JUL – SEP 2026

SECURITY SOLUTIONS TODAY

SAFE CITIES 2.0: BUILDING TRUST THROUGH TECHNOLOGY

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)
1 Paya Lebar Link, #04-01, Paya Lebar Quarter 1 (PLQ 1), Singapore 408533
Tel: +65 6842 2580
ISSN 2345-7112 (E-periodical)

Where Your Safer and Smarter Solutions Meet Asia's Market Demand

3 shows · 39,720 sqm · 46,000 visitors

Join the Secutech Series — Asia's B2B platform for integrated security & fire safety solutions

secutech+ VIETNAM

AI, IOT & ICT FOR SMART SOLUTIONS

9 - 12 September 2026
Hanoi, Vietnam

480 Exhibiting Brands
13,000 Sqm
17,000 Visitors

Concurrent with

fire & safety
presented by Secutech Vietnam

SM building
presented by Secutech Vietnam

Download Info Pack

www.secutechvietnam.com

secutech THAILAND

18 - 20 November 2026
Bangkok, Thailand

400 Exhibiting Brands
11,600 Sqm
14,000 Visitors

Concurrent with

fire & safety
presented by Secutech Thailand

Thailand Smart City Expo

Download Info Pack

www.secutechthailand.com

secutech

21 - 23 April 2027
Taipei, Taiwan

500 Exhibiting Brands
15,120 Sqm
15,000 Visitors

Concurrent with

fire & safety
presented by Secutech

SM building
presented by Secutech

Download Info Pack

www.secutech.com

CONTACT US

Messe Frankfurt (HK) Ltd Taiwan Branch
Ms. Michelle Chu +886 2 8729 1099 #768
INTL@taiwan.messefrankfurt.com

messe frankfurt

AMG SYSTEMS INTRODUCES AMG840 SERIES HIGH-PERFORMANCE NETWORK SERVER APPLIANCE

New 1U rack-mount platform delivers high-speed connectivity, redundancy, and Net-Hawk-ready performance

Castleford, UK – April 2026 — AMG Systems has announced the launch of the AMG840 Series Network Server Appliance, a high-performance 1U rack-mount platform developed for advanced network monitoring, critical infrastructure, and security-focused applications.

Engineered in the UK and USA and manufactured in the UK, the AMG840 Series is purpose-built to support AMG Net-Hawk, the company's network monitoring and management platform. The appliance is also available in entry-level configurations, allowing system integrators and end users to deploy custom operating systems, storage, and applications.

Tom Exley, Technical Director at AMG Systems, explains: "The AMG840 Series supports Intel® 12th and 13th Generation Core™ processors, including i3, i5, i7, i9, and Celeron options, along with up to 64GB DDR4 memory. High-speed connectivity is delivered via six 2.5Gb RJ45 ports and four 10Gb SFP+ ports, enabling deployment in high-bandwidth environments such as transportation networks, utilities, public safety systems, enterprise security, and industrial infrastructure."

Designed for continuous operation, the platform features dual redundant hot-swappable power supplies, supports

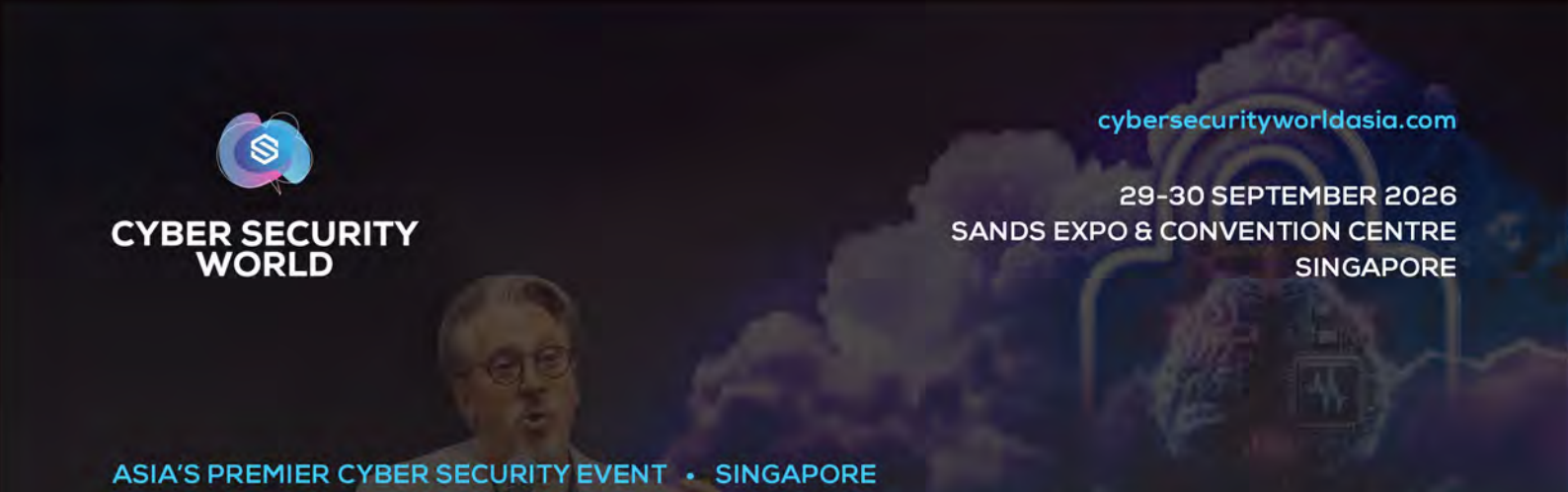
commercial operating temperatures from 0°C to +50°C, and is housed in a robust metal chassis for standard 19-inch, 1U rack installation. The system supports both Windows and Linux operating systems and complies with key requirements, including NDAA and TAA.

Pre-configured AMG840 models are available with AMG Net-Hawk software pre-installed, enabling rapid deployment and reduced integration time, while entry-level models offer maximum flexibility for specialist applications.

The AMG840 Series is available now through AMG Systems and its authorised partners worldwide. AMG believes that advancing transmission technology, maintaining product availability, and providing direct support from its design team give customers worldwide a measurable advantage in today's competitive marketplace. ■

AMG Systems offers an extensive line of fiber-optic, copper, and wireless Ethernet, video, and data transmission equipment that is uniquely designed to meet the needs of the Security, Intelligent Transportation Systems, Utility, and Industrial markets. **Full product line details are available at www.amgsystems.com. Call direct in the US, 1-855-AMGPOE1, or internationally at +44 (0)1767 600777, or email usasales@amgsystems.com for details.**

Image by Freepik



CYBER SECURITY WORLD

cybersecurityworldasia.com

29-30 SEPTEMBER 2026
SANDS EXPO & CONVENTION CENTRE
SINGAPORE

ASIA'S PREMIER CYBER SECURITY EVENT • SINGAPORE

Where Asia's security leaders make decisions.

Meet CISOs, security directors and risk executives from across Asia Pacific evaluating solutions and building the partnerships that matter.

71	20%	33%	15%
COUNTRIES REPRESENTED	BFSI SECTOR ATTENDANCE	SENIOR SECURITY & DATA MANAGERS	CISO / CRSO ATTENDANCE

WHO ATTENDS

- CSIO/ CRSO
- CTO / CIO / CDO
- Security directors
- Senior security managers
- Cybersecurity specialists

KEY SECTORS

- Senior security managers
- Government & public sector
- Technology & IT
- Manufacturing & logistics
- Healthcare

Exhibit at Cyber Security World Asia 2026

Stand space · Conference sessions
Executive Luncheons · Digital and Onsite Branding

INCORPORATING

TECH WEEK SINGAPORE
singaporetechnologyweek.com

CLOUD & AI INFRASTRUCTURE · DEVOPS LIVE · CYBER SECURITY WORLD · BIG DATA & AI WORLD · DATA CENTRE WORLD

ORGANISED BY

CloserStill

CHINESE OPEN-SOURCE TOOLKIT DRIVES SCAM SURGE SPILLING INTO BUSINESS NETWORKS

Infoblox Threat Intel links more than 236,000 scam sites to one framework and logs five million enterprise attempts to reach them.

Singapore, June 26, 2026 — In 2024, a small Argentine town called San Pedro made international headlines when thousands of residents discovered a crypto platform they backed was a scam. This platform, RainbowEx, was the core focus of the story, but the true story went unreported. RainbowEx was not a one-off, but rather a repeatable template built on a Chinese app framework now linked to more than 236,000 scam sites worldwide, many of them touching business networks.

New research by Infoblox Threat Intel shows that scammers have used the framework, called DCloud Uni-App (DCloud), to perpetrate fraud at scale for some time now. According to the research, DCloud is the technical foundation underneath at least 236,493 distinct second-level domains identified as scam infrastructure: from RainbowEx-style fake crypto exchanges to multi-language pig-butchering operations, WhatsApp phishing networks, fake gambling platforms, brand-impersonation sites, and crypto wallet drainers.

