APR – JUN 2026

SECURITY SOLUTIONS TODAY

FUTURE OF INTEGRATED SECURITY: SMARTER, SAFER, CONNECTED

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)

Your Number 1 Choice in Asia's Security and Fire Safety Markets

3 SHOWS
39,720 SQM
45,000 VISITORS

secutech

22 - 24 April 2026
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

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
13,000 Visitors

Concurrent with

fire & safety
presented by Secutech Thailand

Thailand Smart City Expo

Download Info Pack

www.secutechthailand.com

CONTACT US

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

messe frankfurt

INSIDE THE NEXT-GENERATION DATA CENTRE: A THOUGHTFUL, LAYERED AND INTEGRATED APPROACH TO SECURITY

By Tim Martin, vice president and general manager of international markets for Wesco

In the not-too-distant past, security within a data centre equated to little more than a handful of security cameras, a few locked doors, and perhaps one or two security guards working in rotating shifts. From initial planning through the construction phases, and into the deployment phase, the actual security of the data centre was treated almost as an afterthought, with products specified late in the process, and a security-centric design nowhere to be found.

The results were predictable: blind spots, rework orders, and audit risks. That's why they were finished and in operation. Active data centre campuses with ongoing, phased construction presented even more challenges.

Today, the world runs on data; we depend on it, and its security and integrity are paramount. Mission-critical considerations include protecting sensitive data, defending against cyber threats, ensuring uptime and reliability, preventing financial loss, safeguarding physical assets, and meeting compliance and regulatory requirements.

> *"Physical security is now inseparable from resilience, trust and competitive differentiation in the data centre market."*
> ***- Security Industry Association, Securing Data Centres (2025)***

The Challenges of Phased Construction and Why They Matter

Phased construction provides security challenges. When one data hall is active while other areas are still being built, operators must manage changing access routes, mixed traffic, and constantly evolving site conditions. These situations can weaken security controls if they aren't carefully planned from the beginning.

Historically, under-allocation and late value engineering have pushed physical security to a low single-digit percentage of build budgets, only for the costs to return as retrofits and operational issues. Analysts expect nearly 100 GW of new capacity from 2026–2030, with power now the primary site-selection constraint and rack densities constantly climbing, creating conditions that can magnify the price of security missteps.

From the Outside In: A Layered Approach

As the need for data privacy and security has come to the


Image by Freepik

forefront, so too have data centre privacy and security. Owners, architects, engineers, and contractors are increasingly coming around to the idea that data centre integrity requires more than video surveillance; it must also consider perimeter protection, access control, intrusion detection and alarm systems, environmental monitoring, infrastructure and cabling, and fully integrated security and environment management software. And these need to be planned for, long before a shovel breaks ground.

A comprehensive and layered approach to data centre security should include an outer protective layer, a middle protective layer, an inner protective layer, and asset protection. And yes, surveillance cameras can and should be deployed at every layer.

The outer protective layer can include natural or man-made barriers along the property line, such as fencing, security gates, card readers, security-rated landscaping, tree lines, and ridges; all of it can be leveraged to help defend the site.

Next, the middle protective layer serves as added security around the exterior of the building. This can include protective traffic bollards, lighting systems, and even the building design itself, which can be designed and positioned to lessen the risk of attack and penetration.

The inner protective layer begins at every doorway and window. From alarm systems, coded and keyed entryways, and specialized access control, to reinforced doorways and man-traps, occupancy sensors, and hallway design, this layer can incorporate a wide variety of systems to help protect all of the areas and assets within the data centre, from the front door to the data hall.

Lastly, the asset protection layer within a data hall can be implemented at the rack level, helping to secure assets with coded cabinet entry, in-rack cameras, and real-time monitoring.

continue on page 6

MTX
Milipol TechX

MTX (Milipol TechX) 2026

28 - 30 April 2026

Sands Expo & Convention Centre, Singapore

Supercharging Innovation for Our Safer Tomorrow

REGISTER FOR YOUR FREE VISITOR PASS

www.mtx.sg

Smarter: Better Information and Quicker Action

Advanced security systems go beyond simply detecting activity. With accurately configured analytics, operators can distinguish between routine activity and events that genuinely require attention. When intelligence is built into devices such as cameras, controllers, and gateways, and those devices are connected through open, integrated platforms, alerts can trigger a clear and coordinated response. Teams can quickly view the right camera feeds, confirm events through multiple sources, and respond with more confidence and context.

Safer: Cyber-Physical Resilience by Design

Security devices should be managed with the same structure as other technology assets. In a data centre, this means maintaining an accurate inventory of devices, controlling access carefully, managing firmware and software updates, and keeping systems aligned to defined standards. Integrations should be tested regularly so that updates do not create hidden failures.

Connected: Interoperable Ecosystem

Resilience arrives when video, access control, intrusion detection, intercom, and operations comms operate as a single environment. When these systems are integrated, a single event can trigger multiple coordinated actions automatically, for example, securing an entry point, directing cameras to the right location, notifying personnel, and displaying guidance where needed. Finally, bringing security and building systems onto a single pane of glass or a unified view provides faster verification of events and speedier response.

Data centre security is optimized when security is designed in, not bolted on mid-way through or after construction. Whether in a phased-build, live environment, or in a completed campus, the importance of integrated security, embedded perimeter, access control, and surveillance aligned alongside utilities, traffic flows, and phasing, will help reduce later disruptions and ensure that security will support the facility operations.

About Wesco Anixter

Wesco International (NYSE: WCC) builds, connects, powers, and protects the world. Headquartered in Pittsburgh, Pennsylvania, Wesco is a FORTUNE 500® company with approximately $24 billion in annual sales in 2025 and is a leading provider of business-to-business distribution, logistics services, and supply chain solutions.

Wesco provides end-to-end data centre solutions and services supporting data centre operators, owners, end users, and contractors across all stages of data centre design, development, construction, deployment, operations, maintenance, and support. Wesco provides focused expertise and solutions to support the entire data centre lifecycle, including advisory services, site selection, supply chain and deployment services, gray space and white space product specification, and managed services.

From design and planning, through construction, operations, and beyond, Wesco's data centre solutions deliver services for every phase of data centre construction. Wesco can provide holistic solutions and comprehensive program and project management in more than 50 countries, ensuring efficient, reliable, and scalable data centre operations.

Wesco Anixter represents the international go-to-market brand of Wesco and brings to life the company's mission to build, connect, power, and protect the world for its customers and supplier partners in the regions of APAC, CALA, and EMEA. ■

Tim Martin
Vice President & General Manager International Markets, Communications & Security Solutions, ***Wesco Anixter.***

Tim Martin became the Vice President & General Manager International Markets of Wesco Anixter's Communications & Security Solutions (CSS) business in August 2025. He leads the organisations in the Asia Pacific, Europe, the Middle East, and Africa that provide connectivity, power, security, safety, professional audio/ visual, and wireless solutions across a broad range of industries.

Tim is a Wesco Anixter employee through the company's 2020 acquisition of Anixter, joining in 2008. During his tenure at Wesco Anixter, he has held several sales leadership, P&L, and functional roles, including branch/regional management across the APAC region.

Tim has an MBA in Marketing & Business from Macquarie University and is a qualified Electrician with over 30 years' experience in the Electrical and Communications industry across channels, manufacturing, and distribution. He is based out of Wesco Anixter's office in Sydney, Australia.

Altronix®

ACCESS & POWER INTEGRATION…
…ENDLESS POSSIBILITIES

TROVE™ lets you design and deploy your preferred brand of access control with Altronix power solutions in virtually any environment.

- Simplifies board layout & wire management
- Reduces installation and labor cost
- Scalable for any size system
- Available as pre-configured and pre-wired kits

Streamline your access control deployments with **TROVE**™. Only from Altronix.

RUN WITH IT™

ACRE SECURITY UNVEILS ACRE BRIDGE AT ISC WEST 2026

Acre's "Bridge" Delivers Seamless Hybrid Modernization

PLANO, TX — March 17, 2026 — Acre Security, a global provider of integrated security technology, today announced the launch of Acre Bridge, a new device designed to connect existing on-premises access control systems directly to Acre Access Control (AAC). The Acre Bridge empowers organizations to move toward the cloud on their own terms, evolving with their own security needs at a pace that aligns with operational realities.

