OCT – DEC 2022

# SECURITY SOLUTIONS TODAY


## SMART CITIES

The Ultimate Solution for Secure Living

# IN THIS ISSUE






# CONTACT


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

**EDITOR** Navkiran Kaur (sst@tradelinkmedia.com.sg)

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

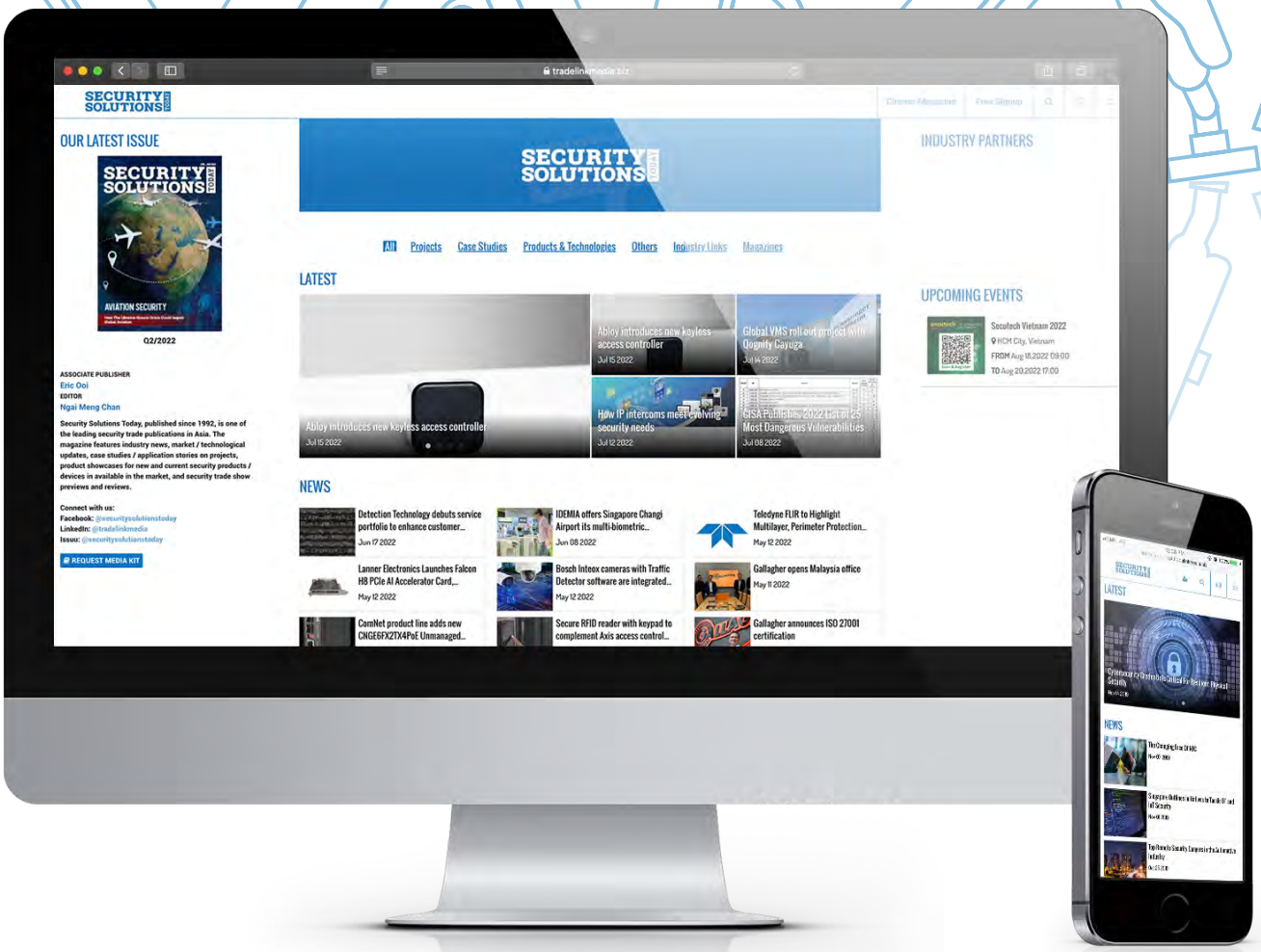
**HEAD OF GRAPHIC DEPT / ADVERTISEMENT CO-ORDINATOR**
Fawzeeah Yamin (fawzeeah@tradelinkmedia.com.sg)

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



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


**SECURITY SOLUTIONS TODAY**
is published quarterly by Trade Link Media Pte Ltd (Co. Reg. No.: 199204277K)
101 Lorong 23, Geylang, #06-04, Prosper House, Singapore 388399
Tel: +65 6842 2580
ISSN 2345-7112 (E-periodical)




# sst.tradelinkmedia.biz

## Visit our website for the latest information

News In The Industry · Upcoming Exhibitions · Download Magazine Issues

# AXIS COMMUNICATIONS LAUNCHES FIRST AXIS EXPERIENCE CENTER IN SINGAPORE AND SOUTHEAST ASIA

*The Axis Experience Center will showcase future-ready innovations and provide a platform to engage with its ecosystem of stakeholders across the region, elevating security standards*

Axis Communications, a network video leader, announced the official opening of the first Axis Experience Center (AEC) in Singapore. Representing the first AEC in Southeast Asia, the state-of-the-art facility is designed to showcase cutting-edge security innovations and solutions, reaffirming Axis' commitment to elevating security standards in Singapore and the broader region for a smarter and safer world.

The S$1M Experience Center was unveiled at Axis Communications' Singapore headquarters in Suntec City on 30 September. The opening was graced by Jacqueline Poh, Managing Director at the Singapore Economic Development Board (EDB), as the Guest-of-Honour. Other distinguished guests included His Excellency Kent Härstedt, Ambassador to Singapore, Kingdom of Sweden, as well as senior leadership representatives from Axis Communications, Boudewijn Pesch, Vice President, Asia Pacific, and Carl Malmqvist, Regional Director, South Asia Pacific.

Through physical product showcases and interactive demonstrations, guests can experience first-hand the ability of future-ready technologies to deliver optimal security outcomes. This includes advanced surveillance systems encompassing features such as audio analytics, intrusion detection, automated access control systems, as well as data analysis tools that yield actionable insights for better decision-making. As the 25th AEC globally, the Singapore facility is envisioned to serve as the center of excellence for the region. It will be joined by new AECs across key cities in the Asia Pacific, such as Kuala Lumpur, Jakarta, Bangkok, Bangalore, Mumbai, and Delhi, among others, unlocking further opportunities for growth and partnerships.

**Boudewijn Pesch, Vice President, Asia Pacific**

**Carl Malmqvist, Regional Director, South Asia Pacific**

Carl Malmqvist, Regional Director of South Asia Pacific at Axis Communications, said, "The digitalization of Southeast Asia has reached a tipping point, driven by increasing awareness of the benefits that digital technologies can provide. We anticipate continued technology adoption and innovation to create opportunities for the growth of advanced security applications. Having an Experience Center in a regional business hub like Singapore provides Axis with the platform to better engage its ecosystem of stakeholders across Southeast Asia, facilitating collaboration essential to meet evolving security requirements in today's increasingly networked environments. We look forward to working closely with trusted partners such as Singapore's Economic Development Board to build smarter, safer, sustainable, and more efficient cities of the future. "

Jacqueline Poh, Managing Director at the Singapore Economic Development Board said, "We expect demand for advanced security solutions that incorporate digital technologies to grow in Southeast Asia as the benefits of digitalization become more widely known. Singapore's strengths and capabilities in network security and advanced analytics, coupled with our hub advantages, make it an ideal location for the Axis Experience Center. We look forward to Axis' plans to enhance our ecosystem by bringing

**Jacqueline Poh, Managing Director, Singapore Economic Development Board**

*continue on page 6*

# MAKE ROOM!

## NOW... MORE CHANNELS OF POWER DISTRIBUTION – by ALTRONIX


Introducing **ACMS12(CB)** 12-Output Access Power Controllers with Fire Alarm Interface, and **PDS16(CB)** 16-Output Power Distribution Modules.

These new stackable sub-assemblies further increase access control capacity when integrated with Altronix Trove Series or virtually any wall/rack mount application - reducing overall equipment and installation costs.

Both feature dual inputs providing selectable 12 or 24VDC from any output with bi-color voltage LEDs for visual identification.

Altronix®

YOUR LEADER IN POWER | BACKED BY A LIFETIME WARRANTY

together private and public sector stakeholders to address important and emerging security challenges." Collaboration with like-minded industry partners both locally and regionally is a key factor in driving Axis' growth in Asia. One such partner is Singtel, with whom Axis is currently exploring 5G use cases for security applications. 5G networks can support increased bandwidth, which is essential for data aggregation and analysis, giving rise to more innovative security solutions in areas such as automation and machine learning.

Dennis Wong, VP of 5G Enterprise & Cloud, Singtel Group, said: "Many enterprises are undergoing rapid digitalization while exploring and developing 5G solutions for deployment in their industries. Singtel's 5G network and Paragon MEC platform have been specially designed to help them address their business needs, improve operational efficiencies, and unlock new opportunities to advance in a 5G world. Such solutions, developed with industry partners like Axis, are currently being showcased and trialed at Singtel's facilities such as the FutureNow Innovation Centre, Centre of Digital Excellence, as well as the 5G Garage, which is a live test facility, training center, and ideation lab. With the opening of the AEC, enterprises have a new avenue to secure the solutions and support they need to help them achieve their digitalization goals and aspirations in Singapore and beyond."

According to industry research, the global physical security industry is forecasted to generate US$153 billion by 2023, with the Asia Pacific being a key driver of this growth. One of the most prominent issues the industry faces is a lack of manpower, making it crucial to adopt advanced technology-first solutions to better secure businesses and optimize operations as digital economies continue to grow. These trends align with Axis' security solutions, making the launch of the Singapore AEC timely for local organizations and positioning the company well for regional growth.

Interested parties may book a tour of the Singapore AEC at https://www.axis.com/experience-center/singapore

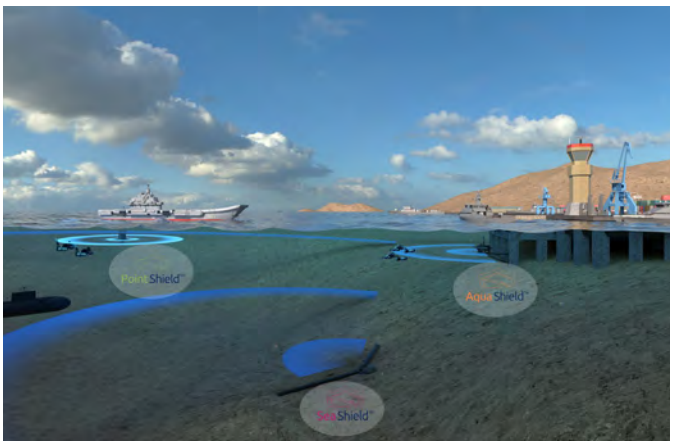
**For more information, please visit: https://www.axis.com/en-sg** ■

## EURONAVAL 2022: DSIT SOLUTIONS LTD. SHOWCASES ITS UNIQUE MULTILAYERED COMPREHENSIVE SONAR-BASED SOLUTION FOR THE DEFENSE OF UNDERWATER STRATEGIC ASSETS AGAINST IMMEDIATE, SHORT- AND LONG-RANGE THREATS

*EURONAVAL 2022, October 18-21, Paris Le Bourget, France, Stand #F-71*

DSIT Solutions Ltd., a global specialist in the development, manufacture, and supply of high-end, comprehensive, and integrated protection solutions against all underwater threat types – showcases at EURONAVAL 2022 its unique, multilayered defense solution for securing strategic assets against the various types of underwater threats in diverse ranges and sea depths. These include, among others, hostile military, terror and illegal activities, intrusion, sabotage, and smuggling by divers, Semi-Submersible Vehicles (SSVs), Autonomous Underwater Vehicles (AUVs), Unmanned Underwater Vehicles (UUVs), Remotely Operated Vehicles (ROVs) and all submarine types.