"This is no longer just a consumer fraud problem. When scam traffic reaches work devices and work networks, companies inherit the fallout, from employee losses to possible data exposure and tougher scrutiny from leadership."
-Zach Edwards,Staff Threat Researcher at Infoblox.

The business spillover is already visible. Infoblox recorded more than five million attempted connections from 985 organizations in 25 industries. No single company drove the volume. It came from many small visits by employees, often after links were sent through WhatsApp, Telegram, or social media.

Consumer scams are increasingly crossing into the workplace through personal devices and office networks, creating fraud risk, data exposure, and board-level questions that standard phishing training does not fully address.

If companies ignore the consumer side of fraud, more of that cost will keep showing up inside the enterprise.

Image by Freepik

About Infoblox Threat Intel

Infoblox Threat Intel is the leading creator of original DNS threat intelligence, distinguishing itself in a sea of aggregators. What sets us apart? Two things: mad DNS skills and unparalleled visibility. DNS is notoriously tricky to interpret and hunt from, but our deep understanding and unique access to the internet's inner workings allow us to track down threat actors that others can't see. We're proactive, not just defensive, using our insights to disrupt cybercrime where it begins. We also believe in sharing knowledge to support the broader security community by publishing detailed research and releasing indicators on GitHub. In addition, our intel is seamlessly integrated into our Infoblox DNS Detection and Response solutions, so customers automatically get its benefits, along with ridiculously low false positive rates.

About Infoblox

Infoblox is a leading platform for preemptive security and hybrid, multi-cloud networking that delivers enterprise resilience and agility. Trusted by over 5,700 customers, including the majority of Fortune 100 companies as well as emerging innovators, we seamlessly integrate, secure and automate critical network services so businesses can move fast without compromise. Visit Infoblox.com, or follow us on LinkedIn.■

Altronix®

NETWAY SPECTRUM

Hardened PoE Switches & Fiber Media Converters

- Deploy IP devices at remote locations with or without local power
- Supports up to 90W per port
- Rapid battery charging provides extended power backup
- 115/230VAC or 277VAC input
- Manage and reset devices remotely with LINQ™ Network Power Management
- Lifetime warranty

Run With It™

altronix.com

DIGICERT INTRODUCES INDEPENDENT TRUST VALIDATION WITH GOOGLE CLOUD FOR CONFIDENTIAL COMPUTING

New collaboration extends the principles of PKI to cloud infrastructure, enabling independent verification of trusted workloads and computing environments

Singapore – June 26, 2026 — DigiCert, a global leader in intelligent trust, has announced a collaboration with Google Cloud to bring independent trust validation to confidential computing environments. By applying the proven principles of Public Key Infrastructure (PKI) to cloud infrastructure, DigiCert will provide cryptographic verification that cloud-hosted systems and workloads are authentic, trusted, and untampered.

As organisations move more sensitive applications, AI workloads, and critical operations to the cloud, trust in the underlying infrastructure has become a foundational requirement. Particularly in regulated industries, organisations are increasingly seeking independent attestation to validate infrastructure integrity and complement cloud provider assurances.

"As organisations handle increasingly sensitive data, the demand for multi-layered infrastructure assurance has grown. For decades, PKI has enabled trusted interactions across the internet. We are now extending those same trust principles to confidential computing and cloud infrastructure."
- Amit Sinha, CEO of DigiCert.

Image by Freepik

DigiCert introduces an independent layer of trust verification by acting as a neutral third-party root of trust. Using cryptographic signatures, certificates, and identity validation, the company independently attests that workloads and computing environments hosted in Google Cloud are operating transparently and as intended. Developed through a year-long collaboration between DigiCert and Google Cloud, the service establishes a new trust model for the confidential computing ecosystem, enabling independent verification of cloud infrastructure while complementing provider attestation.

The initiative builds on the growing adoption of confidential computing, which protects data while it is actively being


Image by Freepik

processed by isolating workloads in secure hardware-based environments. DigiCert's independent attestation capabilities strengthen this model by enabling organisations to verify the integrity and authenticity of the underlying infrastructure.

By combining Google Cloud's confidential computing capabilities with DigiCert's expertise in PKI and digital trust, organisations gain:

- Independent cryptographic verification of workloads and infrastructure.
- Stronger assurance that systems have not been modified or tampered with.
- A common root of trust across distributed cloud environments.
- Greater transparency and confidence for regulated and security-sensitive workloads.

The announcement reflects a broader industry shift toward verifiable trust architectures, where security claims are validated cryptographically rather than assumed implicitly. DigiCert's approach extends the trust framework that secures billions of internet connections today into the next era of cloud and AI infrastructure.

"Confidential computing is built on the principle that customers should be able to verify the integrity of their workloads. By collaborating with DigiCert on independent attestation, we're extending that principle and providing customers with an additional layer of assurance for sensitive cloud workloads."

- Nelly Porter, Director of Product Management, Google Cloud Confidential Computing and Encryption.

About DigiCert

DigiCert is a global leader in intelligent trust. We protect the digital world by ensuring the security, privacy, and authenticity of every interaction. Our AI-powered DigiCert ONE platform unifies PKI, DNS, and certificate lifecycle management to secure infrastructure, software, devices, messages, and AI content, agents, and models. **Learn why more than 125,000 organizations, including 90% of the Fortune 500, choose DigiCert to stop today's threats and prepare for a quantum-safe future at www.digicert.com.** ■

TELTRONIC DEPLOYS TETRA SYSTEM FOR NEW SUBURBAN RAILWAY LINKING MEXICO CITY WITH FELIPE ÁNGELES INTERNATIONAL AIRPORT

Deployment extends secure communications to the new airport branch, supporting safer, more efficient rail operations

Zaragoza, June 25, 2026 — Teltronic, a Spanish company with more than 50 years of experience in the critical communications sector, has deployed the TETRA communications system for the new Buenavista–AIFA suburban railway, connecting Mexico City with Felipe Ángeles International Airport (AIFA). The new line entered service on 27 April.

The new route forms a branch of the existing Buenavista–Cuautitlán line, where Teltronic already provides the communications network. As part of the expansion, the company installed additional base stations to deliver TETRA coverage across the 28-kilometre section between Lechería station and AIFA, ensuring continuous train-to-ground communications along the entire route.

Teltronic has also equipped the 10 trains operating on the new line with its RTP-800 onboard radio system and supplied portable and fixed radios for supervisory, operational, and safety personnel.

"Teltronic has been serving this line for years, and it is particularly important for us to continue supporting the operation as it expands to AIFA, as this reinforces the customer's confidence in our technology and in the local team. Mexico is a country of paramount importance to us, and we will continue to work to consolidate our presence and keep adding value to critical transport infrastructure."

- Felipe Sanjuán, Director of Transport Business Development.

New Line to AIFA

The Buenavista–AIFA railway forms part of the Felipe Ángeles–Mexico City–Pachuca rail project, connecting the Mexican capital with Felipe Ángeles International Airport. The new Lechería–AIFA section was inaugurated on 26 April to improve airport accessibility and enhance mobility across the Valley of Mexico.

The 28-kilometre route includes eight stations serving the municipalities of Tultitlán, Tultepec, Nextlalpan and Zumpango. It is expected to benefit approximately 80,000 passengers each day by reducing travel times while providing a more comfortable and sustainable alternative for journeys between the city centre and the airport.

Given the strategic importance of the line, which is planned to extend to Pachuca in the state of Hidalgo, the Mexican Government has assumed responsibility for operating the rail network. The project is expected to strengthen regional connectivity while supporting safer, more efficient, and sustainable public transport for thousands of daily commuters. ■

MKS INTRODUCES OPHIR® LIGHTIR 15–75 MM F/1.2 LOW-GERMANIUM LWIR ZOOM LENS FOR IMPROVED SUPPLY STABILITY AND HIGH-PERFORMANCE THERMAL IMAGING

Re-engineered LWIR optical design reduces dependency on germanium while maintaining high optical performance for defence and security thermal imaging systems

Andover, MA, June 15, 2026 — MKS Inc., a global provider of enabling technologies, has announced the Ophir® LightIR 15–75 mm f/1.2 LWIR motorized continuous zoom lens, a re-engineered low-germanium optical solution developed to address growing industry concerns surrounding germanium material

continue on page 12

SIDEX – ACDR 2026

in conjunction with FiSAC

CO-EM
Building Resilience and Preparedness Globally
EVENT ORGANISER

SCDF
The Life Saving Force
...for a safer Singapore
STRATEGIC PARTNER

28 - 30 OCTOBER 2026 | SINGAPORE EXPO HALL 3

3 CONFERENCES | 1 WORKSHOP | 1 EXHIBITION

Disaster Resilient Futures: Leadership, Solidarity, Preparedness

PREMIER LEADING PLATFORM FOR FIRE RESCUE, DISASTER MANAGEMENT & EMERGENCY RESPONSE PROFESSIONALS

"This is a gathering of experts from all parts of the world ... not only share their expertise but also learn more to enhance safety and disaster management."

