of any communications purporting to come from easyJet or easyJet Holidays."

Johan Lundgren, easyJet chief executive officer, said: "We take the cybersecurity of our systems very seriously and have robust security measures in place to protect our customers' personal information. However, this is an evolving threat as cyber-attackers get ever more sophisticated.

"Since we became aware of the incident, it has become clear that owing to COVID-19 there is heightened concern about personal data being used for online scams. As a result, and on the recommendation of the ICO, we are contacting those customers whose travel information was accessed and we are advising them to be extra vigilant, particularly if they receive unsolicited communications."

The incident has come a particularly bad time for easyJet, who face the possibility of a large fine under General Data Protection Regulation (GDPR) rules.

Commenting on the breach, Felix Rosbach, product manager at data security specialists comforte AG, said: "The aviation industry is struggling at present given the current pandemic so seeing another major airline succumb to a data breach is not pleasant. On first glance, easyJet has followed the correct procedures and informed all affected customers who have had their sensitive data compromised. However, this situation could have been avoided."

Last year, British Airways (BA) was hit by a record £183m GDPR (intention to) fine after failing to prevent a digital skimming attack in 2018. ■

WINNTI GROUP TARGETS VIDEO GAME DEVELOPERS WITH NEW BACKDOOR MALWARE

Researchers from ESET have discovered a new modular backdoor used by the Winnti Group to target several video game companies that develop MMO (massively multiplayer online) games.

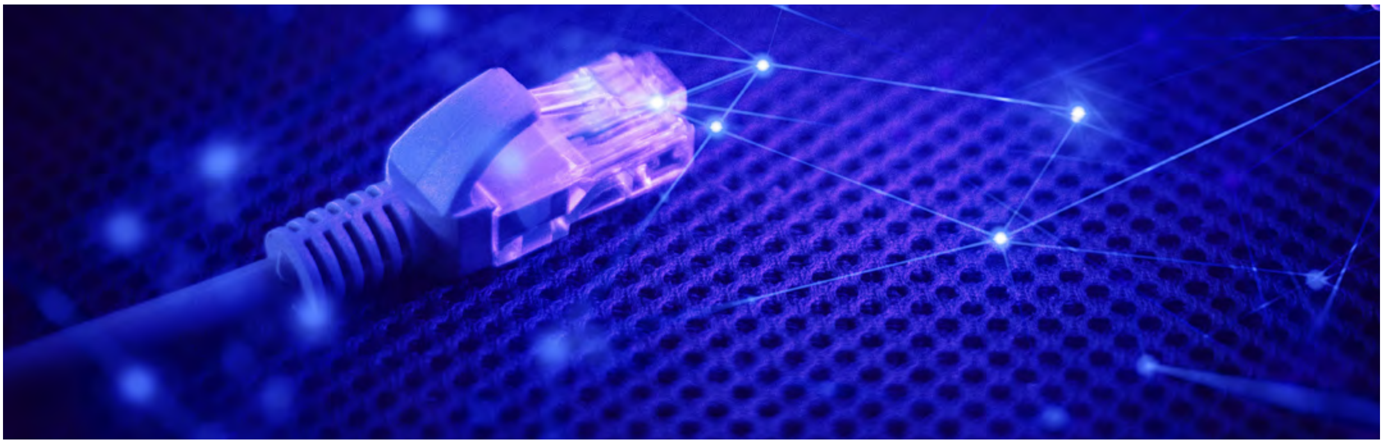
As explained in a blog post, the malware, dubbed 'PipeMon' by ESET, targeted companies in South Korea and Taiwan. The video games developed by these companies are distributed all around the world, are available on popular gaming platforms and have thousands of simultaneous players.

According to researchers, the new modular backdoor is signed with a code-signing certificate likely stolen during a previous campaign and shares similarities with the PortReuse backdoor.

In at least one case, the attackers compromised a company's build orchestration server, allowing them to take control of the victim's automated build systems. This could have allowed the attackers to Trojanise video game executables, although there's no current evidence that has occurred. In another case, attackers compromised a company's game servers. With this attack, it would be possible to manipulate in-game currencies for financial gain, ESET explained.

"Multiple indicators led us to attribute this campaign to the Winnti Group. Some of the command and control domains used by PipeMon were used by Winnti malware in previous campaigns," said Mathieu Tartare, malware researcher at ESET. "Furthermore, in 2019, other Winnti malware was found at some of the same companies that were later discovered to be compromised with PipeMon in 2020." ■

OPENREACH TAPS NOKIA TO EXTEND FULL-FIBRE NETWORK CAPACITY



UK national broadband provision firm Openreach is ramping up its fibre roll-out plans by extending its technology supply deal with Nokia.

Openreach will use Nokia GPON and XGS-PON fibre access technologies as part of its plans to bring ultra-fast, reliable broadband access to 20 million homes across the UK by the mid- to late 2020s, with 4.5 million premises by the end of March 2021, and also provide a platform for the UK's economic post-COVID-19 recovery.

Specifically, it will deploy the 7360 ISAM FX, Nokia 7362 ISAM DF and Nokia ISAM optical network terminals (ONTs).

"We are accelerating our full-fibre build to deliver an ultra-fast, ultra-reliable and futureproof broadband network throughout the UK," said Openreach CEO Clive Selley. "This new digital platform will help our economy to bounce back more quickly from the COVID-19 pandemic – enabling people to continue working from home, and millions of businesses to operate seamlessly online for decades to come.

"Right now, we're making the new network available to around 32,000 homes and businesses every week, and Nokia's innovative solutions are helping us to build it better, broader and faster. Our partnership with Nokia will be critical in helping us to upgrade the nation and hit our target of reaching four and a half million premises by the end of March 2021."

Full-fibre, gigabit broadband roll-out been a hot political issue in the UK for the past six months, and before the coronavirus brought expansion to a halt – mainly due to the lack of engineers being able to enter customers' homes – network deployment was being carried out apace.

As well as levelling up broadband provision for UK citizens, most of whom are now working from home, a nationwide fibre-to-the-home network has the potential to provide a huge economic boost to the UK. Research released by Huawei in April 2020 calculated that delivering "Gigabit Britain" could provide over £50bn gross value added to the economy in five years, growing to £68.8bn in 2030.

In addition, Openreach-commissioned research from October 2019, taken by the Centre for Economics and Business Research, calculated a potential productivity benefit of £59bn to the UK by 2025, enabling 400,000 more people to work from home.

Openreach's new installation will mean its network will be capable of delivering up to 10Gbps symmetrical broadband speeds in the future, in areas where demand for additional capacity is required. Nokia's solution also supports an evolution from current traditional deployments to virtualised access-network control and management, software-defined access networking (SDAN).

Nokia said the new agreement is another key milestone in its partnership with Openreach to deliver multi-Gigabit, next-generation PON connectivity to customers and builds on an extensive end-to-end network framework that has been established over the past years. This includes G.fast technology, which currently allows Openreach to offer 100s of Mbps to homes in areas where fibre is not yet available.

"Ensuring everybody has access to broadband services is critical, especially during unprecedented times like these, when it has become a lifeline to millions working, handling healthcare and learning from home," said Sandra Motley, president of fixed networks at Nokia.

"Our fibre solutions will help Openreach bring enhanced ultra-broadband services to millions of new customers across the UK today, while our 10G PON technology will help to futureproof their network against whatever may come next." ■

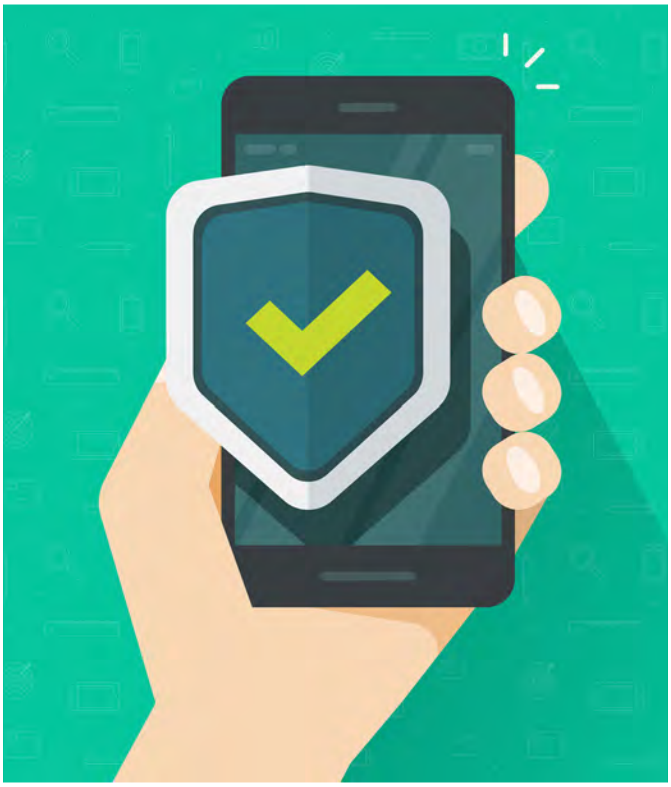
SAMSUNG ELEVATES DATA PROTECTION FOR MOBILE DEVICES WITH NEW SECURITY CHIP SOLUTION

Samsung Electronics Co., Ltd., a world leader in advanced semiconductor technology, introduced a standalone turnkey security solution comprised of a Secure Element (SE) chip (S3FV9RR) and enhanced security software that offers protection for tasks such as booting, isolated storage, mobile payment and other applications. The latest security chip is Common Criteria Evaluation Assurance Level (CC EAL) 6+ certified, the highest level acquired by a mobile component.

"In this era of mobility and contact-less interactions, we expect our connected devices, such as smartphones or tablets, to be highly secure so as to protect personal data and enable fintech activities such as mobile banking, stock trading and cryptocurrency transactions," said Dongho Shin, senior vice president of System LSI marketing at Samsung Electronics. "With the new standalone security element solution (S3FV9RR), Samsung is mounting a powerful deadbolt on smart devices to safeguard private information."

Samsung's new security solution is an enhanced turnkey that follows the first-generation solution (S3K250AF) announced in February. The new security solution is a state-of-the-art component that offers higher assurance levels than its predecessor's CC EAL 5+ with an industry-leading CC EAL 6+ certified-hardware secure element, S3FV9RR, and powerful security software. CC EAL 6+ is utilised in applications that demand the most stringent security requirements in the market such as flagship smartphones, e-passports and hardware wallets for cryptocurrency.

With twice the secure storage capacity, the new security solution also supports hardware-based root of trust (RoT), secure boot and device authentication that brings



mobile security to the next level. Especially for service providers, manufacturers and organisations, secure device authentication is enhanced with the RoT when running proprietary applications on a mobile device.

As a bootloader initiates, a chain of trust is activated through which each and every firmware with approved keys is sequentially validated. This secure booting process is handled by the RoT, guarding the device against any possible malicious attacks or unauthorised software updates.

As a standalone solution, the new security solution can work independently from the security performance of the device's main processor. This makes the solution extremely versatile, expanding the security capabilities of mobile devices, IoT applications, and other devices in all performance levels.

In addition, manufacturers can be assured that devices produced at an off-site location are not tainted with non-authorised firmware. The solution also meets the hardware security module requirements for cryptographic operations outlined by an upcoming mobile operating system version.

Samsung's new security solution, S3FV9RR, is expected to be available within the third quarter of this year. ■

STOCK MARKETS ARE UNBALANCED, INVESTORS WARNED

Wall Street is unbalanced, and investors are in danger of becoming complacent, warns the CEO of one of the world's largest independent financial advisory and fintech organisations.

=The warning from deVere Group's Nigel Green comes as U.S. stock futures indicate another strong open for Wall Street on Tuesday following a long holiday weekend.

Mr Green says: "Wall Street and other stock indices around the world have been, in general terms, rallying in recent weeks as investors jump on fresh COVID-19 vaccine optimism and signals that global economies are beginning to be revived.

"There's an over-riding and far-reaching bullish sentiment in stock markets. However, there are bonafide concerns that investors are in danger of becoming complacent.

"This is because the headline figures of rallying markets are not the best barometers of the economy right now. The upswing on Wall Street, for example, is being driven by a handful of companies all within the same sector: tech."

He continues: "This global economic downturn is different to others as there are clear winners and losers, whereas in previous ones it has been far less clear-cut and more a question of how much all firms were impacted.

"This one has produced enormous financial benefits for some, like tech, and left many struggling and others failing completely."

The deVere CEO says that while the booming sectors such as tech, home entertainment and online retailers might "indicate what the future, post-pandemic economy looks like", it doesn't reflect underlying economic conditions – and this "could catch investors out."

He notes: "Buying an exchange-traded fund, or ETF, which are investment funds traded on stock exchanges, could expose a client to a potentially unbalanced market."

To navigate the markets when they aren't reflecting the slew of current poor economic data, investors are urged to work with an experienced fund manager to help them "seek the significant opportunities but to mitigate potential risks."

Mr Green concludes: "The firms which are 'winners' in this downturn are over-represented on many leading global indices, including the benchmark S&P500 index.

"As such, they do not necessarily serve as the ideal economic gauge for investment decisions.

"Investors must bear this imbalance in mind." ■

75% OF CYBERSECURITY PROS SAY REMOTE WORK DROVE DRAMATIC CHANGE IN FINANCIAL SERVICES CYBER PROGRAMS

The Financial Services Information Sharing and Analysis Centre (FS-ISAC), an industry consortium dedicated to reducing cyber risk in the global financial system, announced that 75 percent of cybersecurity professionals representing financial institutions around the world made dramatic changes to their firm's cybersecurity programs to cope with the rapid shift to remote work due to the COVID-19 pandemic, according to a poll conducted by FS-ISAC.

FS-ISAC polled 871 cybersecurity professionals from financial institutions around the world at its Virtual Summit on May 19, which gathered more than 3000 cybersecurity professionals in the financial services industry. The poll gauged which trends driven by the pandemic had the most impact on their cybersecurity programs.

Key findings include:

- Digital banking tools were ready to securely handle a huge increase in volume as only three percent of respondents saw these tools driving significant program changes
- Eleven percent of respondents said third party risk concerns led to dramatic change
- Forty-six percent reported their financial institution is likely to invest more in cybersecurity post-pandemic

"The accelerated shift to remote work has fuelled a rapid evolution of the cyber threat landscape," said Steve Silberstein, CEO of FS-ISAC. "As the effects of this pandemic continue to unfold, CISOs and cybersecurity teams are constantly adapting their cybersecurity programs to meet a new reality that is everything but normal."

To support its nearly 7,000 members in sharing information about cyber threats, including those derived from the pandemic, FS-ISAC launched the FS-ISAC Intelligence Exchange in April 2020. The platform includes a new cyber intelligence sharing app and a secure chat function for real-time communication and collaboration. Since its launch, more than 6,000 users globally have adopted the new platform. ■

US JEDI CONTRACT DISPUTE DEVELOPS INTO WAR OF WORDS BETWEEN TECH GIANTS

The ongoing legal wrangle between Amazon Web Services (AWS) and the US government over its decision to award Microsoft a $10bn cloud contract has resulted in a public war of words breaking out between the two tech giants.

Microsoft was awarded the decade-long Joint Enterprise Defence Infrastructure (JEDI) contract with the Department of Defence (DoD) in October 2019, much to the dismay of AWS which – up until that point – had been widely expected to secure the contract.

Since then, AWS has repeatedly gone on record to contest the outcome of the procurement process, claiming “significant political interference” from the White House was to blame for it losing out on the deal to Microsoft. AWS is currently in the midst of pursuing legal action in

Photo by Franck V. on Unsplash

To be continued on page 21

an attempt to overturn the results of the procurement, and is understood to have filed another protest with the DoD on 5 May 2020 pertaining to the contract. This protest is confidential and no details about the nature of it have been made public, at the time of writing.

In response to AWS's latest complaint, Microsoft published a blog post on 7 May 2020 in which its corporate vice-president of communications, Frank Shaw, accused Amazon of forcing warfighters across the US to wait even longer to access the technology they need to protect their country.

"Amazon's complaint is confidential, so we don't know what it says. However, if its latest complaint mirrors the arguments Amazon made in court, it's likely yet another attempt to force a re-do because it bid high and lost the first time," wrote Shaw.

"The only thing that's certain about Amazon's new complaint is that it will force American warfighters to wait even longer for the 21st-century technology they need – perpetuating Amazon's record of putting its own interests ahead of theirs."

The JEDI contract centres on the provision of a general-purpose cloud environment that the DoD can use to supports its efforts to downsize its on-premise datacentre estate by moving more of its applications and workloads off-premise.

Shaw also went on to accuse Amazon of trying to "bog down" the delivery of the JEDI strategy with "complaints, litigation and other delays" in an attempt to force the DoD to repeat the procurement process and rescue its "failed bid".

"Think about it: Amazon spent the better part of last month fighting in court to prevent the DoD from taking a 120-day pause to address a concern flagged by the judge and re-evaluate the bids. Amazon fought for a complete re-do and more delay. Amazon lost. The judge granted the DoD's request for a timeout in the litigation to address her concerns," he said.

Photo by Christian Wiediger on Unsplash

"And now Amazon is at it again, trying to grind this process to a halt, keeping vital technology from the men and women in uniform – the very people Amazon says it supports."

While Amazon has cited political interference as the reason it lost out on the contract, Shaw claims Amazon's bid was too high, which is why the firm is doggedly attempting to appeal against the outcome so that it can submit a revised bid.

This claim was also recently made in another Microsoft blog post, authored by its general counsel, Jon Palmer, in mid-April 2020.

"Amazon may make a lot of noise about bias and interference, but the DoD's independent inspector general made it clear that the department established and followed a proper procurement process," said Shaw.

"No one forced Amazon to bid high in the procurement. Amazon alone made the choice to bid high, but now wants to find a way to avoid the consequences of its own bad business decisions."

AWS responded to Shaw's post in kind with a blog of its own, written by its vice-president of worldwide communications, Drew Herdener. In it, Microsoft is accused of attempting to mislead the public with its "self-righteous" and "pontificating" blogs about Amazon's reasons for contesting the outcome of the JEDI contract.

"Microsoft is doing an awful lot of posturing. We understand why. Nobody knowledgeable and objective believes they have the better offering. And, this has been further underscored by its spotty operational performance during the COVID-19 crisis (and in 2020 YTD)," wrote Herdener.

"Microsoft wants us to just be quiet and go away. But, as we've said all along, we believe it's critical for the DoD, the country, and future US government procurements that agencies make decisions free from political retribution and interference, and based fairly and on the facts."

Herdener went on to conclude his post with a warning to Microsoft that AWS has no plans scale back its commitment to getting the procurement process fully scrutinised.

"To be clear, we won't back down on this front regardless of whether Microsoft chooses to try to bully its way to an unjust victory," he wrote.

"We also won't allow blatant political interference or inferior technology to become an acceptable standard. We have great respect and admiration for those who serve and are honoured to support the DoD, but we will not sit idle nor apologise for doing what we believe is right, fair and just." ■

DIGICERT NAMED 2020 GLOBAL COMPANY OF THE YEAR IN TLS CERTIFICATE MARKET BY FROST & SULLIVAN

Frost & Sullivan recognises DigiCert with the 2020 Global Company of the Year Award, based on its recent analysis of the global transport layer security (TLS) certificate market. DigiCert has exhibited strong market leadership in its growth, supporting the adoption of new standards and continually innovating with the industry's best, most modern public key infrastructure (PKI) technology. In addition to the strength in the TLS/SSL market, the company is also focused on new security technologies, such as protecting devices in the Internet of Things (IoT) and developing implementations of post-quantum cryptography (PQC). By developing these technologies and helping define standards to address new security use cases, the company is strengthening its leadership position within internet security.