Set to be unveiled at ISC West 2026, Acre Bridge addresses a growing market reality: most organizations operate hybrid security environments that cannot transition to the cloud overnight.

By synchronizing people, devices, and events between existing controllers and AAC, Acre Bridge allows customers to run existing and cloud-native systems in parallel throughout the transition, without compromise, while unlocking modern capabilities such as mobile credentials and centralized remote management. The launch reflects a broader strategic focus, shaped by partner feedback, to deliver modernization without disruption.

"Last year was about listening and defining our direction forward. Our partners want modernization without disruption and a clearer path to long-term growth. Acre Bridge delivers that flexibility, and now our focus is execution, simplifying how we work together and enabling partners and customers to modernize with confidence
-Kumar Sokka, CEO of Acre Security.

The launch of Acre Bridge coincides with a refreshed global partner program designed to better support partners navigating hybrid and cloud-driven business models. Building on operational investments made over the past year, Acre is also enhancing its partner portal with RevCloud integration to simplify quoting and ordering.

Acre is also introducing a more aligned program structure to ensure incentives, resources, and program tiers better reflect partners' evolving on-premises and cloud business models, along with dedicated market development funds for qualified partners.

Acre's broader strategy centers on a unified security portfolio anchored by Acre Access Control. The platform integrates access control, intrusion, visitor management, and video capabilities into a cohesive solution while continuing to support established on-premises platforms, recognizing their proven reliability and ongoing role in hybrid deployments.

Acre will be demonstrating Acre Bridge at booth #23015 at ISC West, being held March 25-27, 2026, at the Venetian Expo Center in Las Vegas.

About Acre Security

Since 2012, Acre has helped reshape the future of physical security, bridging legacy infrastructure and cloud innovation to deliver solutions that are intelligent, flexible, and ready for what's next. With a team of over 500 professionals across 25+ countries, Acre is committed to helping organizations protect what matters most. ■

Image by Freepik

VIVOTEK PARTNERS WITH TAIWAN'S NATIONAL DEVELOPMENT COUNCIL TO ADVANCE REGIONAL REVITALIZATION

AI-driven Security Solutions Empower Communities and Ecosystems for Sustainable Impact

VIVOTEK, a leading global security solutions provider, has spent the past five years advancing its "Safety Map" sustainability initiative, leveraging its security expertise to strengthen community and environmental resilience. In 2024, VIVOTEK partnered with the Hualien-based regional revitalization team Lamb Social Innovation Studio to assess safety risks and blind spots in Dachen New Village and propose improvement solutions.

The project was selected as a representative case for the 2026 Regional Revitalization and Corporate Sustainability Co-Creation Forum organized by Taiwan's National Development Council, highlighting how collaboration between businesses and local communities can drive sustainable regional development.

Image by Freepik

Embedding Sustainability into Corporate Strategy

Li-Pei Peng, Deputy Minister of the National Development Council, noted that the NDC has also partnered with the Financial Supervisory Commission and the Taiwan Stock

continue on page 10

Exchange to incorporate the regional revitalization initiative into ESG evaluation reference examples starting in 2026. To address growing interest from companies on how to practically engage with regional revitalization efforts, the NDC introduced three partnership models designed to help businesses participate more effectively while enabling local revitalization teams to better connect with corporate partners, build long-term collaborations, share risks, and achieve mutual success.

Working with PwC Sustainability Services Company, the NDC proposed three partnership models: the Accelerator Model, the Value Integration Model, and the Ecosystem Building Model. VIVOTEK's initiative falls under the Ecosystem Building Model: Cross-sector Integrated Action, which emphasizes cross-disciplinary collaboration. Through this approach, corporate resources are connected with regional revitalization teams, academia, and public-sector organizations to address systemic regional challenges while integrating safety into local development.

"VIVOTEK is committed to becoming the most trusted security brand. Through the 'Safety Map' initiative, we put our sustainability vision into action by working with partners to creatively integrate security solutions into local culture and everyday life. We are honored to receive recognition from the National Development Council and look forward to continuing collaboration across industry, government, and academia to promote social safety and build a more sustainable future together."

- Allen Hsieh, Spokesperson and Director of CorpComm & Sustainability Office, VIVOTEK.

Through the project, VIVOTEK employees identified key safety challenges in Dachen New Village and introduced solutions, including accessible facilities, smart lighting, AI-based identification of unfamiliar individuals, and AI-powered cameras. The initiative strengthened community safety while supporting cultural preservation and tourism development. Building on these results, Lamb Social Innovation Studio has gained strong support from local authorities, with public funding allocated to upgrade security infrastructure and improve community living conditions.

Expanding Impact Across Taiwan

Over the past five years, VIVOTEK's "Safety Map" initiative has brought together partners from industry, government, academia, and research institutions, with more than one hundred participants contributing over 3,000 volunteer hours. The program's impact spans communities across Taiwan, including neighborhoods in:

- Zhonghe, New Taipei City
- Happy Home Mental Retardation Training Services Institution in Taoyuan City
- Shuangxi Elementary School in Taipei's Shilin District
- Dachen New Village in Hualien.

Last year, the initiative expanded to the Zhonggua River in Nantou, extending its impact into biodiversity conservation. Working with the National Chung Hsing University USR team, VIVOTEK helped restore the river ecosystem and create habitats for wildlife. In collaboration with DATAYOO, the project leverages its FarmiSpace PRO monitoring service and AI crop monitoring system to analyze crop indices derived from satellite spectral data. The system also captured rare footage of the protected crab-eating mongoose foraging in the area. By combining intelligent security technologies with AI capabilities, VIVOTEK aims to create long-term value for communities and the natural environment. ■

I-PRO INTRODUCES ITS FIRST CAMERAS WITH GENERATIVE AI AT THE EDGE

New flagship fisheye cameras deliver intelligent 360° coverage with easy, intuitive context-rich searches and proactive alerts

Tokyo, Japan, March 19, 2026 — At ISC West 2026, booth #26053, i-PRO Co., Ltd., a global leader in professional security and public safety solutions, will introduce its first cameras with generative AI running fully at the edge, enabling natural-language interaction with live video without relying on cloud services or external servers. Following i-PRO's introduction of generative AI for forensic video analysis in 2025, this introduction marks the next step in the company's GenAI strategy, bringing generative AI from post-event analysis into real-time on-camera operations.

Bringing Generative AI to Real-Time Security Operations

With the new X-series fisheye cameras, i-PRO extends generative AI from post-event investigation into daily security operations such as live incident detection and real-

continue on page 12

NO CHALLENGE TOO TOUGH. NO SOLUTION TOO BOLD.

VISIT US AT

MILIPOL TECHX 2026

SANDS EXPO AND CONVENTION CENTRE, SINGAPORE

28–30 APRIL 2026

BOOTH L1-G01

ST Engineering delivers integrated, cyber safe by design manned unmanned teaming solutions that empower public safety and security agencies to respond decisively to address new threats by seamlessly connecting frontliners, autonomous systems, and intelligent command platforms.

ST Engineering

time alerting. Running directly on the camera without reliance on cloud services or analytics servers, the system enables faster operator response. This launch brings practical, real-time intelligence to the edge, supporting faster and more confident decision-making across everyday security scenarios.

> *"Free text interaction changes the way people work with video. By embedding generative AI directly into the cameras, i-PRO simplifies operators' work by delivering real-time insights that support faster, more confident decisions, regardless of system size or complexity, while keeping data local, secure, and fully under the customer's control."*
> ***- Gerard Figols, Chief Operating Officer, i-PRO.***

Generative AI at the Edge

Generative AI at the edge changes how security teams interact with video, reducing manual configuration, simplifying workflows, and accelerating response. Designed for mission-critical environments, the new line of fisheye cameras combines full 360-degree coverage, advanced imaging performance, and enterprise-grade cybersecurity.