-Mr Jim Pauley, CEO,
National Fire Protection Association

CONFERENCE

3
CONFERENCES

23
SPEAKERS

3
KEYNOTE SPEAKERS

14
TOPICS

SCAN THE QR CODE TO FIND OUT MORE INFORMATION

or visit sidex.sg

availability, supply-chain stability, and long-term program risk.

Designed for VGA 10–12 µm uncooled LWIR detectors, the Ophir LightIR 15–75 mm f/1.2 lens delivers high-performance thermal imaging across a wide range of defence, homeland security, surveillance, and industrial applications while significantly reducing dependence on germanium-based optical materials.

"Germanium has long been a foundational infrared optical material, but increasing global demand, limited raw material availability, export sensitivities, and pricing volatility are creating growing challenges for thermal imaging system manufacturers and long-term defence programs".

- Dr. Kobi Lasri, General Manager, Ophir Optics Products.

"MKS' re-engineered optical architecture was developed to mitigate these risks while preserving the high-performance imaging capabilities required for mission-critical applications. The new Ophir low-germanium optical lenses help customers lower supply-chain and lifecycle risk while maintaining the high optical performance expected from Ophir infrared imaging products."

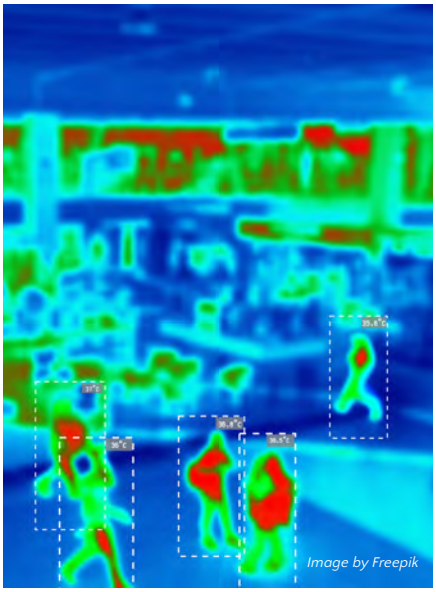
The Ophir LightIR 15–75 mm f/1.2 continuous zoom lens provides a 29.9° WFOV down to 5.8° NFOV horizontal field of view (H-FOV) for 640 × 480 VGA 12 µm detectors, enabling both wide-area situational awareness and long-range target observation in a compact, lightweight package.

Weighing only 349 g and measuring Ø75 × 75.6 mm, this compact low-SWaP low-germanium lens is optimised for airborne, ground, handheld, perimeter security, and unmanned thermal imaging platforms where size, weight, performance continuity, and long-term availability are critical considerations.

In addition to the unique optical design, the Ophir LightIR 15–75 mm f/1.2 continuous zoom lens features advanced hard carbon and Diamond-Like Carbon (DLC) coatings. These coatings are designed to enhance durability and environmental robustness for demanding defence and security applications while ensuring reliable long-term performance in germanium-reduced optical systems.

To support a smooth transition from legacy full-germanium designs, MKS offers dedicated lens-to-detector adapter options that help address the updated back working distance (BWD) and mechanical interface adjustments. These adapter options are designed to minimise integration impact for existing customers while supporting new system designs focused on long-term availability and supply-chain resilience.

The announcement marks the first release in a broader MKS low-germanium LWIR optics portfolio currently under expansion, including additional fixed-focus (1-FOV) lenses covering wide (86°) to narrow (6°) field-of-view configurations for complete VGA 12 µm detector H-FOV coverage.



About MKS Inc.

MKS Inc. (NASDAQ: MKSI) enables technologies that transform our world. We deliver foundational technology solutions to leading-edge semiconductor manufacturing, electronics and packaging, and specialty industrial applications. We apply our broad science and engineering capabilities to create instruments, subsystems, systems, process control solutions, and specialty chemicals technology that improve process performance, optimize productivity, and enable unique innovations for many of the world's leading technology and industrial companies. Our solutions are critical to addressing the challenges of miniaturization and complexity in advanced device manufacturing by enabling increased power, speed, feature enhancement, and optimized connectivity. Our solutions are also critical to addressing ever-increasing performance requirements across a wide array of specialty industrial applications. **Additional information can be found at www.mks.com.**

About the Ophir Brand

Ophir is a brand within the MKS Photonics Solutions Division. The Ophir product portfolio consists of laser and LED measurement products, including laser power and energy meters, laser beam profilers measuring femto-watt to hundred-kilowatt lasers, high-performance IR and visible optical elements, IR thermal imaging lenses and zoom lenses for defense and commercial applications, OEM and replacement high-quality optics and sub-assemblies for CO2 and high-power fiber laser material processing applications. Ophir products enhance our customers' capabilities and productivity in the semiconductor, electronics, packaging, and specialty industrial markets.

For more information, visit www.ophiropt.com. ■

SAFETY & SECURITY ASIA

10 - 12 NOVEMBER 2026
SANDS EXPO & CONVENTION CENTRE
SINGAPORE

CO-LOCATED WITH:

- THE SECURITY EVENT ASIA
- THE FIRE SAFETY EVENT ASIA
- THE HEALTH & SAFETY EVENT ASIA
- THE EMERGENCY SERVICES SHOW ASIA
- PRO INTEGRATION FUTURE ASIA

APAC'S LARGEST EVENT SERIES DEDICATED TO THE SAFETY AND SECURITY OF PEOPLE, PLACES AND ASSETS

ORGANISED BY: Nineteen

BOOK YOUR STAND: WWW.SAFETYSECURITYASIA.COM

NEW FIDO ALLIANCE AND HID STUDY REVEALS MAJOR GAP BETWEEN IDENTITY SECURITY CONFIDENCE AND REALITY

Research reveals 94% of enterprises claim they can revoke employee access within 24 hours, yet 35% experienced delays or failures in the past two years

Cardiff, UK, June 17, 2026 — The FIDO Alliance and HID, a global enabler of trusted identity solutions, have released The State of Physical and Digital Identity in the Enterprise, a new research report examining how organisations manage physical and logical access across their workforces.

Based on a survey of 500 IT and cybersecurity decision-makers across the United States, Canada, the United Kingdom, France, and Germany, the study highlights a significant disconnect between enterprise confidence in identity security and operational reality.

While most organisations believe they can revoke all physical and digital access within 24 hours when an employee leaves, more than one-third report experiencing delays or failures in doing so, contributing to identity-related security incidents.

Key Findings

Confidence remains high, but security incidents persist

- 94% of organisations are confident they can revoke all physical and logical access within 24 hours of an employee leaving.
- However, 35% experienced delays or failures in doing exactly that during the past two years.
- Overall, 70% reported experiencing at least one identity-related security incident.

Governance remains fragmented

- Only 50% of enterprises have unified reporting ownership for physical and digital identity.
- Just 48% have consolidated budget control.
- The finance sector is the most governance-fragmented, with 34% operating separate reporting structures despite strict regulatory obligations.

Identity management is becoming more complex

- 59% of enterprises manage three or more credential and authentication systems.
- 58% say managing digital identity has become more complex over the past two years.

Public sector organisations face the highest incident rates

- The public sector recorded the highest identity security incident rate, with 43% experiencing access revocation failures.
- It also has a 20% manual credential revocation rate—more than double that of the IT and technology sector.

Image by Freepik

Passkey adoption continues, but deployment remains limited

- 93% of organisations are at some stage of passkey adoption, while 65% report high or expert technical familiarity.
- However, only 13% have deployed passkeys at scale.

Phishing-resistant authentication is a priority

The leading reason organisations are adopting passwordless authentication is to reduce phishing and credential-based breach risks (45%), followed by reducing password reset and help desk costs (44%).

"The story in this data isn't about awareness; it's about execution. Ninety-three percent of organizations are on the passkey journey, but only 13% have deployed at scale, and the security incident rates reflect that gap directly," said Andrew Shikiar, Executive Director and CEO of the FIDO Alliance. "Phishing-resistant authentication only delivers its full protective value when deployment is comprehensive rather than selective."

Sean Dyon, Vice President of the Authentication Business Unit at HID, added: "Identity security is no longer just an authentication challenge; it is an enterprise governance challenge. As organizations adopt passkeys, a unified approach to managing physical and digital identity becomes critical. This research shows that fragmented governance, disconnected systems and limited visibility create real business risk."