"Leveraging its superior technology, customising it to regional markets and building a best-in-class customer support system, DigiCert has captured the business of 89% of the Fortune 500 companies and the world's most recognised brands," said Swetha Krishnamoorthi, Industry Analyst at Frost & Sullivan. "Further, DigiCert has successfully integrated the technology strengths of the former Symantec TLS and PKI business to provide an unequalled product portfolio and scalability for partners and customers. DigiCert's certificates and management tools support a wide range of enterprise needs and use cases, ranging from standard TLS to compliance-specific use cases such as Google AMP and EU-trusted qualified certificates for natural persons, legal entities or web authentication (QWACs). The company also supports cloud-based code signing, remote document signing, a host of IoT device authentication and encryption scenarios, large enterprise secure remote access, secure email and much more."

DigiCert CertCentral® TLS Manager enables organisations to issue, discover, renew and revoke certificates in an automated manner.

CertCentral features an intuitive UI and is built on APIs for easy certificate management at any scale. DigiCert's modern and growing DigiCert® ONE platform, which also includes DigiCert® Enterprise PKI Manager and DigiCert® IoT Device Manager, enables management of all types of certificate deployments, such as cloud, on premises, in-country and hybrid environments.

DigiCert has upgraded its infrastructure in a way not seen in its industry to support large installations, regionally-focused deployments and high-volume, rapid certificate enrolments for the world's largest web platform companies. The company's agile product development process allows it to roll out changes and product updates more quickly than competitors. This strategy has helped the company create the industry's first PQC toolkit, which enables companies to create hybrid certificates for testing in their systems.

DigiCert actively engages with industry standards and regulatory bodies to drive the creation and support of new standards and ensure a safe internet and IoT for consumers, including the CA/Browser Forum, IETF, W3C, ASCX9, PCI Council, SAE, CableLabs, CI+, AeroMACS, WinnForum, Industrial Internet Consortium, APWG and NIST NCCoE.

"With its multi-pronged approach to innovation, DigiCert has developed a hyper-converged, agile infrastructure that promises reliability, scalability, resiliency and shorter response time for its customers," noted Swetha. "Its emphasis on user experience and a customer-first approach to product development will ensure its continued domination of the digital certificate market in the long term."

Each year, Frost & Sullivan presents a Company of the Year award to the organisation that demonstrates excellence in growth strategy and implementation in its field. The award recognises a high degree of innovation with products and technologies and the resulting leadership in terms of customer value and market penetration.

Frost & Sullivan Best Practices Awards recognise companies in a variety of regional and global markets for demonstrating outstanding achievement and superior performance in areas such as leadership, technological innovation, customer service and strategic product development. Industry analysts compare market participants and measure performance through in-depth interviews, analyses and extensive secondary research to identify best practices in the industry. ■

HIMA EMPOWERS INDUSTRIAL AND HAZARDOUS INSTALLATIONS WITH REMOTE MAINTENANCE

The HIMA Group introduced a solution for remote maintenance in the industrial context, living up to the standards set by the HIMA Smart Safety Platform (SSP), the world's first scalable safety platform with built-in cybersecurity. The HIMA Group presented the upcoming roadmap and new services complementing the SSP at the 24th Annual ARC Industry Forum held earlier this year.

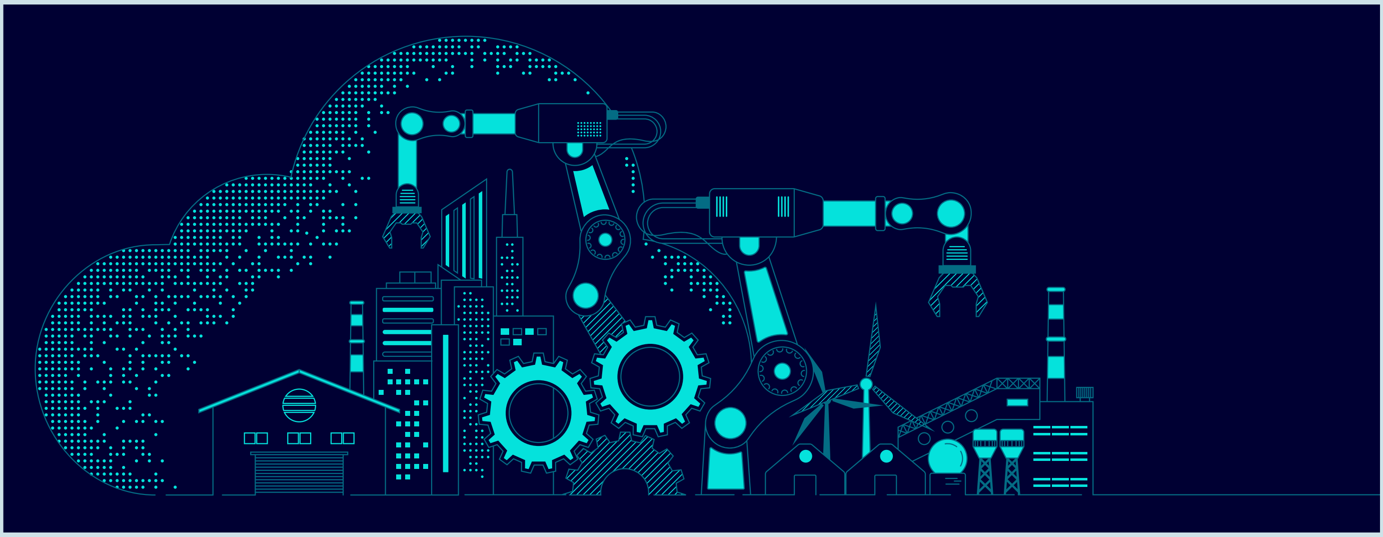
As the HIMA SSP offers a future-proof solution to the process industry that is both safe and secure, the new remote maintenance solution is the perfect and logical addition: It helps to reduce operating costs and increases productivity, while the combination with SSP is protecting the plant against the growing risk of cybersecurity attacks.

"Having both safety and security in mind, many companies face a tough choice, when making a decision regarding remote maintenance", says Dr. Alexander Horch, VP R&D and Product Management at HIMA. "On the one hand, everybody can see the potential of substantial cost advantages if remote maintenance of process systems is carried out via public networks. On the other hand, though, there are substantial security risks to be reckoned with as well. If a company hasn't established effective protection mechanisms, it only takes one weak spot to jeopardise the entire production process. With SSP we made the 'core' secure and now we follow up with a complete unitary solution or remote access, which meets highest requirements regarding safety and security."

To address the challenges all companies in the industrial context face, HIMA's remote maintenance solution fulfils the highest standards for safety and security, without any restrictions on scalability. HIMA clients and new customers alike can easily implement a secure remote maintenance system which conforms to requirements set by the German Federal Office for Information Security (BSI). Hardware, software and support come all from one source, reducing complexity perceptibly.

The future roadmap focuses on the secure connection of mobile workers, encrypted communication via the internet, interface control and internal network segmentation with firewalls, as well as the networking of highly critical systems and 'data diodes'. Data diodes are integral components of modern automation systems such as NAMUR Open Architecture (NOA) or Open Process Automation. Secure data transmission from a highly sensitive area to a less sensitive one places high demands on the components.

Especially when all boundary conditions for performance, operability, economy and safety are taken into account. ■



WATERHOLE ATTACKS AND PHISHING IDENTIFIED AS SINGAPORE'S TOP CYBER THREAT VECTORS IN 2019

Ensign InfoSecurity (Ensign), one of Asia Pacific's largest pure-play cybersecurity firms, unveiled the findings of its Singapore Threat Landscape 2019 report, which identified waterhole attacks, a strategic website compromise attack, and phishing as the nation's top threat vectors in 2019, accounting for 84% of all cyberattacks detected.

The report also revealed that the high technology1 industry in Singapore is the top target for threat actors in 2019. Companies in this sector are attractive targets as threat actors want to exploit their data centre infrastructure to expand their botnet activities as well as target other organisations whose servers are being hosted there.

In 2019, the top five most targeted sectors in Singapore are:

1. High Technology
2. Infocommunications
3. Media
4. Institutes of Higher Learning
5. Financial Services

This report was generated using Ensign's proprietary tools and data models, including Ensign Singapore-centric Cyber Threat Intelligence, Cyber Threat Detection & Analytics engine, and the Ensign IP360 platform which profiles activities and behaviours of anonymous IPs in enterprise network traffic.

"Relevance and context are the most important elements when analysing cyber threat intelligence as threats and trends can differ across geographies, sectors and companies," said Lee Shih Yen, Senior Vice President, Ensign Labs, Ensign InfoSecurity. "Only by combining different global and local cyber threat intelligence sources are we able to derive accurate and deep information about Singapore-specific threats and help organisations bolster their cybersecurity posture by providing contextualised, actionable insights."

Waterhole attacks are the most prevalent threat vector of 2019, contributing to nearly half (47%) of all detected cyberattacks in Singapore. Waterhole attacks occur when an attacker compromises a website and replaces its content with malicious payloads. Unsuspecting victims who then download content from these websites will infect their machines with malware.

This method enables threat actors to execute supply chain attacks where they infect servers containing updates of popular software and replace these updates with malicious codes to spread malware. This allows threat actors to achieve mass infection, especially when the vulnerable web server is popular and trusted by end users.

The other top threat vector in Singapore is phishing (also known as malspam), and almost two out of five (37%) of the detected cyberattacks in 2019 can be attributed to it. Phishing is an effective social engineering technique and a popular tactic for threat actors as it is easy to execute and able to target a wide pool of victims. ■

GUILDONE AND BEATDAPP AGREE TO THREE-YEAR TO TRANSFORM MUSIC STREAMING ROYALTY PAYOUTS

Calgary-based blockchain developer GuildOne Inc. (GuildOne) and Vancouver-based Beatdapp Software Inc. (Beatdapp) are pleased to announce a three-year exclusive agreement to manage digital rights related to streaming media services in India and Japan using blockchain technologies.

Beatdapp tracks every music stream in real-time to create an immutable record secured by its proprietary blockchain, helping labels and artists identify missing music royalties. GuildOne acts on behalf of digital rights holders, such as artists, labels and producers, to identify when their digital assets have been streamed, calculate the royalties that are associated with those assets and execute the royalty transaction, ensuring all parties get paid what they are owed.

Under the terms of this agreement, GuildOne will use Beatdapp's services, along with information provided by rights holders to identify entitlements owed to those rights holders, ensuring that they receive accurate royalty payouts. GuildOne will then use its patent-pending ConTracks smart contract technology on R3's Corda blockchain platform to execute the royalty payments.

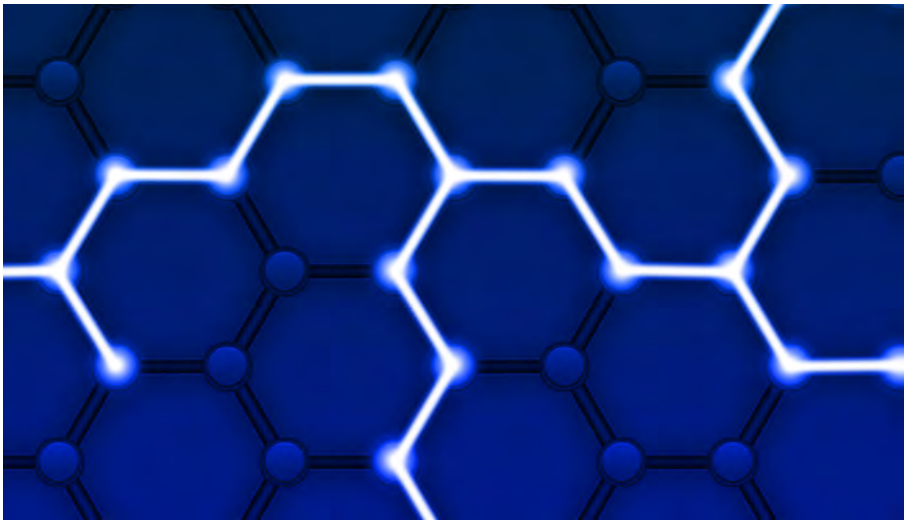
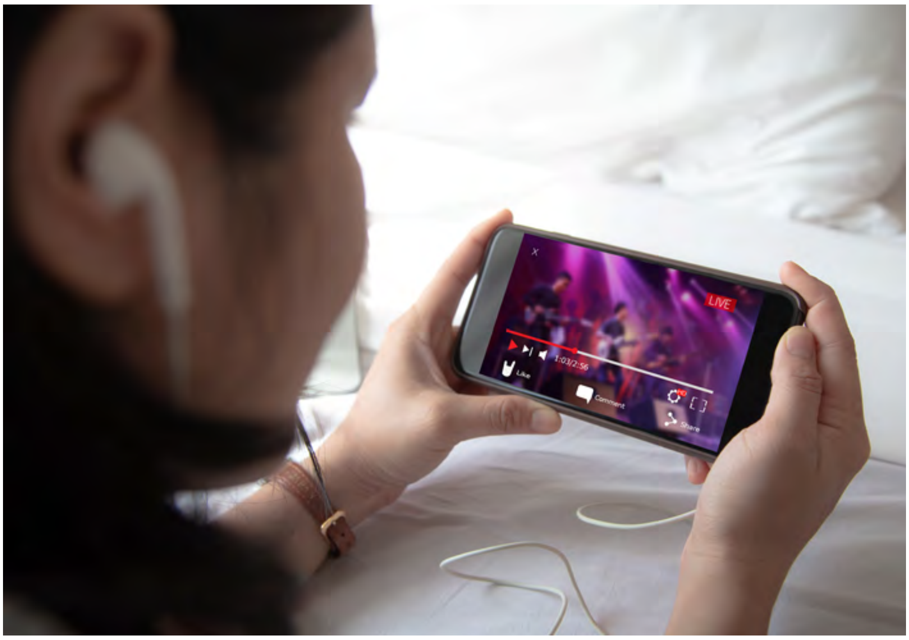


Image by Pete Linforth from Pixabay

James Graham, CEO of GuildOne, states that "This is a transformative event for the streaming industry, bringing together two leaders in the blockchain space to meet the needs of artists, labels and other rights holders."



Variety reports that streaming media accounted for US$11.1 billion globally in 2019, nearly 80 percent of music sales, with that market share expected to increase in coming years. Goldman Sachs estimates that world-wide streaming music royalties will exceed US$34 billion by 2030. Currently, however, up to 15 percent of streaming play count reports are incorrect, leading to billions of dollars in unpaid royalties.

"Beatdapp's technology ensures that labels and artists invoice correctly from the outset, and allows DSPs avoid costly, time consuming audits," said Andrew Batey Co-CEO of Beatdapp. "To partner with a leading expert in the payment space to ensure our verified usage reports yield faster, more accurate payouts to artists and labels is a great outcome for everyone involved. After a year of hard work behind the scenes, we're delighted that day has come!"

"We are excited to work with the team at Beatdapp and have mutual respect for each other's technology," said GuildOne co-founder and CTO Barry Kreiser. "We are particularly looking forward to applying our ConTracks smart contract engine to the burgeoning music royalty market." ■

ANT GROUP AND INTEL FORM PARTNERSHIP TO MAKE IT LEASING MORE ACCESSIBLE TO SMES

Ant Financial Services Group ("Ant Group"), an innovative technology provider, announced a cooperative effort with Intel to make it much easier and cost-effective for SMEs to lease IT equipment, leveraging the application of blockchain technology to strengthen transparency and build a system of trust.

Using proprietary blockchain technology, the partnership aims to empower the IT equipment leasing industry while accelerating the digital transformation of SMEs, many of which have seen their capital flows and supply chains disrupted amid the COVID-19 pandemic.

This partnership draws from Ant Group and Intel's complementary strengths to bolster transparency and efficacy among IT leasing vendors, enabling them to serve more SMEs and help them grow their businesses with improved efficiency and lowered cost.

Ant Blockchain, Ant Group's proprietary productivity blockchain platform, can help all parties in the entire IT rental and leasing process to build trust with each other. Intel's cloud device management technology helps leasing vendors to check the use status of the authorised hardware device using Intel's CPU. Increasing the level of trust and transparency among all parties in the leasing process enables financial institutions, such as insurance companies and SME loan providers, to swiftly make informed decisions about businesses, giving SMEs greater flexibility to expand their operations.

"We are excited to partner with Intel as we continue to help millions of SMEs transform their businesses and operations," said Geoff Jiang, Vice President of Ant Group. "Blockchain technology can play a pivotal role in building a solid system of trust among multiple parties and bringing more value to consumers, vendors, and the communities they operate in."

Yali Liang, Vice President of Sales, Marketing and Communications Group of Intel, said, "With Ant Blockchain, we can help SMEs reduce fixed costs and alleviate pressure from IT equipment maintenance, which will accelerate the digital transformation of SMEs through IT rental industry."

Zugeliang, a Hangzhou-based IT equipment leasing platform, used Ant Blockchain to increase the level of trust among all parties involved in its leasing processes in 2019. Since then, the platform has seen a six-fold increase in the number of orders and a 200% improvement in the rate of timely payments. ■

PROPERTYGURU TOUTS 3D VIRTUAL VIEWINGS WITH STORYTELLER

The COVID-19 pandemic has not dampened demand for private properties, at least among the wealthiest buyers, some of whom have been snapping up prime real estate across Asia-Pacific – even without virtual tours.

But for most property seekers, virtual tours are a must at a time when property showrooms are shuttered, prompting property developers to speed up their digital initiatives. These could be virtual reality showcases that offer a glimpse into a property, along with fly-by views of the development and its vicinity.

Sensing this market opportunity, PropertyGuru, a Singapore-based property technology company that serves 24.5 million property seekers across Southeast Asia through its online property portal, has built a new feature called StoryTeller into its FastKey property sales platform that enables developers to showcase their properties digitally to prospective buyers through 3D visualisation.

"From a property industry perspective, it is clear that consumers want an immersive viewing experience for their comfort and safety," said Jeremy Williams, chief business officer of PropertyGuru. "Behaviours are going to change to some extent post-COVID-19, and while the consumer will still want to physically see the property, we believe the number of physical viewings will reduce."

Jason Gregory, managing director of FastKey, a platform that automates the property sales cycle which PropertyGuru acquired four years ago, said StoryTeller is being powered by Foyr's cloud-based visualisation software.

To be continued on page 27

"We've been planning this for a while, but we accelerated our investment to get it to market because of the COVID-19 situation," said Gregory. "And this stuff is not easy – it's an extreme specialisation, so rather than build, we went with the partner route."

Gregory said StoryTeller can be integrated with a developer's inventory management system through application programming interfaces (APIs), enabling property seekers to get real-time information on whether specific units in a development are available.

During a demonstration of StoryTeller, Gregory showed off immersive views of a condominium's facilities, including the gym and swimming pool, before zooming in on the interior features of an apartment. With data supplied by developers and other sources, prospective buyers can even visualise the views from an apartment's windows.

Gregory said this data could include property brochures, floor plans and CAD (computer-aided design) files. "If developers are ready to build a sales gallery, then they're ready for StoryTeller, because we take that same information and we're digitising it, because it's important that the property looks the same when you visit the sales gallery," he said.

At the sales gallery, said Gregory, buyers could also use StoryTeller to get an augmented reality view of a development to identify individual units – which developers would otherwise display using a separate whiteboard or digital screen.

To ensure data privacy, Gregory said the personally identifiable information of StoryTeller users is encrypted and sent to developers, while data about buyer interest related to specific aspects of a development gleaned from browsing behaviour is anonymised and aggregated.

PropertyGuru is launching StoryTeller in five Southeast Asian markets—Singapore, Thailand, Malaysia, Indonesia, and Vietnam—and has already seen "spectacular interest" in the new feature during a webinar attended by 750 property developers.

"We really think this is a big opportunity, and we're approaching this in some ways as a little bit of a land grab," said Williams. "We will be very aggressive and leverage our relationships with developers across various touch points in the business to drive mass adoption." ■

EXABEAM INVESTS FOR GROWTH ACROSS ASIA PACIFIC AND JAPAN TO MEET INCREASING DEMAND FOR SMARTER SIEM

Exabeam, the Smarter SIEM™ company, announced a significant investment in its operations across the Asia Pacific and Japan (APJ) region to meet growing demand for its cybersecurity solutions and capitalise on record momentum, with over 100% year-over-year growth for fiscal year ending January 2020. The company tripled its workforce in the region through the recruitment of additional team members across sales, pre-sales, channel, marketing and customer support across APJ and more than doubled the team in Japan.