At the core of the new fisheye cameras is a generative AI engine running fully on the edge, utilizing Ambarella™'s CV72 AI vision SoC. This enables real-time free-text detection based on natural-language descriptions rather than predefined rules or rigid attribute lists. Detection logic and feature extraction are performed entirely on the camera, without reliance on cloud services or external servers.

For live monitoring, operators can describe what they want to detect in plain language—such as "person lying down" or "delivery truck," and the camera continuously monitors for those conditions, triggering alerts when detected. Because detection runs directly on the camera, the system delivers low-latency response, simplified deployment, and reduced infrastructure complexity.

Faster Investigations with a Privacy-Focused Design

For forensic investigations, generative-AI-powered free text search enables operators to locate people, vehicles, or objects across recorded video by typing a natural-language description. Feature extraction and metadata generation are performed on the camera, while the free text search itself is executed via i-PRO Active Guard using this on-camera metadata.

For VMS integration, i-PRO Active Guard performs free text search across recorded video, while real-time free text detection and feature extraction remain fully on-edge. This architecture ensures sensitive video data remains on-premises, supporting privacy, compliance, and data-sovereignty requirements.

By leveraging metadata rather than raw video streams, i-PRO's approach

Image by Freepik

continue on page 14

messe frankfurt VIETFAIR

secutech+

VIETNAM

AI, IOT & ICT FOR SMART SOLUTIONS

9 - 12 September 2026

Friendship Cultural Palace, Hanoi

480+	13,000	17,000
Exhibiting brands	Square meters	Visitors

Concurrent events

fire & safety presented by Secutech Vietnam

SM building presented by Secutech Vietnam

Download Show Info

messe frankfurt NCC

secutech

THAILAND

18 - 20 November 2026

QSNCC, Bangkok

400+	11,600	14,000
Exhibiting brands	Square meters	Visitors

Concurrent events

fire & safety presented by Secutech Thailand

Thailand Smart City Expo

Download Show Info

supports privacy-first deployments and responsible AI usage by design. Together, these capabilities reduce investigation time from hours to seconds, lower manual workloads, and help operators and partners automate workflows, accelerate response, and improve operational efficiency.

Expanding Edge Intelligence

Additional AI capabilities include AI On-Site Learning to adapt detection to the unique characteristics of each environment, and AI Processing Relay, which brings AI analytics to non-AI cameras through the new X-series models.

High-Performance Imaging for Demanding Environments

The cameras feature a true 12.5MP fisheye sensor, delivering clear, detailed panoramic views in both indoor and outdoor deployments. AI Noise Reduction (AI-NR), a core imaging differentiator of i-PRO cameras, significantly reduces noise and motion blur in low-light conditions, delivering clearer and more detailed images even in dark or nighttime environments.

By improving image clarity at the source, AI-NR enhances evidentiary value and improves the accuracy and reliability of AI-based detection and metadata generation. Combined with IR illumination and an optional white LED for full-color visibility, the camera ensures precise detection and reliable insights even in complete darkness.

Open Platform with Enterprise-Grade Security

Built on i-PRO's open architecture, the new cameras support Docker containers, allowing secure deployment of custom or third-party AI applications directly on the device. This flexibility helps organizations avoid vendor lock-in and extend the value of their existing systems.

Advanced cybersecurity features such as Secure Boot, signed firmware, and FIPS 140-3 Level 3 compliance make the camera suitable for high-security environments.

Outdoor models include an IK11 and IP69-rated rugged housing, ensuring reliable operation in harsh conditions ranging from transportation hubs and industrial facilities to campuses and public venues.

A New Standard for Panoramic Security

Fisheye cameras are often chosen to eliminate blind spots and reduce infrastructure complexity. With the new X-series fisheye lineup, i-PRO extends that value by combining panoramic coverage with generative AI at the edge, delivering intelligence that is faster to deploy, easier to use, and designed to scale without cloud dependency.

With 360° coverage from a single device, organizations can reduce camera counts, cabling, storage, and licensing requirements, further lowering total system costs while simplifying installation and long-term maintenance.

The new X-Series fisheye cameras with generative AI at the edge will be available globally beginning June 2026.

Image by Freepik

About i-PRO

i-PRO Co., Ltd., is a leading global manufacturer of edge computing cameras for security, safety, and medical applications. With over 60 years of expertise in high-quality and reliable hardware, the company now pioneers the transformation of video data into practical applications.

i-PRO products are designed for flexible customization and integration to meet the specific needs of any use case. We are committed to the ethical and responsible use of AI and cybersecurity for data integrity, and provide our partners, customers and users with innovative and sustainable technologies. i-PRO joined the United Nations Global Compact in 2023. ■

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

SIEMENS UNVEILS NEXT-GEN FIRE SAFETY PROTECTION, PAVING THE WAY FOR AUTONOMOUS BUILDINGS

- Siemens' new Sinteso Nova and Cerberus Nova fire detectors transform traditional fire detection into proactive, smart, connected safety solutions through cloud connectivity.
- Advanced detection, combined with ease of modernization, provides tailored advantages for facilities across industries.
- The fully IoT-connected portfolio enables 24/7 self-checks, real-time monitoring, remote diagnostics, and predictive maintenance.

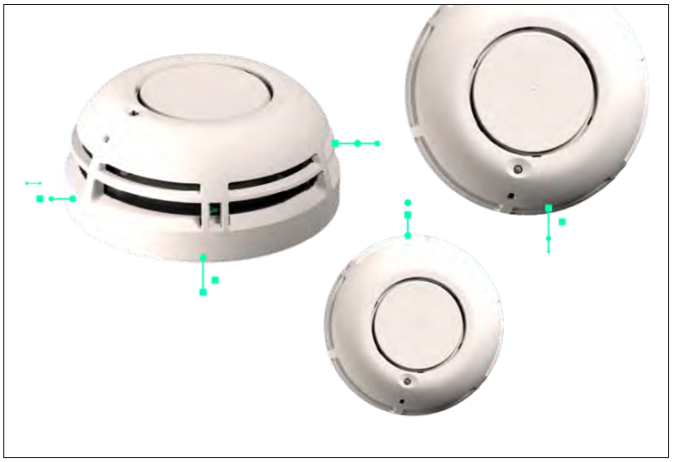
Siemens Smart Infrastructure today unveiled its new Sinteso Nova and Cerberus Nova fire detector portfolio, set to transform traditional fire safety into a proactive, smart, and connected approach. This portfolio is part of the foundation of technologies paving the way toward autonomous buildings.

The new systems enhance operational safety, streamline service team efficiency, allow for easy system upgrades, and unlock data-driven digital services through cloud connectivity. They are designed to meet the needs of various industries such as healthcare, higher education, data centers, and commercial real estate.
In healthcare facilities, where patient safety and operational efficiency are both essential, Siemens' new fire detectors ensure performance with continuous, autonomous detection. The automated Disturbance-Free Testing (DFT) technology runs self-checks around the clock, reducing systems' potential downtime. With the support of the Smoke Entry Supervision (SES) technology, which monitors smoke entry points in real time, safety teams can intervene immediately before risks escalate.

Additionally, the ASAplus technology, incorporating multi-wavelength optical and dual thermal detection, minimizes false alarms, decreasing unnecessary evacuations. The fully IoT-enabled detectors are compatible with cloud-based applications, such as Siemens' Building X Fire Apps. These capabilities provide facility teams and service providers with shared, actionable data insights and allow for real-time monitoring, remote diagnostics, and predictive maintenance.

Data centers' high density of electrical systems and the need for continuous operations create unique fire safety risks, including overheating and electrical failures. Siemens' Sinteso Nova and Cerberus Nova detectors not only help maximize the uptime of critical IT and electrical infrastructure but also provide transparency on system conditions. Automated self-checks, cloud-based monitoring, and predictive maintenance allow facility teams to respond quickly and proactively, reducing disruptions and protecting these critical assets efficiently.

Other industries, such as higher education and commercial



real estate, often operate multiple, widely distributed buildings, making centralized fire safety management essential. Siemens' Sinteso Nova and Cerberus Nova detectors help facility teams maintain consistent protection standards across all sites by providing continuous monitoring, reducing the risk of unnecessary disruptions, and supporting proactive maintenance. This holistic approach provides an oversight of widely dispersed facilities and ensures reliable and resilient operations across the entire building portfolio.