The findings highlight the growing importance of unified identity management, governance, and phishing-resistant authentication as organisations strengthen both physical and digital security across increasingly connected environments. ■

DigiTech ASEAN Thailand

Co-located with: AI CONNECT

"Digital Solutions for Business"

25-27 NOVEMBER 2026

Hall 7-8, IMPACT Exhibition Center, Bangkok, Thailand

FREE VISITOR REGISTRATION

BOOK YOUR BOOTH

For more information, please contact:

Tel: +662-833-5370

or email info@digitechasean.com

DigiTechASEAN

www.digitechasean.com

Show Hosts | Strategic Partners | Organizer

depa NIA IMPACT MUANG THONG THANI

SIEMENS BRINGS DIGITAL INTELLIGENCE TO FIRE SAFETY

Siemens' new Acend Intelligent portfolio transforms fire safety notification into a digital, connected, and data-driven system

Disturbance-Free Testing technology and individual device activation reduce manual effort, maximise uptime, and enable location-specific alerts. Cloud connectivity, predictive maintenance, and remote capabilities pave the way to human-centric autonomous buildings.

Siemens has unveiled its new Acend Intelligent notification portfolio, transforming traditional fire safety into a digital and connected approach. With the new offering, fire safety notification evolves from a reactive function into a data-driven, operationally integrated system that enhances safety while minimising operational disruptions. This marks an important technological milestone on the path toward human-centric autonomous buildings.

In environments where uninterrupted operations are critical, including healthcare, hospitality, commercial real estate, and data centres, fire safety notification must work reliably without causing disruption. Acend Intelligent addresses this with its integrated Disturbance-Free Testing (DFT) technology, allowing system checks to be carried out without triggering audible or visual alarms.

Each device—from horns and strobes to speakers and combination appliances with both audible and visual signalling—can be monitored and activated individually. This enables operators to verify device performance and detect faults more quickly. Facility management teams and fire safety technicians can also check system readiness remotely across all connected devices, reducing the need for physical inspections.


Image by Freepik


Image by Freepik

Even in the event of wiring faults, the built-in Class X isolation technology keeps the system operational by isolating faults while ensuring the rest of the network continues to function. Through its connection to Siemens' cloud-based Building X Fire Apps, a suite of monitoring and diagnostic applications, personnel can test systems remotely, anticipate maintenance needs, and reduce manual effort, supporting safe and efficient operations.

> *"As buildings become increasingly connected and digitalised, safety systems must evolve alongside them. With Acend Intelligent, we are transforming fire notification into a foundational technology for these next-generation environments by combining cloud connectivity, real-time data, and digital integration."*
>
> ***- Peter Nebiker, Head of Fire Safety, Siemens Smart Infrastructure Buildings.***

The Acend Intelligent portfolio is also designed with resource efficiency and circularity in mind, including the use of recycled materials. It carries the Siemens EcoTech environmental product performance label for enhanced sustainability transparency.

The portfolio is designed for and available in markets where UL certification standards apply, including the United States, Canada, and selected markets across Latin America, the Middle East, and Asia. ■

9-11 SEPT 2026

SINGAPORE

OSH ASIA

Where Industry Leaders Take the Stage to Drive the Future

Marina Bay Sands Singapore | www.osha-singapore.com/booth-enquiry/

VISION FOR A SAFER AND HEALTHIER WORKPLACE

SAFETY @ WORK

HEALTH @ WORK

SECURITY @ WORK

Held in:

Passion Made Possible

Supported by:

SINGAPORE EXHIBITION & CONVENTION BUREAU

A+A

Knowledge Authority:

MINISTRY OF MANPOWER

WSHCOUNCIL

Organized by:

Messe Düsseldorf Asia

GREATER MANCHESTER POLICE INSTALLS A ROHDE & SCHWARZ SECURITY SCANNER FOR CUSTODY SEARCHES

Longsight Custody Suite will be equipped with QPS201 security scanners from Rohde & Schwarz with the intention of reducing the need for strip searches. Longsight is the first custody suite in England to feature a security scanner with high-resolution millimeter wave technology. The security scanner will improve operational efficiency, strengthen search procedures, and support ongoing improvements, with a particular focus on the treatment of women and girls.

Munich, June 15, 2026 — The QPS201 will be used as an additional screening step to check whether detainees may be concealing items such as weapons, drugs or other prohibited objects. The contactless scan is safe, fast, and designed to protect privacy. Instead of generating images of the person being scanned, the system displays any potential threat on a standardised digital avatar.

Millimeter wave technology can detect metallic and non-metallic objects concealed under clothing, including liquids and powders. The waves penetrate clothing but are reflected by the skin and are harmless to body tissue. The scanner's automated image analysis distinguishes between everyday items, such as buttons or zippers, and potential threats.

This targeted approach can reduce the need for more intrusive searches, support detainee dignity, and improve safety for custody staff. By combining advanced detection, automated analysis, and privacy-focused screening, the R&S QPS201 supports more efficient and respectful custody search procedures.

Rohde & Schwarz

Rohde & Schwarz is striving for a safer and connected world with its Test & Measurement, Technology Systems and Networks & Cybersecurity Divisions. For over 90 years, the global technology group has pushed technical boundaries with developments in cutting-edge technologies. The company's leading-edge products and solutions empower industrial, regulatory and government customers to attain technological and digital sovereignty. The privately owned, Munich based company can act independently, long-term and sustainably. Rohde & Schwarz generated a net revenue of EUR 3.16 billion in the 2024/2025 fiscal year (July to June). On June 30, 2025, Rohde & Schwarz had more than 15,000 employees worldwide. ■

Image by Freepik

DETECTION TECHNOLOGY EXPANDS SHANGHAI OPERATIONS TO SUPPORT CUSTOMER SUCCESS AND GROWTH

Detection Technology Plc press release 11 June 2026 at 13:00 (EEST)

Detection Technology, a global leader in X-ray detector solutions, today announced the successful relocation and expansion of its Shanghai branch, marking an important milestone in the company's DT2030 strategy. The upgraded facility enhances Detection Technology's service, product development, and testing capabilities, supporting customer success and the company's strategic objectives.

The expanded Shanghai site has been designed to enhance collaboration and improve operational efficiency. With the facility's floor area having nearly doubled, the increased space enables closer cross-functional collaboration, faster response to customer needs, and more efficient execution of development activities.

"The expansion of our Shanghai operations is an important step in executing our DT2030 strategy. Our strategy is built on helping customers succeed through smart, data-generating X-ray detector solutions and outstanding usability. By investing in quality, innovation, and product development capabilities, we are strengthening our ability to create value for customers and deliver differentiated solutions that address evolving market needs. These enhancements deepen our customer engagement, support sustainable growth, and strengthen our position as we expand our TFT X-ray detector business across applications and geographical markets."

- Chen Wu, President, APAC Business Uni, Detection Technology.

As part of the expansion, Detection Technology has further invested in its R&D environment to support the development of next-generation detector solutions. Enhanced testing and validation capabilities enable the company to evaluate detector performance in application-specific environments that closely reflect real customer use cases, including industrial inspection and computed tomography applications.

The upgraded facilities support more efficient product validation and faster translation of customer insights into product improvements. These investments strengthen the company's ability to address increasingly demanding imaging challenges across industrial, security, and medical applications while accelerating customer-driven innovation.

The company has also enhanced its quality capabilities through investments in quality control processes, testing environments, and operational excellence. These improvements support consistent product quality, reliability, and performance, helping customers achieve dependable results in demanding imaging applications. The expanded facility also supports planned team growth and provides additional space for collaboration with customers and partners. Improved workspaces and meeting facilities foster knowledge sharing, support the development of local expertise, and strengthen the company's ability to serve customers in a rapidly evolving market.


Image by Freepik

Located in Shanghai's Minhang District, the new facility provides excellent access to customers, partners, talent, and transportation networks within one of China's leading industrial and technology hubs. The location supports closer collaboration with customers and strengthens Detection Technology's ability to serve customers worldwide.

Detection Technology

Detection Technology is a global provider of X-ray detector solutions and services for medical, security, and industrial applications. The company's solutions range from sensor components to optimized detector subsystems with ASICs, electronics, mechanics, software, and algorithms. It has sites in Finland, China, France, India, and the US. The company's shares are listed on the Nasdaq First North Growth Market Finland under the ticker symbol DETEC.

www.deetee.com ■

LUKAS LAUNCHES E4 RANGE AT INTERSCHUTZ TO STRONG INDUSTRY RECEPTION

Erlangen, DE - June 10, 2026 — LUKAS has unveiled its new E4 range of rescue tools at Interschutz, the world's leading trade fair for fire and rescue services. The launch attracted strong interest from global fire and rescue professionals, with the range receiving a highly positive response during live demonstrations and hands-on trials.