DSIT will present its uniquely combined and integrated proven capabilities and systems – with the ShieldTM Sonar Family – demonstrating smart and comprehensive hermetic protection and defense solutions from underwater threats for ports, harbors, shore & offshore sites, as well as other strategic assets, including underwater pipelines and cables, at sea and on land.




DSIT's advanced solutions secure all layers from the immediate to short & long ranges as well as from shallow to deep-water threats, providing relevant and applicable protection & security solutions for militaries, HLS, and Law Enforcement agencies.

*continue on page 7*

DSIT's multilayered defense solution seamlessly integrates an array of proven capabilities and systems into one comprehensive solution. The solution includes the ShieldTM family of sonars, such as the SeaShieldTM ASW sonar and the AquaShieldTM Diver Detection Sonar (DDS) that cost-effectively handle immediate, close-range threats and are both stationary sonar systems. A land-based mission control system manages these sonars, deployed in coastal & littoral waters – utilizing advanced signal processing and displays and machine learning techniques for automation algorithms – and reduces operator workload and required expertise. Highly advanced hardware with the latest-generation processing capabilities ensures these sonar systems' superior performance with a minimal footprint.

The PointShieldTM Portable Diver Detection Sonar (PDDS) system protects strategic assets and ships when onboard vessels are in shallow waters.

"DSIT Solutions Ltd. is proud to present its unique and comprehensive Underwater Security System of Systems at EURONAVAL, showcasing a full Underwater Defense suite, which is based on the company's proven capabilities and vast experience in underwater technologies and threat environments," says Mr Hanan Marom, the company's VP Business Development, Marketing & Sales. "Our solutions are modular, cost-effective, present tailor-made capabilities according to specific customer needs, and are compatible with other existing platforms' systems." ■

## OPENTEXT KICKS OFF OPENTEXT WORLD BY INTRODUCING CLOUD EDITIONS 22.4 AND PROJECT TITANIUM

*Innovations unveiled deliver on the OpenText commitment to elevating every person and organization to gain the information advantage*

At OpenText World, OpenText™ (NASDAQ: OTEX), (TSX: OTEX), announces Cloud Editions 22.4 (CE 22.4), a series of impactful innovations driving forward the company's Project Titanium to deliver seamless complete and integrated information management in the cloud. With strengthened offerings in the public and private cloud, CE 22.4 innovations unlock tremendous value for customers, providing them the tools, solutions, and trust to help solve their biggest hurdles and excel in a world of accelerated change.

"OpenText is empowering organizations to drive digital-led transformations and prepare for the critical and expanding business requirements of modern work, environmental, social, and governance (ESG), as well as artificial intelligence," said Mark J. Barrenechea, CEO & CTO, OpenText. "Cloud Editions 22.4 is an important milestone in our journey to complete and integrate information management in the cloud. Titanium, our next generation cloud platform,

*Image by rawpixel.com on Freepik*

will help customers accelerate their cloud-based digital transformation and future AI applications."

During his OpenText World keynote address today, Barrenechea is sitting down for a fireside chat with OpenText customer Cardinal Health to speak about their modernization journey: "As a crucial link between the clinical and operational sides of healthcare, it's essential to have a secure, reliable cloud-based EDI platform to provide life-saving products to our customers," said Denise Hemmert, VP of Platform Services at Cardinal Health. "I'm excited to join OpenText World to discuss how we are leveraging digital capabilities to modernize our technology infrastructure to better serve manufacturers, providers, health systems, and patients across the healthcare ecosystem."

At OpenText World this week, much will be revealed around the CE 22.4 release.

### CE 22.4 Simplifies Opportunities to Increase Customer Engagement and Responsiveness

Customer experience is of critical importance in today's digital world. In a recent OpenText global survey, eight in ten respondents (80%) experience information overload, making it crucial for businesses to personalize every web and communication experience and provide customers with the right content at the right time and through the proper channels to help cut through this cluttered environment.

*continue on page 8*

In 22.4, new capabilities in OpenText Experience Cloud make it faster and easier to increase relevancy, consistency, and responsiveness across the entire customer journey with two new must-have solutions for Customer Experience Management (CXM) and Digital Experience Management (DXM) use cases. These solutions are delivered in a unified environment and bring together key capabilities across OpenText applications Exstream (CCM), TeamSite (WCM/CMS), Media Management (DAM), Experience CDP, and Core Experience Insights, all within a composable platform out of the box.

Additional enhancements to OpenText™ Exstream and OpenText™ TeamSite are critical to the new Experience Cloud solutions. OpenText™ Exstream accelerates time to market for digital communications across channels and formats with seamless electronic signature processing integrated with Core Signature and automated archiving to OpenText InfoArchive. The new enhancements also provide no-code dynamic charting and display components for visually engaging communications. OpenText™ TeamSite is at the core of every customer experience platform, and 22.4 offers the ability to configure and compose unique intelligent digital workplaces to improve productivity and surface relevant data insights for improved decision making. Combined with a new integration to Google BigQuery, web developers and content creators will benefit from dynamic AI/ML-driven data processing to deliver more personalized and relevant experiences and communications.

## CE 22.4 Empowers Workforces with Smarter, Simpler, and Savvier Solutions to Master Modern Work

OpenText is committed to empowering workforces across all industries to gain information advantage through frictionless, automated, and simplified experiences, and 22.4 has several innovations enabling workforces to excel at modern work. Accessing content where and when needed is simplified with OpenText ™ Core Content and its new integration with Microsoft®. Consumers can now open or save documents to Core Content directly from Microsoft Office Desktop applications and view, edit, or co-author directly within Core Content – boosting productivity while maintaining integrity.

Staying ahead and staying secure is easier with ready-to-run business scenario templates from OpenText ™ Extended ECM. The newest addition to the growing Business Process Library is the latest Real Estate Management Business Scenario that streamlines the management of globally dispersed real estate assets – a time-intensive process all enterprises face. Extended ECM also enhances compatibility with SAP applications with support for SAP S/4HANA Harmonized Document Management, standardizing integrations to accelerate time to value with fewer resources.

Additionally, OpenText also continues to manage the risks associated with eDiscovery with enhancements to OpenText™ Axcelerate, improving productivity for legal teams. Delivering project oversight and superior insights through enhanced reporting, 22.4 introduces a new configurable dashboard and reporting framework for Axcelerate based on the Magellan Business Intelligence and Reporting (MBIR) platform that includes a variety of new enhancements for faster decision-making and cost control. This new feature also comes at no extra cost while eliminating the need for third-party add-on tools.

Focused on making OpenText Business Network available to companies of all sizes, the new Microsoft Dynamics 365 Business Central Order to Cash Adapter Kit for OpenText Business Network Cloud Foundation offers mid-market size companies with limited internal electronic data interchange (EDI) skills, to be able to exchange order to cash-related business documents electronically with key trading partners. Businesses can now leverage a scalable B2B integration environment that can support changing business needs and help streamline order fulfillment processes with seamless integration to Microsoft Dynamics 365.

## CE 22.4 Offers Trusted Solutions for Better Cyber Resilience in a Disruptive World

With the complexity of the digital world today, information advantage is being able to access digital information with comprehensive digital forensic investigation tools. With CE 22.4, OpenText continues to focus on modernizing forensic investigations, with enhancements to OpenText™ EnCase Forensic and OpenText™ EnCase Endpoint Investigator, including the support of new cloud connectors for Facebook Messenger, Slack, Microsoft 365 Archive, enhanced workflows, and Mac collections. In addition, to enhance threat detection and incident response, OpenText™ EnCase Endpoint Security adds the ability to conduct off-VPN anomaly detection and manage custom automated response actions. CE 22.4 also enables scalable network visibility and faster collection and analysis of external Packet Capture (PCAP) with OpenText™ Network Detection & Response.

For more on all the CE 22.4 innovations, please read our blogs. Additional information and demonstrations on these and other innovations will be presented by OpenText EVP and Chief Product Officer Muhi Majzoub during his October 5th OpenText World keynote.

**For more information, please visit: https://www.opentext.com/patents** ■

## MSAB LAUNCHES A FLAGSHIP FEATURE – A NEW MTK EXPLOIT THAT ALLOWS INVESTIGATORS TO ACCESS DATA IN MORE LOCKED DEVICES

*MSAB, a world leader in mobile forensics, announces its third major software release for 2022. Together, these updates help empower every investigation with digital forensic solutions – for a safer world.*

"The sole focus of MSAB is on delivering high-quality digital forensic solutions to ensure reliable forensic evidence. We have been striving to equip our customers with solutions that allow access to critical information in the first hours of their investigations with a focus on resolving more cases faster", says Joel Bollö, CEO of MSAB.

The updated mobile forensics solution for digital data recovery, XRY, comes with significant extraction and decoding capabilities for more devices, with the total number of supported devices exceeding 42,860 and more than 4,247 app versions.

"MSAB understands the complex challenges that come with the diversity of devices. With the new release, we are proud to ensure support for the latest iOS 16 and Android 13. MSAB is also launching a new MTK Exploit. This is the beginning of an exhaustive list of devices for which we can offer full physical data extractions from locked MTK chip-based handsets." says Joel Bollö, CEO of MSAB.

MSAB solutions are in a continual state of ongoing development, and its digital forensics solutions can significantly assist law enforcement agencies in investigating crime, gathering intelligence, investigating fraud, and fighting corruption.

"We endeavor to continually improve the quality of our products. That is why the MSAB digital forensic analysis solution, XAMN, combines ease of use, powerful searching capabilities, and unparalleled efficiency. The new release introduces a detailed audit logging function which gives a deep level of detail about the actions taken during the review of digital evidence within XAMN. The software is now optimized for Data Protection compliance," says Bradley Sipes, Chief Product Officer at MSAB.

**For more information, please visit: www.msab.com** ■

## LEADING TRADE FAIR FOR CIVIL SECURITY IS ALREADY SETTING ITSELF UP FOR 2024

*Civil protection and civil defense will be a new focus of Security Essen ASW and politics support platform for exchange and procurement*

Security Essen, a leading trade fair for civil security, is expanding its range of products and services. It was announced today at Messe Essen that the topics of civil protection and civil defense will be added as a new focus in 2024. The background to this is the current situation in politics, the environment, and society and the resulting necessities. "At Security Essen, we not only depict the latest developments but also integrate upcoming significant concerns of society with foresight," explains Oliver P. Kuhrt, CEO of Messe Essen. "The topics of civil protection and civil defense are becoming increasingly important, and it is no longer possible to imagine a security fair without


*continue on page 10*

them. Therefore, with the next Security Essen 2024, we will offer all players their own platform as well as a network for exchange, information, and procurement."

The Alliance for Security in Business, ASW (Allianz für Sicherheit in der Wirtschaft), is particularly active in the field of this prevention. ASW West Managing Director Dr. Christian Endreß has analyzed a wide variety of scenarios over the years, which have now become a reality: "A flood of the century, a pandemic, a war in Europe, impending energy shortages and cyber attacks on critical infrastructures - what was unthinkable until recently has now come to pass. Here, it is important to protect the population with foresight." Possibilities for this are already available on the market. One example, according to Endreß, is SMS warnings to people in disaster areas. Security Essen will bring together this know-how of technological innovations and organizational solutions at Messe Essen. Companies, political players, and those responsible for civil defense can exchange ideas in the newly created theme area "Civil Protection and Civil Defence". The strategic planning for the implementation, which will now be realized for the first time from 17 to 20 September 2024 at Security Essen with its own exhibition hall, has already been underway for some time. Support comes not only from associations such as ASW but also from politics. NRW's Minister of the Interior Herbert Reul said: "We welcome the initiative of I N F O R M AT I O N Messe Essen to show the topic of 'Civil Protection and Civil Defense' as a separate focal point at Security Essen in future."