In addition, Exabeam is localising its product offerings for the Japanese market with the first release scheduled for later this quarter, and since mid-2019, the company provides in-country infrastructure failover with dual data centres, available in Tokyo and Osaka. This regional growth closely follows the recent announcement of an exclusive distribution agreement in Australia and New Zealand with cybersecurity specialist Orca Tech.

Exabeam is strengthening its commitment to the APJ region on the back of growing demand from organisations looking to save on data ingestion costs associated with their legacy security information and event management (SIEM) systems.

Customers are also turning to the Exabeam Security Management Platform (SMP) to reduce investigation times for security teams and better utilise junior security analysts by providing them with user-friendly security tools that automate threat investigation and response.

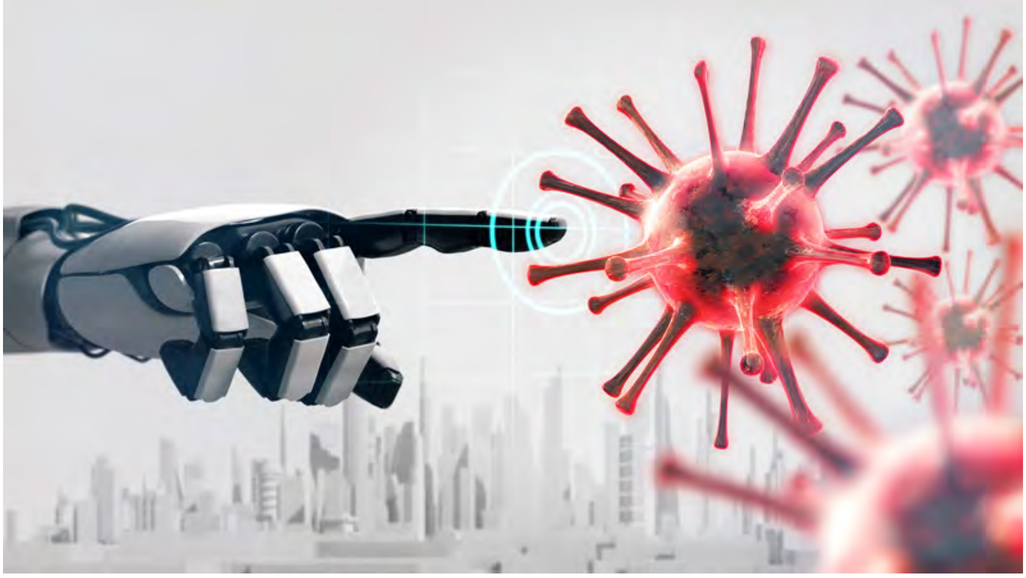
“We are seeing significant demand from organisations across the region looking to save costs and drive efficiencies in the SOC,” commented Gareth Cox, vice president of sales, APJ at Exabeam. “Adding to our team, building a partnership with Orca Tech and localising our offerings to better support customers underlines our commitment to the entire region, and we’re confident that we’ll see our momentum continue to accelerate.”

“As a valued partner to Exabeam in Japan, we are pleased with their commitment to further invest for growth. As a result of Exabeam’s willingness to support our sales efforts with additional headcount and localisation of Exabeam offerings, we expect to continue the momentum throughout the year as we address local market demand to prevent insider threats and drive efficiencies in the SOC,” commented Hiroshi Honjo, head of cyber security and governance at NTT DATA.

To help organisations understand the value of augmenting their existing SIEM environments with behaviour-based advanced analytics, in May 2020, Exabeam introduced a complimentary SaaS Analytics Review, a promotional offer available exclusively through Exabeam channel partners in APJ. Customers receive a custom report outlining anomalous VPN and user network activity and security alert prioritisation in comparison to their existing SIEM.

“With so many employees now working from home, organisations are introducing new applications and deploying a number of cloud services to ensure business continuity and keep critical services up and running,” said Cox. “The SaaS Analytics Review provides visibility into normal and abnormal activities with these new applications and user access locations so organisations can assess their security gaps. We also recently extended our range of Exabeam Cloud Connectors to reliably collect logs from more than 40 cloud services into Exabeam Data Lake, Exabeam Advanced Analytics, and any other SIEM tool. The newest additions include connectors to critical remote work tools from Zoom, Workday and Ping Identity, further enabling secure, distributed workforces.” ■

SK TELECOM INTRODUCES 5G-POWERED AUTONOMOUS ROBOT TO HELP FIGHT AGAINST COVID-19

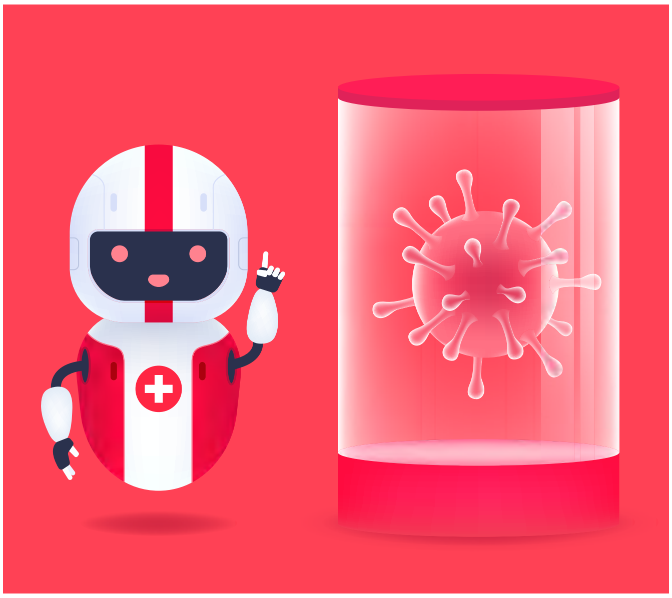


SK Telecom announced that, together with Omron Electronics Korea, it developed a 5G-powered autonomous robot to enable a systematic and efficient response against the coronavirus (COVID-19).

Built with cutting-edge technologies, including 5G, AI, autonomous driving and IoT, the robot carries out diverse activities such as contactless temperature screenings for visitors and disinfection of the building.

Upon detecting visitors, the robot automatically moves towards them to check their body temperatures using a thermal imaging camera. In case the measured temperature is 37.5°C (99.5°F) or higher, it sets off an alarm and alerts the control centre. Based on this data transmitted over 5G network in real time, SK Telecom will be able to take necessary measures like prohibiting people with suspicious symptoms from entering the building, etc.

In addition, equipped with UV lamps and two automatic floor disinfectant sprayers, the robot automatically disinfects the building. It can achieve 99.9 percent disinfection of 33 square meters of surface areas in just 10 minutes.



Applied with SK Telecom's self-developed AI-based video analysis solution, the 5G robot will also able to identify places where people are gathered and then move to the location to play a message stressing the importance of social distancing. It will also identify people who are not wearing face masks and request them to wear one.

Moreover, SK Telecom will ensure greater efficiency in both operation and management of the robot through the application of its big data analytics solution Metatron. Metatron will analyse the robot's component management data collected via IoT sensors to check the real-time status of the robot and perform predictive maintenance.

SK Telecom and Omron Electronics Korea plan to deploy the 5G-powered robot at their headquarters first and will officially launch the device in Korea this year and in global markets next year.

"As a leading ICT company, SK Telecom is seeking ways to help relieve the unprecedented situation brought by the coronavirus," said Choi Nag-hun, Vice President and Head of Industrial Data Business Unit of SK Telecom. "We will continue to introduce diverse services fit for the non-face-to-face era by leveraging our ICT including 5G and AI."

"The 5G autonomous robot is an innovative case where cutting-edge technologies have been applied to overcome the crisis caused by the coronavirus," said Kim Young-ho, President of Omron Electronics Korea. "The collaboration between Omron Electronics Korea and SK Telecom will serve as a great example showing how businesses can contribute to resolving social issues." ■

VMWARE AND PARTNERS JOIN FORCES TO BOLSTER ENTERPRISE MOBILITY AND BUSINESS CONTINUITY

VMware, a leading innovator in enterprise software, has mobilised its partner ecosystem across Asia Pacific and Japan to help customers connect, accelerate, scale and protect their organisational assets as they work through business and societal disruption. With unprecedented number of people now working remotely, VMware has teamed up with its partners to accelerate enterprise mobility to enable business continuity and resilience in the region. By working closely with its partners, VMware has amplified its ability to help enterprises across the region implement their business continuity plans quickly, with minimal operational disruptions.

The approach involves:

- Connecting and engaging workforces via Digital Workspace solutions with seamless access to critical applications via organisational or personal devices
- Accelerating the performance of enterprise applications as remote connections increase
- Scaling elastic capacity quickly as new remote users come online and service demand rises
- Protecting all endpoints as workers more securely access organisational assets remotely

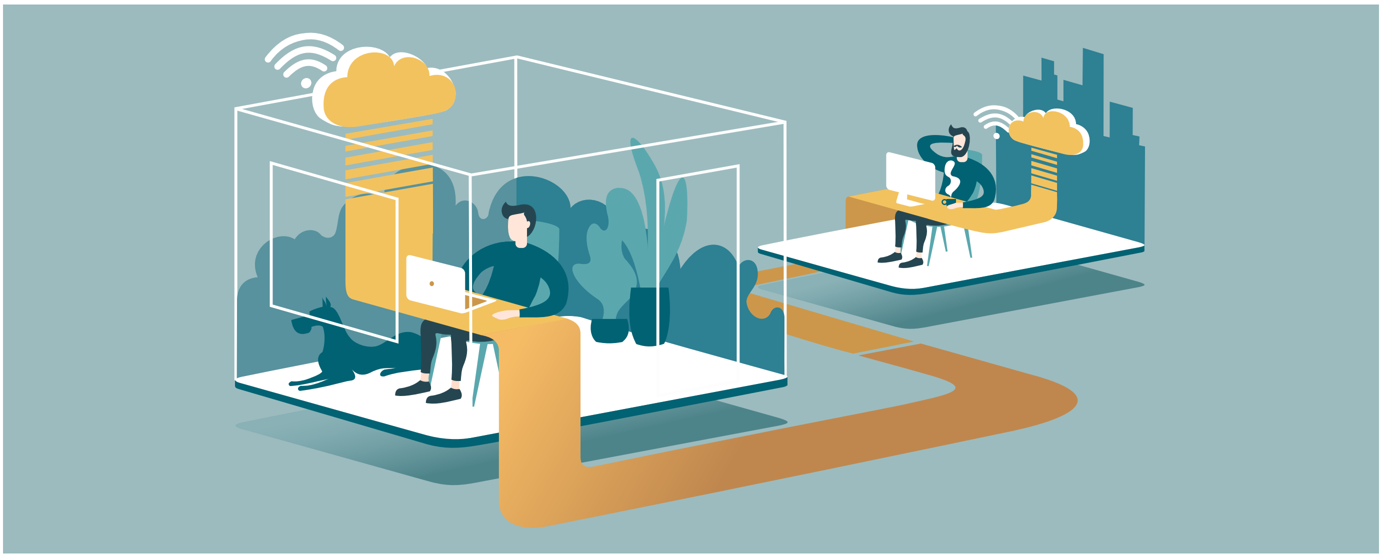
"As our customers navigate challenges never faced before, it is no exaggeration to say the future of work has forever changed. In this new normal, customers need employees to be able to work seamlessly in a secure environment, anywhere, anytime," said Uma Thana Balasingam, vice president, partner business, VMware Asia-Pacific and Japan. "Our partners continue to act as trusted advisors, helping customers adapt and thrive. They have been relied on to set up remote working capabilities, architect cloud and app infrastructure, and deploy intrinsic security solutions for many in a matter of weeks, and sometimes sooner. We are extremely grateful for all their efforts over the past few months."

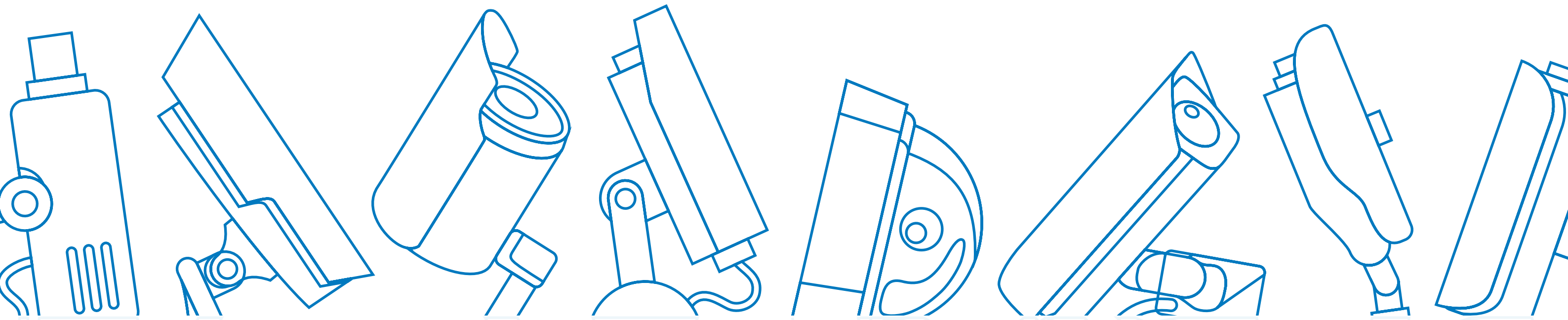
VMware's push towards strengthening Asia's enterprise mobility ecosystem follows the company's recent enhancements to its technology portfolio to enable businesses to Connect, Accelerate, Scale and Protect businesses as they cope with the new normal:

▪ VMware Workspace ONE to provide all employees with a more secure digital workspace on across any device, including personal mobile devices, desktops, and laptops. Harnessing the power of our Disaster-Recovery-as-a-Service (DRaaS) cloud computing solutions to enable maximum accessibility. The platform will also enable Users without a Windows device to remote access their Window's desktop at work using VMware Horizon. In addition, VMware Assist allows remote live troubleshooting of devices.

▪ VMware SD-WAN by VeloCloud enables organisations to rapidly deploy high performance branch access to cloud services or private data centres, giving them the ability to scale their networks swiftly to provide the workforce with optimised access to critical resources anytime, anywhere.

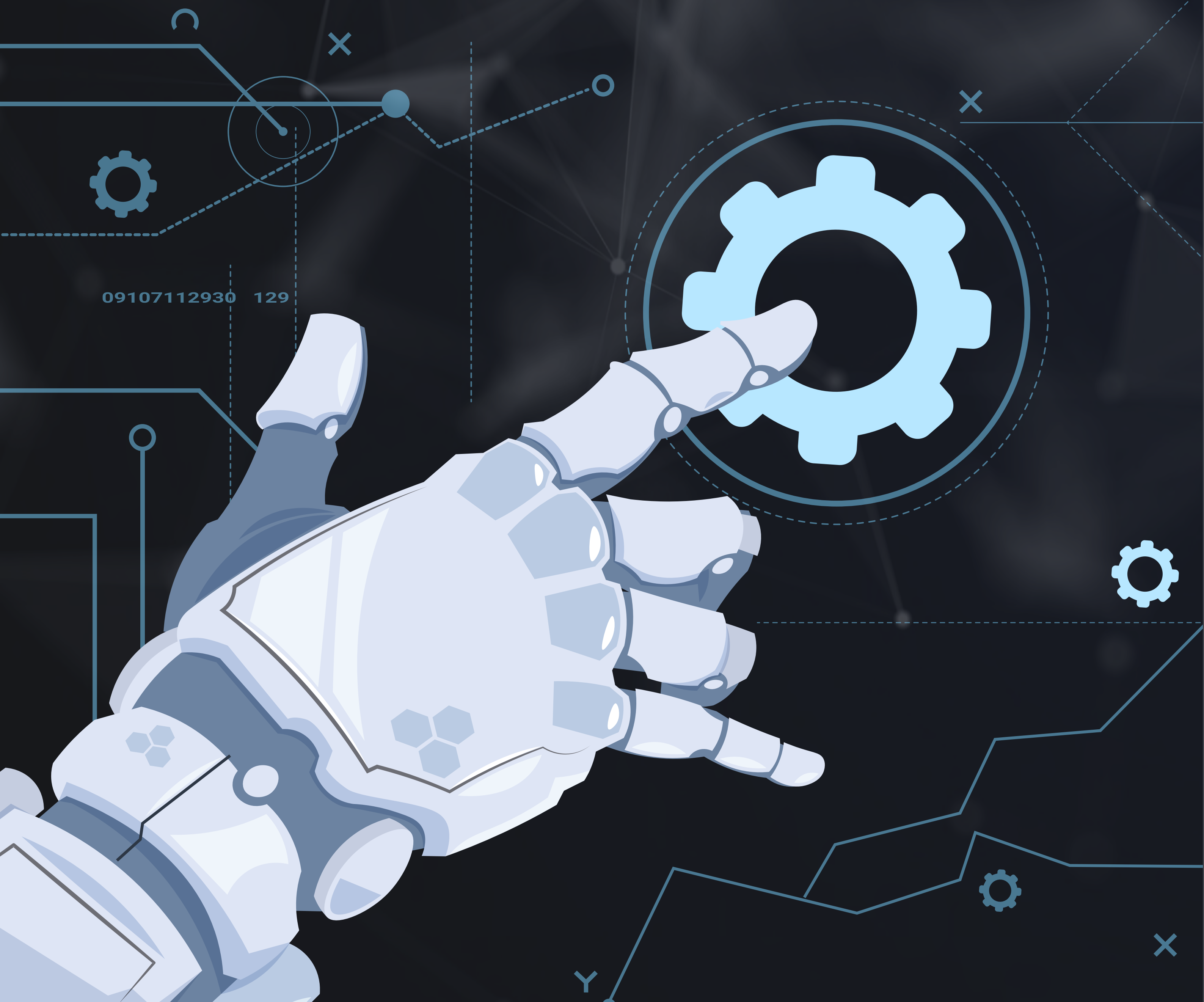
▪ VMware Carbon Black Cloud to enable machine learning and behavioural analytics to empower security teams to harden, prevent, detect, and respond to any threat, vulnerability or risky system configuration in real-time. Thereby better securing endpoints and workloads for businesses to provide a safe and more secure digital workspace for their remote workforce. ■



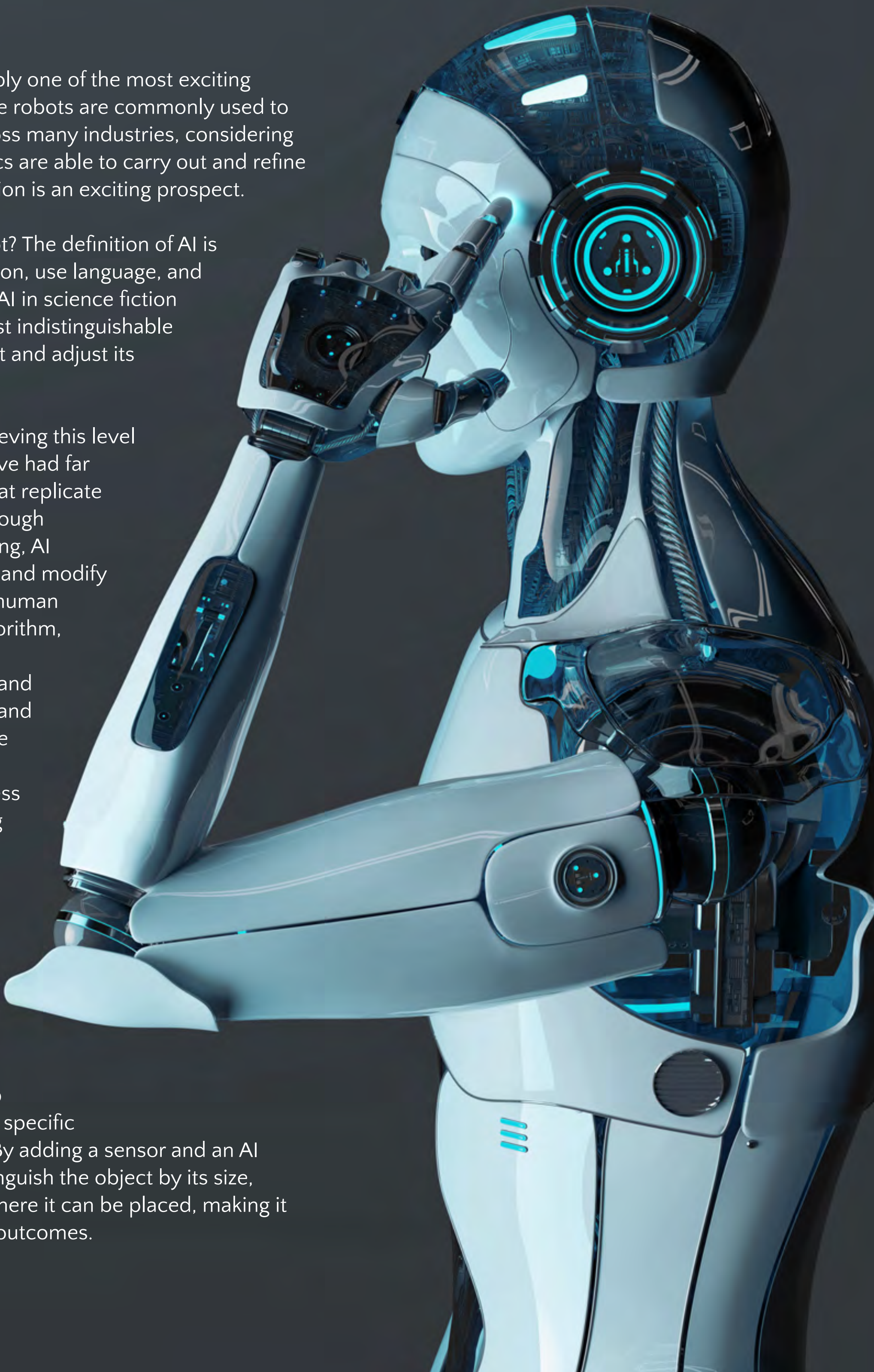


AUTOMATION AND ARTIFICIAL INTELLIGENCE

By CJ Chia



We can observe automation at work across many industries today; so what lies beyond? Robots powered by artificial intelligence that are capable of learning and refining processes without human intervention looks to be next down the line, but with it comes a gamut of security considerations.