Greater Control, Clarity, and Confidence

The E4 range is designed to deliver greater safety, control, clearer feedback, improved visibility, and enhanced operational safety. Built as a complete system, it supports faster, more confident decision-making while improving consistency in both training and real-world incidents. The IP68-protected LUKAS battery is designed to perform in extreme environments and can even be replaced underwater, while further integration with the Captium™ platform provides geofencing and tracking functions to help protect equipment against theft and misuse.

Built for Real-World Rescue

Firefighters operate in unpredictable, high-pressure environments, from complex vehicle extrications to incidents involving new materials and technologies. E4 has been developed around these realities, ensuring reliable performance in rain, mud, darkness, and confined spaces. With optimised ergonomics, balanced handling, and a 360° grip, the tools allow precise control even in challenging conditions, reducing strain and supporting smoother operation.

Smarter Feedback on the Incident Ground

E4 provides real-time insight into tool performance, including remaining force and available stroke. A roll warning system helps prevent unsafe angles, while an integrated light bar ensures clear visibility of the working area.

These features reduce guesswork and help crews work with greater accuracy and confidence when it matters most.

Innovation with Proven Reliability

Through integration with the Captium™ platform, E4 extends feedback beyond the tool itself. Operational data - such as performance, battery condition, and tool behaviour - is captured and turned into clear, actionable insights. Captium™ enables early detection of issues and provides real-time visibility across the fleet, ensuring tools remain predictable, reliable, and ready for use. It transforms individual tool feedback into a connected system that supports better decisions before, during, and after every incident.

> *"We built E4 around the reality of rescue. Crews are working under pressure in difficult conditions, and they need equipment they can trust immediately. E4 gives improved safety, clearer feedback, better visibility and the control to act confidently and decisively."*
>
> ***- Daniel Engelhardt, EU and ROW Rescue and Extrication Manager at LUKAS.***

Ready for the Challenges Ahead

E4 represents a shift in rescue equipment design - bringing together power, precision, and total control in a system built for the full lifecycle of rescue work. It is designed to help fire and rescue services meet today's challenges while preparing for the future. The e4 range is available to buy now from LUKAS' global dealer network.

About Lukas

LUKAS Hydraulics, a leader in hydraulic technology since the late 1940s, is renowned for its innovative and high-performance products. Based in Erlangen, Germany, LUKAS revolutionized emergency response equipment by introducing the world's first hydraulic rescue shears in 1972. As part of the IDEX Corporation, LUKAS combines global expertise to deliver powerful, reliable, and user-friendly hydraulic tools, ensuring top-quality standards "Made in Germany." With a comprehensive dealer network, LUKAS supports emergency services and industrial operations worldwide, enhancing safety and efficiency.

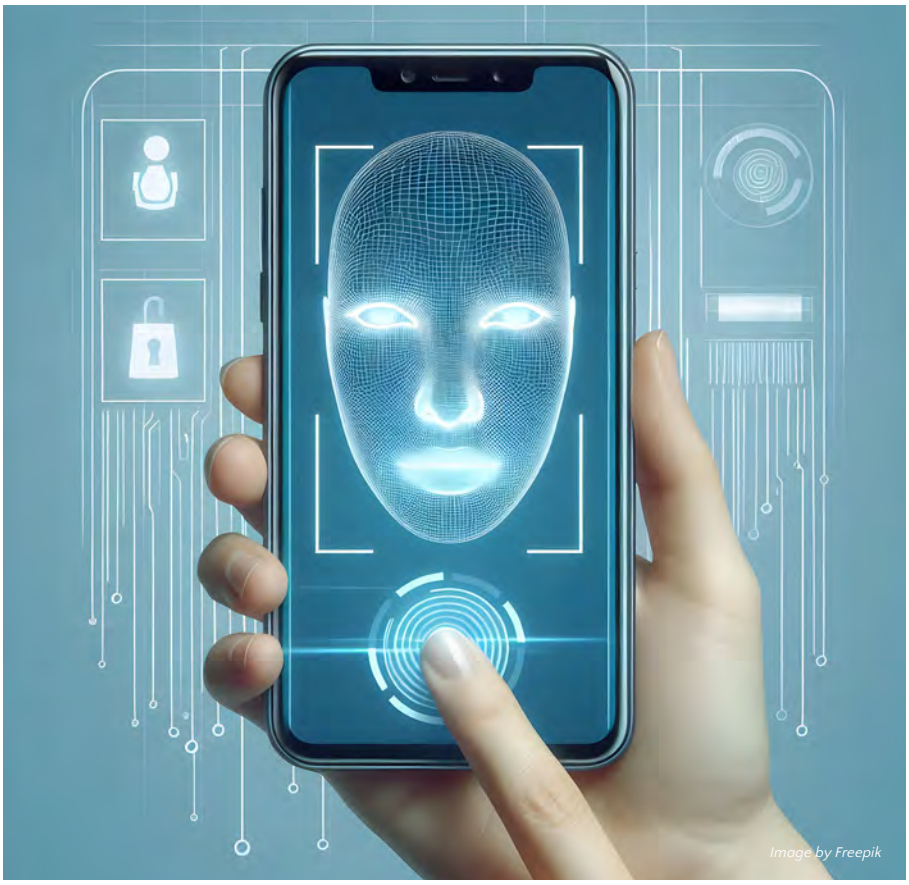
About IDEX Fire & Safety

IDEX Fire & Safety unites trusted brands to innovate customer experience and integrated solutions, enhancing fireground and rescue scene safety. Brands include Akron Brass, Alco, AWG, Captium, Class 1, Dinglee, Godiva, Hale, HURST Jaws of Life®, Lukas, SAM, Vetter, and Weldon. IDEX Fire & Safety is part of IDEX Corporation [NYSE: IEX], specializing in fluid and metering technologies, health and science technologies, and diversified products. ■

SUPREMA UNVEILS BIOSTATION 3 MAX: FLAGSHIP AI BIOMETRIC TERMINAL FOR IDENTITY-FIRST SECURITY

New benchmark in access control that delivers trusted multi-factor authentication and broad credential support on a hardened platform

Seoul, Korea – May 14, 2026 – Suprema, a global leader in AI-powered access control and security solutions, today announced the launch of BioStation 3 Max, the company's new flagship AI biometric terminal. Built around a single conviction, trust engineered into every door, BioStation 3 Max consolidates Suprema's full range of authentication methods: face and fingerprint biometrics at the core, with RFID, mobile, QR, and PIN. It all comes together on one hardened, identity-first platform, sub-second face matching, a premium 7-inch touchscreen, purpose-built for corporate lobbies to mission-critical entrances.



Designed for Security and Trust

As access terminals become networked endpoints, hardening the device is no longer optional; it is the foundation of trust. A hardened Linux OS with Secure Boot ensures only signed firmware ever executes. A CC EAL6+ certified secure element protects credentials and cryptographic keys at the silicon level. Biometric templates are encrypted, device communication is TLS-secured, and an active tamper response triggers immediate alerts on physical compromise. For deployments where user privacy is paramount, BioStation 3 Max supports Template-on-Mobile and Template-on-Card options, which store biometric data on the user's personal device or smart card instead of centralized servers, providing privacy-first options for sensitive environments.

Unparalleled AI Performance

Busy entrances are unforgiving. A terminal that hesitates creates queues, slows throughput, and compounds into operational cost across every access point. Powered by Suprema's latest AI engine on a dedicated NPU, BioStation 3 Max matches faces in under 0.3 seconds—even for people in motion. Dual 2MP visual and IR cameras deliver liveness detection and anti-spoofing that hold up against printed photos, replay videos, and 3D masks. BioStation 3 Max handles sunglasses, masks, varied angles, and shifting lighting without slowing the line. The terminal scales to 100,000 enrolled users.

Made to Be Seen, Built to Last

BioStation 3 Max is where authentication, user feedback, and intercom communication come together. A 7-inch IPS touchscreen delivers clear authentication prompts, face positioning guidance, and custom-branded messaging, while a built-in VoIP intercom with SIP integration lets visitors speak directly to reception at attended entrances. IP65 and IK06 ratings protect against dust, water, and impact across demanding indoor and outdoor environments. The terminal supports speed-gate and wall mounting, with PoE+ on select models delivering power and data over one cable. "BioStation 3 Max defines the new standard for identity-first security," said Hanchul Kim, CEO of Suprema Inc. "Biometric authentication, certified hardware security, and superior AI performance, brought together in one flagship terminal. Trust, engineered into every door." ■

DAHUA TECHNOLOGY INTRODUCES APOLLO BP3EW-4G TO EXPAND WIRE-FREE 4G SECURITY MONITORING

Hangzhou, China - April 20, 2026 — Dahua Technology has launched the APOLLO BP3EW-4G, a new wire-free 4G security camera under its WITHS series, designed to deliver simplified deployment, continuous monitoring, and dependable performance in remote and power-limited environments.