"The launch of our Sinteso Nova and Cerberus Nova fire detection portfolio is a game-changer in ensuring all alarms are as accurate as possible. By moving from periodic checks to continuous, data-driven, self-supervising systems, we're laying the foundation for truly human-centric, autonomous buildings. By automating testing, delivering real-time insights, and enabling remote action, these solutions protect people while freeing up staff to focus on strategic priorities. This shift isn't just about innovation, it's about smarter, safer, and more efficient operations."
- Peter Nebiker, Head of Fire Safety at Siemens Smart Infrastructure Buildings.

continue on page 18

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

depa NIA

Organizer

IMPACT MUANG THONG THANI

No matter the industry, the best-in-class Siemens Sinteso Nova and Cerberus Nova detectors represent a transformative approach to fire safety. They allow for stepwise upgrades while ensuring continuous protection, making them suitable for both green- and brownfield projects. Existing fire panels remain compatible, eliminating the need for a rip-and-replace approach. By allowing for plug-and-play integration, including automatic transfers of configured settings, these systems offer seamless modernization while reducing installation time and risk.

Carrying an environmental product performance label, Siemens' EcoTech for enhanced sustainability transparency, the detectors are not only made of recycled plastics, but also promote environmentally responsible design, resource efficiency, and circular economy principles. The Sinteso Nova and Cerberus Nova fire detectors are part of the Siemens Xcelerator portfolio, an open digital business platform that enables customers to accelerate their digital transformation more easily, faster, and at scale. The offering has been developed in Switzerland, where it is also being produced. ■

WHY ZERO-TRUST PRIVILEGED ACCESS MANAGEMENT MAY BE ESSENTIAL FOR THE SEMICONDUCTOR INDUSTRY

By Shane Barney, Chief Information Security Officer, Keeper Security

The semiconductor industry has long been the foundation of the global digital economy, powering innovation across telecommunications, automotive, defense, and cloud computing. With shifting geopolitical dynamics and heightened economic security concerns, semiconductor manufacturing is more important to national strategy than ever before.

Japan, once a global leader in the semiconductor industry, is now undergoing a strategic and security-driven transformation. Innovation, speed, and quality manufacturing have made the country a technological powerhouse for decades. As Japan enters fiscal year 2026, cybersecurity is no longer just an operational concern; it is a national economic security imperative that will shape the future of the country's semiconductor ecosystem.

The Japanese Ministry of Economy, Trade and Industry (METI) has announced a fundamental shift in how strategic semiconductor assets will be protected. Starting in April 2026, any organization receiving government semiconductor subsidies must comply with the Operational Technology (OT) Security Guidelines for Semiconductor Device Factories, introduced in October 2025.

This requirement formally designates semiconductor plants as critical infrastructure, alongside power grids, telecommunications, and water systems, and reinforces a secure-by-design approach to protecting next-generation manufacturing.

From Policy to Mandate

In the past, Japan's technology regulations were largely advisory. However, that innovation-first approach is evolving. The government is increasingly linking economic security to the stability and integrity of the semiconductor supply chain. METI's multibillion-dollar investments now include strict requirements for data sovereignty, infrastructure resilience, and operational security controls.

This shift reflects a global reality: interconnected supply chains cannot tolerate weak identity or access controls at any point. As seen in sectors such as healthcare, aviation, and energy, compliance alone is no longer sufficient. Semiconductor manufacturers must demonstrate operational maturity, resilience against advanced threats, and disciplined governance over privileged access.

At the core of this shift lies a critical question: who has access to sensitive systems, and how is that access

continue on page 20

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

Book Your Booth Today!

Supported by:

SINGAPORE EXHIBITION & CONVENTION BUREAU

A+A

Held in:

SG Passion Made Possible

Organized by:

Messe Düsseldorf Asia

continuously controlled, monitored, and verified?

Identity as the New Security Boundary

Traditional cyber defenses, such as perimeter defenses, network microsegmentation, end-to-end encryption, and real-time automated threat detection, remain essential. Yet in modern operational technology environments, identity and privileged access controls represent the most critical layer of defense. In semiconductor fabrication plants, these controls determine who can access critical systems and manufacturing data, and who can modify production tools and workflows.

Semiconductor fabrication plants rely on engineers, third-party vendors, and automated systems. The traditional "castle and moat" security model, which implicitly trusts users inside the network, is obsolete. Organizations must adopt a modern, zero-trust security architecture that assumes every user, system, and device must be continuously verified before access is granted and maintained.

Under the Principle of Least Privilege (PoLP), organizations ensure that every identity – human, non-human (NHI), or AI agent receives only the minimum level of access required to perform its function. This approach significantly reduces the impact of credential theft and insider threats by preventing breaches from spreading laterally through the organization.

For third-party vendors supporting specialized fabrication systems, Just-In-Time (JIT) access enables temporary, time-bound privileges as an alternative to persistent, high-risk credentials. This eliminates standing access and reduces long-term exposure.

Taken together, these zero-trust principles form the operational backbone required to meet subsidy-linked OT security mandates. Privileged Access Management (PAM) operationalizes these principles, providing centralized visibility, policy enforcement, and real-time oversight across hybrid OT and IT environments.

Protecting Semiconductor Intellectual Property

Controlling access is only one part of the equation. Once identity is verified and access is granted, organizations must ensure that underlying data, intellectual property and production telemetry remain protected against compromise or exfiltration. Zero-trust security architectures govern who can interact with systems while encryption and secrets management protect what those systems contain.

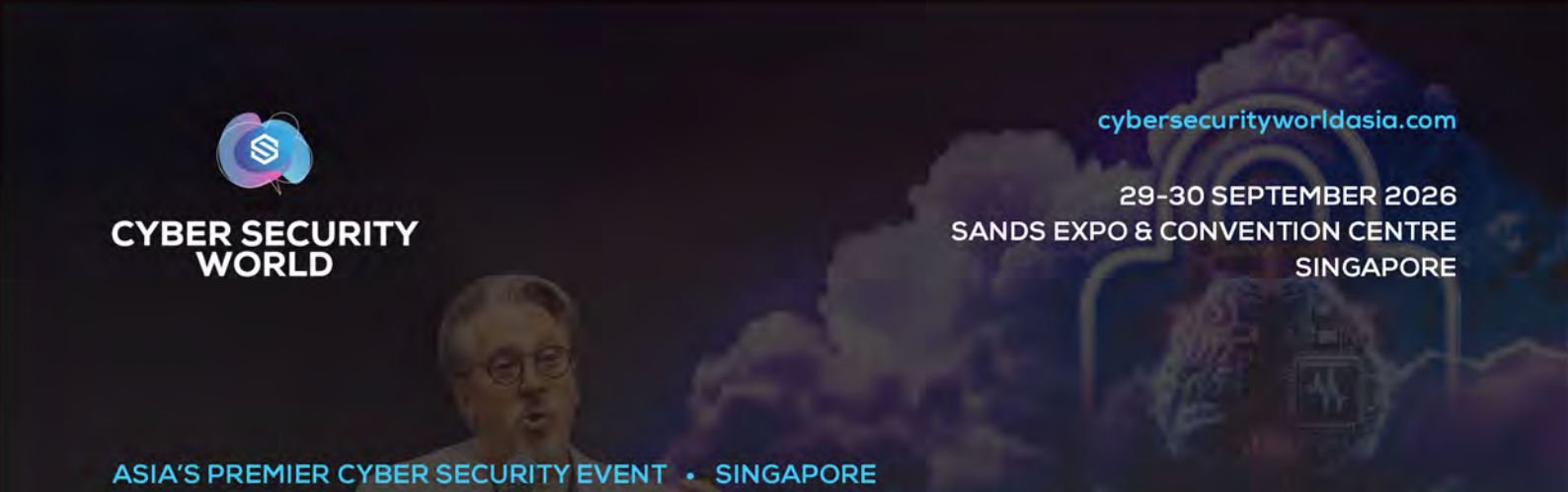
In semiconductor manufacturing, protecting digital blueprints and production telemetry is as critical as safeguarding physical equipment. These assets represent the industry's intellectual property and competitive advantage. Securing them requires encryption built to the highest industry standards, strict identity governance, and comprehensive auditability across all systems.