**For more information, please visit: www.security-essen.de ■**

## SIGNED VIDEO FOR BODY-WORN CAMERAS ENSURES THE AUTHENTICITY OF VIDEO EVIDENCE

Axis Communications announces a new cybersecurity feature for Axis body-worn cameras. Available with firmware release 11.0, signed video provides an additional layer of protection for body-worn solutions helping to enforce trust in video evidence. This valuable feature adds a cryptographic checksum into the video stream allowing the video to be reliably traced back to the unique Axis camera where it was produced and verifying that the footage hasn't been tampered with.

Whether in criminal or civil investigations, it's vital that the authenticity of video surveillance can be presented without question. Because any doubt, however small, can be used to undermine the relevance of the video evidence. Now, thanks to the signed video, it's possible to verify the authenticity of the video throughout the entire chain of custody.

Within Axis cameras, the signed video uses the Axis Edge Vault hardware component, one of the key security features built into Axis products. Axis Edge Vault is a secure cryptographic compute module which can be used for cryptographic operations on securely stored certificates. It provides tamper-protected storage, enabling each device to securely store sensitive data and provide for secure execution of applications.


Key benefits of signed video:

- Helps ensure trust and assurance of video evidence
- Provides authentication at the point of capture
- Easy integration thanks to the open-source framework

Axis body-worn solutions allow wearers to view video files on a mobile device or even in the VMS/EMS after the camera is docked and synched. However, for security purposes, camera wearers cannot access or share footage directly from the camera. The signed video provides an additional layer of protection for body-worn solutions so customers can rest assured that the authenticity of video evidence is protected—from the point of capture to the courtroom.

**For more information, please visit: www.axis.com ■**

# IDESCO ID MOBILE ACCESS SOLUTIONS MAKE ACCESS CONTROL AND ACCESS CREDENTIAL MANAGEMENT MUCH EASIER

*New mobile access solutions*

Door access with mobile phones is constantly increasing. Mobile phone is excellent for carrying digital access rights – secure, convenient, and available to everyone. The mobile credential is transferred from the phone to the reader using the phone's Bluetooth connection. The connection between the reader and phone is protected by secure encryption – the same as mobile payments use. Mobile access by phone also enables using the phone's own security locking, such as fingerprint, as a part of the verification process. This option is unavailable with traditional physical transponders without a separate, often expensive biometric reader.

Mobile access and Idesco ID mobile access solutions make access control, especially access credential management, and their delivery to users much easier. So far, previous mobile access solutions in the market have been merely cloud-based services. System installers have had to implement separate cloud services for mobile access credential management parallel to their own access control system. They have had to register to this separate cloud service whenever they want to manage mobile access rights.

Idesco ID is a service for managing mobile access rights in an existing access control system where traditional, physical transponders are also managed. Indeed, it enables sending mobile credentials to users' phones directly from their own system without the need to register to parallel systems.

Mobile access with Idesco ID is an economical and environment-friendly solution, especially for temporary access rights. You don't need to assign physical plastic cards or transponders for your customers if they need access rights only for a couple of days. If you manage and assign temporary access rights for management personnel, mobile access rights are convenient; you can send them remotely to their phones, saving time and resources.

Idesco ID provides different options for using the service. If an organization regularly sends new mobile credentials to phones, continuous Idesco ID Enterprise service could be their best choice. Another option is to send mobile credentials to all phones in a lump, meaning that the Idesco ID service is used only during this transfer.

Small organizations, sending mobile credentials only occasionally, could benefit most from Idesco ID Entry level solution. There, the user first downloads the Idesco ID application, which creates a mobile credential in their phone, then lets it be read into the system by a separate Enrollment Station device, e.g., in reception.

Whatever mode of service you choose, you always manage access credentials in your own system, and Idesco ID will not become a part of your own system. Mobile app users don't need to create accounts in the cloud or manage passwords. Only their phone number or additionally also email address is needed from them, and that is only for sending the mobile credential. After sending, their phone number and email address are removed from the Idesco ID service. ■

# SOLARWINDS LAUNCHES NEW GLOBAL TRANSFORM PARTNER PROGRAM, INCLUDING SUPPORT FOR MANAGED SERVICE PROVIDERS

*Transform offers channel partners strong profit potential, significant growth opportunities, and industry-leading tools and resources*

SolarWinds (NYSE:SWI), a leading provider of simple, powerful, and secure IT management software, today announces the launch of the SolarWinds Transform Partner Program to support and drive growth for the company's valued global channel partners. The new channel program is designed to transform the way SolarWinds partners with industry-leading technology distributors, value-added resellers (VARs), global system integrators (GSIs), managed service providers (MSPs), and cloud partners around the world.

SolarWinds Transform allows partners to accelerate digital transformation for their customers through simple and AI-powered SolarWinds® observability solutions designed for today›s modern, distributed, hybrid, and multi-cloud network environments. Transform offers SolarWinds partners strong profit potential, significant growth opportunities, and world-class tools and resources. The new program provides SolarWinds partners with several benefits, including financial incentives, performance rebates, enablement and training programs, an enhanced Partner Portal, and new marketing and sales support.

"Our purpose at SolarWinds is to enrich the lives of the people we serve. For our customers, this means providing secure solutions that make managing multi-cloud environments simple and cost-effective. And for our partners, it means creating greater opportunities for shared growth," said Sudhakar Ramakrishna, president and chief executive officer (CEO) of SolarWinds. "We are building further on our monitoring leadership and are now evolving our business to deliver the best solutions in full-stack observability, service management, and database monitoring. Our exciting portfolio and value proposition enable us – and our partners – to help accelerate our customers' business transformation wherever they may go in their cloud journey."

As a vital component of the company's growth strategy, Transform provides a new model for partners to offer their clients world-class SolarWinds technology solutions through SaaS and cloud-connected, on-premises deployments. This new partner program follows the launch of SolarWinds Hybrid Cloud Observability as a comprehensive, integrated, and cost-effective solution designed to increase performance and reduce remediation time across on-premises and multi-cloud environments.

As the first solution built on the new SolarWinds Platform and leveraging the company's Secure by Design principles, Hybrid Cloud Observability helps organizations shift from reactive to proactive IT postures as they meet the challenges of hybrid IT. And with the Transform launch, SolarWinds adds a new partner category to support MSP partners with an engagement mode for MSPs ranging from the global scale to regional providers. MSPs can now offer SolarWinds Hybrid Cloud Observability to provide full-scale observability with flexible licensing and pricing models designed to offer them and their customers the flexibility and scale they value.

"We're so thankful for our amazing partners and are excited to celebrate our joint successes," said Jeff McCullough, vice president of worldwide partner sales, SolarWinds. "Our partner relationships are critical as we move forward with a bold plan to grow our business through customer-centric technology innovations. Together with our partners, we share a vision to transform the IT management software market completely."

The new program represents the company's enhanced emphasis on channel growth and development. While channel partners have been integral to the company's success throughout its more than 20-year history, Transform is the first formal SolarWinds channel program. Consistent with the company's customer-first approach, Transform was developed in close partnership with more than 2,000 existing SolarWinds partners.

With over 300,000 customers, including 498 of the top Fortune 500® companies, SolarWinds is rated a leading provider of IT[1] and network management[2] software. Customers regularly provide high ratings[3] for SolarWinds solutions across observability, network management, application performance, and database management. The company's Secure by Design initiative, designed to make SolarWinds a leader in enterprise software security, has been critical to the development of the new SolarWinds Platform, unifying observability and services management to consistently deliver simple, secure, AI-powered solutions for IT Ops, DevOps, CloudOps, and SecOps teams.

**For more information, please visit: www.solarwinds.com** ■

## UNION COMMUNITY CO., LTD. AND TOUCHLESS BIOMETRIC SYSTEMS AG SIGNED AN MOU TO EXPAND THEIR GLOBAL PARTNERSHIP


Union Community, one of the largest multi-modal biometric security solution companies in Korea, and Touchless Biometric Systems, Global Leader for touchless biometric solutions, announced that they had signed a Memorandum Of Understanding (MOU), to expand their partnership on a global level.

Through this MOU, the two companies plan to intensify their cooperation in technology and also in the distribution of their product ranges in different parts of the world. This partnership will fuel the growth and help the two companies to expand their global presence and underline their leading role in the biometric world.

Shin Yo-sik, CEO of Union Community, said, "The MOU with TBS for Union Community's global expansion is an important step to accelerate our ambitious growth plans. It will help us to further strengthen our market position."

"The two partners are highly complementary in terms of markets and offerings. While TBS is specialised in challenging and customised solutions, Union gives us access to an extended range of state-of-the-art hardware. For our customers, it's the best of two worlds." says Stefan Schaffner, CEO at TBS.

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

## PRADEO ACQUIRES YAGAAN AND STRENGTHENS ITS CYBERSECURITY SERVICES UNIFICATION STRATEGY

*By ensuring mobile device and application security from their design to their execution, Pradeo covers the entire spectrum of the mobile security chain.*

Pradeo, a leading company specialises in mobile fleet and application security, enters into exclusive negotiations for the acquisition of Yagaan, an application security software company based in France. Thus, the mobile security leader is strengthening his path toward unifying cybersecurity services by providing comprehensive expertise and solutions in the fast-growing mobile security market.
In 2021, the global mobile security market was valued at $3.96 billion1, and the global application security market was valued at $6.95 billion2, with respective projections of +20.75% and +18.3% CAGR from 2021 to 2028.

Recognised as one of the leaders in its field by the largest international analyst firms and awarded multiple times for

*continue on page 14*

the ultra-relevance of its offer, Pradeo wanted to expand its technology with a strategic component dedicated to the testing of applications' source code.

Pradeo's objective is to become the sole contact for CISOs, application developers, auditors, device manufacturers, and other cybersecurity stakeholders for all issues related to the protection of mobile applications and associated web services, as well as smartphones and tablets.
"With its European roots, Pradeo leverages its sensitivity to data privacy to take a global leadership position. The adoption of Pradeo's mobile security solutions by Fortune 500 companies is a clear endorsement of its implementation," said Nicholas J. Baugh, Best Practices Research Analyst at Frost & Sullivan.

Thanks to the acquisition of Yagaan, whose team has conceived and developed code mining, disruptive technology for auditing applications' source code, Pradeo is expanding its market share and consolidating its global development. Once again, the company proves its technological lead and can now take pride in mastering the entire mobile security value chain, from the design of mobile applications and associated web services (security by design) to the detection and response to threats targeting mobile devices.

Created in 2017, Yagaan has 10 employees who will join the Pradeo team to bring its staff count to 60. Further hirings are planned by the end of the year to support the company's growth. Yagaan teams will remain based in France.

"Europe is fortunate to have a number of extremely successful businesses in its territory. However, each of them has to compete with powerful unified offers, often foreign, which prevail because of their ease of use. European companies need to unify their services by targeting very specific markets to become global champions," said Clément Saad, Co-founder and CEO of Pradeo.

"We share with Pradeo the same taste for technological excellence and the need to unify cybersecurity solutions. By integrating Yagaan's expertise and strategic source code auditing technology, Pradeo covers the entire mobile security chain and adds web application security to its portfolio. By forging a common destiny, this move consolidates Pradeo's leadership and puts us at the forefront of the global cybersecurity market," added Hervé le Goff, CEO of Yagaan.

The amount of the transaction is not disclosed.