Built around the WITHS philosophy of Simple, Smart, and Secure, the new model provides a flexible surveillance solution for diverse locations such as farms, orchards, reservoirs, holiday homes, and other off-grid sites. It integrates high-definition imaging, intelligent detection, long-lasting power, and rugged construction into a compact system.

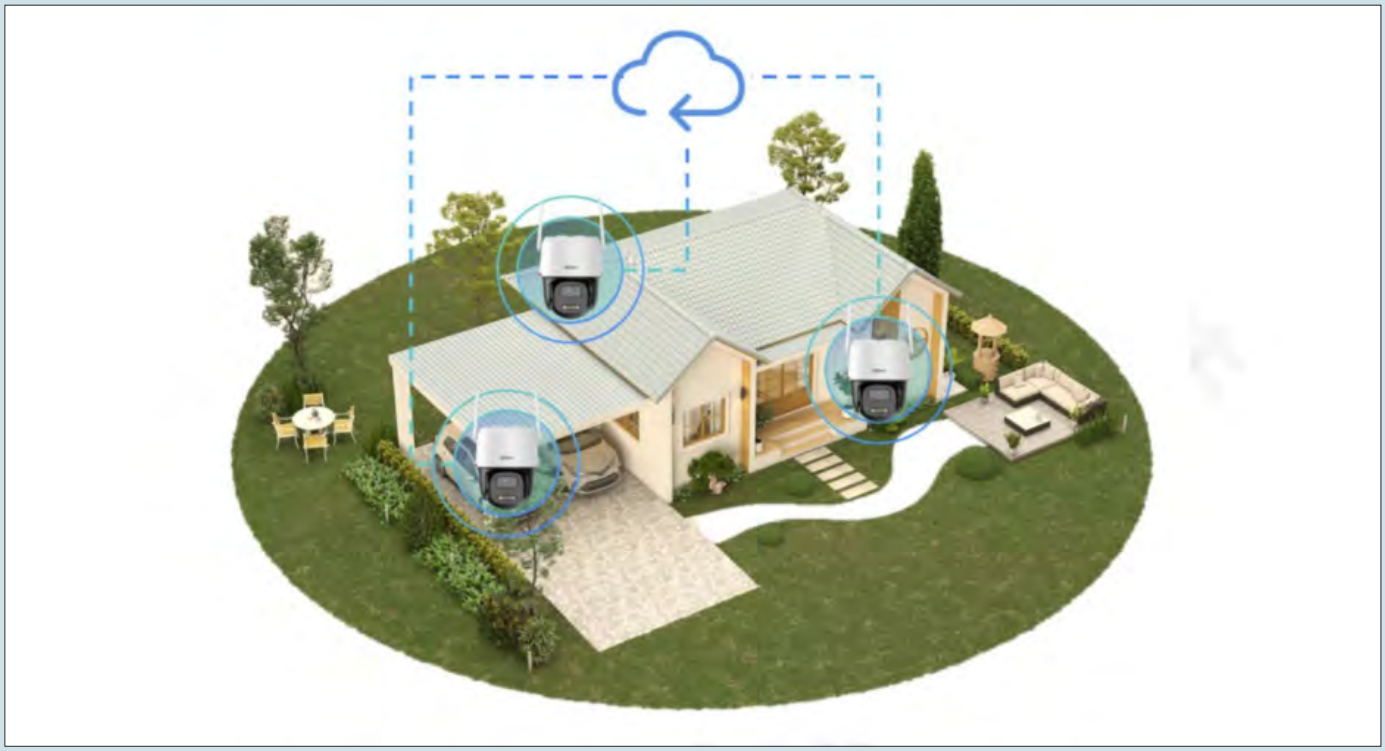
A central highlight of the APOLLO BP3EW-4G is its 2K imaging capability, which ensures that visual details remain sharp and clear within a wide-angle coverage for everyday monitoring. Presenting a "super clear, super wide" solution, it helps users capture more visual detail across larger outdoor spaces.

The device also features AOV (Always-on Video) mode, enabling extended, around-the-clock recording while maintaining low power consumption. The camera lowers its frame rate for static scenes to conserve energy, then quickly switches to a higher frame rate when motion is detected.

Application scenarios of APOLLO BP3EW-4G

This approach supports continuous protection while reducing the risk of missed events.

Power endurance is another major feature of APOLLO BP3EW-4G. It includes a built-in rechargeable 10,000mAh battery and is paired with solar charging support, allowing for all-day operation with minimal wiring and no reliance on a traditional power supply. This wire-free design simplifies installation and makes the camera practical for locations where electrical infrastructure is limited or unavailable.



The camera is wire-free with built-in rechargeable battery — no cables, no limits.

continue on page 23

The camera provides longer detection distance (up to 30 meters).

To improve alarm accuracy, the camera is equipped with AI detection for both human and vehicle targets. It is designed to filter out irrelevant movement, reduce false alarms, and provide timely notifications when significant activity occurs. In AOV mode, the device can detect targets at distances of up to 30 meters and transition to a higher frame rate within seconds.

Another notable highlight of the camera is WizColor low-light imaging, which enables the camera to produce brighter, more vivid full-color video under ambient light conditions. It reduces the need for spotlights at night while still preserving visibility and scene detail in darker environments.

Furthermore, the camera also has an IP66 protection rating, supporting operation in harsh outdoor conditions. It is equipped with flame-retardant materials and a secure internal design for the SIM and SD cards, reinforcing the product's positioning as a durable and reliable option for exposed or remote installations.

With the APOLLO BP3EW-4G, Dahua continues to expand its WITHS portfolio, offering an intelligent monitoring solution that is easy to deploy, energy-efficient, and adaptable to demanding outdoor scenarios. By combining 2K imaging, always-on recording, rechargeable and solar-supported power, AI detection, WizColor night monitoring, and IP66 durability, APOLLO BP3EW-4G serves as a practical solution to the growing demand for simple but capable wire-free security.

About Dahua Technology

Dahua Technology is a world-leading video-centric AIoT solution and service provider. Committed to enabling a smarter society and better living, Dahua has deployed its products, solutions, and services in 180+ countries and regions, covering transportation, manufacturing, education, retail, banking & finance, energy, environmental protection, and various industries. The company has more than 23,000 employees, with over 50% of R&D technicians.

Focusing on technological innovation, Dahua has established five major research institutes, with annual R&D investment accounting for approximately 10% of its sales revenue. The company continues to explore emerging fields based on in-depth insights and the layout of AIoT, and has extended its innovative businesses, including iRAYPLE, Pixfra, Waythcan, Wisualarm, etc. In line with its core value of "Customer Success, Employee Achievements", Dahua strives to provide the market with excellent quality and service, create more value for customers, and proactively contribute to a safe, low-carbon, beautiful and harmonious world. ■

Interview with **Troy Wu** *by Security Solutions Today, in conjunction with* **Milipol TechX 2026**

Interviewee: Troy Wu, Business Development Manager, Biometric Identity Technologies, Asia Pacific, HID

As governments and critical infrastructure operators across the Asia Pacific accelerate investments in trusted identity systems, biometrics is becoming a cornerstone of modern security architecture.

From border management and national ID programmes to law enforcement and mobile identity verification, organisations are looking for solutions that combine operational efficiency with uncompromising security at scale. At Milipol TechX 2026, HID showcased its latest biometric identity technologies and secure issuance innovations, demonstrating how next-generation facial and fingerprint recognition systems are evolving to meet the demands of real-world deployments.

In this ***Q&A with Security Solutions Today, Troy Wu, Business Development Manager, Biometric Identity Technologies, Asia Pacific at HID,*** *discusses advances in biometric accuracy, speed, and interoperability, the growing role of mobile identity and edge AI, and how HID is helping governments and enterprises tackle challenges such as spoofing, false positives, and fragmented identity ecosystems through an integrated approach to biometric security.*

At Milipol TechX 2026, what key breakthroughs in fingerprint and facial recognition is HID showcasing that materially improve accuracy and speed?

Troy Wu: Accuracy and speed have long been the defining benchmarks for biometric systems, but their true value lies in how consistently they perform under real-world conditions. In high-volume environments such as border crossings, organisations have traditionally faced a difficult compromise: prioritise accuracy at the expense of throughput or increase processing speed by lowering accuracy thresholds.

At HID, we've focused on eliminating that trade-off. Our biometric solutions are engineered to perform reliably in demanding, high-pressure environments where operating conditions are unpredictable and passenger volumes are constantly increasing. By processing large volumes of biometric data simultaneously, our systems deliver high throughput without compromising identification accuracy, enabling organisations to maintain secure and efficient operations at scale.