Artificial Intelligence (AI) is probably one of the most exciting field in robotics. At a point where robots are commonly used to automate simple processes across many industries, considering a future where intelligent robotics are able to carry out and refine processes without constant human operation is an exciting prospect.

But just how plausible is an intelligent robot? The definition of AI is a machine that has the ability to learn, reason, use language, and formulate original ideas. Portrayals of true AI in science fiction conjures up visuals of a robot who is almost indistinguishable from a human, fully able to react to context and adjust its behaviour and response accordingly.

As things stand, we are nowhere near achieving this level of artificial intelligence, but AI scientists have had far more progress with limited AI machines that replicate specific elements of intellectual ability. Through machine learning and reinforcement learning, AI machines are able to learn from past data, and modify their actions based on input with minimal human intervention. Consider Google's search algorithm, and Facebook's recommendation engine, which to some extent tailor search results and advertisements to the user's search terms and personal preferences. Chess computers are also formidable opponents to most chess players, by storing information on past chess matches and various moves, and analysing the best move to make in the game it is currently playing based on the situation.

With AI powered robots, the AI would be the brain, while the robot is a physical body with sensors that enables the machine to interact with the real world in a tangible manner. An example of a simple robot would be one that can be programmed to pick up an object and place it in another location a specific number of times, or until it is told to stop. By adding a sensor and an AI algorithm, the robot becomes able to distinguish the object by its size, colour, shape, or weight, and determine where it can be placed, making it suitable for tasks with more variables and outcomes.

Such robots with limited AI are already able to be put in practice in research labs and even in our own homes. For example, the Roomba 980 is a model of robotic vacuum that is able to use artificial intelligence to scan the size of the room, identify obstacles, and remember the most efficient routes for cleaning. Kismet, a robot at M.I.T's Artificial Intelligence Lab, is able to recognise human body language and voice inflection, and responds differently according to these factors.

The State Of Intelligence

Before delving into the state of artificial intelligence robotics currently, as well as future prospects and concerns, it's important to lay the groundwork for good understanding of the state of artificial intelligence technology. Despite the media sometimes presenting AI as a troubling and unknown entity, the field of AI is an exciting one to follow. There is much room for these machines to mature, and many projects have ended in failure due to the complexities of machine learning, but all of these failures are necessary to pave the way for future success.

Take for example Microsoft's bot, Tay, unveiled in 2016. The bot was described as an experiment in conversational understanding. The focus of the AI was its natural language processing—its ability to process and engage with people in casual conversation, and to some extent, see how the AI would recognise context and emotions based on the language used. In less than a day, the bot had turned from an innocent experiment into a racist monster.

The reality of how this happened is significantly less terrifying than an AI run amok, beyond human control. In fact, the reason the AI failed was an entirely human one. Launched on twitter, the bot was built to respond to users who tweeted at it using public data that had been cleaned and filtered. But it also made use of machine learning to take in new inputs live, and use them to bolster its

As things stand, we are nowhere near achieving this level of artificial intelligence, but AI scientists have had far more progress with limited AI machines that replicate specific elements of intellectual ability. Through machine learning and reinforcement learning, AI machines are able to learn from past data, and modify their actions based on input with minimal human intervention.

responses. While many users were taking part in harmless fun, some went on to feed Tay with problematic statements, which the bot's programming failed to filter out. The result, Tay's responses randomly reflected these problematic tendencies.

While not all AI are built for conversation, the problem that Microsoft ran into with Tay is one that's applicable to AI technology in different contexts. How does one enable a machine to learn without human supervision, while avoiding the problems that might arise from bad inputs? In order to keep a bot secure, the programming it starts with should be robust enough to filter out negative behaviour and responses which would impact its performance.

Of course, an AI that can do this learning independently—operating with what is akin to the human conscience to make good decisions—would be the ultimate goal. Until then, it is entirely up to the programmers of an AI to minimise the risk of the AI picking up unwanted behaviours.

Another interesting example of AI and how it is misrepresented or misunderstood, is an AI system that was being developed by Facebook, and was shut down after it developed its own language back in 2017. Portrayed by many news sources as a close shave, the initial reporting seemed to imply that scientists at Facebook shut down the AI because they were unable to understand what the robots, nicknamed Alice and Bob, were communicating with each other. The truth was far less scandalous.

The system was an attempt to stimulate dialog and negotiation, and the robot was given a set of items, with preferences for items it wanted more than others. It was then supposed to negotiate with another robot and decide how to split these items.

Both robots had been fed with training data in English, but extracted data was essentially a series of words and phrases, with the robot putting them together based on how likely this phrase was going to help the robot achieve its desired outcome. When the two robots ended up talking to each other, the only measure of their success became how well they distributed the items, and the robots started to learn their own form of communication. At this point, the conversation was shut down, because it had stopped providing useful results.

While the experiment came to a close, it was far from a waste of time. Facebook engineers noted that the

project was an important step towards creating chatbots that could reason, converse, and negotiate, key steps in building a personalised digital assistant. While these examples are of AI that were not placed in a robotic body, the developments and findings of digital AI is important for similar breakthroughs in AI that are employed in a more physical context.

Intelligent Security Robots

Today, there is an increasing demand for security robots, with the market for these machines reaching $2.11 billion within the US alone in 2018. These robots use various connected technologies and artificial intelligence to patrol a specified area, allowing human security officers to perform more critical tasks in some cases.

While the specification and exact function of a security robot differs according to its maker, they generally use AI and image recognition software to explore the space that needs to be patrolled, with additional sensors like proximity and collision sensors helping them avoid obstacles. During its patrol, an AI security robot can make use of its AI and machine learning algorithms to label what its cameras detect—combine this with databases and image recognition software, and you have a robot that is able to distinguish between a human, an animal, and a vehicle, and possibly even recognise specific faces.

The AI in these security robots can also help security officers decide more easily how to react to various alerts. For example, if a loud sound is detected, the AI might decide that it can get a closer look by zooming in, or to activate a siren or an alarm. For now, these decisions still fall under the jurisdiction of human operators, but it is not difficult to envision a future where AI robots are intelligent enough to make these decisions with a high degree of accuracy.

While the technology seems promising, there are a few factors that do make it difficult for mass implementation. For one, this technology is often too expensive for the average consumer and small businesses to afford, or too niche that it is unable to fulfil the need for versatility that smaller operations often require. Other limitations that currently exist the difficulty in employing these robots for outdoor surveillance, the possibility that humans damage these expensive machines by accident or as an act of violence, and the fact that each design is often only suitable for a specific use. While it might take time and research to overcome these limitations, it is almost certain that these will be resolved, giving way to newer, more capable AI robots. Of course, this brings with it new concerns, like the ethics of using AI to monitor a population, but as with all challenges relating to personal and community security in relation to smarter technology, we will require a combination of legislative guidance and organisational cooperation to find solutions that are acceptable to society and each government. ■

The AI in these security robots can also help security officers decide more easily how to react to various alerts. For example, if a loud sound is detected, the AI might decide that it can get a closer look by zooming in, or to activate a siren or an alarm.

5 Misconceptions And Facts About IoT In Manufacturing

IoT is a new face of the digital transformation, although some organisations are not aware of its full capability and still have some confusion about how it can leverage IoT in many ways, including in manufacturing.

By Intech Systems Pvt Ltd, Republished From IoT for all

Digital transformation is happening in every part of business, especially manufacturing. Factories are no longer aloof from the other business processes and workers are no longer complaining about the siloed data. Information about each step of manufacturing is available to use and share securely from anywhere and any device.

In this manufacturing transformation, IoT (Internet of Things) plays a significant role. According to a study, of all the business who chose to implement IoT, 94 percent have already seen a return on their IoT investments.

However, there are many misconceptions regarding IoT that makes manufacturers apprehensive about implementing IoT in their manufacturing operations. Here are the top 5 misconceptions about IoT and the facts.

Misconception: IoT Is Not for Small And Medium Sized Enterprises (SMEs)

Fact: IoT is suitable for organisations of any size.

Many organisations think that IoT is only for large enterprises that can afford the time and efforts needed to implement it. In reality, organisations of any size can implement IoT as recent developments in IoT have made it easy to implement and cost-effective. Open-source software like Azure IoT makes it easier for SMEs to leverage IoT in their manufacturing without building comprehensive IoT infrastructure or dedicated IT and engineering teams. Thus, the potential benefits manufacturers can get by leveraging IoT outweighs any concerns about cost or time.

Misconception: IoT Is Not Secure

Fact: IoT exposes security issues, but an active security strategy mitigates risk.

One of the major concerns for manufacturers about IoT is that it is not secure. The fact that the connected devices communicate over the cloud poses security challenges to manufacturers. However, as standardisation and security awareness improves, IoT will probably become as secure as other IT infrastructure. Although there will always be some potential risk when connecting devices to the internet, an active security strategy helps reduce threats and increase the long-term value of your IoT infrastructure.

Misconception: IoT Is Unnecessary

Fact: IoT helps gain business insights that increase business productivity and ensure operational efficiency.

Though the benefits of IoT in manufacturing outweigh the myths associated with it, manufacturers still think IoT is not necessary. Many of them think that they won't be ever able to use the amount of information produced by IoT systems. According to McKinsey, around 60 percent of the IoT industry's projected $11.1 trillion value in 2025 will depend on data integration and analysis. So it is possible that as your business grows, any unutilised data may suddenly become valuable. Also, IoT doesn't only generate information but also enables you to gain insights across the supply chain, create new revenue sources, and optimise the equipment life cycle.

Misconception: IoT Is Only About Connecting Devices With Sensors

Fact: IoT is all about gaining in-depth business insights to make better decisions

IoT does include connecting the devices and machines with sensors but there is much more to IoT than that. Other than physical devices, IoT also involves networks, cloud, gateways, APIs, etc. Thus, connecting is just the foundation of IoT. But the main motive of IoT is to generate real-time data insights to enable actions and thus, decision making. When the devices are connected to produce business insights, manufacturers can predict outcomes, prevent operation failures and better augment the system uptime.

IoT does include connecting the devices and machines with sensors but there is much more to IoT than that. Other than physical devices, IoT also involves networks, cloud, gateways, APIs, etc. Thus, connecting is just the foundation of IoT.

Misconception: IoT Is Expensive

Fact: IoT implementation costs are decreasing and it also helps in building new revenue streams in the long run.

That IoT is costly is one of the biggest myths too. Obviously, investing in IoT requires finance but what organisations look at is only the cost part and not the benefits they get from IoT. Once IoT is implemented, the actionable insights that are generated reduce costs of production, thereby increasing efficiency and productivity. The result is fewer expenses and more growth, which boosts profits.

Understanding the Importance of IoT in Manufacturing

With the increase in the competition, it is important to reduce the shop floor costs while also serving the customers right. The current trend is of automation and business intelligence which uses real-time data insights and monitors the data continuously to prevent any loopholes in production.

All in all, the potential of the factory connected with IoT increases multi-fold. So, ensure that your organisation is not lagging behind in the digital transformation journey because of some misconceptions. ■

10 AI Use Cases In Manufacturing

Manufacturing companies are turning to AI to streamline the way they do business and increase efficiency. Here are 10 common use cases.

By Lindsay Moore, TechTarget

A factory filled with robot workers once seemed like a scene from a science-fiction movie, but today, it's just one real-life scenario that reflects manufacturers' use of artificial intelligence. Manufacturers can benefit from AI in a number of ways. Here are 10 examples of AI use cases in manufacturing that business leaders should explore.

1. Cobots Work With Humans

Collaborative robots - also called cobots - frequently work alongside human workers, functioning as an extra set of hands.

While autonomous robots are programmed to repeatedly perform one specific task, cobots are capable of learning various tasks. They also can detect and avoid obstacles, and this agility and spatial awareness allows them to work alongside - and with - human workers.

Manufacturers typically put cobots to work on tasks that require heavy lifting or on factory assembly lines. For example, cobots working in automotive factories can lift heavy car parts and hold them in place while human workers secure them. Cobots are also able to locate and retrieve items in large warehouses.

2. RPA Tackles Tedious Tasks

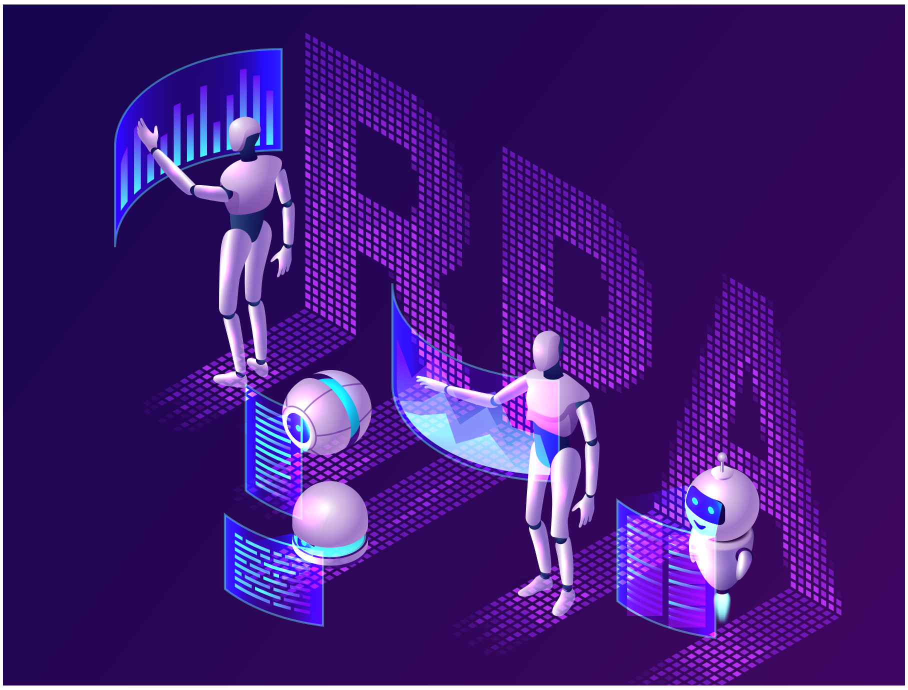
While manufacturing companies use cobots on the front lines of production, robotic process automation (RPA) software is more useful in the back office. RPA software is capable of handling high-volume, repetitious tasks, transferring data across systems, queries, calculations and record maintenance.

RPA software automates functions such as order processing, so that people don't need to enter data manually, and in turn don't need to spend time searching for inputting mistakes. In this way, RPA has the potential to save on time and labour.

3. Digital Twins Help Boost Performance

Companies can use digital twins to better understand the inner workings of complicated machinery.

A digital twin is a virtual model of a physical object that receives information about its physical counterpart through the latter's smart sensors. Using AI and other technologies, the digital twin helps deliver insight about the object.



Companies can monitor an object throughout its lifecycle, and get critical alerts, such as a need for inspection and maintenance.

As an example, sensors attached to an airplane engine will transmit data to that engine's digital twin every time the plane takes off or lands, providing the airline and manufacturer with critical information about the engine's performance. An airline can use this information to conduct simulations and anticipate issues.

4. Predictive Maintenance Improves Safety, Lowers Costs

Manufacturing plants, railroads and other heavy equipment users are increasingly turning to AI-based predictive maintenance (PdM) to anticipate servicing needs.

If equipment isn't maintained in a timely manner, companies risk losing valuable time and money. On the one hand, they waste money and resources if they perform machine maintenance too early. On the other, waiting too long can cause the machine extensive wear and tear. The latter can also expose workers to safety hazards.

PdM systems can also help companies predict what replacement parts will be needed and when.

5. Lights-Out Factories Save Money

An AI in manufacturing use case that's still rare, but which has some potential, is the "lights-out factory." Using AI, robots and other next-generation technologies, a lights-out factory is designed to use an entirely robotic workforce and run with minimal human interaction.

Manufacturers can potentially save money with lights-out factories because robotic workers don't have the same needs as their human counterparts. For example, a factory full of robotic workers doesn't require lighting and other environmental controls, such as air conditioning and heating. Manufacturers can economise by adjusting these services.

Robotic workers can operate 24/7 without succumbing to fatigue or illness and have the potential to produce more products than their human counterparts, with potentially fewer mistakes.

6. Machine Learning Algorithms Predict Demand

AI systems that use machine learning algorithms can detect buying patterns in human behaviour and give insight to manufacturers.

For example, certain machine learning algorithms detect buying patterns that trigger manufacturers to ramp up production on a given item. This ability to predict buying behaviour helps ensure that manufacturers are producing high-demand inventory before the stores need it.

7. Inventory Management Prevents Bottlenecks

Some manufacturing companies are relying on AI systems to better manage their inventory needs.

AI systems can keep track of supplies and send alerts when they need to be replenished. Manufacturers can even program AI to identify industry supply chain bottlenecks.

For example, a pharmaceutical company may use an ingredient that has a short shelf-life. AI systems can predict whether that ingredient will arrive on time or, if it's running late, how the delay will affect production.

8. AI Boosts Supply Chain Management

One strong AI in manufacturing use case is supply chain management. Large manufacturers typically have supply chains with millions of orders, purchases, materials or ingredients to process. Handling these processes manually is a significant drain on people's time and resources and more companies have begun augmenting their supply chain processes with AI.