FIPS 140-3, the current U.S. and Canadian government standard for validating cryptographic modules, establishes a strong encryption baseline. Encryption alone is insufficient, however. If an attacker compromises an overprivileged identity, even the strongest cryptography can be undermined.

This is where integrated secrets management becomes essential. Automated scripts, APIs, and infrastructure tools rely on machine identities and embedded credentials. Without centralized governance,

Image by Freepik

continue on page 22



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

these NHIs become invisible attack vectors. Modern PAM must secure, rotate, and monitor these secrets to prevent lateral movement and unauthorized access. Unified password, secrets, and connection management reduces credential sprawl and enforces consistent policy across human and non-human identities.

These controls are especially critical as industrial espionage, AI-powered cyber attacks, advanced ransomware, and nation-state targeting of advanced manufacturing continue to escalate.

Proof Through Continuous Oversight

The METI mandate emphasizes demonstrable, evidence-based security. Organizations must provide continuous, auditable proof that controls are functioning effectively. Point-in-time compliance is no longer sufficient.

Zero-trust architectures and modern PAM platforms enable this level of visibility by integrating credential management, secure access, and session control into a unified, policy-driven framework.

To meet subsidy-linked requirements, semiconductor manufacturers should implement:

- **Session monitoring and recording** to track privileged activity
- **Regular access reviews** to eliminate privilege creep
- **Independent validation**, including certifications such as SOC 2 and ISO 27001/27017/27018
- **Unified secrets management** for full lifecycle control of credentials and machine identities

Building on Strength

The global semiconductor industry recognizes that trust must be verified and continuously enforced. As Japan strengthens its semiconductor ecosystem, it is reinforcing a broader truth: Security maturity underpins economic competitiveness.


Image by Freepik

As April 2026 approaches, industry leaders have an opportunity to modernize their security architectures. A secure-by-design strategy built on zero trust, privileged access management, and continuous monitoring enables innovation without compromising resilience.

In an era defined by economic statecraft and supply chain competition, cybersecurity is no longer a back-office IT function. It is a strategic enabler of national resilience and long-term industrial leadership.

By protecting identities, privileged access, and critical manufacturing systems, organizations do more than meet regulatory mandates; they strengthen Japan's posture as a trusted and secure global semiconductor partner. ■

HID HIGHLIGHTS TOP PKI TRENDS, THREATS, AND INNOVATIONS SHAPING THE AGE OF AI, AUTOMATION, AND POST-QUANTUM COMPUTING

As certificate lifespans shrink, modern PKI strategies require solutions that scale, integrate, and stay ahead of emerging threats

Cardiff, UK. March 31, 2026 – HID, a global leader in trusted identity solutions, today announced the release of its Public Key Infrastructure (PKI) in the Age of AI and Automation market study, revealing how more than 300 IT leaders in the United States and Europe are responding to emerging PKI challenges in AI, automation, and post-quantum computing.

The study identifies the trends, threats, and innovations that are shaping this fast-moving market, equipping security leaders with actionable insights to align their strategies with emerging opportunities and future demands.

Automation becomes a high priority

By minimizing the threat of human error, automation decreases the risk of certificate-related incidents, a benefit that is growing increasingly urgent as certificate lifespans shrink. This includes Transport Layer Security (TLS) certificates, the digital credentials that secure encrypted connections across websites and applications.
The CA/Browser Forum has already approved a phased reduction of TLS certificate validity from 398 days to just 47 days by 2029, making manual certificate management increasingly unsustainable and driving automation to the top of the security agenda.

In response, 67% of executives surveyed are already automating renewal processes. Automation also enhances scalability and helps organizations secure dynamic environments like IoT devices and AI agents. Executives from organizations large and small have made it one of their top priorities, with 61% of respondents saying they plan to invest in PKI automation in the next 24 months.

PKI-as-a-service (PKIaaS) gets traction

PKIaaS eliminates the need for on-premise hardware and servers, ensuring seamless automation from issuance to renewal and revocation. However, while 76% of organizations have incorporated cloud components into their PKI infrastructure, only 23% use fully cloud-based deployments.
Enterprises with more than 100,000 employees tend to prefer hybrid PKI deployments, suggesting that organizations seek to balance the flexibility of PKIaaS with the security and control of on-premise infrastructure.

Compliance brings clear benefits

With the growing swarm of regulations from GDPR, Cyber Resilience Act, NIS2, HIPAA, and more, compliance has become a strategic driver of PKI adoption. The cost of getting it wrong is high, as nearly half of executives (45%) list regulatory compliance among the primary business goals they hope to achieve through PKI, while 39% measure it as a formal key performance indicator.

Image by Freepik

continue on page 24

Post-Quantum Cryptography (PQC) readiness is slower than expected

As quantum computing matures, it poses a fundamental threat to today's encryption: bad actors are harvesting encrypted data today, intending to decrypt it once quantum capabilities catch up. Yet despite the recognized threat, adoption remains cautious. Only 12% of surveyed respondents are piloting PQC, 25% are developing internal plans, and 37% are monitoring evolving standards.

With PQC expected to be one of the most complex cryptographic transitions that the industry has ever experienced, larger enterprises and U.S.-based organizations are taking note. According to the survey, organizations with more than 50,000 employees are two to three times more likely to run PQC pilots than smaller companies.

AI Agents emerge as a new identity category

While AI standards continue to evolve, securing both customer interactions and bot-to-bot exchanges is a pressing priority. The study finds that 34% of organizations cite AI agent certificates as a top trend, reflecting the PKI community's proactive adaptation to AI-driven trust requirements. Adoption is slightly higher in the United States (18%) than in Europe (13%). The full market study includes additional data and further analysis.

About HID

HID powers the trusted identities of the world's people, places, and things. We make it possible for people to transact safely, work productively, and travel freely. Our trusted identity solutions give people convenient access to physical and digital places and connect things that can be identified, verified, and tracked digitally.

Millions of people around the world use HID products and services to navigate their everyday lives, and billions of things are connected through HID technology. We work with governments, educational institutions, hospitals, financial institutions, industrial businesses, and some of the most innovative companies on the planet.

Headquartered in Austin, Texas, HID has over 4,500 employees worldwide and operates international offices that support more than 100 countries. HID is an ASSA ABLOY Group brand. **For more information, visit www.hidglobal.com.** ■

MERCURY ANNOUNCES COMMERCIAL LAUNCH OF EMBEDDED APPLICATION ENVIRONMENT

From concept to execution, Mercury's app environment is live and powering the next phase of access control innovation.

Singapore – March 31, 2026 – Mercury Security, a global leader in open architecture access control hardware, today announced the commercial launch of its embedded application environment. With developer onboarding active and partner applications in progress, the platform moves from concept to execution, enabling technology partners and OEMs to build and deploy secure applications directly on Mercury MP Intelligent Controllers equipped with the latest Mercury firmware.

From Groundwork to Execution

Mercury introduced its embedded application environment one year ago to expand what access controllers can do. Today's announcement marks the platform's transition from preview to commercial launch.

The platform extends Mercury's open architecture by allowing approved applications to run directly at the edge. By embedding business logic and integrations on the controller itself, organizations can accelerate innovation, strengthen security, and scale functionality without reengineering their core infrastructure.

Supported by a structured developer program, technology partners follow a four-step onboarding process that includes submitting proposals, collaborating with Mercury on technical evaluation, accessing development tools, and completing a security review prior to distribution. This framework ensures applications meet performance and cybersecurity expectations while helping partners bring solutions to market faster.

Spotlight on App Developers

The launch highlights the growing community of OEMs and developers building on Mercury's platform. By providing a secure, open environment at the controller, Mercury empowers partners to create new capabilities that operate directly at the edge.

continue on page 25

Innovation is no longer confined to upstream systems. Applications can now enhance integration, analytics, and orchestration within the controller itself. This ecosystem approach allows partners to differentiate their offerings while delivering additional value for end users.