Where are biometric systems delivering the most tangible impact today, border control, law enforcement, or national ID programmes, and why?

Troy Wu: Each of these sectors is mission-critical, but they place different demands on biometric technology. In border control, the primary objective is to improve throughput while maintaining strong security. Biometrics helps automate identity verification, reduce manual intervention, and keep passenger flows moving efficiently.

For law enforcement, reliability is the overriding priority. Biometric systems support critical processes such as booking individuals into custody, where every identification decision must be accurate and dependable.

National ID programmes, meanwhile, require scalability and interoperability. Governments need solutions capable of managing large populations while enabling secure information sharing across multiple agencies. Increasingly, organisations are also looking for platforms that deliver long-term cost efficiency and measurable returns on investment alongside strong security.

False positives and spoofing remain persistent risks. How is HID mitigating these challenges in high-security environments?

Troy Wu: Mitigating these risks requires a layered approach rather than relying on a single technology.

Our solutions incorporate advanced liveness detection and anti-spoofing capabilities that help distinguish genuine users from fraudulent attempts. We also leverage multimodal biometrics by combining facial and fingerprint recognition, providing higher confidence in identity verification while significantly reducing false positives.

Beyond that, our algorithms are continuously trained using diverse datasets to strengthen resilience against emerging attack techniques and evolving threat landscapes. Equally important is protecting the biometric data itself, which is why we place strong emphasis on security safeguards at both the system and broader infrastructure levels.

Facial recognition is now widely deployed for contactless identity checks. How mature is the technology in balancing convenience with security at scale?

Troy Wu: Facial recognition has reached a high level of maturity across many everyday applications and is now widely deployed for contactless identity verification. However, mission-critical environments such as airports, customs checkpoints, and public services continue to present unique challenges.

The key issue is balancing convenience with regulatory compliance and uncompromised security. In some deployments, organisations still reduce accuracy thresholds to improve processing speed, but doing so inevitably increases security risks.

The next stage of evolution will focus on overcoming these operational edge cases. Our goal is to enable organisations to achieve both high throughput and consistently high accuracy, even under the demanding conditions found in large-scale public infrastructure.

HID emphasises an end-to-end biometric lifecycle. Why is this integrated approach more effective than standalone deployments?

Troy Wu: Identity security is strongest when every stage of the biometric journey is connected—from enrolment through to verification.

Standalone deployments often create fragmented identity ecosystems where different agencies or systems operate independently, making interoperability difficult and reducing operational efficiency.

HID addresses this by providing an open, modular approach that integrates seamlessly with existing hardware, readers, and backend biometric identification platforms. This flexibility allows organisations to deploy a complete end-to-end solution or integrate our technologies into their existing infrastructure while maintaining a unified, trusted identity ecosystem.

Looking ahead, how will biometrics evolve to support mobile identity and real-time verification in the field?

Troy Wu: The future of biometrics is becoming increasingly mobile, intelligent, and real-time.

We're seeing growing demand for on-device biometric verification, allowing identity checks to be performed directly in the field rather than relying exclusively on centralised backend systems. Edge AI is central to this evolution, enabling capabilities such as image capture, quality assessment, liveness detection, and biometric matching to take place directly on the device. This significantly reduces latency while improving responsiveness and overall system performance.

At the same time, governments are accelerating the adoption of digital identities, with trusted biometric verification forming a critical foundation for these initiatives. Over the next three to five years, we expect even closer integration between mobile identity platforms and field-ready biometric systems, particularly across law enforcement, border management, and immigration applications. ■

Public–Private Synergy: *Building the Backbone of Next-Gen Smart and Secure Cities*

Inside the Billion-Dollar Alliance Between Governments and Tech Giants Engineering Tomorrow's Safe Cities

- *Global safe-city market growing from $27.28B (2021) to $87B by 2030, fueled by joint AI/IoT investment.*
- *Neither side builds Safe Cities 2.0 alone — government sets policy and funding, industry builds the tech (India, NYC, China, Gulf cases).*
- *AI could cut crime 30–40% and response times 20–35%, but trust, interoperability, and data governance remain the real hurdles.*

Can governments alone keep cities safe in an era of AI-driven crime, cyber threats, and growing urban complexity?. Can private technology companies build trusted security systems without public oversight?. Increasingly, the answer to both is no.

Safe Cities 2.0 is being built through public–private synergy, where governments provide policy and oversight, while industry delivers the innovation and expertise that modern urban security demands.

The scale of this transformation is evident. The global safe-city market is projected to grow from US$27.28 billion in 2021 to US$87 billion by 2030, driven by investments in AI, IoT, and real-time intelligence.

As these partnerships reshape homeland security, the challenge is no longer just deploying smarter technology; it's ensuring collaboration delivers resilient, accountable, and trusted cities.

Why Public–Private Partnerships Became the New Security Model

Governments Set the Direction
Governments remain at the centre of every safe-city programme, defining

Images by Freepik

security priorities, allocating funding, establishing regulatory frameworks, and coordinating law enforcement and emergency services. But as cities become more connected and threats more complex, public agencies are increasingly looking beyond traditional procurement models to deliver next-generation capabilities.

Industry Powers the Innovation

Artificial intelligence, IoT sensors, cloud platforms, cybersecurity, and integrated command centres are largely developed and deployed by the private sector. Technology providers, telecom operators, and systems integrators bring the expertise needed to connect thousands of devices into a unified operational ecosystem capable of delivering real-time situational awareness.

A Shared Responsibility for Urban Security

Neither sector can deliver Safe Cities 2.0 in isolation. Governments provide leadership, oversight, and public accountability, while industry drives innovation and long-term technology development. Together, they are creating resilient, data-driven security ecosystems that are redefining how cities prevent, respond to, and recover from evolving homeland security challenges.

Beyond the investment, the impact is becoming measurable: AI-enabled smart-city technologies could help reduce crime by 30–40% and cut emergency response times by 20–35%, highlighting why governments and industry continue to deepen their collaboration.

Collaboration in Action: How Cities Are Putting the Model to Work

The public–private partnership model is no longer theoretical. Across the world, governments are working

Image by Freepik

"There is a lot of mistrust between communities and the police, and what we have seen again and again is that traditionally marginalised low-income communities are less likely to call for help. Introducing technology like gunshot detection empowers your police officers and law enforcement agencies to respond and help the community."

– Jeff Merritt

Image by Freepik

with technology providers, telecom operators, and systems integrators to build security ecosystems tailored to their unique urban challenges. While each programme differs in scale and governance, the underlying principle remains the same: combining public oversight with private innovation to strengthen urban resilience.

India: Modernising Urban Security at Scale

India's Safe City Programme demonstrates how government funding and private-sector expertise can work together to modernise public safety.

Supported by the Nirbhaya Fund, projects across eight cities integrate thousands of CCTV cameras, emergency call boxes, analytics platforms, and Integrated Command and Control Centres (ICCCs).

In Bengaluru, Honeywell delivered Phase 1 by deploying more than 7,000 cameras, creating a connected surveillance network that supports law enforcement and emergency response.

United States: Turning Data into Situational Awareness

New York City's Domain Awareness System, developed jointly by the NYPD and Microsoft, illustrates the power of integrated intelligence. By combining CCTV feeds, automatic licence plate recognition, and other public safety data into a single operational platform, the system enables authorities to identify patterns, monitor incidents, and coordinate responses more effectively.

China: Scaling Integrated Surveillance

China has taken collaboration to an unprecedented scale through programmes such as Sharp Eyes and Skynet, working closely with domestic technology companies including Hikvision. Millions of connected cameras, AI-enabled analytics, and facial recognition capabilities provide extensive situational awareness, demonstrating how government policy and private-sector innovation can rapidly expand urban security infrastructure.

The Gulf: Building Security into New Cities

Rather than retrofitting existing infrastructure, Gulf nations are embedding digital security into city planning from the outset. Dubai's Oyoon platform, Abu Dhabi's Falcon Eye, and Saudi Arabia's NEOM integrate AI, connected sensors, and command centres as core components of urban development, reflecting a long-term vision where security is designed into the city's digital foundation rather than added later.

The Technology Stack Behind Safe Cities 2.0

Modern safe-city platforms are built on a multi-layered digital architecture that integrates sensing, communications, analytics, and command-and-control capabilities into a unified operational environment. Rather than functioning as standalone technologies, these components form an interoperable ecosystem that enables real-time situational awareness and coordinated multi-agency response.