**For more information, please visit: www.pradeo.com ■**

## GALLAGHER DELIVERS GOLD STANDARD WITH NEW UK NATIONAL HIGH-SECURITY TEAM

Global security manufacturer, Gallagher, is delighted to announce their new United Kingdom National High-Security Team. The dedicated team, led by Jason Hunter, National High-Security Manager, will support an established high-security portfolio while growing and strengthening relationships with customers across government and critical national infrastructure sectors.

Matt Page will be supporting the team as Technical Account Manager of High Security, along with Kevin Godfrey, Strategic Business Development Manager of High Security, and Matt Wills, Technical Business Development Manager of High Security.

"With our new High-Security team in place, we're excited to continue developing the dialogue on high security while ensuring we meet the highest standards as a security manufacturer," says Richard Huison, Gallagher's Regional General Manager for the UK and Europe. "Our team brings many years of experience, with both a broad security knowledge and a strong understanding of the high-security space, to support our customers with their complex security needs."

Jason joined Gallagher in 2017, bringing over 10 years of broad security experience, including

*continue on page 15*

Hostile Vehicle Mitigation solutions in the Middle East and landmine clearance and UXO disposal for UN and multinational oil and gas organisations. Upon joining Gallagher, Jason worked closely with Kevin on perimeter solutions and, more recently, has been focussed on delivering high-security projects, as well as business development in the Southwest of England and Wales.

"I'm excited to take on this new role and am looking forward to leading our talented team to continue the great work we're already doing – supporting our customers to protect what matters most," says Jason.

*Image by rawpixel.com on Freepik*

Gallagher has long demonstrated their commitment to delivering security solutions to meet the highest standards – earlier this year, they announced they were the first manufacturer to achieve the latest Cyber Assurance for Physical Security Systems (CAPSS) 2021 standard, with their Command Centre software and High-Security Controller 6000. They are also proud to be the only security manufacturer that sits across multiple categories in the Catalogue for Security Equipment (CSE) – including Access Control, CAPSS Approved, and Detection and Tracking systems.

Furthermore, as a testament to their reputation in the high-security space, Gallagher was invited to work with the Cabinet Office in the development and testing of the GovPass standard.

**For more information, please visit: www.gallagher.com ■**

## SUCCESS FOR GJD AND THE AVA GROUP AT THE GLOBAL SECURITY EXCHANGE 2022 EXHIBITION

GJD, an Ava Group company, exhibited at the Global Security Exchange 2022 exhibition alongside its sister companies, Future Fibre Technologies (FFT) and BQT Solutions. The trade show was located at the impressive Georgia World Congress Centre in Atlanta, GA, USA, from the 12th of September to the 14th of September, 2022.

Ava Group security experts met delegates from all over the world and existing and new customers. Visitors to the booth experienced the most advanced detection technology, received knowledgeable security insights, and learnt about the benefits of external detection.

Ana Maria Sagra-Smith, GJD's Sales and Marketing Director, commented: "It was the first time GJD has exhibited at GSX, and it was a great success. Thank you to all our customers, prospective customers and partners who visited our booth over the last few days."

GJD proudly showcased its latest perimeter protection solutions consisting of IP surveillance, wired and wireless detectors, innovative LED lighting solutions and ANPR cameras. Products in the GJD range identify genuine threats and create alerts when an intruder crosses the boundary rather than when it is too late and they are already inside the premises. GJD has been providing reliable detection and intelligent deterrent solutions for the global security market for nearly 40 years. If you were not able to meet GJD at GSX, you could still learn about the company's external detectors and LED illuminators.

**For more information, please visit: www.gjd.co.uk ■**

# PRISMA CLOUD DELIVERS CONTEXT-AWARE SOFTWARE COMPOSITION ANALYSIS TO SECURE DEPLOYMENT OF OPEN SOURCE SOFTWARE

*New SCA module offers proactive vulnerability remediation based on runtime context to achieve seamless code-to-cloud security*

Open source software is a critical component of cloud-native applications, allowing developers greater speed and modularity without having to reinvent the wheel each time they code. However, as the Unit 42 Cloud Threat Report, 2H 2021 found, open-source software can often contain known vulnerabilities, which can open organizations up to significant risk. Palo Alto Networks (NASDAQ: PANW), the global cybersecurity leader, today introduced the industry's first context-aware software composition analysis (SCA) solution to help developers safely use open-source software components. The integration of SCA into Prisma® Cloud further demonstrates why Palo Alto Networks is the leading provider of cloud-native security.

Traditional SCA solutions are standalone products that can produce a large number of alerts but lack the runtime context to help fix vulnerabilities. With the addition of SCA to the Prisma Cloud platform, developers and security teams can proactively surface and prioritize known vulnerabilities that impact the application lifecycle (i.e., code, build, deploy and run). Prisma Cloud SCA delivers deep dependency detection and remediation of vulnerabilities in open-source software before applications reach production. It can also help developers prioritize remediation based on software components that are already in use. These capabilities are not possible when SCA solutions are deployed as single-point products.

"Developers leveraging open source software should be able to build applications with the confidence they aren't opening the organization up to risk," said Ankur Shah, senior vice president of Prisma Cloud, Palo Alto Networks. "With the average application consisting of 75% open source components, SCA on Prisma Cloud is key to protecting the organization from code to cloud and empowering developers to build with speed."

As a complete cloud-native application protection platform (CNAPP), Prisma Cloud is context-aware at every stage of the application lifecycle to provide a unified view of risk across organizations' cloud environments. Where current approaches to cloud security rely on siloed products that provide intermittent visibility without remediation, Prisma Cloud approaches cloud security with a comprehensive, prevention-first framework. With a 188% increase in cloud incident response cases over the past three years, this shift in approach has become mandatory.

A complete code-to-cloud CNAPP needs to incorporate the following five key principles in order to keep organizations safe:

- Security from code to cloud — protects applications at every stage of the development lifecycle — from code, build, deploy and run.
- Continuous, real-time visibility — uses real-time and contextual security analysis of cloud environments to help prevent misconfigurations, vulnerabilities, and threats.
- Prevention-first protection — stopping attacks and defending against zero-day vulnerabilities to drive down mean time to remediation.
- The choice for every cloud journey — aligning security needs with current and future cloud priorities by supporting a breadth of cloud service providers, workload architectures, continuous integration and continuous delivery (CI/CD) pipelines, integrated development environments (IDEs), and repositories with a unified platform
- Cloud scale security — consistently secures applications as cloud environments scale.

In addition to SCA and to further increase the safety of cloud-native applications, Prisma Cloud introduced a software bill of materials (SBOM), among other capabilities, for developers to easily maintain and reference a complete codebase inventory of every application component used across cloud environments. Implementing SCA and SBOM ensures Prisma Cloud aligns with these principles.

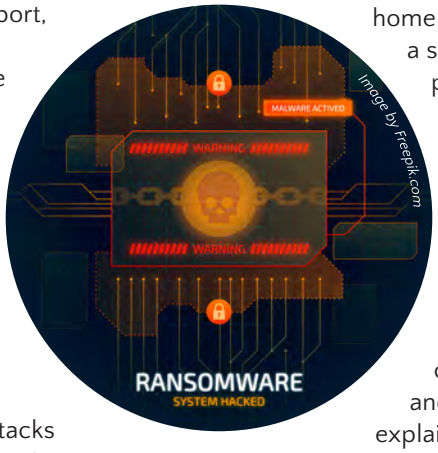
"Buyers looking for cloud-native security solutions need to keep the requirements of microservices security protection in mind. The 'bolted-on' and 'whack-a-mole' approaches are a thing of the past," said Frank Dickson, program vice president, Security, and Trust at IDC. "Security should be embedded throughout the application development life cycle. This means that buyers need to fundamentally change their approach to security; although they need to continue to protect their run-time environments, they must also embrace solutions that embed security in the application development process, an approach referred to as 'shift left.' Shift left requires one to think less about security products and more about continuous security processes."

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

# ESET THREAT REPORT T2 2022: RDP ATTACKS SEE FURTHER DROP; RANSOMWARE LOSES WAR-RELATED MESSAGING

- Following a sharp decline observed in T1 2022, the total number of RDP attack attempts declined by a further 89%; the likely reasons for the decline are post-COVID return to offices, improved security, and the Russia-Ukraine war.
- China (76%), Singapore (41.3%), and Russia (30%) had the highest ratio of spam emails.
- Politically motivated ransomware declined; operators turned their attention from Russia back to their usual targets, such as the United States, China, and Israel.
- Emotet continued to be active, with detections seen mainly in Japan and Italy; according to ESET telemetry, its operators took time off in August.
- ESET phishing feeds revealed a sixfold increase in shipping-themed phishing URLs, with the most commonly impersonated brands being USPS and DHL.
- Web skimmer known as Magecart constituted three-fourths of all banking malware detections, leaving far behind the rest of the malware strains in the category.
- Cryptocurrency threats went down along with the price of bitcoin; however, the previously declining category of Cryptostealers grew by almost 50%.

ESET released today its T2 2022 Threat Report, summarising key statistics from ESET detection systems and highlighting notable examples of ESET's cybersecurity research. The latest issue of the ESET Threat Report (covering May to August 2022) sheds light on the changes in ideologically motivated ransomware, Emotet activity, the most-used phishing lures, how the plummeting cryptocurrency exchange rates affected online threats, and the continuation of the sharp decline of Remote Desktop Protocol (RDP) attacks. ESET analysts think these attacks continued to lose their steam due to the Russia-Ukraine war, along with the post-COVID return to offices and overall improved security of corporate environments.




Even with declining numbers, Russian IP addresses continued to be responsible for the largest portion of RDP attacks. "In T1 2022, Russia was also the country that was most targeted by ransomware, with some of the attacks being politically or ideologically motivated by the war. However, ESET Threat Report T2 2022 shows that this hacktivism wave has declined in T2, and ransomware operators turned their attention towards the United States, China, and Israel," explains Roman Kovác, Chief Research Officer at ESET.

According to ESET telemetry, August was a vacation month for the operators of Emotet, the most influential downloader strain. The gang behind it also adapted to Microsoft's decision to disable VBA macros in documents originating from the internet and focused on campaigns based on weaponized Microsoft Office files and LNK files. The report also examines threats primarily impacting home users. ESET phishing feeds showed a sixfold increase in shipping-themed phishing lures, most of the time presenting the victims with fake DHL and USPS requests to verify shipping addresses. "In terms of threats directly affecting virtual and physical currencies, a web skimmer known as Magecart remains the leading threat going after online shoppers' credit card details. We also saw a twofold increase in cryptocurrency-themed phishing lures and a rising number of cryptostealers," explains Kovác.

The ESET T2 2022 Threat Report also reviews the most important findings and achievements by ESET researchers. They uncovered a previously unknown macOS backdoor and later attributed it to ScarCruft, discovered an updated version of the Sandworm APT group's ArguePatch malware loader, uncovered Lazarus payloads in trojanised apps, and analyzed an instance of the Lazarus Operation In(ter)ception campaign targeting macOS devices while spearphishing in crypto-waters. ESET researchers also discovered buffer overflow vulnerabilities in Lenovo UEFI firmware and a new campaign using a fake Salesforce update as a lure.

Besides these findings, the report also summarises the many talks ESET researchers have given in recent months and introduces talks planned for AVAR, Ekoparty, and many other conferences.

**For more information, please visit: https://www.welivesecurity.com/2022/10/05/eset-threat-report-t2-2022/** ■

## SAFETURE SIGN RISK INTELLIGENCE PROVIDER RISKLINE

Safeture has signed Danish risk intelligence company Riskline as a content provider.
The Riskline agreement underlines Safeture's offer as an open tech solution and as "risk intelligence agnostic."