For example, a car manufacturer may receive nuts and bolts from two separate suppliers. If one supplier accidentally delivers a faulty batch of nuts and bolts, the car manufacturer will need to know which vehicles were made with those specific nuts and bolts. An AI system can help track which vehicles were made with the defective nuts and bolts, making it easier for manufacturers to recall them from the dealerships.

9. AI Systems Detect Errors

Manufacturers can use automated visual inspection tools to search for defects on production lines. Visual inspection equipment—such as machine vision cameras—is able to detect faults more quickly and accurately than the human eye.

For example, visual inspection cameras can easily find a flaw in a small, complex item – for example, a cellphone. The attached AI system can alert human workers of the flaw before the item winds up in the hands of an unhappy consumer.

10. AI Systems Help Speed Product Development

Some manufacturers are turning to AI systems to assist in faster product development, as is the case with drug makers.

AI can analyse data from experimentation or manufacturing processes. Manufacturers can use insights gained from the data analysis to reduce the time it takes to create pharmaceuticals, lower costs and streamline replication methods. ■

Actian Avalanche Real-Time Connected Data Warehouse Adds Integration

Actian is expanding its Cloud Data Warehouse with data integration capabilities to enable users to onboard and search data from both cloud and on-premises data sources.

By Sean Michael Kerner, TechTarget

With growing volumes of real-time data coming from different sources, it can often be a challenge to integrate all that data into a data warehouse.

Hybrid data management vendor Actian, based in Palo Alto, Calif., is looking to help solve the real-time data integration challenge with its new Avalanche Real-Time Connected Data Warehouse Solution, launched April 22. The offering brings together Actian's Avalanche Cloud Data Warehouse with the company's data integration capabilities to create the new platform.

Among key features are the ability to integrate with real-time data pipelines as well as a federated hybrid query capability to search for data across different sources, both on premises and across multiple cloud deployments. Like many vendors, Actian recognises the need to provide cloud-based systems, said David Menninger, an analyst at Ventana Research. However, the vendor has also recognised that many organisations will have a mix of on-premises and cloud data processing requirements. Menninger noted that his firm's research shows the need for hybrid support as a critical requirement since less than a quarter of organisations are purely cloud-based.

"Every organisation needs to integrate a variety of data sources into its data warehouse and increasingly organisations are processing more and more data in real time," Menninger said.

From Ingres To Cloud Data Warehouse

Actian has a long history in the database market and was known as Ingres until 2011, when the company rebranded. The Ingres database first emerged in 1980 and was a pioneer in the relational database market. Ingres is still used by organisations today and the evolution of the core structured database technology underpins Actian's current efforts.

Actian launched the Avalanche Cloud Data Warehouse in March 2019, bringing analytics and data warehouse capabilities to the cloud. Emma McGrattan, senior vice president of engineering at Actian, noted that typically the first thing users do after creating a data warehouse is to populate it with data. Actian has an existing data integration technology known as DataConnect, which was extended to work in the cloud and rebranded as Avalanche Connect in 2019.

Before the new Avalanche Real-Time Connected Data Warehouse release, the Avalanche Connect technology wasn't seamlessly integrated, McGrattan said. She noted that the data warehouse and integration technologies were coming from different development teams at Actian and users would have had to engage with two different support teams for deployment.

"What we've done now is unified the team and the technologies, so the data integration is just kind of a natural extension of the warehouse," McGrattan said. "So when you first create your warehouse, if you want to import some data, you've got the ability then to customise templates and pull in the data."

In the cloud, organisations also need to connect to data from SaaS-based applications such as Salesforce, NetSuite and ServiceNow. Connecting SaaS data to the Avalanche Real-Time Connected Data Warehouse is enabled with customisable templates that Actian provides to make the integration process easier for users.

Connecting Data In The Cloud

McGrattan said the new integrated Avalanche Real-Time Connected Data Warehouse can now pull in data from a variety of different sources ranging from basic CSV-based data sets, to streaming data technologies including Apache Kafka, as well as information hosted in data lakes. The system can also be used to connect to on-premises sources of data that run within an organisation's own data centre.

In the cloud, organisations also need to connect to data from SaaS-based applications such as Salesforce, NetSuite and ServiceNow. Connecting SaaS data to the Avalanche Real-Time Connected Data Warehouse is enabled with customisable templates that Actian provides to make the integration process easier for users.

While Actian is now providing a built-in integration capability as part of its cloud data warehouse, McGrattan said there could also be use cases in which an organisation wants to use a purpose-built ETL (extract, transform and load) tool. To that end, she noted that Actian has existing partnerships with multiple ETL vendors including Talend, Dell Boomi, SnapLogic and Matillion among others.

"We're providing the ability for customers to retain the investment that they've made in ETL and have that just work with the Avalanche platform as well," she said.

Federated query reaches across cloud data warehouse resources

Another key feature that the Avalanche Cloud Data Warehouse enables is federated query, which enables users to search across both on-premises as well as cloud data.

McGrattan said Actian is looking at building more intelligence into the cloud data warehouse platform, including machine learning and artificial intelligence workload support.

"On the integration side of things we'll continue to build out more templates and really simplify the task of bringing in large data volumes from a variety of sources," McGrattan said. ■

Armar-6 Shows How Helper Robots Can Work In Ocado Warehouses

Collaborative robot is the result of the five-year SecondHands project with academia to develop a robot that can support human workers.

By Cliff Saran, ComputerWeekly.com

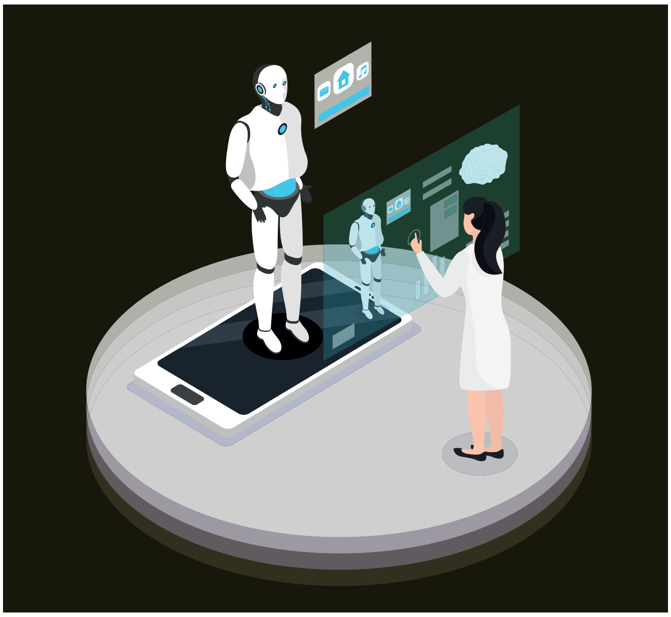
The European Union's SecondHands Horizon 2020 robotics project has been completed, resulting in Armar-6, a humanoid robot that can help workers with maintenance tasks. It was developed by Ocado Technology and its academic partners across Europe in a five-year project.

Launched in 2015, the mission was to develop a collaborative robot, or "cobot" assistant, to improve the safety of people working in industrial environments by proactively offering assistance to humans in maintenance tasks. Along with Ocado Technology, the consortium developing the robot included the Ecole Polytechnique Fédérale de Lausanne (EPFL), Karlsruhe Institute of Technology (KIT), Sapienza University of Rome, and University College London (UCL).

The original project goals included the ability for the robot to hold, lift, reach or pass objects. According to Ocado Technology, the overall goal was to develop a robot that could take on responsibility for tasks such as heavy lifting and support roles, enabling people to concentrate on the "skilled" part of a job.

The underlying robot platform, the Armar-6, was developed at the KIT specifically for the project

The robot can respond to natural language commands, as well as inferring when a person needs help and proactively offering it, as well as lift, hold and pass objects of a wide range of shapes and sizes using dexterous manipulation. The project team behind Armar-6 said it can also learn how to assist with a variety of maintenance tasks in a range of environments.



requirements with respect to human-robot interaction. The robot is the sixth generation and youngest member of the Armar family of humanoid robots.

Tamim Asfour, a professor at KIT, said: "Robots with sophisticated manipulation, interaction, and learning abilities, such as Armar-6, will provide a second pair of hands to people in need of help at home and at work. The achievements in the project are important steps towards building humanoid robots with embodied intelligence."

The robot can respond to natural language commands, as well as inferring when a person needs help and proactively offering it, as well as lift, hold and pass objects of a wide range of shapes and sizes using dexterous manipulation. The project team behind Armar-6 said it can also learn how to assist with a variety of maintenance tasks in a range of environments.

Aude Billard, a professor at EPFL, said: "The breakthroughs demonstrated in 'hand-over' scenario, 'guard removal and insertion', 'guard co-manipulation' and 'obstacle avoidance' will play a crucial role in having reliable robots that can be used in everyday scenarios."

Ocado Technology believes collaborative robots such as Armar-6 will be key for solving many societal challenges – both as assistive robots in industry, and out in the wider world. Graham Deacon, robotics research fellow at Ocado Technology, said: "Humanoid robots are key for improving flexibility and safety in industrial contexts in a way that is genuinely useful.

"The same technologies that enable the Armar-6 to communicate and interact with humans, like natural language comprehension, soft manipulation and 3D spatial awareness, also mean the robot could be developed further to help in other situations, such as in helping to reduce contamination, or in assisted living."

The robot has been tested working alongside Ocado Technology employees in one of Ocado's highly automated warehouses. Lourdes Agapito, a professor at UCL, said: "It was really valuable to be able to test in the Ocado warehouse as a real-world environment. The dynamic, constantly changing conditions tested our vision, robotics, and language processing algorithms to go beyond the current state of the art."

Fiora Pirri, a professor at Sapienza University, added: "These artificial intelligence innovations have been made possible thanks to the close collaboration of all the partners. The challenging real-world environment of the Ocado customer fulfilment centre allowed us to develop a reasoning system and perception algorithms to provide support in industrial maintenance tasks." ■

Asset Tracking in Factories: Where Innovation and Asset Management Meet

Asset tracking will improve efficiency, output, and safety in addition to greatly improving processes around asset management.

By Leverege, Republished from IoT for all

The ways that factories can benefit from IoT are numerous. One of the biggest facets of IoT that will benefit factories is asset tracking. From tracking tools and parts to tracking people, there is a myriad of ways for factories to take advantage of asset tracking. Asset tracking will improve efficiency, output, and safety in addition to greatly improving processes around asset and inventory management.

Tool Tracking

The first set of use cases for asset tracking in factories centres around tracking tools. On the surface, it is easy to tell how tracking tools and enabling employees to know where they are will cut down on idle time spent searching. The real benefit is knowing how often tools are being used and where. From this, managers will be able to predict when tools will fail and need to be replaced, or when maintenance will need to be performed, eliminating downtime. In addition to this, the optimal placement for tools, and the exact number of devices that are needed can be determined.

Parts Tracking

The next set of use cases for asset tracking is tracking parts. For parts with a shelf life, ensuring that they are routinely rotated and used can directly cut down on waste. In

> **Every type of factory could benefit from becoming smart and implementing an asset tracking solution. Factories are hungry for innovation and asset management needs more for tracking inventory than their current systems.**

addition to this, tracking parts from receiving can eliminate "Ghost Assets". Ghost assets are parts that are received and forgotten about in the factory. As always, the insights provided by data are extremely valuable. By tracking parts and knowing how fast they are being used, purchasing becomes extremely accurate preventing both excess and shortages.

Tracking parts comes with many financial insights as well. Though tracking what parts come in and how fast they get processed and shipped out, accurate income projections can be produced. In addition to this, if done well, tracking parts can be extremely effective for both auditing and fraud detection. With a lot of physical parts moving, they can be in various locations or even moving through the assembly line. Both of these can be very time consuming and manual processes. The ability to automate these tasks through an asset tracking solution would be an advantage for any medium to large scale factory.

Employee Tracking

The third set of use cases comes from tracking employees. These use cases do not provide as much direct ROI as the use cases from tracking parts or tools, but they can still be critical.

Directly tracking employees in dangerous factories, enabling fast emergency support, and ensuring that people are only in areas that they have access to are only a few of the use cases. There is a small amount of insight to be gained from this, such as tracking employees' movement to see if some parts are stored too far off of the assembly line. Additionally, if employees are in potentially dangerous situations, tracking their movements can prevent workplace injury or harm.

Although tracking employees can be very beneficial, it also has the potential to be abused. Being able to audit every position an employee has been in throughout the day, every day could potentially turn employees into robots or cogs. There are many stories about factory workers in authoritarian settings where they are limited in when they can use the bathroom. It's important to keep in mind both the benefits and drawbacks of certain types of asset tracking, especially if you're dealing with tracking humans.

Every type of factory could benefit from becoming smart and implementing an asset tracking solution. Factories are hungry for innovation and asset management needs more for tracking inventory than their current systems. ■

How IoT Will Revolutionise Pharmaceutical Manufacturing

Pharma is big business, but what it's not generally recognised is, in large part, a manufacturing business with complex supply chains, finicky chemical processes and products that have to meet stringent quality controls.

By Alex Jablokow, IoT for all

Few of those outside the industry think about how drugs are made safely, efficiently and at scale with reliable quality and in precisely measured doses.

Even more interesting is the simple fact that pharma often produces sophisticated drugs using manufacturing processes that are decades out of date, and which are being phased out in comparable industries, such as chemical manufacturing.

Batch Processes And The Difficulties Of Transition

Drugs are typically produced with a batch process, with involves mixing compounds in large vats, followed by long delays to measure the quality of each intermediate product, and then moving to another step, sometimes in another facility. Machinery is not used continuously. Information about conditions, status, and quality is often distributed in a wide variety of separate systems. Some critical data is still gathered and stored in paper-based logs.

Manufacturing would be more efficient if it were continuous and used in everything from automobiles to the chemical industry, where compounds move through the plant without stopping, being tested, and measured along the way—which plays to the strengths of IoT. Continuous manufacturing can also respond more flexibly to demand. If more is needed, you can just run the process for longer to incrementally increase product, while increasing amounts with batch require starting an entirely new batch, with all the delays and possibilities of oversupply that implies.

Manufacturing would be more efficient if it were continuous and used in everything from automobiles to the chemical industry, where compounds move through the plant without stopping, being tested and measured along the way—which plays to the strengths of IoT.

Unfortunately, the route to modernised manufacturing processes in pharma is not a straightforward one.

A Regulation-Driven Industry

Given the possible consequences of errors in drug manufacturing, pharmaceuticals are heavily regulated. These regulations have helped delayed manufacturing processes—and will now be driving change.

When the Food and Drug Administration (FDA) approves a drug, it's not just the active compound that is part of the approval. The details of the manufacturing process itself-down to plant layout-are included. Any change in the process requires explicit regulatory approval with attendant paperwork. In other industries, continuous process improvements, with faster access to inventory here and a step eliminated there, are part of a company's competitive advantage. Pharma manufacturing transformation requires significantly more planning.

The FDA has recognised the inherent regulatory difficulties and formed the Emerging Technology Team (ETT) with the goal of encouraging the adoption of new manufacturing methods, particularly continuous manufacturing. The intention is that they will meet with pharma companies early in development, before any regulatory submission. Any proposed manufacturing process will be extensively vetted prior to submission for approval.

While the FDA has a huge influence on global drug approvals, it's far from the only such agency. There are more than 100 pharmaceutical regulatory authorities across the globe, each of which a global pharma manufacturer must take into account when planning a change in the manufacturing process.

Early Successes

The ETT has already proved its effectiveness. Vertex has been using continuous manufacturing for Orkambi, a cystic fibrosis drug since 2015. Janssen (now part of Johnson & Johnson) switched to continuous manufacturing for its HIV drug, Prezista, in 2016, after a long development period. Both interacted closely with the FDA to ensure approval of the manufacturing process before submitting the drugs for approval. J&J points particularly to combining formerly separate testing and sampling steps, enabled by IoT sensors, as a significant improvement.

Advantages Of Compliance

The advantages of IoT for regulatory compliance can be a big part of its business case since IoT provides the ability to monitor and document all events, variations and concentration at every step of the manufacturing process. The collected data from IoT sensors enables plant operators to know what is going on during the entire process. This also provides sophisticated tracking for recalls if a specific run of a compound turns out to be associated with some problem. IoT also allows for monitoring and documenting the activities of contract manufacturing organisations (CMOs), which carry out much of the actual manufacturing. Pharma supply chains are increasingly complex, with the manufacturing of the active pharmaceutical ingredient (API), overall formulation, and packaging taking place in different places, often by different contracted vendors.

Therefore, the demands of pharma regulators for monitoring, tracking, and reporting can drive IoT adoption as well as slow it down. Regulatory compliance is an often-underappreciated IoT driver.

IoT And The Road Ahead For Pharma Manufacturing

Pharma manufacturing equipment tends to be extremely expensive, as are the constituent ingredients, and the conditions under which they are manufactured have to be kept within extremely narrow tolerances.

Continuous manufacturing will make the consequences of equipment failure anywhere along the line more serious. Batch processing can wait in one place or another for a bit, making it a somewhat more forgiving of single-point equipment failure. Real-time asset management using IoT sensor data and predictive maintenance will be essential.

In addition to the cost of a stopped line, there is the issue of maintaining quality, the most important consideration for the FDA. They always err on the side of caution, so any drug run with possible quality issues is guilty until proven innocent.

So anticipating failures, replacement based on wear, and a minimal amount of unplanned downtime will make it easier to manage manufacturing quality, efficiency, and compliance while remaining flexible for changing market needs. ■

How Connected Devices Are Changing The Manufacturing Industry

Manufacturers are implementing Industrial IoT (IIoT) devices to leverage predictive maintenance, data analytics, and more.

By Transcendent, Republished From IoT for all

The Internet of Things (IoT) is the network of physical objects embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data. Products with wireless connectivity (e.g. lightbulbs, thermostats, or Alexa) are more present in people's homes today than not.

One report suggests that 79 percent of U.S. consumers have at least one connected device at home. But the technology actually has its roots in a world that predates the rise of smart appliances: Industrial manufacturing.

The Industrial Internet of Things (IIoT) "takes networked sensors and intelligent devices and puts those technologies to use directly on the manufacturing floor, collecting data to drive AI and predictive analytics."

Robert Schmid, Deloitte Digital IoT Chief Technologist stated, "In IIoT technology, sensors are attached to physical assets. Those sensors gather data, store it wirelessly, and use analytics and machine learning to take some kind of action."

IIoT is changing the manufacturing industry. It's transforming traditional, linear manufacturing supply chains into dynamic, interconnected systems. IIoT technologies help to change the way products are made and delivered. They make factories more efficient and safer for human operators. In some cases, they save facilities millions of unnecessary dollars.

Predictive Maintenance In The Workplace

One of the many benefits of IIoT is how it can improve operating efficiencies. For example, if a machine goes down, connected sensors can determine where the issue is occurring and trigger a service request to an engineer. IIoT can also work together with an EAM CMMS where engineers can receive these generated requests on their mobile device and immediately go to the location to repair or assign it to another engineer near the asset.

IIoT can also predict when a machine will likely breakdown or when its useful life cycle is about to end—before it ever happens. It's taking a preventive maintenance approach to the next level by saving facility owners thousands of dollars on unwarranted repairs or replacements.

To illustrate the amounts that IIoT can help a facility to save, we can picture a facility paying a worker $16/hour to check 16 meters around the property manually once daily will cost $3,840. If this person were to check the same meters once per hour to try and decipher changes it would cost $92,160. Imagine checking the meters every minute or every second; it becomes humanly impossible to do so without the use of IoT and machine learning.

Machine learning can decipher small changes in meters at scale. Workers can then analyse those changes to start that next level of predictive maintenance.

Beyond saving time and money, IIoT can keep workers safe. If an oil well is about to reach a dangerous pressure condition, for example, operators will be warned well before it explodes based on the nature of the sensors and vibration analysis. Sensors can even be used to manage and monitor workers' locations in case of an emergency or evacuation.