Edge Sensing and Data Acquisition

The foundation of the stack consists of distributed edge devices, including high-definition IP cameras, automatic licence plate recognition (ALPR) systems, facial recognition terminals, acoustic gunshot detection sensors, environmental monitoring devices, UAVs, and

IoT endpoints. Increasingly, edge AI enables these devices to perform object classification, behavioural analysis, and metadata extraction locally, reducing latency and bandwidth requirements before transmitting actionable data upstream.

Communications and Network Infrastructure

The sensing layer is supported by resilient communications infrastructure comprising fibre-optic backbones, private LTE and 5G networks, software-defined networking (SDN), and secure IP transport. High-bandwidth, low-latency connectivity enables continuous transmission of video streams, telemetry, and operational data while supporting mission-critical applications across geographically distributed environments.

AI, Analytics, and Data Fusion

At the intelligence layer, AI engines aggregate and correlate data from multiple sources to generate contextual situational awareness. Advanced video analytics perform facial recognition, object detection, intrusion monitoring, crowd-density estimation, behavioural analysis, and anomaly detection. Machine learning models, geospatial intelligence (GIS), and event correlation platforms fuse structured and unstructured data, enabling predictive risk assessment and accelerated decision-making.

Integrated Command and Control

The Integrated Command and Control Centre (ICCC) serves as the operational core of the ecosystem. Built on Physical Security Information Management (PSIM) and Command-and-Control (C2) platforms, ICCCs consolidate feeds from surveillance systems, emergency services, traffic management, access control, public safety communications, and critical infrastructure monitoring into a Common Operating Picture (COP).

Image by Freepik

This enables cross-agency coordination, resource allocation, incident orchestration, and real-time operational decision support.

Cybersecurity and Data Governance

As Safe Cities become increasingly software-defined, cybersecurity has evolved into a foundational layer rather than a supporting function. Zero Trust architectures, end-to-end encryption, identity and access management (IAM), Security Information and Event Management (SIEM), Security Operations Centres (SOCs), and continuous threat monitoring are now essential to protecting critical infrastructure.

At the same time, data governance frameworks define data ownership, retention policies, auditability, and regulatory compliance, ensuring that operational effectiveness is balanced with accountability and public trust.

Building Trust Through Technology

Technology may power Safe Cities 2.0, but trust determines their success. As AI and surveillance become central to public safety, communities must see these technologies as tools that protect them, not simply monitor them.

For governments and law enforcement, that means using technology to improve transparency, responsiveness, and public confidence. This is especially important in communities where trust in law enforcement has historically been low.

Ultimately, technology alone cannot build trust. Long-term public confidence depends on transparent governance, responsible AI, strong cybersecurity, and clear

accountability that ensure innovation serves both citizens and public safety.

The Challenges Shaping the Next Generation of Safe Cities

Challenge	Why It Matters
Interoperability	Many cities still operate fragmented legacy systems that cannot seamlessly exchange data, limiting real-time situational awareness and coordinated multi-agency response.
Data Ownership and Governance	As surveillance data flows across government agencies and private partners, questions over ownership, access, retention, and accountability become increasingly complex.
Cybersecurity Risks	Every connected camera, sensor, and command platform expands the attack surface, making cyber resilience essential to protecting critical infrastructure and public safety operations.
AI Governance and Ethics	Facial recognition, behavioural analytics, and predictive AI are advancing faster than regulatory frameworks, raising concerns around privacy, bias, transparency, and accountability.
Vendor Lock-in and Technology Sovereignty	Dependence on proprietary platforms or a limited pool of technology suppliers can reduce operational flexibility, increase lifecycle costs, and expose cities to geopolitical and supply-chain risks.

The Road Ahead: From Smart Cities to Intelligent Security Ecosystems

Safe Cities 2.0 is evolving beyond surveillance into a connected digital ecosystem where artificial intelligence, edge computing, cloud platforms, and predictive analytics work together to enhance urban resilience. Rather than investing in isolated technologies, governments are increasingly prioritising platforms that can adapt to emerging threats, integrate new capabilities, and support multiple public services through a single operational framework.

Open Architectures Will Replace Closed Ecosystems

Cities are gradually moving away from monolithic, single-vendor deployments in favour of modular, interoperable platforms. Open APIs and standards-based architectures allow agencies to integrate cameras, sensors, analytics engines, and command software from multiple vendors, reducing vendor lock-in while extending the lifespan of critical infrastructure.

AI Will Become a Decision-Support Tool

Artificial intelligence is shifting from passive video analysis to proactive operational support. Large language models, computer vision, and predictive analytics are beginning to assist operators by correlating data, identifying anomalies, and prioritising incidents, enabling faster and more informed decision-making without replacing human oversight.

Cyber Resilience Will Become Core Infrastructure

As urban security becomes increasingly software-defined, cybersecurity will no longer be viewed as a supporting function. Secure-by-design architectures, Zero Trust frameworks, continuous monitoring, and resilient communications networks will become fundamental requirements for protecting critical infrastructure and maintaining operational continuity.

Trust Will Define the Next Generation

The future of Safe Cities will not be determined solely by the sophistication of AI or the number of connected devices. Long-term success will depend on whether governments and industry can build systems that are interoperable, transparent, secure, and trusted by the communities they serve. In the next phase of urban security, trust will become as valuable as technology itself. ■

Image by Freepik

COMING SOON

AUG 11 – 13 2026
Indo Security & Forum 2026
Jakarta, Indonesia
https://indosecurity.com/

SEP 2 – 4 2026
Security Exhibition 2026
Sydney, Australia
https://www.securityexpo.com.au/

SEP 9 – 12 2026
Secutech Vietnam 2026 *(Page 3)*
Hanoi, Vietnam
www.secutechvietnam.com

SEP 9 – 12 2026
OS+H Asia 2026 *(Page 17)*
Singapore
www.osha-singapore.com

SEP 22 – 25 2026
Security Essen 2026
Essen, Germany
www.security-essen.de

SEP 29 – 30 2026
Cyber Security World Asia 2026 *(Page 5)*
Singaopore
www.cybersecurityworldasia.com

OCT 28 – 30 2026
SIDEX-ACDR 2026 *(Page 11)*
Singapore
https://sidex.sg/

NOV 18 – 20 2026
Safety & Security Asia 2026 *(Page 13)*
Singapore
www.safetysecurityasia.com

NOV 18 – 20 2026
Secutech Thailand 2026 *(Page 3)*
Bangkok, Thailand
www.secutechthailand.com

NOV 18 – 20 2026
Secutech Thailand 2026 *(Page 3)*
Bangkok, Thailand
www.secutechthailand.com

NOV 25 – 27 2026
DigiTech ASEAN Thailand 2026 *(Page 15)*
Bangkok, Thailand
www.digitechasean.com

APR 21 – 23 2027
Secutech Taiwan 2027 *(Page 3)*
Singapore
www.secutech.com

SUBSCRIPTION FORM

Email your order to:
yvonne.ooi@tradelinkmedia.com.sg

PRINT

Please (√) tick in the box.

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

Singapore	○ SGD$70.00	America, Europe	○ SGD$220.00
Malaysia / Brunei	○ SGD$120.00	Japan, Australia, New Zealand	○ SGD$220.00
Asia	○ SGD$180.00	Middle East	○ SGD$220.00

☐ **Southeast Asia Construction**
Since 1994

DIGITAL

Bathroom + Kitchen Today
Since 2001

Lighting Today
Since 2002

Southeast Asia Building
Since 1974

Security Solutions Today
Since 1992

Bathroom + Kitchen Today
is available on digital platform.
To download free PDF copy,
please visit:
http://bkt.tradelinkmedia.biz

Lighting Today
is available on digital platform.
To download free PDF copy,
please visit:
http://lt.tradelinkmedia.biz

Southeast Asia Building
is available on digital platform.
To download free PDF copy,
please visit:
http://seab.tradelinkmedia.biz

Security Solutions Today
is available on digital platform.
To download free PDF copy,
please visit:
http://sst.tradelinkmedia.biz

Personal Particulars

Name: _____

Position: _____

Company: _____

Address: _____

_____

Tel: _____ 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

☐ Bank transfer payable to:
Trade Link Media Pte Ltd

Bank Details

Account Name:	Trade Link Media Pte Ltd
Account Number:	033-016888-8
Name of Beneficiary Bank:	DBS Bank
Address of Beneficiary Bank:	12 Marina Boulevard, DBS Asia Central, Marina Bay Financial Centre Tower 3, Singapore 018982
Country:	Singapore
SWIFT Address/Code:	DBSSSGSG

☐ PAYNOW to:
Trade Link Media Pte Ltd

PAYNOW option is applicable for **Singapore companies only**.

Company Registration Number: 199204277K

* GST inclusive (GST Reg. No: M2-0108708-2)

ADVERTISE WITH US TODAY!

Email us at info@tradelinkmedia.com.sg.

Scan to visit our website