Riskline is one of the world's leading travel risk insights companies leveraging AI and professional analysts to process more than 100,000 data sources providing accurate and timely risk assessments. In a world characterized by geopolitical uncertainty and potentially challenging and risky situations, updated, accurate data is required to act quickly. The Riskline collaboration will strengthen the functionality and dynamic of Safeture's platform as it adds risk intelligence sources, allowing the customers to choose or add different risk intelligence sources to the platform and thereby have a unified view that will benefit their overall risk management.
"Riskline has been on our radar for a long time. As we have moved forward with our open tech solution and to become "risk intelligence agnostic," a collaboration was made possible. By offering Riskline's world-class intelligence to our tech platform for mass communication and positioning, the agreement will open for business opportunities globally," says Magnus Hultman, CEO of Safeture.

"It is great to enter into a partnership with another Nordic company that helps keep people safe and informed worldwide through its emphasis on providing high-quality duty-of-care solutions. Our information will allow Safeture users to make smarter decisions in an increasingly volatile risk environment" - Kennet Nordlien, CEO of Riskline.

Through this new collaboration, more organizations and businesses will be better equipped to support their employees, manage potential risks of sending people overseas, and proactively prepare themselves based on up-to-date live information.
Safeture continues to evaluate intelligence providers to give customers the best possible intelligence opportunities and emphasize the benefits of an open tech solution.

**For more information, please visit: www.safeture.com.** ■

## TECH COMPANIES SHOULD PREPARE FOR THE NEXT WAVE OF UNKNOWNS, SAYS DELOITTE INDUSTRY LEADER

*Amidst supply chain disruptions, Yang Chi Chih recommends that companies review channel performance and relationships with partners.*

Deloitte Southeast Asia's Technology, Media & Telecommunications Industry Leader Yang Chi Chih has more than two decades of public accounting experience in serving local, multinational, and listed companies in Singapore and the United States.

He has advised companies on their initial public offerings on the Singapore Exchange and led teams in system audits to identify improvement areas in accounting and reporting systems. Chi Chih has been involved in audit and assurance work with telecommunications and technology companies in Singapore, Southeast Asia, and South Asia over the past 15 years.


Chi Chih is also adept in International Financial Reporting Standards reporting engagements and has conducted seminars on changes and updates on financial reporting standards.

As one of the esteemed judges in this year's Asian Technology Excellence Awards, he has provided insights for aspiring auditors and startup entrepreneurs on career milestones and securing funding for the business. He has also discussed the current state of the Technology, Media & Telecommunications industry and how it evolved over the years.

### What are your career milestones from your experience as an audit professional, and what advice would you give aspiring auditors?

Besides being admitted to the Partnership, my secondment to the Deloitte US firm as a manager was one of the significant milestones in my

*continue on page 19*

career. The experience allowed me to not only widen my network and build connections with other professionals in the industry but also deepened my perspectives on the profession.

I would advise aspiring auditors to proactively seek opportunities and make full use of them when they come along. You should also take ownership of your career and always strive for continuous learning to remain relevant in this competitive global market. Never be afraid to step out of your comfort zone and embrace challenges; these are [the] best opportunities to help you grow and develop. Lastly, I would recommend aspiring auditors to network and build a relationship with professionals across all industries to better understand the business's commercial side.

### What advice would you give startup entrepreneurs who are in the process of securing funding?

They should be clear on their business plan and the objectives of securing funding, i.e., how will the funds help to propel growth? Why should investors support your venture instead of your competitors?

In some cases, taking external funds would typically mean having to meet aggressive revenue goals and financial milestones. Startup entrepreneurs must be prepared to be accountable for meeting the investors' objectives.

Given the increased demand for internet connectivity brought by the pandemic, what are the latest advancements in the telecommunications industry?

The pandemic has brought an increase in demand for faster broadband connectivity and new services. Consumers are now more technology-centric, especially with the prevalence of digital customers. This has resulted in the need for telecommunication operators to double down on both business and digital transformation.

According to Deloitte's 2021 advanced wireless survey, three-quarters of key decision-makers believe that advanced wireless communications could create a significant competitive advantage for their organization. Wi-Fi 6 and 5G technology are already seen as the most critical wireless technologies, and their importance will continue to grow, especially in the enterprise market.

### How has the Technology, Media & Telecommunications Industry changed in Southeast and South Asia in the last 5 years?

The rise in network traffic during the pandemic has not translated to higher revenues for telecommunications operators in the region. Factors such as travel restrictions hampered roaming revenues, and telecommunications operators are also facing declining profits due to Over-the-top (OTT) players, who typically do not have to invest huge capital expenditure in network infrastructure and do not consume extensive bandwidth on the network.

In terms of the media, people sought more entertainment at home as they tend to avoid larger in-person events due to lockdowns and social distancing rules. The competition amongst streaming video-on-demand (SVOD) providers for the time, attention, and bank accounts of viewers will continue, fueled by customers with multiple subscriptions, greater cost sensitivity and savviness, and generational differences in entertainment preferences.

As remote or hybrid work becomes commonplace, chipmakers should look towards building more plants in more places to keep up with the demand, and we expect to see more semiconductor factories in Southeast Asia as companies seek to diversify and build resilience in their supply chain. With supply chain disruptions extending far beyond the semiconductor sector, technology companies will also need to start preparing for the next wave of unknowns by working with their partners to review channel performance and relationships, change and adapt channel programs, and figure out new ways to go to market together.

Several telecommunications operators in Southeast Asia have started to invest in digital and enterprise services to diversify beyond connectivity services. However, the pace of development has not caught up with the likes of leading telecommunications operators in [the] United States and Europe. Lured by the potential benefits of new advanced use cases, enterprise interest in 5G edge computing applications and private cellular networks is beginning to emerge. Whilst the supplier ecosystem and business model for delivering enterprise-oriented 5G edge computing and private network solutions remain undefined and fluid, they may start solidifying within the year. With many other players, such as networking equipment companies, hyperscalers, and system integrators vying for market share, operators will need to act quickly to define how they should best participate in this emerging market.

### What emerging technologies can we expect to see and hear about more in the next few years?

At Deloitte, we expect to see more enterprise use cases being developed and applied to the following up-and-coming areas, such as the Metaverse. Artificial Intelligence and Machine Learning will continue to be key trends. It is also anticipated that Digital Reality (such as Augmented Reality and Digital Twin) will become more mainstream in enterprise applications. ■

# SECURONIX DETECTS NEW COVERT ATTACK CAMPAIGN TARGETING MILITARY CONTRACTORS

Securonix Threat Research team recently discovered a new covert attack campaign targeting multiple military/weapons contractor companies, including likely a strategic supplier to the F-35 Lightning II fighter aircraft. The stager mostly employed the use of PowerShell, and while stagers written in PowerShell are not unique, the procedures involved featured an array of interesting tactics, persistence methodology, counter-forensics, and layers upon layers of obfuscation to hide its code.

Additionally, the remote infrastructure or command and control (C2) involved with the stager was relatively sophisticated.

## Target Analysis and Attack Chain

The attack started in the late summer of 2022 and targeted at least two high-profile military contractor companies.

The overall attack chain can be seen in figure 1 below, which highlights the initial compromise phase of the attack.

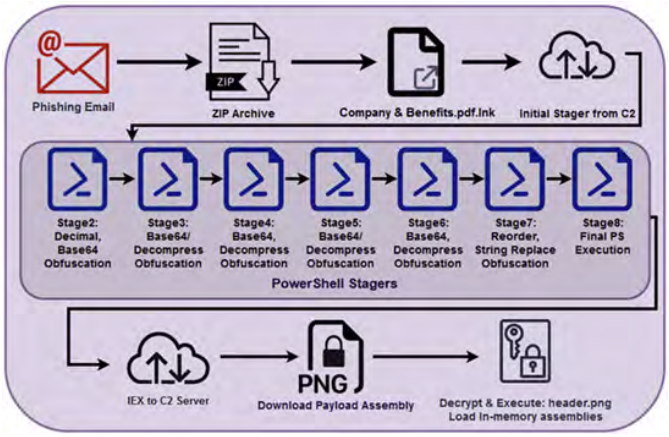



**Figure 1: Attack Chain**

## Initial Infection: Shortcut to Code Execution

As with a lot of targeted campaigns, the initial infection begins with a phishing email sent to the target containing a malicious attachment. Similar to that of the STIFF#BIZON campaign reported earlier this year, the phishing email contains a compressed file containing a shortcut file, in this case, "Company & Benefits.lnk."

The shortcut file does some tricky things to avoid detection. First, it attempts to hide its execution by calling forfiles rather than cmd.exe or powershell.exe.

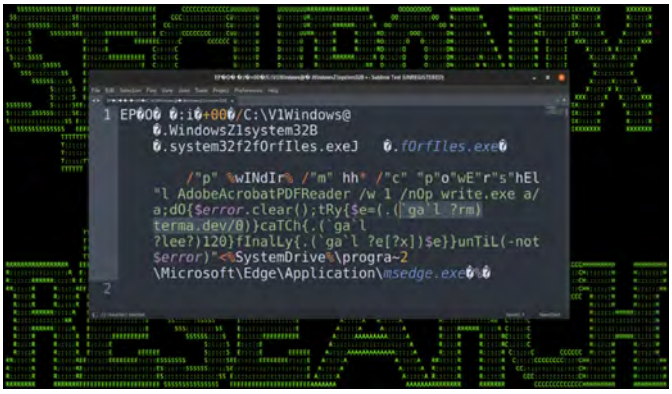


**Figure 2: Company & Benefits.pdf.lnk**

It then takes the powershell.exe executable file, copies it to C:\Windows, renames it to AdobeAcrobatPDFReader, and then uses it to execute the rest of the PowerShell string. Logs generated from Sysinternals Sysmon identify this in figure 3 below.

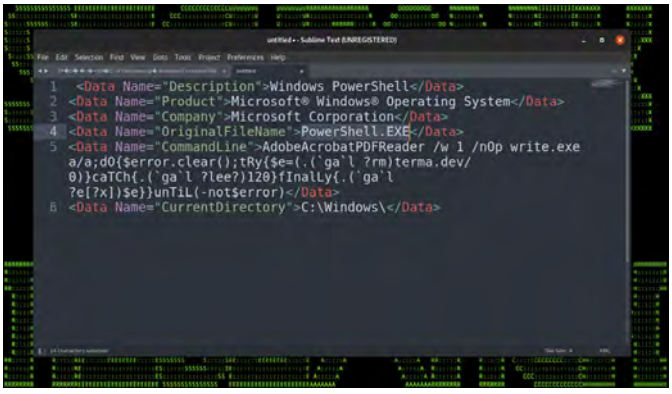


**Figure 3: Windows logs showing renamed PowerShell.exe**

The rest of the powershell script runs on a loop with a 120-second timeout or until an error is not produced. C2 communication is attempted at the URL: hxxps://terma[.]dev/0 to pull down the initial stager.

## Conclusion

Overall, it is clear that this attack was relatively sophisticated, with the malicious threat actor paying specific attention to opsec. There were a lot of relatively recent attack techniques at play, some of which were unfamiliar and required additional analysis, such as leveraging the PowerShell Get-Alias commandlet to perform an invoke expression.

Leveraging the registry, WMI subscriptions, scheduled

*continue on page 21*

tasks, and incorporating Lolbins with the process was overall clever and needs to be monitored for. While this was a very targeted attack, the tactics and techniques used are well-known, and it is important to stay vigilant.

### Securonix Recommendations and Mitigations

- Avoid downloading unknown email attachments / lnk files from non-trusted sources.
- Deploy PowerShell script block logging to assist in detections.
- Deploy additional process-level logging, such as Sysmon, for additional log coverage. Additionally, sysmon installed on the host will prevent next-stage payload execution.
- Pay specific attention to attempts to disable security monitoring tools, including SIEM.
- Scan endpoints using the Securonix seeder hunting queries below.