One of the many benefits of IIoT is how it can improve operating efficiencies. For example, if a machine goes down, connected sensors can determine where the issue is occurring and trigger a service request to an engineer. IIoT can also work together with an EAM CMMS where engineers can receive these generated requests on their mobile device and immediately go to the location to repair or assign it to another engineer near the asset.

IIoT Is Changing The Manufacturing Industry

IIoT is already boosting efficiency, productivity, and safety within the workplace. The future looks bright for several industries. Let's take a look at how some companies are taking advantage of IIoT technology.

Infrared thermography allows engineers and mechanics to see electrical systems, mechanical equipment, building applications, and fluid systems through the use of thermovision.

Engineers can spot faulty connections, abnormal motors, pipe temperatures and tank levels through this IIoT equipment, which shows different colours without having to touch the equipment. This reduces the risk of engineers getting hurt on the job.

DAQRI, a company focused on AR technology, developed an AR-enabled smart helmet for industrial use. Engineers can see 4D images above assets in their facilities that prompt them with instructions and also give them a mapping of all asset functionality. This wearable technology allows engineers to discover asset information faster. It also closes the knowledge gap for new hires.

Another company called UpSkill connects the workforce through AR in its wearable technology, guiding technicians in real-time to complete tasks, checklists, work orders, and allowing them to forward media to managers.

This equipment is becoming more prevalent and as more machines become connected to the internet. Approximately 50 billion machines will be connected on the internet by 2020. As the pace of the connectivity revolution increases, it's becoming imperative for facilities and industries to adopt these devices and make them apart of their facility operations.

A CMMS has the capability to provide maintenance management and staff with an automated tool capable of scheduling inspections, preventive maintenance, managing inventory, work orders, and retrieval of recorded asset history.

Technicians can perform actual work with instructions on handhelds, enter how long it takes to complete work orders, filter through past work orders, and close out of the system.

The possibilities are almost endless when it comes to how IoT, AR, VR, and machine learning can help facilities with energy savings, labour savings, employee safety, and more. IIoT is changing the manufacturing industry. The future is a scary and exciting thing but ultimately inevitable for change.

All the information is recorded in real-time, so managers can access the information instantaneously.

The ability to track your work, document it, and send it to managers could be paired with wearable technology, like the companies above, to provide engineers with an elevated view of assets through thermal technology or the ability to see instructions on assets and use that data to train new hires and not have to worry about on-boarding.

A CMMS could also benefit from machine learning, using algorithms to monitor assets like meter readings and the ability to calculate readings by the second which would be humanly impossible to do. This will cut down on extraneous labour costs and allow facilities to allocate dollars elsewhere.

The possibilities are almost endless when it comes to how IoT, AR, VR, and machine learning can help facilities with energy savings, labour savings, employee safety, and more. IIoT is changing the manufacturing industry. The future is a scary and exciting thing but ultimately inevitable for change. ■

AI And Specialty Analytics Are Changing Video Surveillance

As more data is analysed, video storage requirements expand for your customers.

By Jason Bonoan, Global Product Marketing Manager for Seagate Technology, and Alan Ataev, Chief Sales and Marketing Officer at AxxonSoft

Detecting high-risk scenarios before they escalate is one of the core motivations behind the development of artificial intelligence (AI) for security applications. With AI in the quiver, operators deploying surveillance solutions can move beyond mere monitoring to leverage every video frame and piece of data available to identify threats and inform emergency response. AI is still an emerging technology; however, the benefits that its capabilities deliver are designed to minimise risks, maximise crime prevention, and save lives.

In the past, video footage was archived for a short time before being overwritten. Today, segments of AI—such as video analytics, machine learning, and deep learning—make use of the high volumes of data generated by IoT ecosystems to distinguish meaningful patterns in data sets, which are then translated into insights that are bolstering crime deterrence strategies around the world. This technology takes a more holistic view of data, connecting individual data points to describe what is happening, in order to quickly identify high-risk situations before they escalate.

Growing Demand

The overall market for real-time video analytics was estimated at $3.2 billion worldwide in 2018 and is expected to grow to $9 billion by 2023, according to London-based Brandessence Market Research. AI is no longer just a buzzword or a trend – it is becoming an integral component of our ever-growing datasphere.

Contrary to popular belief, AI is not the exclusive property of development powerhouses like Google, Amazon or Apple, who largely use AI to optimise speech and image recognition as well as content curation. Growing physical security concerns have also been a catalyst for steady growth in AI.

The active shooter threat has positioned schools among the early adopters of AI; in fact, they comprised estimated $450 million portion of the market in 2018, according to IHS Markit. "We are looking for (solutions) that help us to identify things either before they occur or maybe right as they occur so that we can react a little faster," Paul Hildreth, emergency operations coordinator for Atlanta's Fulton County Schools, told the Los Angeles Times in a Sept. 2019 interview.

AI-based video analytics also create efficiencies and offering non-security-related insights for businesses. In the retail market, for example, store owners using surveillance cameras with analytics can spot shoplifters and alert security personnel to intervene in real time. In-store analytics can also measure hotspots, visitor flow, dwell time and product display activity. Smart cities are also leveraging networks of intelligent sensors for data capture and to organise system response to incidents as they unfold, as well as improve processes like traffic flow.

Police in New York, New Orleans and Atlanta now use cameras equipped with video analytics to improve investigations. In Hartford, Conn., a police network of 500 cameras includes some AI-enhanced units that can search hours of video to find people wearing certain clothes or use license-plate recognition to identify places where a suspicious vehicle was last seen. These units can also issue loitering alarms, detect discarded objects and people as well as objects that enter a pre-defined field. These deployments represent some of the early adopters of video analytics in surveillance applications in the United States.

The Rise of Behavioural Analytics

Behavioural analytics, a subset of AI, has emerged as one of the tools to do just that. Bringing together emerging computer hardware, deep learning and the proliferation of data that make up today's datasphere, behavioural analytics recognise hazardous situations based on the detection of certain human postures – perhaps a cashier's raised arms or an individual crouching near an ATM.

Behavioural analytics can also be used to ensure workplace safety – for example, tracking whether employees are holding the handrails when using the stairs and sending man-down alerts. Some software can even detect a potential gunman in real time, transmitting instant alerts to first responders to help minimise the risks to students, employees and facilities.

The adoption of behavioural analytics will only grow in the future. In the meantime, behavioural analytics has increased awareness of the value of AI-fortified surveillance systems and their benefits to enterprises across several industries.

Infrastructure Needs to Keep Up

As AI analytics put surveillance solutions on the front lines of crime detection, the data storage and technologies powering these solutions must operate at the highest level. Neural networks can meet a facility's needs by learning from video material obtained on-site; but none of that learning is able to take place if recording throughput is not highly reliable. Moreover, none of those deep learning insights will

> **Behavioural analytics can also be used to ensure workplace safety – for example, tracking whether employees are holding the handrails when using the stairs and sending man-down alerts. Some software can even detect a potential gunman in real time, transmitting instant alerts to first responders to help minimise the risks to students, employees and facilities.**

Deploying AI-enabled NVRs and appliances at the edge enables initial analysis to take place on-site, nearest where the data was first captured. This reduces latency and improves efficiency; thus, for example, enabling security personnel at a university to receive immediate notification if an unauthorised individual, detected by an outdoor camera, walks into a football stadium after hours.

be able to benefit an organisation if video frames are dropped due to low-performing storage systems.

In order for intelligent surveillance systems with AI analytics to function optimally, edge to cloud storage infrastructure must evolve. To accommodate such an influx of video and metadata from the surveillance AI, a new architecture that leverages both edge and cloud computing is needed. Storage manufacturers refer to this configuration as IT 4.0.

Deploying AI-enabled NVRs and appliances at the edge enables initial analysis to take place on-site, nearest where the data was first captured. This reduces latency and improves efficiency; thus, for example, enabling security personnel at a university to receive immediate notification if an unauthorised individual, detected by an outdoor camera, walks into a football stadium after hours.

With IT 4.0 architecture, after basic processing takes place at the edge, video and data are then transferred to a centralised environment for long-term retention and deep learning. Continuing with the education example, a university operating a public or private cloud could aggregate video and data from all surveillance systems deployed across the various departments on campus. With this holistic picture, school directors could identify foot traffic patterns on campus and other insights to aid in operations planning.

Building storage to accommodate standard surveillance systems is one thing; however, building storage to support Big Data applications that use dozens of high-definition cameras and process AI events simultaneously is quite another. Drilling down to the storage components, it is critical for integrators to consider the hard drives powering their customers' appliances and servers. These hard drives must "write" large quantities of data, as footage is transmitted from the edge to the cloud, and "read" that same data in real time, in order to detect, identify and deliver intelligent insights.

As a best practice, integrators should swap out standard hard drives – which are only designed to operate 40 hours a week – in favour of surveillance-optimised hard drives built for 24/7 workloads. They should also look for built-in health monitoring software so that any issues that could lead to data loss are identified prior to failure. Data recovery services to add additional peace of mind for customers. ■

How To Monitor User-Generated Content In A Video World

User-generated enterprise video is gaining popularity but can cause headaches for IT if left unchecked. Learn how to manage and monitor user-generated content.

By Micah Levine, TechTarget

Consumer markets have long embraced user-created video. For more than a decade, sites like YouTube have enabled users to upload and share their videos. Now, enterprise adoption of user-generated video is on the rise, prompting questions about monitoring, management, and storage.

User-generated video is one of the emerging use cases for enterprise video, according to a report from Aragon Research, based in Morgan Hill, Calif. The rise in user-generated content is due, in part, to vendors making it easier to shoot, edit, and distribute video, the report found.

Today, employees can use smartphones to shoot, edit, and upload video at a moment's notice. People are inherently visual, and organisations are shifting to more visual communications, said David Maldow, founder of market research firm Let's Do Video, based in Davie, Fla.

"When we want to learn something, we don't want to read about it," he said. "We go to YouTube."

Employees create videos for multiple reasons, such as updates on team projects, tutorials on new tools and weekly progress reports. These quick-to-make-and-distribute videos lead to fewer emails and phone calls, he said.

Organisations no longer need to invest in elaborate setups with lights, microphones, and expensive cameras to shoot video, said Irwin Lazar, analyst at Nemertes Research, based in Mokena, Ill. But making video more accessible also means organisations need a plan to monitor user-generated content, he said.

Monitoring User-Generated Content

Unchecked user-generated video can create security problems. Monitoring the content of a video is as important as managing where it's published, Maldow said. If an unmonitored video is published, it could result in sensitive company information becoming public, he said.

Monitoring user-generated content primarily focuses on ensuring the video content is appropriate for the organisation. Content needs to be monitored for factors like language, private information, and potential copyright violations. Organisations should have a review system to avoid publishing unmonitored content.

Monitoring user-generated content primarily focuses on ensuring the video content is appropriate for the organisation. Content needs to be monitored for factors like language, private information and potential copyright violations. Organisations should have a review system to avoid publishing unmonitored content.

Vendors that specialise in video streaming, management, and distribution, such as Kaltura and Mediasite, enable organisations to set permissions for actions like publishing a video. Placing barriers, such as a designated person to approve video, prevents unvetted content from being published, Maldow said.

In addition to setting publishing permissions, video vendors can provide provisioning for access to published videos. Video tutorials or training material make sense for everyone to have, but not everyone in an organisation needs access to a recording of a meeting that discusses quarterly projections, Maldow said.

Provisioning access to published content enables organisations to ensure videos with sensitive information are only seen by the appropriate parties, Lazar said.

AI Management For User-Generated Content

Though not yet widely available, some vendors are exploring how AI can help with user-generated enterprise video management. Media management company Cloudinary, for example, uses AI to monitor and edit videos, auto tag videos, provide structured metadata and search video libraries. AI can also analyse video network traffic.

"Video files are huge; they take up a lot of space," Maldow said. "If someone posts a video and it suddenly starts getting a lot of traffic, it can eat up all of your bandwidth and prevent people from sending emails."

Some video platforms, such as Kaltura, offer AI-driven analytics for bandwidth and storage. These dashboards can track how much bandwidth video uses over time, as well as how storage space is being used for video. The information from these analytics tools enables organisations to better manage video traffic.

User-Generated Video Needs Storage And Search Functionality

Organisations that support user-generated video need to make uploaded videos easily searchable. Video is only effective if it's readily available when needed, Lazar said.

For example, someone could shoot a video tutorial explaining how to navigate a tool, instead of answering repeated emails from team members. Video needs to be tagged and stored in a way that's easily found, Maldow said. Tagging enables users to give a video searchable context by ascribing keywords about its content.

While some organisations have turned to consumer video hosting sites, like YouTube – with its tagging system, playlist capabilities, and familiar interface – for their video hosting needs, they aren't the ideal option for enterprise video, Maldow said.

YouTube is a public site, and while videos on a channel can be set to private, it lacks the security measures and cohesive branding that an enterprise video channel will likely need. But video platform vendors, such as Mediasite, are including many of the same sought-after features, such as tagging and playlists. ■

Why Video Content Analytics Has A Critical Role To Play In The Pandemic

Intelligent analytics can help protect the public and prevent the spread of coronavirus.

By Stephanie Weagle, Chief Marketing Officer of BriefCam

As organisations continue to confront unprecedented challenges during the coronavirus pandemic, industry and government leaders worldwide are seeking reliable solutions and technologies that can help them adjust to the "new normal" in a productive and safe way. One technology that stands out for its ability to flexibly support many evolving urgent needs is Video Content Analytics; specialised software that processes video to identify, categorise, and index objects in video footage to drive mission-critical intelligent analysis.

With recent advancements in AI and deep learning, video content analytics (VCA) offers several important benefits that may not immediately come to mind when considering traditional video surveillance technology. Using its newer features for a growing range of applications, intelligent video surveillance offers much more than post-incident investigative support. In fact, VCA is now on the front lines as an instrumental solution for empowering public safety agencies and private businesses to protect our society and prevent the spread of the coronavirus.

VCA Solutions At Work In The Pandemic

Intelligent analytics software detects all objects—and even recognises faces—in a video scene and, by extracting identified objects, classifying, and indexing them, video content analysis makes video searchable, actionable, and quantifiable. Object and face recognition capabilities ultimately enable users to leverage video to better understand their environment to work more productively and respond proactively and preventatively to evolving situations and emergencies. Examples of key features of VCA solutions that support the most pressing needs during the pandemic include real-time alerts for pre-defined unsafe behaviours, people counting and line crossing to facilitate occupancy awareness and face recognition for contact tracing. The actionable data provided by VCA with these capabilities support the decision-making and response processes in this uncharted time.

The New Normal Requires Greater Situational Awareness

Today's video surveillance networks with analytics solutions go far beyond delivering conventional security benefits. Organisations can leverage video content analysis to configure rule-based alerts that are based on extensive object class and attribute filters, as well as face recognition, appearance similarity, directional data and more. These features allow corporations, campuses, and other organisations to improve specific situational awareness, which is the ability to isolate, understand, evaluate, and interpret data from extensive and varying environments as they change, and circumstances develop.

As cities, states, and countries work to contain the spread of COVID-19, deepening situational awareness across all sectors of a community including businesses of all sizes, healthcare institutions, educational campuses, law enforcement and local government, has very quickly become a top priority. With evolving social public health recommendations such as social distancing, the need to be constantly and completely informed about what is happening and there has never been greater.

Keeping a watchful eye on important areas can be a daunting and stressful task, especially for highly active and large areas, such as hospitals and healthcare facilities that need to prevent bottlenecks in ambulance bays and preclude overcrowding in waiting rooms, as well as watch for any suspicious or problematic dwelling and loitering across its campus. In environments like these, VCA can be used to identify those hotspots and automate alerts to specific behaviours or circumstances, so that the scene can be assessed, and action can be taken accordingly.

Beyond healthcare facilities, heightened situational awareness also has increasing benefits to all those responsible for the protection of people and places and compliance with evolving public health regulations. From building maintenance to retail store operations, owners of essential services businesses, law enforcement and other managers, there are new safety requirements to uphold and risks to mitigate.

As the world continues to adapt to the new realities brought about by the coronavirus, it is becoming clear that the need for increased situational awareness around crowding and people counting support will remain a priority for the foreseeable future. Of course, the need for situational awareness and real-time intelligence extends beyond COVID-19, and occupancy tracking and people counting is a constant requirement for retail environments to proactively prevent losses, checkout abandonment and much more.

As the world continues to adapt to the new realities brought about by the coronavirus, it is becoming clear that the need for increased situational awareness around crowding and people counting support will remain a priority for the foreseeable future. Of course, the need for situational awareness and real-time intelligence extends beyond COVID-19, and occupancy tracking and people counting is a constant requirement for retail environments to proactively prevent losses, checkout abandonment and much more.

Why People Counting Is Key

People counting is a particularly important video analytic capability right now as it provides the ability to detect the increase or decrease of people in a pre-defined area. Knowing how many people are coming and going into and out of a certain location allows agencies and organisations to comply with public health recommendations, such as social distancing. This is especially helpful for essential retailers that need to monitor the number of people in stores and the length of checkout lines, as well as healthcare facilities that need to ensure that waiting rooms and other areas are not overcrowded.

Intelligent video surveillance can allow for rule-based alerts that send notifications when thresholds of people/customers have been exceeded. Analytic-driven people counting can serve to protect the public and prevent the spread of COVID-19 in several ways including managing building maintenance and cleaning, complying with public health recommendations, and redirecting traffic to prevent bottlenecks.

Organisations can take a more dynamic approach to building maintenance and cleaning by configuring count-based alerts for area entryways and triggering notifications for cleaning crews when more than a certain number of people have entered the space. This way, operations managers can ensure that the property, especially sensitive areas such as public kitchens and bathrooms, remain clean and disinfected.

Beyond everyday cleanliness, as organisations work to comply with the latest public health recommendations, best practices and operating protocols, they can use VCA to seamlessly and continually monitor their occupancy statistics with real-time video content analytic people counting to facilitate compliance and protect visitors and staff, regardless of the venue.

They can also proactively avoid unnecessary crowding and prevent bottlenecks by detecting mounting traffic as it forms. By configuring people counting alerts for tight hallways and spaces, operators can monitor and identify potential crowding and proactively avoid this situation by sending personnel to redirect traffic to other walkways or access points or by producing signage that achieves the same effect. In an airport or transit hub, for instance, dynamic occupancy alerting can help ensure that travellers move swiftly through check-in and security checkpoints for safer and more streamlined visitor experience.

People counting is effective for virtually any situation where preventing crowding and optimising traffic flows is connected to customer satisfaction and/or safety. Having real-time, relevant situational awareness enables employees to use the data more effectively, and ultimately predictively, both in times of crisis and in the face of everyday challenges.

How Video Analytics Can Accelerate Contact Tracing

The concept of contact tracing has quickly become vital as authorities worldwide look to flatten the COVID-19 curve. Understanding the interactions between people and objects in their environment is required in order to trace infected individual's contact with other people and things. Manual contact tracing is difficult and time-consuming, but video content analytics can accelerate and aid this effort tremendously. With multi-camera search capabilities specific men, women, and children can be identified quickly and accurately through VCA. Accurate face recognition can also be used to pinpoint specific people of interest.

People counting is effective for virtually any situation where preventing crowding and optimising traffic flows is connected to customer satisfaction and/or safety. Having real-time, relevant situational awareness enables employees to use the data more effectively, and ultimately predictively, both in times of crisis and in the face of everyday challenges.

While contact tracing has been used for other purposes, it can be very effective in the efforts to combat coronavirus. The basic process for contact tracing with VCA for coronavirus starts with medical testing, followed by identification, tracking, contact tracing and finally guidance. Official medical testing is the first step to confirm that an individual has tested positive for the virus. Once an individual verifies testing positive for the virus, the systems administrator adds the individual's digital image to the VCA platform for rapid video filtering based on face recognition.