Partner Application Highlights

Mercury is working with three new partners to demonstrate the range of innovation possible within the app environment:

- **Commend Edge Bridge:** The Commend Edge Bridge app will deliver real-time, hardware-level data directly and securely to Commend device displays and audio products, without requiring any middleware.
- **HiveWatch:** The HiveWatch app on Mercury controllers will securely connect access control hardware to HiveWatch's cloud security operations platform. Security teams will gain centralized visibility into physical security events, with the ability to isolate device health events at the panel level, enabling faster diagnostics, proactive maintenance, and more efficient incident response.
- **KeyShare Connect by PassiveBolt:** The KeyShare Connect app will enable government-issued digital IDs, such as mobile driver's licenses, to be verified for physical access within a Mercury-powered environment, running natively on the Mercury controller at the edge. Together, PassiveBolt and Mercury will help eliminate the need to issue, manage, or pay for separate access credentials.

"This is a milestone moment. We've laid the groundwork with a secure, open controller platform and validated distribution through OEM channels. We've created an environment where partners and developers can build apps on MP Controllers. Now, we have the program and tools to support a growing list of certified app developers."

- Steve Lucas, Vice President of Sales, Mercury Security.

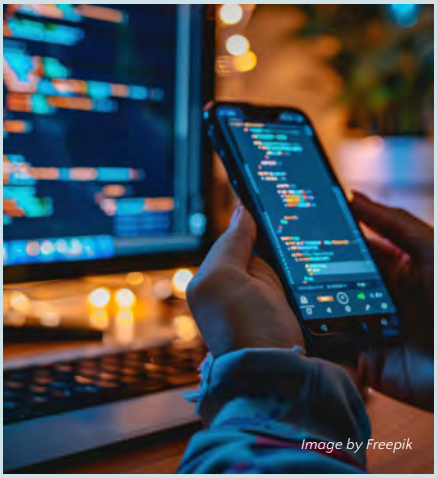


Image by Freepik

These partner applications will join the Mercury KS210 device app, which enables OEMs to integrate up to 32 KS210 OSDP server cabinet locks per controller.

Built for Secure Growth

Security and governance are foundational to the embedded application environment. Applications undergo structured testing to ensure performance integrity and alignment with enterprise cybersecurity expectations.

Controllers designed on open standards allow partners to integrate more efficiently while giving end users flexibility to adapt over time. As regulatory requirements evolve and integration needs expand, the Mercury app environment supports phased modernization rather than wholesale replacement.

To learn more about the Mercury application environment and access developer onboarding resources for building applications, visit the website.

About Mercury Security

Founded in 1992, Mercury Security is at the forefront of innovation in access control. With over 30 years of expertise and commitment to open architecture, Mercury has built a future-proof platform that ensures seamless interoperability between leading software and technical solutions.

As the trusted controller platform supplier for open architecture-based deployments, Mercury has more than 5 million controllers installed worldwide. In collaboration with our partners and parent company, HID, Mercury continues to drive innovation by establishing controller standards that promote long-term stability and adaptability in the ever-evolving security landscape. **For more information, visit mercury-security.com.**

About HID

HID powers the trusted identities of the world's people, places, and things. We enable people to transact safely, work productively, and travel freely. Our trusted identity solutions give people convenient access to physical and digital places and connect things that can be identified, verified, and tracked digitally. Millions of people around the world use HID products and services to navigate their everyday lives, and billions of things are connected through HID technology.

We work with governments, educational institutions, hospitals, financial institutions, industrial businesses, and some of the most innovative companies on the planet. Headquartered in Austin, Texas, HID has over 4,500 employees worldwide and operates international offices that support more than 100 countries. HID is an ASSA ABLOY Group brand. **For more information, visit www.hidglobal.com.** ■

SEE WILDFACES AND LENOVO'S JOINT SOLUTION AT HKTDC'S PRESS CONFERENCE ON APRIL 1ST, 2026, AT 2.30 PM

In a strategic move, Lenovo and WildFaces have joined forces for InnoEX 2026 (Joint Booth 3D-A27), embedding each other's products in their own offerings.

"At InnoEX, we are showcasing how Lenovo, together with one of its key ecosystem partners, is bringing AI into real-world deployment. By integrating Lenovo's edge computing and OEM capabilities with industry solutions, we empower partners to provide customer-centric solutions that turn data into actionable insights, increase operational efficiency, and deliver tangible business impact."

- Serena Cheung, General Manager Lenovo. Hong Kong and Macau

Image by Freepik

With 10+ international patents, WildFaces offers Real-Time Multi-Sensory (video, sound, and smell) AI software for moving sensors, such as flying drones, body-worn cameras, and walking robots.

Using its unique "Intuitive AI" with its Quick Training Engine (requiring 10 or fewer datasets for training any new models), the system can emulate complex human intelligence without Deep Learning and expensive, power-hungry GPUs, ensuring fast and cost-effective deployment.

At InnoEX the two companies will display their joint products, including a RoboDog that can smell very much like a real dog, a world first by incorporating a WildFaces eNose. It can differentiate between many complex smells.

It can be sent into areas where it may be too dangerous to send humans, such as down mine shafts to smell noxious gases or in industrial environments to detect gas leaks. And all WildFaces' analytics are ultimately powered by Lenovo's computing power.

Other WildFaces' patented "WildAI on the Move" software, mounted on flying drones providing real-time anomaly detection for Predictive Maintenance, will also be showcased at RoboPark. ■

SECURONIX PROMOTES AJAY BIYANI TO SENIOR VICE PRESIDENT, APJ TO ACCELERATE REGIONAL GROWTH

Appointment reinforces commitment to scaling AI-powered security operations across the Asia Pacific and Japan.

Singapore – February 26, 2026 – Securonix, Inc., a six-time Leader in the Gartner® Magic Quadrant™ for SIEM, today announced the promotion of Ajay Biyani to Senior Vice President, Asia Pacific and Japan (APJ). In his expanded role, Ajay will lead regional strategy, go-to-market execution, partner ecosystem development, and customer success initiatives across the region.

Since joining Securonix, Ajay has played a pivotal role in expanding the company's presence across APJ. He has led cross-functional teams spanning sales, channels, and customer success, supporting a workforce of more than 100 professionals. Under his leadership, the company achieved sustained

continue on page 27

double-digit year-over-year growth and increased adoption of its Unified Defense SIEM platform across key industries, including financial services, telecommunications, and government. Ajay has also been instrumental in strengthening the regional MSSP and channel ecosystem, with strategic partnerships driving significant pipeline growth and accelerating SaaS adoption among enterprise customers.

With over 20 years of experience in engineering, enterprise sales, and regional leadership, Ajay has previously held senior roles at ForgeRock, Verizon Enterprise Solutions, and Wipro Technologies. He has served as Vice President, APJ at Securonix since October 2022.

"APJ represents one of the most dynamic cybersecurity markets globally," said Scott Sampson, Chief Revenue Officer, Securonix. "Ajay's leadership, strong partner relationships, and consistent execution have been key to our regional success. As we continue to scale our Unified Defense SIEM platform powered by agentic AI, his role will be critical in driving further growth and customer trust."

> *"Organizations across APJ are navigating rapid digital transformation alongside increasing regulatory demands and cyber risk. My focus will be on strengthening our partner ecosystem, supporting customers in adopting AI-driven security operations, and enabling them to become both breach-ready and board-ready."*
> ***-Ajay Biyani***

Securonix continues to invest in APJ as a strategic growth region, advancing its vision of delivering AI-driven, cloud-native security operations that unify detection, investigation, and response across the threat lifecycle.