### MITRE ATT&CK Techniques

| Tactics | Techniques |
|---|---|
| **Initial Access** | T1566: Phishing |
| **Defense Evasion** | T1027: Obfuscated Files or Information |
| | T1140: Deobfuscate/Decode Files or Information |
| | T1202: Indirect Command Execution |
| | T1005: Data from Local System |
| | T1562.001: Impair Defenses: Disable or Modify Tools |
| | T1112: Modify Registry |
| **Execution** | T1059.001: Command and Scripting Interpreter: PowerShell |
| | T1047: Windows Management Instrumentation |
| **Persistence** | T1547: Boot or Logon Autostart Execution |
| | T1053: Scheduled Task/Job |
| | T1053.005: Scheduled Task/Job: Scheduled TaskT1546.003: Event Triggered Execution: Windows Management Instrumentation Event Subscription |

**For more information, please visit: www.securonix.com ■**

# KANSAS CITY INTERNATIONAL AIRPORT'S SUPERIOR CUSTOMER EXPERIENCE JOURNEY BEGINS AND ENDS IN THE PARKING GARAGE

TKH Security (formerly Park Assist) has begun installing the previously awarded Automated Parking Guidance System (APGS) contract through JE Dunn Construction in conjunction with the Kansas City Aviation Department (KCAD) in Kansas City, MO. Landing in spring 2023, the Kansas City Aviation Department will open a new single terminal representing a total transformation of Kansas City's air passenger experience. Part of this project will be a 6,219-space parking garage with a location adjacent to the terminal, plus dedicated curb spaces for taxis and ride-sharing platforms and shuttles; all planned to maintain Kansas City International's convenient experience as travelers arrive and depart.

"We're excited to add this technology to our parking garage for the new terminal. Our customers will feel the biggest positive impact. Year to date, our passenger count is up 35 percent, and for most of them, the parking garage is the first and last touchpoint. We wanted to extend our superior customer experience to this area," said the Manager of Parking Services, Katy Sell. "The APGS also will allow us to maximize utilization of our parking facilities. The constant stream of data analytics will assist with parking garage operation efficiency."

With TKH Security's new smart-sensor M5 camera-based APGS, customers will have the means to efficiently find an available parking space. Each smart sensor can monitor up to six parking spaces simultaneously. The bright, red, and green color-coded LED lights on

*continue on page 22*

the smart sensors instantly visually direct motorists to available spaces. Reducing time to park by up to 63%, the APGS will help travelers arrive at their gates quickly.

"I am very excited to have our company selected for this project. The Kansas City Aviation Department developed a new terminal that meets the public's expectations of superior customer experience and ease of finding open parking spaces while reducing the carbon footprint of both the airport and vehicles," said Regional Account Manager Jeff Sparrow. "This custom package of smart-sensor products Kansas City Airport chose is another example of how they put travelers first."

**Image credit Build KCI**

Kansas City International Airport's APGS package also includes:

- VMS NAV signs, which will be placed at key decision points for drivers to assist with wayfinding,
- S2, which allows parking management to monitor surface lots,
- Park Alerts, which notify operators when certain vehicles enter the building, including VIP passengers,
- Park Finder, which helps drivers find their vehicle in seconds,
- And an API package that provides the Aviation Department with a secure connection to a limitless set of third-party parking-related solutions.

On the Kansas City International Airport project, TKH Security is proud to also partner with JE Dunn, Structure Inc., TIBA, Max Electric, and American Legacy.

**For more information, please visit: www. tkhsecurity.com ■**

## OKTA STUDY REVEALS GROWING NUMBER OF APAC ORGANIZATIONS EMBRACING ZERO TRUST, AND NEARLY ALL RECOGNISE THE IMPORTANCE OF IDENTITY TO NEXT-GENERATION SECURITY

*Zero Trust Security helps organizations thrive in the era of hybrid work and increasingly sophisticated cyber threats*

Okta, Inc. (NASDAQ: OKTA), one of the leading independent identity providers, today revealed that a growing number of Asia-Pacific (APAC) organizations are embracing Zero Trust Security initiatives to overcome the challenges of today's dynamic cyber threat landscape.

The State of Zero Trust Security in Asia Pacific 2022 report, commissioned by Okta and conducted by Pulse Q&A, found that the percentage of APAC organizations that had implemented a Zero Trust Security initiative had grown by 18 points from the 2021 figure to reach 50%. While the rate of Zero Trust adoption among APAC organizations (18% YoY growth) was lower than the global figure (31% YoY growth), almost all (96%) respondents in APAC have a defined Zero Trust security initiative in play or plan for 2022.

The report also found that APAC organizations were slower to recognize the importance of leaving passwords behind in the quest for stronger security and identity and access management (IAM) to combat increasingly sophisticated cyber threats. Of all organizations worldwide, those in APAC had the lowest adoption of passwordless access, with only 0.5% having implemented it and only 10% planning to implement it in the next 18 months.

There is a growing consensus among global organizational thinking that an identity-first approach to Zero Trust is not only paramount but essential. This allows organizations to fully leverage identity and access management (IAM) by integrating it with other critical security solutions into a powerful central control point for intelligently governing

*continue on page 23*

access among users, devices, data, and networks. The research found that 80% of global organizations consider identity important to their overall Zero Trust security strategy, and an additional 19% say identity is business critical. APAC respondents rated the importance of identity to their overall Zero Trust security strategy at 83%, while an additional 15% say identity is business critical.

While securing data, networks and devices continues to rank as the top priority among surveyed organizations; a growing proportion recognizes the importance of people to an identity-centric security model. The report found organizations in the APAC region place a greater emphasis on automating the provisioning and de-provisioning of employees and working on privileged access for cloud infrastructure over the coming 18 months. The responses forecast an increase from 22% to 76% adoption and from 43.5% to 88% adoption, respectively.

## Nearly all APAC organizations acknowledge identity is key to Zero Trust Security

"By adopting Zero Trust Security, organizations can position themselves to overcome the challenges presented by hybrid work–including mobile and remote working–by adopting an identity-centric approach to network and resource access rather than relying on outdated security models based on the traditional network perimeter," says Ben Goodman, SVP and General Manager for the Asia Pacific, Okta. "Our research showed that while APAC organizations lagged behind their global counterparts in implementing Zero Trust Security, 98% of respondents recognized that identity was important or business-critical to that approach."

Despite the concept of Zero Trust Security being discussed as early as 2009, many APAC organizations and leaders lack an understanding of its benefits. This elevates risk in an environment of increasingly sophisticated security threats.

However, most APAC organizations are acutely aware of the need to stop malicious actors from compromising their people, systems, and data to the extent that 75% of those surveyed prioritized security over the useability of business-critical applications and resources, unlike most of their global counterparts.

Of those APAC organizations that have yet to implement a Zero Trust Security initiative, 38% said they planned to do so over the next six to 12 months.

Unfortunately, as with many ICT projects, the global talent crunch presents a sizable challenge; 31% of APAC organizations cited talent and skills shortages as a challenge, followed by a lack of stakeholder buy-in and lack of awareness of Zero Trust Security solutions, both cited by 18% of respondents.

*Image by rawpixel.com on Freepik*

## Investment commitments in Zero Trust Security Upheld

The report found that APAC organizations typically followed through on their 2021 commitments to invest in Zero Trust Security. Last year, 76% of regional organizations pledged to increase their Zero Trust Security budgets moderately or significantly, and 82% of APAC organizations in this year's survey reported a moderate or significant increase.

Zero Trust Security is a security framework based on the assumption that every user, device, and IP address accessing a resource is a threat until proven otherwise and requires organizations to implement rigorous security controls to verify anything that attempts to connect to the corporate network. The rapid take-up of mobile, cloud, and hybrid working has put pressure on organizations to replace increasingly redundant 'castle and moat' security models with more agile, holistic approaches centered on identity. In the context of Zero Trust Security, identity is an actor–whether human or process–that wants access to data for purposes that include retrieval, deletion, and modification. With an identity-centric approach, organizations can give the right people the right level of access to the right resources in the right context, with access assessed continuously.

To complete the State of Zero Trust Security in Asia Pacific 2022 report–which assesses the maturity of identity and access management in APAC organizations and where they reside on the journey towards a full Zero Trust security posture–Pulse Q&A surveyed 200 security leaders across the region. The survey questionnaire covered the Zero Trust initiatives organizations had in place and how they planned to prioritize these over the near and long term.

**For more information, please visit: www.okta.com** ■

# ADDRESSING DATA TRANSFORMATION CHALLENGES AT BIG DATA & AI WORLD 2022

- 87% of APAC financial services organizations are frustrated by data in driving decision-making
- Creative data technology provider InterSystems to share insights on data transformation and how to unlock its true potential
- Big Data & AI World - Asia's most anticipated big data, analytics, and artificial intelligence event

While businesses are focusing on improving operational efficiency, they are struggling with messy data in disparate silos, shifting regulatory environments, and governance priorities. 87% of Asia-Pacific (APAC) financial services organizations are frustrated trying to use their data to drive decision-making, according to InterSystems' latest study, "The Top Data and Technology Challenges in Financial Services Across Asia Pacific."

This major concern will be addressed at the Big Data & AI World 2022 event held from 12th to 13th October 2022 at Marina Bay Sands, Singapore. It is the 5th edition of Asia's most exciting big data, analytics, and artificial intelligence event. The award-winning event connects data and AI innovators, technologists, and business leaders, to help make data-driven decisions and intelligently shape their businesses.

Many Asia-Pacific (APAC) companies are trying to transform into data-led organizations. However, it is proving far more complicated than their leaders expect, and delivering the right data to support critical business needs is becoming increasingly challenging. Volumes and varieties of data are often spread across multiple systems within a business and may be stored in inconsistent formats with different naming conventions.

The main challenges are ensuring the data gathered is accurate, making sense of it, and turning it into practical and innovative solutions. Kenneth Kuek, Country Lead at InterSystems, Singapore, will address these issues in his keynote presentation entitled "The Data Management Secrets Behind Successful AI Initiatives." He will share insights on data transformation and how organizations can unlock their true potential to innovate and become more productive and agile.

"Everyone is talking about being data-led, but very few are actually able to practice data-first decision-making. While many institutions across APAC strive to give their best value to customers and would like to respond promptly to critical business needs, they struggle with data silos and outdated data," said Kuek.

Based on the same InterSystems survey in 2022 with business leaders of financial services across the APAC region, 98% of organizations recognized that there are data and application silos within their organization, but when it comes to priorities, only 54% are looking to master data management in the next 12 months across APAC.

"This impacts their business significantly more than most companies realize because leaders don't have real-time information, hence need to make assumptions. It also makes it difficult for them to clearly understand enterprise-level risk. Dysfunctional data management also means loss of competitive advantage and difficulty in complying with rapidly changing data regulations," he highlighted.

To complicate things further, many companies in the region paradoxically want more data while already struggling with current data management. APAC is set to be the fast-growing economy at the forefront of the global digital landscape, with data transformation as a key driving factor. But the risk is instead of offering a competitive advantage, data becomes a burden due to various barriers. These include data skills gaps, data silos, manual processes, business silos, and data privacy and security weaknesses.

"However, within these challenges lies an opportunity. Building an ecosystem that is truly efficient and transforming the way businesses use data will unlock their full potential. The first three steps to prioritize in data transformation is to replace legacy systems, gain access to real-time data and improve regulatory compliance," added Kuek.

Participants of Big Data & AI World 2022 can find out more about solving data transformation challenges at Kenneth Kuek's keynote address at the AI theatre session on the event's first day. InterSystems is a provider of next-generation solutions dedicated to helping customers solve the most critical data challenges.