During the tracking process, the operator can use the VCA system to identify the appearances of the individual across cameras and environments. To conduct contact tracing, the VCA platform is then used to pinpoint the people with whom the infected individual has come into contact, as captured by video surveillance. This produces vital information on who else may be at risk, which enables the organisation to identify and notify other at-risk individuals and to provide appropriate direction on the next steps based on public health recommendations.

Charting a Course for the Future

While much remains uncertain as the pandemic develops, the importance of maintaining public safety and health is constant. Today intelligent video surveillance can help organisations across the board from small retail stores to large healthcare organisations, respond to rapidly changing needs relating to compliance with public health ordinances and support for contact tracing. Going forward, and beyond the pandemic, these powerful situational awareness capabilities will continue to provide lasting value across organisations in many ways through both existing and new uses of intelligent video content analytics solutions. ■

Video's Pivotal Role In The Internet of Things

Video plays a pivotal role in the IoT, generating an immense amount of data from connected devices. This data has the potential to be transformed from reactionary and investigative uses to allow users to take a more proactive approach to business operations and management.

By ONVU Technologies, IoT for all

According to a recent report published by Gartner, there will be 5.8 billion enterprise and automotive Internet of Things (IoT) endpoints in use by 2020, which represents a 21 percent increase over 2019. Of these endpoints, the research firm forecasts that more than 20 percent will consist of physical security devices, including video surveillance cameras which have long comprised a significant portion of the market of installed connected products around the globe.

So, how did a technology that once relied on bundles of coax cable strung together in a room full of grainy monitors become one of the most prevalent internet-enabled solutions of our time? The answer is relatively simple: convenience and functionality.

The security industry's migration from analogue to network video has been long a winding one, to say the least. Although the IP camera was invented more than 20 years ago, the technology didn't gain widespread adoption until many years later when it became apparent that the numerous benefits of networkvideo—advanced integrations, remote access, and improved archival and evidence retrieval just to name a few—outweighed the simplicity of analogue. When the price points of high-definition IP video equipment finally came more in line with analogue, the tipping point was finally reached, and IP cameras have proliferated the market since.

A New World Of Video Intelligence

Perhaps the greatest selling point of IP cameras today, however, is the level of intelligence that organisations can glean from their use, which simply wouldn't be possible without the IoT architecture in which they are now deployed. While much has been made recently about facial recognition and the potential privacy concerns that come with that, it's but one of the myriad benefits of contemporary video surveillance technology. Networks of cameras can be leveraged by organisations for a wide range of applications, security and otherwise.

While the primary purview of most camera deployments remains post-

Recent advancements in artificial intelligence (AI) and machine learning have also opened a brave new world of intelligent data that cameras can deliver. Though there's currently a lot of marketing hype in the industry about the capabilities of advanced video analytics, the fact is these systems can identify and classifying objects with incredible accuracy, which will only improve as the technology matures.

event analysis of security incidents, many end users are broadening the scope of their systems to provide analytics like people counting and dwell time to improve operations and customer service. With most cameras being IoT-enabled, this information can be easily filtered through an analytics dashboard to give end-users a real-time view of their business to determine where more resources need to be devoted. As a result, rather than being the cost centre that security has typically been viewed as within most businesses, they're now becoming a business enabler by helping other departments within the organisation perform their jobs better.

Recent advancements in artificial intelligence (AI) and machine learning have also opened a brave new world of intelligent data that cameras can deliver. Though there's currently a lot of marketing hype in the industry about the capabilities of advanced video analytics, the fact is these systems can identify and classifying objects with incredible accuracy, which will only improve as the technology matures.

One of the biggest problems historically, for security, has been managing the numerous false alarms generated throughout a typical day by various sensors. With a camera in place powered by underlying software that can decipher between humans, animals, vehicles and other objects, those alerts can be triaged and confirmed or denied quickly by security personnel, thus reducing alarm fatigue.

Security Beyond Video Forensics

In addition to the wealth of data and advanced functionality that surveillance cameras can provide on their own, they can also be combined with other physical security systems, such as access control and intrusion detection that are also now making their way to IoT, to provide capabilities that once seemed impossible. In fact, there has been an increased emphasis of late in leveraging video combined with card readers to provide enhanced identity verification at various access points that require an additional layer of security. In this type of application, users can present their access credential to the reader as they normally would while a camera running facial recognition in the background verifies their identity.

Some organisations are also combining cameras with other IoT sensors to address the age-old problem of tailgating, particularly in locations where traditional solutions like turnstiles aren't feasible. Access readers combined with AI-powered cameras can provide end-users with alerts when an unauthorised entry in these locations is detected so the incident can be quickly addressed. The threats posed by active shooters and data theft make this type of capability essential for organisations of all sizes.

Implications for the Broader IoT

The proliferation of IoT devices also means that video surveillance has a much larger role to play in the overall smart cities and buildings landscape. For example, many cities either have or are working to combine roadway sensors and lights with cameras to improve the flow of traffic. In addition to traffic control, cameras have also been integrated with some instances with environmental sensors, such as rain gauges, to monitor water levels in flood-prone areas.

When it comes to building automation, cameras are also playing a pivotal role, working in conjunction with things like HVAC and lighting systems to intelligently adjust the environment based on occupancy. Given the increasing push for organisations to "go green," the ability to reduce energy consumption is a major initiative within today's environmentally conscious businesses and IoT security devices are helping them achieve this goal.

Innovations on the Horizon

Though it may seem like video has reached its full IoT potential, the reality is we've only begun to scratch the surface of what's possible. New technologies like Lidar (light detection and ranging), which use lasers to measure reflected light off objects to create a 3D image, are already being combined with video to improve perimeter security at critical infrastructure sites. Developers are also now using license plate recognition (LPR) and video surveillance to provide smart cities and even private businesses like malls with the ability to give drivers real-time information on parking and traffic conditions and even assign parking spots. As such, the role of video surveillance in the IoT will only grow in importance in the years ahead. ■

Tekya Auto-Clicker Malware Exploits Kids' Android Apps

Google has removed multiple apps for children that were found to contain Tekya auto-clicker malware.

By Alex Scroxton, ComputerWeekly.com

Over 50 Android applications, 26 of them targeted at children, with over a million downloads between them, have been removed from the Google Play Store, after security researchers at Check Point found them to contain an auto-clicker malware dubbed Tekya.

Tekya generates money for cyber criminals by committing mobile ad fraud by pretending to be a user clicking on legitimate ads and banners sourced from legitimate online ad agencies, including Google's AdMbo, AppLovin', Facebook and Unity. It does this by exploiting Android's MotionEvent input movement (i.e. touch) reporting mechanism to imitate a human user clicking on an ad.

The malware was able to avoid detection and infiltrate the Google Play Store by obfuscating its malicious intentions in native code configured to run only on Android processors – this means that Google's security system, Google Play Protect, was unable to spot it, and nor was Google's VirusTotal service.

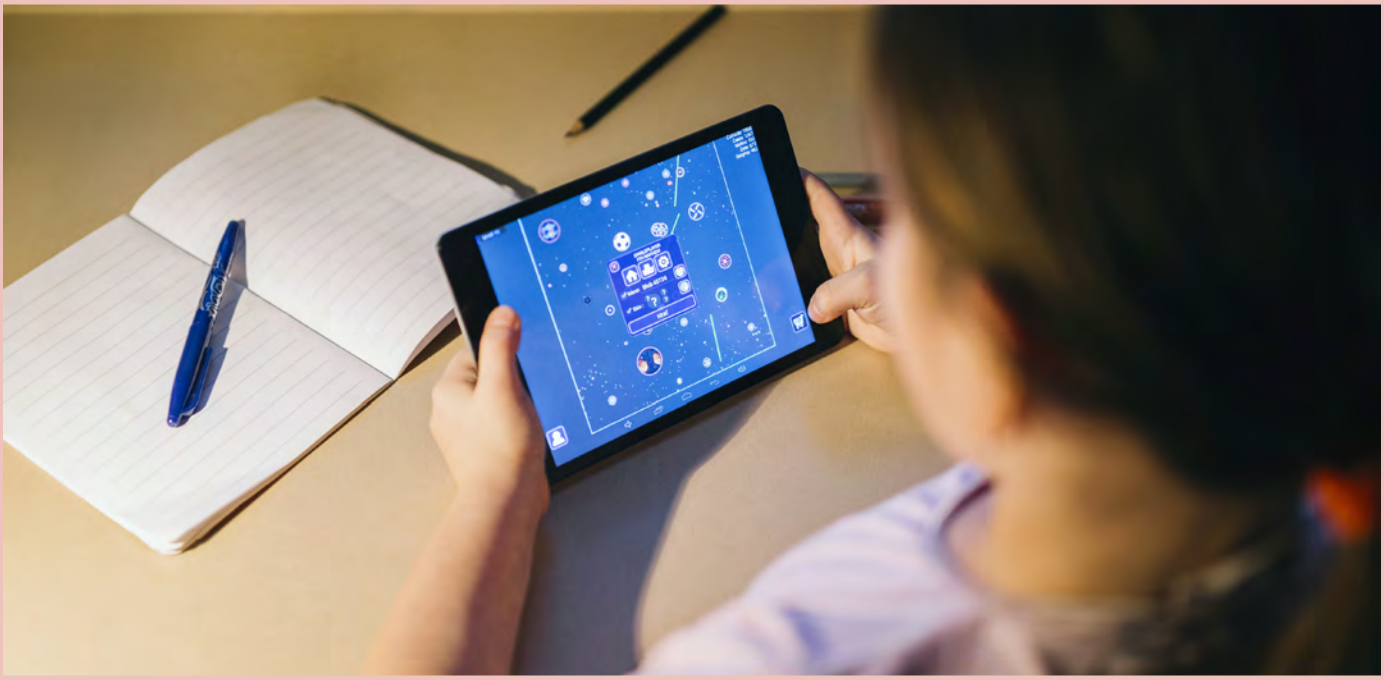


Photo by Matam Jaswanth on Unsplash

If you suspect you or your child has downloaded one of the infected apps – which are listed in full on the team's disclosure blog – you should uninstall it from your device immediately, check that your security patches are completely up to date, and consider using a mobile security service to spot and prevent future infections.

The cloned, infected apps uncovered by Check Point ranged from puzzles to racing games, as well as utility applications such as cookery apps, calculators and translators.

"To us, the amount of applications targeted and the sheer number of downloads that the actor successfully infiltrated into Google Play is staggering," said Aviran Hazum, Check Point's manager of mobile research.

"Combine that with a relatively simple infection methodology, it all sums up to the learning that Google Play Store can still host malicious apps," he said. "It is difficult to check if every single application is safe on the Play Store, so users cannot rely on Google Play's security measures alone to ensure their devices are protected."

The team who uncovered Tekya, which besides Hazum included threat researchers Danil Golubenko and Israel Wernik, disclosed their findings to Google, which removed the malicious apps in early March 2020.

Nevertheless, with over a million collective downloads, a great many users will have been compromised. If you suspect you or your child has downloaded one of the infected apps—which are listed in full on the team's disclosure blog—you should uninstall it from your device immediately, check that your security patches are completely up to date, and consider using a mobile security service to spot and prevent future infections.

With children across the UK now confined to their homes during the Covid-19 coronavirus crisis, leading to increased device usage across the board, parents should take additional steps to monitor and secure any devices being used by their children.

With schools left unable to bear any responsibility for educating children about online harms and malicious apps, security awareness and training organisation the Sans Institute has issued guidance on how to secure children's activity online.

With malicious apps still sneaking into the Google Play Store with alarming regularity, and almost three million apps now available, keeping on top of the threat is an impossible task for any one person to do.

As previous disclosures by Check Point have shown, Google's own internal security protections are still repeatedly missing the mark, despite a number of recent improvements.

Check Point warned that "users cannot rely on Google Play's security measures alone to ensure their devices are protected". ■

Legacy AV Defenceless Against Onslaught Of Evasive Malware

More than two-thirds of malware detected by WatchGuard in the last three months of 2019 was able to evade signature-based antivirus products, rendering them effectively useless in most instances.

By Alex Scroxton, ComputerWeekly.com

The volume of evasive malware—malware that can easily get round signature-based antivirus systems—grew to record levels in the final months of 2019, with two-thirds of samples detected by WatchGuard Technologies' Firebox appliances during the fourth quarter now able to do this – a dramatic increase from the 2019 average of 35%.

This not only suggests that obfuscated or evasive malware is becoming the rule, rather than the exception, but highlights that many popular security products are now losing significant utility and are in danger of becoming legacy services in the face of the always-evolving cyber criminal underworld.

"Our findings from Q4 2019 show that threat actors are always evolving their attack methods," said Corey Nachreiner, chief technology officer at WatchGuard.

"With over two-thirds of malware in the wild obfuscated to sneak past signature-based defences, and innovations like Mac adware on the rise, businesses of all sizes need to invest in multiple layers of security."

Nachreiner added: "Advanced AI or behavioural-based anti-malware technology and robust phishing protection like DNS filtering will be especially crucial."

In a new report released today, WatchGuard said it was seeing a number of emergent trends around malware, including a jump in popularity in adware targeting macOS environments. One of the top compromised websites found by WatchGuard hosted an adware called Bundlore that poses as an update to Adobe Flash. This tallies with other observations, notably a February 2020 study conducted by Malwarebytes.

WatchGuard also found widespread phishing campaigns exploiting a Microsoft Excel vulnerability that was first disclosed in 2017. This exploit, widely seen in the UK, enables the download of a number of different types of malware onto the victim device, including a keylogger called Agent Tesla, which was one of the earliest malware strains to exploit the Covid-19 coronavirus outbreak before it became a global emergency.

Elsewhere, WatchGuard found that SQL injection attacks became the top network attack in 2019, spiking by 8,000% in just one year, as well as a tendency among cyber criminals to use automated malware distribution. It said many attacks were hitting

between 70% and 80% of all Firebox appliances in a single country, which suggests threat actors are automating their attacks much more often than before.

WatchGuard draws its data from anonymised Firebox Feeds on active unified threat management (UTM) appliances whose owners have opted into data sharing to support security research. It has about 40,000 appliances in the programme, which during the final quarter of 2019 collectively blocked almost 35 million malware variants at the rate of 860 samples per appliance, and 1.9 million network attacks at the rate of 47 attacks per appliance. ■

3 Answers To The Cybersecurity Skills Gap

Experts warn that hiring more people is not one of them.

By Anthony Israel-Davis, Senior Manager of Tripwire

By this point, every organisation that needs a skilled team of cybersecurity professionals knows about the skills gap.

Companies in all industries are fishing for the freshest cybersecurity talent in a shrinking pond of potential candidates: The latest (ISC)2 Cybersecurity Workforce Study found that the U.S. alone faces a shortage of 500,000 positions. Meeting that demand would mean a 62 percent increase in available cybersecurity professionals. When looking at the global workforce, that number is a staggering 145 percent.

The skills gap creates problems for those responsible for managing security teams (security managers, directors and CISOs). While out-of-the-box approaches—like hiring talent with non-security backgrounds to learn security skills on the job—open up more possibilities for solving this problem, companies can find additional ways to boost their teams without adding headcount. Hiring alone isn't the only option to fill the skills gap. Sure, you want to find top talent with the best experience, but there are three other methods for closing the skills gap that you can implement in the meantime.

Hiring alone isn't the only option to fill the skills gap. Sure, you want to find top talent with the best experience, but there are three other methods for closing the skills gap that you can implement in the meantime.

1. Let Managed Services Pick Up the Slack

Outsourcing some of your core security tasks to a well-established managed services provider instantly augments your security team's capabilities. You can do this by selecting one pillar of your cybersecurity strategies—such as vulnerability management, compliance framework alignment, or configuration management—and apply managed services to just that pillar. For broader coverage, choose a service that gives you a well-rounded combination of multiple areas that need to be covered.

A key benefit of this approach is that you don't need to purchase additional servers, databases, or OS licenses, each of which also requires maintenance and administration. Another option is a hybrid approach—taking on a residential engineer. A RE from your chosen managed service provider gives you on-the-ground help running your cybersecurity program for a specified amount of time.

2. Get Better Company-Wide Security Education

Everyone in your company uses email, which is still a leading attack vector year after year. Your overall security posture is harmed by thinking of the security team as the only people responsible for your organisation's security. In NIST's Cybersecurity is Everyone's Job, a report by the National Initiative for Cybersecurity Education Working Group says, "Unfortunately, many organisations limit security responsibilities to designated security personnel that perform specialised security functions. Effective security must be enterprise-wide, involving everyone in fulfilling security responsibilities. Each member of the group, from the newest employee to the chief executive, holds the power to harm or to help, to weaken or strengthen, the organisation's security posture."

System administrators and IT staff are just as responsible for keeping threats at bay as security-focused personnel. The same goes for the HR department, marketing professionals, and anyone else who handles company data. A truly mature organisation will begin to self-enforce and monitor, and this is a cultural shift that comes from building security into the organisation. Without good company-wide security education, filling the skills gap will only take an organisation so far.

3. Automate Basic Cybersecurity Controls

How much of your security process can be automated? Automating is a third way to manage operational shortages arising from the skills gap. For example, you cannot manually audit logs every day—there is just too much data. Security information and event management (SIEM) can do much of that work for you. Vulnerability assessments are another arduous process if performed manually. Ideally, you can write rules so that when your tools pick up a vulnerability it can fix it without human involvement or integrate with an ITSM tool to automate the workflows. We will never be able to react as quickly as computers, but an agent or sensor can act upon what it finds right away.

As more workloads are moved to the public cloud, companies are looking for solutions that automatically remediate configuration and security weaknesses. Automation makes a security team more efficient and any process that is predictable and repeatable is a good target. ■

5 Critical Issues Cybersecurity Teams Face With COVID-19

How organisations address the new reality during the short-haul may have long term consequences.

By Andrew Homer, Vice President of Business Development at Morphisec

With companies across the globe implementing mandatory work from home policies at a never-before-seen rate as they seek to take refuge from COVID-19, many questions have arisen about the long-term difficulty of protecting the cybersecurity of remote workers and network infrastructure.

As workforces adjust to the new reality of working from home, employees are being subjected to spotty home-based, WiFi networks that are less secure and working on non-hardened devices. Today's antivirus and EDR tools depend on network connectivity, which limits their overall effectiveness. It's an undoubtedly stressful time for security professionals as endpoint security becomes a last line of defence. In fact, we're already beginning to see the repercussions with cyber-attackers pinpointing these vulnerabilities and leveraging Coronavirus-themed threats.

While COVID-19 has indisputably magnified concerns across the board, the cybersecurity risks of working from home aren't new. The remote employee movement reached into practically every industry long before this global health pandemic befell us. What's different now is the rapid need to change and the vast scale of remote workers that are exponentially increasing the attack surface. More employees have moved to Work From Home (WFH) environments at one time than ever before in history.

Securing Spotty Home Wi-Fi With Spotty Antivirus Protection

Most modern organisations, whether in the private or public sector, have extensive network monitoring and security tools in place. These include firewalls, network analysis and forensics, and email spam filters designed to catch malicious code and phishing attempts before they even access employee computers. When an employee works remotely, all that protection goes away. In a study on mobile workforce security, 81% of organisations reported they had seen Wi-Fi related security incidents in the last year, with 62% of these occurring in cafés and coffee shops.

Man-in-the-middle attacks, network spoofing, and packet sniffing of unencrypted traffic are the most common. Furthermore, the problem with antivirus and detection tools is that they need a constant network connection to be even slightly effective at blocking attacks. This doesn't work in spotty Wi-Fi scenarios. While many Wi-Fi attacks are crimes of opportunity and pose more danger to employee personal data than to your business, they still can put your organisation at risk. Confidential information can be compromised if sent over public or even home Wi-Fi, access credentials stolen, and even malware introduced.

Even with a password-protected home Wi-Fi network, you aren't going to have the sheer scale of monitoring tools that a corporate office does. There is also no guarantee that the password protecting that home network isn't used elsewhere, or even that it meets the standards of good governance established within the organisation. With the cost of a data breach increasing from $7.1 million in 2018 to $8.64 million in 2019, according to Ponemon Institute research, it's vital that companies utilise advanced threat protection alongside traditional antivirus in their security stacks given its spotty efficacy in work from home scenarios.