About Securonix

Securonix is transforming security operations with its Unified Defense SIEM platform powered by agentic AI. Built to operate across the entire threat lifecycle, the cloud-native platform integrates detection, investigation, and response while enabling a productivity-driven AI operating model for security operations centers. Recognized as a Leader in the Gartner® Magic Quadrant™ for SIEM and a Customers' Choice by Gartner Peer Insights™, Securonix delivers scalable, outcome-driven security operations for global enterprises. ■

SMARTER, SAFER ACCESS: INTEGRATING BIOMETRICS AND INTELLIGENT ENTRANCE CONTROL ACROSS ASIA

Across Asia, organisations are increasingly adopting integrated security strategies to protect critical infrastructure, corporate facilities, and high-value assets. Rapid urban development, the rise of smart buildings, and the expansion of data centre infrastructure are driving demand for access control solutions that are not only highly secure but also efficient and user-friendly.

The Convergence of Biometrics and Entrance Control

A key trend shaping the future of physical security is the convergence of biometric authentication with intelligent entrance control. By combining advanced identity verification technologies with

controlled pedestrian access systems, organisations can create a seamless security ecosystem that enhances both safety and operational efficiency.

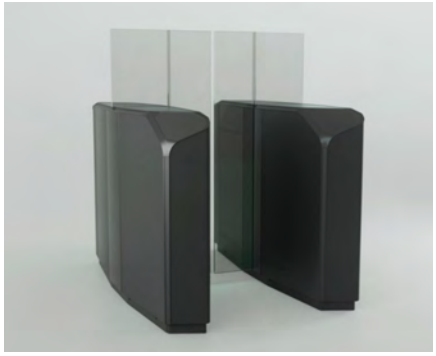
Main Hardware International (MHI), a regional provider of security and entrance control solutions, supports projects across Singapore, Malaysia,

continue on page 28

India, Japan, and the Philippines. The company collaborates closely with global technology partners to deliver integrated solutions aligned with modern security requirements, particularly across sectors such as corporate offices, commercial buildings, data centres, and critical infrastructure.

One example of advanced biometric technology is the IXM TITAN, developed by Invixium. Designed for enterprise-grade security environments, TITAN supports multimodal biometric authentication, including facial recognition combined with fingerprint or finger vein verification. In addition to biometrics, the device also supports RFID cards, PIN codes, and mobile credentials, enabling flexible multi-factor authentication strategies.

Equipped with a high-performance processor and a 21-megapixel camera, the device delivers fast and accurate user identification while supporting large user databases of up to 100,000 biometric identities. Its rugged aluminium construction, combined with high ingress and impact protection ratings, ensures reliable operation in both indoor and outdoor environments, making it well-suited for demanding installations such as industrial facilities and data centres.



Enabling Seamless and Secure Access

Complementing biometric authentication is intelligent entrance control technology such as the SpeedStile FP Glide from Gunnebo Entrance Control. Designed for high-traffic environments, this premium speed gate combines sophisticated security detection with contemporary architectural design.

The FP Glide features an innovative telescopic sliding gate mechanism that enables wider passage while optimising installation footprint. Dynamic LED guidance intuitively directs users through the lane, while advanced sensor arrays and fraud detection algorithms help identify unauthorised access attempts, including tailgating, crawling, or climbing over the barrier.

When integrated, biometric readers and entrance control systems create a powerful layered security solution. Users authenticate their identity using biometrics or digital credentials, while the entrance control system manages secure and controlled passage through the facility. This integration ensures that only authorised individuals gain access, while maintaining a smooth and efficient flow of people.

As organisations across Asia continue to modernise their security infrastructure, integrated access control ecosystems, combining biometric authentication with intelligent entrance control, will play an increasingly critical role in delivering smarter, safer, and more connected environments. ■

CERTIS AND FIELDAI FORM STRATEGIC PARTNERSHIP TO DEPLOY AUTONOMOUS ROBOTICS IN REAL-WORLD SECURITY OPERATIONS

Certis Group, Singapore's leading provider of integrated security and operations solutions, has announced a strategic partnership with FieldAI, a US-based leader in general-purpose autonomous robotics, to advance cost-effective robotic applications in complex, real-world security operations.

continue on page 29

Orchestrating Humans, Robots, and Operations at Scale

Autonomous robotics technology has progressed rapidly, with security deployments already underway across global markets. The partnership between Certis and FieldAI is designed to enable scalable deployment of autonomous robotics across large, multi-site security operations by creating an integrated ecosystem of general-purpose robots, command systems, operational workflows, and human teams.

This collaboration brings together FieldAI's advanced AI-driven autonomy with Certis' operational orchestration and deployment expertise, powered by the Mozart™ orchestration platform, which coordinates robots, human teams, workflows, and command systems in real-world environments.

Together, Certis is helping shape the operating model for autonomous security—building on FieldAI's proven deployments to enhance how autonomous systems are integrated into live operations, while establishing benchmarks for safe and reliable deployment at scale.

A Partnership Grounded in Real-World Operations

FieldAI's autonomy technology will be integrated with Certis' command-and-control platforms and operational workflows, enabling autonomous robots to operate alongside human security teams across diverse environments. These include public infrastructure, transport hubs, commercial and industrial facilities, as well as remote or high-risk locations. Designed for flexibility and scalability, the robots will perform routine and repetitive tasks, allowing security personnel to focus on higher-level analysis and critical response. The deployments aim to improve operational efficiency and resilience while maintaining service quality and safety, combining both companies' strengths in system reliability and human-robot coordination at an unprecedented scale.

"The security industry currently employs more than 30 million workers globally and operates in increasingly complex and labour-constrained environments, where reliability, safety, and accountability are non-negotiable. For robotics to be viable at scale, they must integrate seamlessly with human teams, operational workflows, and command systems. This partnership with FieldAI reflects our approach of working with leading technology companies to deploy solutions that perform consistently in live, mission-critical environments."

- Ng Tian Beng, President and Group CEO, Certis

Advancing Autonomous Capabilities Through Integration

At the core of FieldAI's technology are its Field Foundation Models™, general-purpose autonomy software that enables robots to operate safely in complex, dynamic, real-time environments, without reliance on prior maps, predefined routes, or supporting infrastructure. As robots encounter new environments, learnings are shared across the fleet, continuously improving performance at scale.

FieldAI's autonomy software will integrate with Certis' orchestration and fleet management systems to support applications such as autonomous patrols, real-time incident detection, remote supervision, and coordinated human-robot response, while enabling scalable deployments at reduced cost.

"The real world is complex and unpredictable. That's why we built autonomy that focuses on managing uncertainty while continuously learning across deployments. Because the FieldAI system does not rely on prior maps or pre-planned routes, customers can deploy quickly and scale across sites with minimal setup. Certis operates some of the most complex security environments globally, and integrating our technology with its orchestration platforms allows us to advance these capabilities where they matter most, in live operations at scale."

- Ali Agha, Chief Executive Officer, FieldAI

Looking Ahead

FieldAI has opened an office in Singapore to support ongoing deployments and integration efforts with Certis. The company will also exhibit at ISC West 2026, taking place from March 23–27 in Las Vegas.

The collaboration will initially focus on security applications, with additional use cases such as inspection, facilities monitoring, and intelligent field operations expected to follow. Both companies will also work together on training, safety validation, and operational frameworks to support responsible deployment. The partnership reflects a shared commitment to scaling practical robotics solutions that integrate seamlessly with human operations, helping organisations build safer, more resilient environments amid growing labour constraints and operational complexity. ■

From Isolated Systems to Integrated Security: **The Future Is Smarter and Safer**

- *Connecting cameras, sensors, access controls, and AI analytics creates a complete view of operations, reducing blind spots and improving threat detection.*
- *Combining analytics, automation, and real-time insights helps teams prioritize threats and allocate resources more effectively.*
- *Even with automation, skilled security teams are essential to interpret data, make judgment calls, and guide AI systems effectively.*

Image by Freepik

Once, security was simple: a lock on the door, a camera in the hallway, and a guard at the desk. Each system worked on its own, keeping watch in silos. It got the job done, but it left gaps. As workplaces and threats grew more complex, gaps weren't acceptable anymore.

That's why integrated security became a must. By connecting cameras, sensors, access points, and AI analytics, organizations could see the bigger picture and respond faster. And the numbers speak for themselves: the global integration security market is set to jump from $15.8 billion in 2021 to $55.5 billion by 2031, while 78 % of security operations centers now use AI to catch risks humans might miss.