Also, on the event's first day, Kuek will be conducting a 60-minute interactive workshop alongside Bryan Hoon, Sales Engineer from InterSystems, on "How Next Generation Architectures Are Driving Trusted Business Insights and Innovation." They will walk participants through some of the largest projects that InterSystems are working on to unify multiple data sources, bringing complete visibility in real-time to teams when they need it the most to make strategic decisions. ■

# WHY NOW IS THE PERFECT TIME TO UPGRADE YOUR CUSTOMERS' OUTDOOR CONTROLLED SECURITY LIGHTING

With the soaring cost of living and the nights getting darker, it is so important to make sure your customers' properties are protected against theft and crime. Motion detector-activated outdoor security lighting provides strong intruder deterrent solutions, protects properties from theft, and provides reliable, high-quality visible lighting.

## Peace of mind and increased safety

External security lighting is essential to deter intruders from entering or vandalizing properties. Sufficient lighting ensures that intruders are reliably detected and clearly identified on CCTV. It is also used to illuminate dark spots around the property.

It is important to remember, that in addition to having controlled security lighting in areas where crime is high, security lighting is also crucial in areas with low crime rates, as it is common for expensive homes and cars to be regular targets for theft and vandalism. With the cost-of-living rise and the festive season fast approaching, there are many more opportunistic burglars, so it is crucial to ensure your customers have sufficient and reliable security lighting.

- Security lighting provides a clear field of view around the external area of the property; this makes it easy to see people who may be trespassing.
- Security lighting makes it safe for people who are entering the property in the dark, as trip hazards are reduced.
- Smart timer functions can create an occupancy pattern, which will discourage burglars from targeting a property.
- Security lighting makes people feel much more comfortable going outside when it is dark or in the early hours of the morning.

## Applications

Controlled Security lighting is perfect for a wide range of sectors, including residential, commercial, and industrial sectors. It is perfect for a variety of applications to illuminate the front of houses, driveways, roads, pathways, alleyways, and car parking.

## Key Features

Lights can be set on and off via a timer; this is particularly helpful in deterring intruders, as homes that are unoccupied or not displaying lights are more likely to be burgled. GJD's security lighting products use energy-efficient technology, which means the end customer can keep costs as low as possible. Another key feature is the programmable functions, so the installer and end customer can easily program the controllers to function exactly how they need it to.

GJD's security lighting systems will provide the end customer with an audible warning of potential intruders. Last but not least, GJD's security lighting controllers can control up to four zones with one single control unit. This can be easily expanded to extend lighting with additional expansion units.

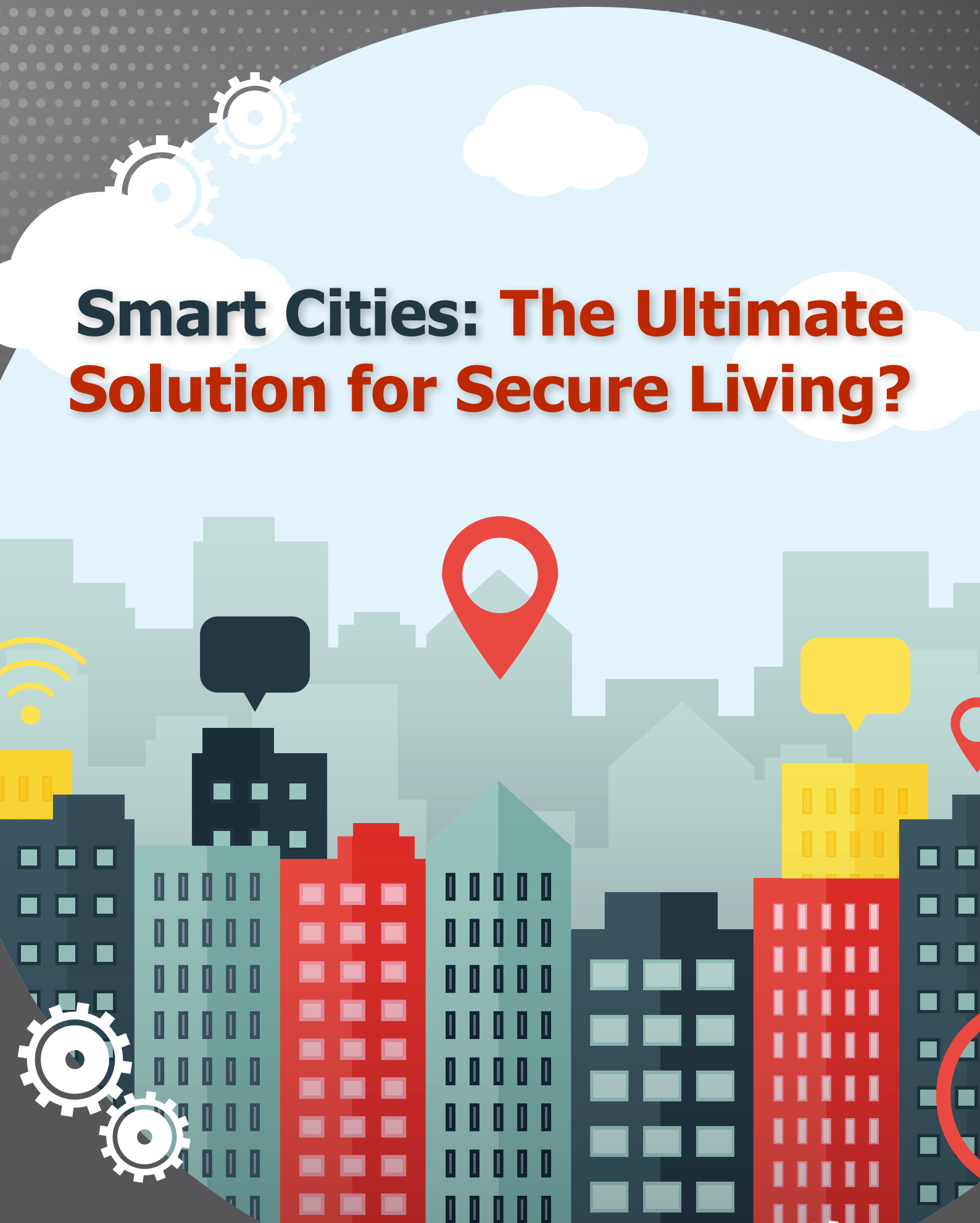
## Benefits

- The end-user may benefit from reduced insurance costs.
- Well-lit areas significantly reduce the chances of a break-in occurring.
- Perfect for deterring, detecting, and clearly identifying intruders.
- Energy-efficient and cost-effective.

GJD's energy-efficient security lighting systems enable the user to monitor, control, and switch outdoor lighting for separate zones.

**For more information, please visit: www.gjd.co.uk ■**

# Smart Cities: The Ultimate Solution for Secure Living?



We all know that our planet is in trouble. Climate change is real, and it's transpiring right now. The effects are already being felt by humans and animals alike, and things will only worsen if we don't do something about it. But what can we do?

One solution that has been gaining much traction lately is the concept of smart cities. According to the United Nations, 68% of the world's population is projected to live in urban areas by 2050. With this rapid urbanization comes the need for sustainable living solutions that can help accommodate the influx of people. By employing technology to create more efficient systems, smart cities have the potential to drastically reduce our carbon footprint and help us live more sustainable and secure lives.

Below, we will explore what exactly a smart city is and how it can be the ultimate solution for secure living. We will also discuss some challenges that need to be overcome before smart cities can become a reality.

## What Factors Demarcate a City as Smart City?

Smart city designers employ cutting-edge technologies such as mobile cloud computing, electronics, networks, sensors, and machine learning to enable the disparate parts of smart cities to collaborate and engage with the network architecture. This leads to enhanced efficiency and effectiveness of city services, a higher quality of life for those who live there, and a more sustainable environment overall.

For a city to be considered "smart," it must have four essential characteristics:

- **An intelligent transportation system:** A smart city will have a transportation system that uses advanced technologies to move people and goods efficiently. This could include things like electric vehicles, self-driving cars, ride-sharing, and bike-sharing.
- **A digital infrastructure:** A secure digital infrastructure that allows for the easy exchange of information between different parts of the city is a must. This means it can contain wireless networks, broadband internet, and cloud computing.
- **Sustainable development:** Smart cities will use renewable energy sources, green building practices, and efficient water management systems.
- **Smart governance:** There should be a government that uses data and technology to make informed decisions about allocating resources. For instance, a city can use big data to identify social issues or sensors to monitor environmental conditions.

## Supporting Actors of Smart Cities

When a smart city becomes more established, the need for additional support to maintain and improve infrastructure, services, and quality of life becomes apparent. Just as a city cannot function without its supporting cast of water and electricity providers, police and fire departments, and transportation systems, a smart city cannot function without its own supporting actors.

These supporting actors of smart cities can be divided into three main categories:

- Technology providers
- Service providers
- FinTech companies

Technology providers are the companies that develop and provide the hardware and software that form any smart city's backbone. This includes everything from sensors and data collection devices to cloud-based analytics platforms. Service providers are the companies that manage and operate the various

services that make up a smart city, such as public transportation, waste management, energy management, etc. FinTech companies are the financial technology firms that provide the financing and investment capital needed to build and operate a smart city.

Each of these categories of supporting actors is essential to the success of a smart city. Without technology providers, there would be no way to collect or analyze the data needed to make informed decisions about improving efficiency and quality of life. Without service providers, there would be no one to actually implement those improvements. And without FinTech companies, there would be no way to finance the construction or operation of a smart city in the first place.

Even the experts in the field are expressing their views on how private sectors are helping boost the development of smart cities. Alice Charles, Head of Cities & Real Estate at the WEF (World Economic Forum), said that the transitioning role of the private sector in smart cities from "selling widgets and gadgets to the cities" to "promoting an outcome-driven model." Businesses are focusing on technologies that allow urban leaders to achieve their goals. This model requires stronger collaborations among cities, the private sector, civil society, and academia. Illustrations include the Smart Cities Challenge by Infrastructure Canada, City Possible by Mastercard, and the Helsinki Energy Challenge.

*Image by vectorpouch on Freepik*

**A smart city employs technology and data to improve the efficiency of urban systems and the quality of life for its citizens. Using things like sensors, big data, and artificial intelligence, a smart city can make informed decisions about how to allocate resources to improve the city's functioning as a whole.**

## Smart Cities' Benefits

A smart city employs technology and data to improve the efficiency of urban systems and the quality of life for its citizens. Using things like sensors, big data, and artificial intelligence, a smart city can make informed decisions about how to allocate resources to improve the city's functioning as a whole.

Some of the ways that a smart city can help its citizens include:

- **Public safety:** A smart city can use data and technology to improve the efficiency of its emergency response systems. This could include using sensors to monitor traffic conditions and identify accidents or AI to dispatch the nearest available ambulance.
- **Transportation:** Public sectors can use sensors to monitor traffic conditions and identify congestion or use AI to optimize public transportation routes.
- **Energy efficiency:** Data analysis can be used to identify energy-saving opportunities, such as better management of street lighting or more efficient use of air conditioning.
- **Waste management:** Sensors can help to monitor the level of garbage in bins and optimize pick-up schedules. AI can be utilized to identify patterns in waste generation and recycling.
- **Improved healthcare:** IoT in healthcare promises to connect data collected from smart devices and sensors to obtain valuable insights. Technology may play a vital role in healthcare observation and assist

with the early detection of health problems.
- **Enhanced education:** Technology can personalize learning, make classrooms more interactive, and improve communication between teachers and students.

When all these factors are achieved, the citizens' quality of life automatically improves.