Combining Windows 10 Built-In Antivirus with Advanced Protection

With antivirus protection struggling in remote environments, there may be a better way to allocate security stack budgets for today's reality. The full migration to Windows 10 is nearly complete and that means more than one billion employee devices are now on the new operating system. Today, every Windows 10 workstation has free robust embedded Windows Defender Antivirus (AV) capabilities that are top-ranked by AV-Test.

Simply disabling the third-party antivirus tool automatically turns on Windows Defender Antivirus. This allows companies to immediately adopt a singular antivirus solution across their entire remote workforce.

However, like all signature-based antivirus, Windows Defender only protects users from known threats, leaving

> Man-in-the-middle attacks, network spoofing and packet sniffing of unencrypted traffic are the most common. Furthermore, the problem with antivirus and detection tools is that they need a constant network connection to be even slightly effective at blocking attacks.

employees largely susceptible to in-memory exploits, advanced malware, fileless attacks and zero days. But with the reallocated budget from their previous legacy antivirus solution, companies can look to pair this free antivirus with protection that works to combat zero-day attacks.

Companies such as Towne Properties, who are managing a distributed workforce, have been able to leverage Defender AV alongside advanced threat protection in a lightweight stack that doesn't miss unknown threats, while also simplifying operations for a lower total cost of ownership.

Bracing for Browser-Based Attacks

Increased use of SaaS software accessible via a web browser is a parallel trend to the work from home movement. However, as workers go about their daily routine during this pandemic, they're browsing more than ever before; internet traffic across the globe is up anywhere from 20-50% in the last week alone!

Given how fast this pandemic has evolved, no company is fully prepared for their entire organisation working from home. That means they don't have time or the resources in place to harden endpoint devices before they leave the office. With more people working from home on their personal devices, there are going to be more people accessing SaaS solutions. That opens up employees to browser-based attacks via malicious plugins and web-based exploit kits that are designed to breach passwords, IDs, and much more.

One way to defend against browser-based attacks is through browser isolation, which uses a browser in the cloud to access a website so any malicious threats are kept away from key local resources. Cybersecurity teams also need to be on top of their remote workers to ensure they are only using business-related plugins and extensions with internet and email usage.

Addressing Distributed SecOps With Remote Support and Moving Target Defence

A major difference in enterprise security during this pandemic is security operations teams — whose roles typically require in-person teamwork and a significant human element that's centralised on deciding which alerts are good, which are bad, and how to perform remediation — are working from home too.

This increases the need for both better remote support tools and set-and-forget protection that is working before an attack happens and without needing any onsite team members. Remote support tools enable IT to solve the problems their work from home employees have without needing a physical presence. For organisations with a wide footprint, these solutions have fast become a critical necessity.

However, remote desktop tools also offer a new attack surface for threat actors. A few short months ago, it was discovered that ConnectWise Control was being abused to deliver the Zeppelin ransomware. Attackers can use phishing tactics on remote employees to have them install a similar remote desktop tool, which can then be leveraged to deliver a payload. Better yet is looking to set-and-forget types of advanced endpoint protection such as Moving Target Defence (MTD) that can hide key memory from attacks without the need to recognise the threats it's facing.

As endpoints serve as the last line of defence, MTD creates confusion for attackers by scrambling the locations of .dlls, memory structures and commonly used resources.

Authorised enterprise programs such as browsers used by remote workers are given secret locations so they can function normally. And those locations are kept in flux, with new locations being generated each time an authorised program activates.

Cloud-native patching solutions are a similar option. With cloud-native patching, employees can be updated regardless of their connection to the network. They don't have to worry about firewalls or VPN limitations. If their device is online in this scenario, a remote worker's device can be updated.

MTD technology is designed to secure web-based user sessions from cyberattack; regardless of the way remote employees access their critical applications, the underlying processes within moving target defence protection enables them to do so securely. Web-based exploit kits are designed as evasive malware and the process-morphing capability of moving target defence blocks these techniques without the need for updates.

Virtually Patching Problem Areas

Industry best practices demand patching software vulnerabilities as soon as a patch is released, in order to shorten the time period in which the organisation is at risk. But what happens when an employee needs a big patch update while using home Wi-Fi? With research finding 60% of data breaches are caused by exploiting a software vulnerability that was known but which the victim had not yet patched, protection coverage that includes exploit prevention becomes even more valuable.

Typically, you can only patch systems that are inside the VPN, and not busily working at the time of the patching process. This means that your most vulnerable machines, ones belonging to employees that travel frequently, and that use dubious Wi-Fi connections in coffee shops, will not be patched often, in the best of cases.

This brings the need for virtual patching, a term originally coined by Intrusion Prevention System (IPS) vendors. It is the process of addressing a security vulnerability by blocking attack vectors that could exploit it. Various technologies can be used to shield vulnerabilities before they can be exploited. An organisation can, therefore, be protected without incurring the cost and the operational pain of downtime for emergency patching, patching cycles, and of course, the added cost of breaches in an unpatched system.

Cloud-native patching solutions are a similar option. With cloud-native patching, employees can be updated regardless of their connection to the network. They don't have to worry about firewalls or VPN limitations. If their device is online in this scenario, a remote worker's device can be updated.

In the Face of COVID-19, Optimised Functionality is Key

Organisations facing this unprecedented increase in work from home employees need to be aware of the risks their remote personnel present. There's no doubting the long-term impact COVID-19 will have on business operations and the bottom line, but taking some of the above steps can ensure that critical data and systems are safe while remote workers are still served.

As the world battles to overcome this crisis, the need to work remotely isn't going to disappear any time soon. It's a new reality that comes with multiple rewards, alongside an increased risk of cyberattack. But as businesses seek ways to increase cash flow and streamline performance in these trying times, it's those who implement protective measures for their employees that will have the highest likelihood of coming out the other side. Only then will their business be able to continue functioning securely over the long term as we work through this crisis. ■

Cloud-Native Threats in the COVID-19 Pandemic

There is no honour among thieves, and in particular among those thieves who are seeing a COVID-19 pandemic business opportunity in cyberspace.

By Paolo Passeri, Cyber Intelligence Principal, Netskope

Despite the warnings issued by public and private organisations, themed phishing campaigns, fake Coronavirus tracking apps loaded with malware and deceptive COVID-19 websites continue to take a toll on individuals and enterprises.

Not a day seems to pass without news of some kind of threat exploiting and capitalising on the current climate of fear and uncertainty.

With the global adoption of social distancing measures, remote working has increased exponentially since the beginning of the pandemic. Many organisations have taken advantage of this situation to implement remote access projects and deploy technologies to extend productivity beyond the traditional corporate walls more quickly than they would have without COVID-19.

In the last few months, this has meant a seismic shift to cloud applications, collaboration and conferencing tools, and mass adoption of remote access technologies (traditional VPNs or Zero Trust access).

These factors have dramatically accelerated the breaking down of the traditional corporate perimeter, leaving organisations exposed to new risks. Remote workers are

Remote workers are now the weakest link of the enterprise and easy prey for cyber-criminals. They are more vulnerable for several reasons: firstly because of the emotional distress COVID-19 brings – concern for the current situation as well as future implications – and secondly, because, in most cases, remote working has been enforced without educating employees about the risks.

now the weakest link of the enterprise and easy prey for cyber-criminals. They are more vulnerable for several reasons: firstly because of the emotional distress COVID-19 brings – concern for the current situation as well as future implications – and secondly, because, in most cases, remote working has been enforced without educating employees about the risks.

Another reason is because many of the recent remote access projects have been implemented as part of a contingency plan rather than a strategic business approach, prioritising productivity over security, and without a thorough analysis of the implications on security and additional pressure on existing on-prem infrastructure.

As a result, it's no surprise that cyber-criminals have quickly found easy ways to exploit the current landscape. For example, phishers have seen collaboration platforms as low-hanging fruit, and in practice any service – whether it's Zoom, Webex or Teams – has almost immediately been impersonated in malicious phishing campaigns.

Of course, phishing is not the only threat affecting remote workers. We have seen a proliferation of malicious campaigns relying on fear or finance to lure the victims to install malware by clicking on a malicious attachment. In these cases, serving the malware from a cloud service is particularly effective with remote workers.

With traditional VPN models, organisations backhaul all the endpoint traffic to the corporate termination point. This model doesn't fit with the nature of cloud traffic and there are non-negligible impacts on bandwidth consumption, performance and user experience (consider the example of cloud conferencing applications). This has led organisations to disable the split tunnelling resulting in a loss of visibility (and security) of traffic outside of the VPN tunnel. This shadow traffic, made of personal and unsanctioned cloud applications, poses a serious risk because it isn't inspected and creates a gate to corporate resources.

In this context, GuLoader is particularly interesting. GuLoader is a malware downloader, first observed in late December 2019 when it was used to distribute the Parallax Remote Access Tool. Since then, it has become more and more popular, and has been used to distribute different malicious payloads, including the AgentTesla keylogger, the NanoCore RAT (both used in COVID-19 themed campaigns), as well as additional remote access tools like Netwire, and Remcos.

The interesting aspect of GuLoader is its ability to download the encrypted payload from cloud services like Google Drive or OneDrive – more proof that the cloud is as compelling for cyber-criminals as it is for businesses.

Cloud services are particularly advantageous for malicious actors, since they offer simplified hosting, are easy to manage, allow a lot to switch between different payloads and provide better evasion capabilities as they are implicitly trusted or whitelisted. Additionally, legacy web security defences, which weren't designed to inspect cloud services, lack context i.e. is this a corporate or personal cloud service, and are unable to understand the language of APIs that drive the modern web.

GuLoader has jumped on the COVID-19 bandwagon, and is being used by threat actors in multiple malware distribution campaigns with a similar modus operandi. GuLoader is delivered to the victim via emails resembling those that come from the World Health Organisation, and is disguised as an e-book that provides guidance on how to be protected during the outbreak. Once opened it downloads and executes the FormBook information stealer directly from Google Drive.

FormBook is a malware available as-a-service, and relatively easy to set up and operate – even for low-skilled criminals. Unfortunately, it is simple and very dangerous. The malware can steal multiple types of information such as keystrokes, clipboard, and authentication data from the browser session.

Unfortunately, COVID-19 is presenting criminals with an opportunity to exploit multiple evasion techniques: the emotional distress of the victim – amplified under the pandemic – the authority of a trusted international organisation (directly involved in the fight against the virus), and a familiar service like Google Drive.

When implementing a remote access solution, organisations must consider educating users, and making cloud-native security a core component of the solution, and not as an optional add-on. ■

Prudential Turns To AI To Secure Computer Networks Against Cyber Attacks

Prudential, the UK's largest listed insurer, is turning to artificial intelligence to protect its computer networks in the US, Asia and Africa from malware hackers and internal threats.

By Bill Goodwin, ComputerWeekly.com

Financial services group Prudential is setting up security operations centres in Asia and the US that will allow it to monitor potential security threats on more than 100,000 devices on its networks.

The company, the UK's largest listed insurer, is rolling out artificial intelligence (AI) driven software that can identify unusual activity on its computer networks and automatically isolate hacking or malware attacks across its IT networks in more than 14 countries.

The project will allow security analysts in two operations centres in Asia and the US to respond to potential hacking, malware or insider threats around the clock.

Prudential plc, a life insurance and financial services company with annual revenues of $94bn in 2019, plans to deploy technology developed by Darktrace, a Cambridge University spin-off, across Asia and Africa before the end of the year.

The company, which demerged from its UK M&G insurance operations in October 2019, is focusing on

developing its business in Asia—which accounts for more than half its profits—and the US.

Tony Reed, assistant vice-president for cyber security delivery and incident response at Prudential plc, said the project will give Prudential's security analysts a picture of threats across the company's entire computer networks for the first time.

Reed said that Darktrace's self-learning software, known as "the enterprise immune system", will reduce the time security analysts have to spend trying to interpret unusual events on the network by half.

The software has proved itself in Prudential's US operation, Jackson National Life Insurance, which manages assets of $260bn, over the past five years.

"We are able to react faster because we are finding things faster. We are saving a tonne of analyst time," Reed said in an interview with Computer Weekly. "Something that would normally take an analyst anything from an hour to two hours to dig into is instantaneous."

When Reed joined Jackson from HP in 2015, Jackson's chief information security officer, Guillermo Guerra, tasked him with the job of bringing the company's security levels up to the level of maturity expected of a large financial institution.

"Even back then, the attacks were getting harder to find. They were attacking faster than you could keep up with. So we needed a tool where we would not be relying on the human element," he said.

It was difficult for security analysts to track what systems Jackson's clients were logging into, what devices were talking to each other, and what data was coming in and out of the company, said Reed, but Darktrace's software offered a solution.

One of the complicating factors was that the insurance company used two 'active-active' datacentres to keep simultaneous back-ups of its critical data.

"Having the ability to monitor the entire network 24 hours a day, and actions taking place without an analyst having to go in and do research and spend a couple hours on it, made the choice pretty easy," he said.

Jackson's IT team installed network probes and software to monitor 35,000 devices on the company's internal networks with assistance from Darktrace's engineers.

Active Back-Ups

One of the complicating factors was that the insurance company used two 'active-active' datacentres to keep simultaneous back-ups of its critical data.

It took time for Darktrace to learn which devices in one datacentre should be talking to which corresponding devices in the second datacentre.

The software, said Reed, more than covers the cost of its annual subscription by cutting the time it takes the company's 14 security analysts to investigate incidents.

"Even if I had doubled the staff, I wouldn't be confident that we would see everything and stop everything that we're doing today. Humans just can't learn that quickly," he said. "So it pays for itself every year just in that."

Even five years ago, a data breach could have cost the company millions of dollars in repair costs, providing crediting monitoring to its 700,000 clients and working with regulators.

"Switching from a perimeter defence model to an AI model was the biggest [and quickest] way we saw to eliminate or reduce the risk of having a security event," he said.

Learning On The Job

In January 2019, Prudential's US business introduced Darktrace's Antigena software, which is able to identify potential security threats and cut them off within seconds of detecting them.

The software works by learning how the company's network and staff normally operate so that it can identify unusual behaviour that might indicate malware or an insider attack from someone who is able to access computer systems within the organisation's firewall.

Reed is using the software to detect email threats which he estimates account for over 90% of attacks directed against companies. For example, if the Antigena software spots large files of data being sent out of the company, it can intervene to prevent it.

> The software works by learning how the company's network and staff normally operate so that it can identify unusual behaviour that might indicate malware or an insider attack from someone who is able to access computer systems within the organisation's firewall.

The software is faster, said Reed, than having to submit a ticket to a network specialist, by which time it may be too late.

So far, the insurance company has not experienced any major external attacks. But it has been able to stop an internal incident that could have led to customer data leaving the company and might have required the company to pay for credit monitoring services for the clients affected.

Once Darktrace software is running in Asia and Africa, Reed plans to introduce a "follow the sun" programme to monitor the security of company's networks worldwide.

This will replace the current model which requires Jackson's security analysts to work 12-hour shifts in both the US and Malaysia.

This shift-work system is not ideal, as very little activity takes place on the US or Asian networks after business hours, said Reed.

"It is super quiet [at night]. So a lot of times we'll tell them 'Go look at this alert' or 'Take this training' if nothing happens," he said.

In the future, security analysts in the US will monitor the company's network traffic across all locations during the day US time, before handing over to a security operations centre in Malaysia.

Darktrace's software is used by 3,000 organisations including BT, First Great Western, Metro Bank, Ocado, TSB and William Hill. The company signed a partnership deal with McLaren Racing in February. ■

Remote Workers Often Not Provided Secure Tools

The number of employees working from home is increasing, but the security technology to support them is not being deployed.

By Dan Raywood, Infosecurity Magazine

According to a survey of 694 IT security administrators and practitioners, most companies fail to authenticate remote workers properly or inadequately inspect their network traffic for threats.

The research, conducted by Cato Networks, found 68% of respondents said their organisations fail to deploy enough prevention or authentication technologies for remote users. In particular, 37% do not use multi-factor authentication (MFA) for remote users, while 55% of respondents fail to employ intrusion prevention software, or anti-malware technology, while 11% fail to inspect traffic altogether.

“A lack of security enforcement on remote access users should be of serious concern for IT managers: enterprises cannot enable widespread remote access at the expense of security protections,” said Yishay Yovel, CMO of Cato Networks. “Enterprises should be able to provide remote access for all users anywhere, in minutes, with the security protections and network optimisations they have in the office.”

Brian Honan, CEO of BH Consulting, told Infosecurity that the numbers did not surprise him, as many companies were already struggling to roll out better authentication technologies for remote users before the global pandemic hit.

He said: “With the rush to support remote working for many more users, companies rapidly expanded their remote access solutions or migrated systems to the cloud; this rush was to ensure the business could survive and support staff to continue working.

“However, now that those immediate goals have been met and our response to the pandemic may be more long term than initially planned, companies need to review the security and resilience of their remote access solutions.”

The news follows research from earlier this week, when a Tripwire survey found 94% of cybersecurity professionals were more concerned about security in the wake of COVID-19. Its survey of 345 IT security professionals found that 89% said remote working had made the job more difficult. Additional findings included:

- 49% said they cannot effectively secure employees’ home office environments
- 41% said it is more challenging to manage what devices are connecting to their corporate networks
- 38% said it is hard to gain visibility into remote assets and systems

The survey also found that 53% of respondents were increasing security investment with 28% investing in new tools.

“The massive shift to working remotely represents a huge change for organisations’ attack surfaces,” said Tim Erlin, vice-president of product management and strategy at Tripwire. “It’s no surprise that security professionals are finding it challenging to monitor and minimise the new attack surfaces.” ■

SUBSCRIPTION FORM

Fax your order to **+65 6842 2581** or email us at **info@tradelinkmedia.com.sg**

Please (√) tick in the boxes.

□ Southeast Asia Building
Since 1974

SOUTHEAST·ASIA
CONSTRUCTION
Cover Story:
Basalt processing for Vietnam's National Route 1A highway
Features:
MRT SSP Line project in Malaysia
Snorkel launches 'mega boom'
Market Talk: Manitou

□ Southeast Asia Construction
Since 1994

SECURITY SOLUTIONS TODAY
UNRAVELING UNMANNED AERIAL VEHICLES
Regulating the growing applications of drone technology

□ Security Solutions Today
Since 1992

***1 year** (6 issues)*
per magazine

Singapore	SGD$60.00
Malaysia / Brunei	SGD$105.00
Asia	SGD$155.00
America, Europe	SGD$185.00
Japan, Australia, New Zealand	SGD$185.00
Middle East	SGD$185.00

□ Bathroom + Kitchen Today
Since 2001

***1 year** (4 issues)*

Singapore	SGD$32.00
Malaysia / Brunei	SGD$70.00
Asia	SGD$85.00
America, Europe	SGD$135.00
Japan, Australia, New Zealand	SGD$135.00
Middle East	SGD$135.00

Lighting Today
Since 2002

Lighting Today is available on digital platform.To download free PDF copy please visit:

http://lt.tradelinkmedia.biz

Personal Particulars

Name: ______________________

Position: ______________________

Company: ______________________

Address: ______________________

____

Tel: ____________ **Fax:** ____________

E-Mail: ______________________

IMPORTANT

Please commence my subscription in ____________________(month/year)

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
Co. Reg. 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: ____________

See us at these upcoming events!

Event	Date	City	Country	Website	Page
GSX 2020	21 – 23 Sep 2020	Atlanta	U.S.A.	www.gsx.org	OBC
IFSEC SEA 2021	15 – 17 Jun 2021	Kuala Lumpur	Malaysia	www.ifsec.events/kl/	IFC
IFSEC Philippines 2021	21 – 23 Jul 2021	Manila	Philippines	www.ifsec.events/philippines/	IBC