With these systems already shaping today's workplaces, the next question is: what comes next? This issue of Security Solutions Today dives into the future of integrated security. Plus, it explores the trends and transformations that will define smarter, fully connected protection.

The Payoff of Integrated Security in 2026

Today's integrated security platforms go beyond cameras and alarms, combining identity management, threat detection, analytics, and automation into one connected system that delivers real business value.

1. Fewer Security Incidents, Faster Response
A company innovating with AI-driven contract platforms consolidated multiple security tools into a single integrated system. This helped them cut security operations center incidents by 50 % slashed alert-triage times by up to 80 %. Plus, it reduced the mean time to resolution to around 25 minutes.


Image by Freepik

2. Seamless Visitor and Contractor Management
Integrated platforms now track temporary workers in real time, syncing access rights and operational schedules in one system. This cuts administrative work by up to 50 %.

3. Cross-Building Threat Alerts
Multi-site enterprises can detect patterns across locations. For example, an unusual login in one office triggers security checks across all sites within seconds, preventing coordinated breaches.

4. Reduced False Alarms
By linking access control, cameras, and sensors, organizations can cut unnecessary alerts. This saves security teams hours of manual verification. Eventually, it allows them to focus on real threats.

4 Trends Shaping the Future of Integrated Security

1. Context-Aware Zero Trust
Zero Trust is moving beyond simple credential checks to become dynamic. Modern systems continuously evaluate every access attempt based on a live risk score, taking into account:

- Behavior patterns: Is the user acting like themselves, or deviating from normal habits?
- Device posture: Is the device compliant, updated, and secure?
- Geolocation: Is the request coming from a trusted location or an unusual area?
- Operational context: Time of day, critical systems accessed, and environmental data from connected sensors.

With this approach, the system predicts risky behavior before access occurs. For instance, it can detect unusual work patterns or abnormal sensor readings and automatically enforce micro-segmentation policies, restricting access to sensitive zones only when truly safe.

The result is a security posture that is adaptive, continuous, and predictive, capable of adjusting in real time to protect people, devices, and data. The best part? It all happens without slowing down day-to-day operations.

2. Edge Intelligence and IoT Integration
Edge AI is transforming integrated security from reactive monitoring into distributed decision-making networks. Cameras, sensors, and IoT

"As the security industry continues to evolve, edge (and ambient) intelligence will become the backbone of modern surveillance and protection systems. Organizations that embrace edge AI will gain competitive advantages by improving response times, reducing costs, and enhancing security operations."

– Niranjan Maka, CEO and co-founder SmartHub.ai.

devices analyze data locally, share insights in real time, and trigger coordinated actions like adjusting HVAC in emergencies or isolating compromised devices.

With edge computing, security becomes resilient to latency and central server failures, enabling autonomous, site-level intelligence that scales across global operations. Around 72 % of IT managers report that their organizations have already implemented edge computing solutions to some degree, not just planning for the future but actively running projects.

3. AI That Acts, Not Just Alerts
Modern AI doesn't just spot problems, it solves them. AI-powered video analytics watch feeds in real time, spotting unusual behaviors like someone loitering in a restricted area or a crowd forming unexpectedly.

Image by Freepik

It can also recognize license plates, detect safety gear compliance, and track patterns over time, predicting potential incidents before they happen. Coupled with automated response systems, AI can reroute traffic or send alerts to the right teams instantly. This makes security proactive rather than reactive.

4. Privacy-First Designs
Integrated security is getting smarter, but privacy can't be ignored. Modern platforms are built with privacy-by-design, ensuring threat detection works without unnecessarily exposing personal data. Techniques like anonymization, selective data retention, and automated compliance monitoring let organizations track risks while protecting identities.

This approach also helps organizations stay compliant with GDPR, CCPA, and other regulations, reducing legal exposure. More importantly, it builds trust with employees, visitors, and customers, showing that security systems can be both effective and ethical. In an age where surveillance is scrutinized, privacy-first design ensures that safety and personal rights go hand in hand.

Future Tech Beyond 2026: Shaping Integrated Security

Quantum-Enhanced Security Analytics
Quantum computing is set to redefine how integrated security handles data. By processing massive datasets at unprecedented speed, systems can detect complex threats across networks and physical sites almost instantly.

Quantum-enabled platforms can simulate thousands of attack scenarios, predict vulnerabilities, and optimize responses in real time. This level of computation allows security teams to move from reactive defense to predictive, enterprise-scale threat management, covering multiple facilities networks with intelligence and speed that conventional systems can't match.

Swarm Robotics & Autonomous Response Units
AI-controlled drones and ground robots are becoming


Image by Freepik

the next generation of mobile security forces. These autonomous units can patrol campuses, monitor perimeters, and respond to incidents in real time, providing eyes and action where human guards or static cameras can't.

Working as coordinated swarms, they share data, cover larger areas, and provide instant situational awareness. For organizations with sprawling campuses or multi-site operations, this technology makes security faster, more flexible, and highly scalable, allowing teams to respond to threats efficiently without increasing headcount.

Digital Twin Security Simulations
Organizations are increasingly building digital replicas of their buildings, networks, and operational workflows to simulate attacks, test responses, and evaluate vulnerabilities.

These "digital twins" give security teams a safe, risk-free environment to experiment, identifying weak points before they can be exploited in the real world.

Running multiple scenarios from cyber intrusions to physical breaches, teams can optimize defenses, improve response strategies, and anticipate threats.

Cognitive Biometrics & Emotion Detection
The next frontier in integrated security is understanding intentions and cognitive states. In the future, the systems will begin to analyze micro-behaviors, stress indicators, and brainwave patterns to identify potential insider or outsider threats.

Combined with access control and AI analytics, this will allow security platforms to predict risky behavior before it manifests physically, adding a proactive layer of protection.

The Hidden Hurdles of Tomorrow's Security

Challenge	Why It Matters
Quantum Quandaries	Quantum computing could unlock unmatched threat detection, but it also introduces attack methods that traditional defenses can't handle.
Rogue Robots	AI-controlled drones and ground bots increase coverage, but coordination errors could cause accidents or security gaps.
Simulation Blind Spots	Digital twins simulate threats safely, yet unexpected real-world behaviors may still slip past.
Edge AI Glitches	Distributed intelligence allows instant local decisions, but hardware or software failures could leave critical areas unprotected.

Looking Ahead: The Human Touch in Security

Integrated security is moving beyond cameras and alarms, into systems that predict and respond to risks in real time. Yet technology alone isn't enough.

The future depends on skilled people working alongside these systems. Human judgment, intuition, and experience will remain essential for interpreting insights, making critical decisions, and responding to unexpected situations.

The goal is clear: a safer, smarter workplace where threats are anticipated, not just reacted to, and where human expertise guides technology to keep everyone one step ahead. ■


Image by Freepik

COMING SOON

APR 28–30 2026

Milipol Asia Pacific 2026 *(Page 11)*
Singapore
https://www.mtx.sg/

APR 22– 24 2026

Secutech International 2026 *(Page 1)*
Taipei, Taiwan
https://secutech.com

MAY 7 – 9 2026

Intersec Shanghai 2026
Shanghai, China
https://intersec-shanghai.hk.messefrankfurt.com/shanghai/en.html

MAY 19 – 21 2026

ISNR 2026
Abu Dhabi, UAE
https://www.isnrabudhabi.com/

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 13)*
Hanoi, Vietnam
www.secutechvietnam.com

SEP 9 – 12 2026

OS+H Asia 2026 *(Page 19)*
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 21)*
Singaopore
www.cybersecurityworldasia.com

NOV 18 – 20 2026

Secutech Thailand 2026 *(Page 13)*
Bangkok, Thailand
www.secutechthailand.com

NOV 10 – 12 2026

Safety & Security Asia 2026 *(Page 15)*
Singapore
www.safetysecurityasia.com

NOV 25 – 27 2026

DigiTech ASEAN Thailand 2026 *(Page 17)*
Bangkok, Thailand
www.digitechasean.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