## Relation between Smart Cities and the Privacy & Security of Residents

Mobile devices are the primary means of interacting with a smart city's network infrastructure, but they also present new challenges to the security and privacy of users. Their data could be vulnerable to attack by third parties. Abi Sen's study, "Preserving Privacy of Smart Cities Based on Fog Computing," proposed using fog computing properties – such as caching, cooperating, and acting as a broker between users – in conjunction with the cloud to mitigate these security threats.

The study proposed three new ways to protect the privacy of mobile devices within smart cities.

- The first way used foggy dummies to obscure the user;
- The second employed a blind third party where trust is established between them to guard against server providers;
- And lastly, the third approach utilized a double foggy cache so that traditional cooperation could settle any issues arising from distrust between peers.

Abi Sen's work suggests the benefits of these strategies without the need to completely trust the party. According to the authors, there is less overhead than private information retrieval, and the service provider cannot gather data on user behavior.

Furthermore, privacy-preserving authentication (PPA) protocols have

emerged as a promising cryptographic approach to provide both authentication and privacy protection features for smart cities. The research, "Security and Privacy of P2P Networks in Emerging Smart City," conducted by Hongwei Li, aimed to compare the suitability of the PPA protocol for mobile services within a smart city context. The findings illustrated that the proposed PPA protocol would require less computation and communication than other competing protocols when deployed in smart city mobile application applications.

The IoT also has an important position in smart city infrastructure as it handles data collection and analysis from dispersed sensors and smart devices. External and internal assaults are the two most common types of attacks on IoT gadgets. The vulnerability of IoT-based applications is closely linked to the network paradigm, in which physical items such as sensor-based devices collect data on critical interactions within the network and communicate via wireless or wired connections. The uploaded, processed, and stored data may reveal key vulnerabilities in the form of man-in-the-middle assaults and denial-of-service attacks.

Consequently, unless precautions are taken, IoT infrastructure may severely jeopardize smart cities' physical security and privacy since data gathering and transfer via this technology might be extremely damaging. Privacy may be readily compromised owing to the high degree of interaction between people, devices, and sensors; as a result, this data must be fully safeguarded.

Therefore, it's a long way to go to make a smart city more secure and private. Research signifies that the most critical factor in making a city "smart" is not the technology itself but rather how it is designed, managed, and used. That's why it's so important for cities to focus on creating a comprehensive strategy for privacy and security – one that considers the unique needs and challenges of the city, its residents, and its businesses.

## Parting Words

There's no question that smart city technology has the potential to make our cities more efficient, sustainable, and livable. But as with any new technology, privacy and security risks also need to be considered. Furthermore, the cybersecurity and physical security risks associated with smart city technology are often interdependent, and a comprehensive approach is required to address both. However, if we collaborate, we may see the advantages of smart city technology outweigh the risks and help create truly safe, secure, and private cities that do not impede national security. ■

# ONFIDO LAUNCHES MOTION, THE NEXT GENERATION OF FACIAL BIOMETRIC TECHNOLOGY, IMPROVING VERIFICATION SPEED BY 12X

- Next-generation facial biometric technology improves verification speed by 12X, detecting the presence of a real physical person in seconds
- iBeta PAD Level 2-rated technology protects against display attacks and sophisticated 2D and 3D masks, improving fraud detection by 10X
- Whitepaper outlines AI bias reduction providing fairer customer verification

Onfido, the leading global digital identity verification and authentication provider, today unveiled Motion, a next-generation biometric liveness solution to enhance its Real Identity Platform, launched in May. Motion delivers seamless, secure, and inclusive customer verification and is iBeta Level 2 certified. With a simple head-turn capture, businesses can automate customer onboarding and assess more customers more quickly and efficiently while significantly reducing their fraud exposure. Identity fraud has risen 43% year-over-year, with sophisticated fraud increasing 57% as criminals employed smarter tactics, utilizing realistic 2D/3D masks and deploying display attacks (for example, showing a picture of a person on a screen) to try to spoof verification systems. And with 9 out of 10 consumers comfortable accessing digital services, the opportunities for fraudsters are increasing. Not only must companies now provide more accurate fraud measures when verifying new and existing customers, but they must also ensure they can establish trust with potential customers in under 10 minutes or risk losing them. Luckily, consumers are increasingly embracing biometrics, with 77% reporting that biometrics are more convenient than legacy verification methods.

Motion is built on Onfido's award-winning AI technology, Atlas, ensuring users benefit from fast, accurate, and fair AI with next-generation fraud detection performance on a global level. Using Motion, user bias is reduced across all ethnicities, thanks to Onfido's advanced machine learning models. These models have been trained to identify hundreds of thousands of fraud samples and analyze different elements of an identity document and facial biometric to stop fraud and reduce bias. Read our whitepaper [attached] to find out more. The Onfido Real Identity Platform is designed to secure trust between organizations and their customers throughout the customer lifecycle. It automatically verifies a customer's identity using a smart combination of award-winning document and biometric verification, trusted data sources, and passive fraud signals. With the addition of Motion, 95% users can now be onboarded in 10 seconds or less, with false rejection rates and false acceptance rates of less than 0.1%.

## Watch: Onfido Motion in Action

Onfido customer usage of biometrics has increased 160% year-over-year as more companies want to safeguard


their businesses while providing the best user experience possible. The market-leading compliance platform Amiqus used to digitally onboard staff welcomed Motion:

"The Amiqus platform is certified to the highest standard by the UK Government and DBS digital identity schemes. Hundreds of regulated businesses and public sector organizations operating at scale rely on us to deliver accessible, robust, and seamless staff onboarding and pre-employment screening," said Callum Murray, CEO and Founder of Amiqus. "Motion by Onfido is a fantastic addition to this capability and arrives at a time when employers are acutely aware of the need to meet digital right-to-work requirements."

The micro-mobility and scooter platform Check is one of the first Onfido customers to use Motion:

"Using Onfido Motion, it's very clear to our customers what is being asked of them when being verified," said Rick Van't Hof, Product Owner, Check. "It enables them to set up an account in seconds and be on their way on one of our mopeds while enabling us to keep operating costs low and run efficiently as an agile and high-growth business."

"In today's fast-paced digital world, providing the best

*continue on page 31*

user experience is everything. Consumers demand to be able to access products and services in seconds whilst also knowing they are secure," said Alex Valle, Chief Product Officer, Onfido. "Motion helps achieve this with a biometric liveness solution that provides simple, fair and secure access to online services from banking and gaming to crypto, rental cars and scooters."

Configuring Motion is easy with Onfido Smart Capture SDK, enabling it to fit seamlessly into an organization's customer workflow. Thanks to intelligence drawn from leveraging deep, diverse datasets built from over a decade of verifying global identities, Motion is one of the most accurate and fair liveness solutions available. ■

---

# NEW DESIGO CC V6 BUILDING MANAGEMENT PLATFORM ADDS NATIVE CLOUD CONNECTIVITY

- Updated Desigo CC V6 connects to Building X, Siemens' cloud-based open platform and AI-enabled suite of applications
- Enhanced cybersecurity with extended support to IEC 62443-3-3 SL2
- New Flex Client features to improve user experience
- Fulfills BACnet B-XAWS profile for cross-domain advanced workstation and BACnet Secure Connect

Siemens Smart Infrastructure has unveiled the latest version of Desigo CC, its integrated building management platform for the digitalization of buildings of any size. With the software update, Desigo CC V6 offers native cloud connectivity and an improved user experience and is among the first building management platforms worldwide to fulfill the BACnet B-XAWS profile for cross-domain advanced workstations and BACnet Secure Connect.

## Native cloud connectivity to Building X

Desigo CC now connects to the recently launched Building X, Siemens' cloud-based open platform and AI-enabled suite of applications. Building operators can now monitor and manage multiple Desigo CC sites with the Building X Operations Manager cloud application. With 24/7 access to cloud-connected buildings from anywhere, unnecessary physical site visits are reduced, and response times are improved.

Using the Operations Manager, operators can now securely connect to Flex Client, the HTML5 client application, without a complex VPN setup. This functionality can be enabled in countries where Building X is currently available.

## Enhanced cybersecurity

Developed, operated, and maintained with cybersecurity in mind, Desigo CC meets the highest protection requirements, adding support for additional IEC 62443-3-3 SL2 scenarios. It also allows for adaptation to customers' advanced IT infrastructure, offering improved user management and increased password security.

## Advanced user experience

Along with a state-of-the-art user interface, the Desigo CC Flex Client receives additional software features to enhance the user experience, focusing on building automation operators. Highlights include Log Viewer for easy and efficient log data analysis, Flex Client Report Viewer to generate, view, and download reports, and the ability to manage recipients and groups with the new application for notifications. These enhancements make end-users daily operations more intuitive and efficient and enable seamless site operation, whether on-premise or hybrid deployments.

## Cross-domain certification

For integrating different subsystems, Desigo CC supports the manufacturer-independent BACnet standard to monitor and control all subsystems with one common BMS. Desigo CC is among the first building management platforms certified with a cross-domain profile B-XAWS 1.16. Desigo CC supports the profiles B-AWS, B-ALWS, B-ACCWS, and profile B-XAWS, as well as the BACnet/SC protocol. It enables the encryption of data traffic based on certificates, ensuring a secure connection between all BACnet devices.

With a modular design, Desigo CC has the flexibility across different disciplines to adapt to buildings and projects of any size. Engineer-friendly functions, workflows, and migration tools also allow for the optimization of engineering costs and simplification of migration projects.

Desigo CC V6 will be shown for the first time at Light + Building 2022 in Frankfurt, Germany, October 2-6. Visit us in Hall 11.0, B56, and read more about Siemens presence at the show, here.

**For more information, please visit: www.siemens.com/smart-infrastructure *(Siemens Smart Infrastructure)*, www.siemens.com/desigocc *(Desigo CC)* and www.siemens.com/buildingx *(Building X)*** ■

# COMING SOON

**JAN 17 – 19 2023**
**Intersec Middle East 2023**
Dubai, UAE
https://intersec.ae.messefrankfurt.com

**MAR 29 – 31 2023**
**ISC West 2023**
Las Vegas, USA
https://www.discoverisc.com/global/en-us/isc-west.html

**APR 25 – 27 2023**
**The Security Event 2023**
Birmingham, United Kingdom
https://www.thesecurityevent.co.uk

**APR 27 – 29 2023**
**Secutech India 2023**
Mumbai, India
https://secutechindia.in.messefrankfurt.com

**APR 26 – 28 2023**
**Secutech Taiwan 2023**
Taipei, Taiwan
https://secutech.tw.messefrankfurt.com

**AUG 16 – 18 2023**
**Secutech Vietnam 2023**
HCMC, Vietnam
https://secutechvietnam.tw.messefrankfurt.com

**SEP 11 – 13 2023**
**GSX 2023**
Dallas, USA
https://www.gsx.org

**OCT 3 – 5 2023**
**Intersec Saudi Arabia 2023**
Riyadh, Saudi Arabia
https://www.intersec-ksa.com

**NOV 1 – 3 2023**
**Secutech Thailand 2023**
Bangkok, Thailand
https://secutechthailand. tw.messefrankfurt.com

# SUBSCRIPTION FORM

*Email us at* ***info@tradelinkmedia.com.sg***

Please (√) tick in the boxes.

## PRINT


☐ **Southeast Asia Building**
*Since 1974*


☐ **Southeast Asia Construction**
*Since 1994*

***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) per magazine*

| | |
|---|---|
| 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 |

## DIGITAL


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

http://lt.tradelinkmedia.biz

☐ **Lighting Today**
*Since 2002*


***Security Solutions Today***
is available on digital platform.
To download free PDF copy,
please visit:

http://sst.tradelinkmedia.biz

☐ **Security Solutions Today**
*Since 1992*

**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: _____


# ADVERTISE WITH US TODAY!

Email us at info@tradelinkmedia.com.sg.

Scan to visit our website