OCT – DEC 2026

SECURITY SOLUTIONS TODAY



SECURING CRITICAL INFRASTRUCTURE

IN THIS ISSUE

4 **In The News**
Updates From Asia And Beyond

28 **Focus**
+ Delve into strategies and technologies protecting power plants, transport systems, and data centres from both physical and cyber threats

32 **Cover Story**
+ Beyond the Firewall: Securing Critical Infrastructure in the Age of AI

36 **Calendar Of Events**







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: Magnific.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)

Disclaimer: The editor reserves the right to omit, amend or alter any press release submitted for publication. The publisher and the editor are unable to accept any liability for errors or omissions that may occur, although every effort had been taken to ensure that the contents are correct at the time of going to press.

The editorial contents contributed by consultant editor, editor, interviewee and other contributors for this publication, do not, in any way, represent the views of or endorsed by the Publisher or the Management of Trade Link Media Pte Ltd. Thus, the Publisher or Management of Trade Link Media will not be accountable for any legal implications to any party or organisation.

Views and opinions expressed or implied in this magazine are contributors' and do not necessarily reflect those of Security Solutions Today and its staff. No portion of this publication may be reproduced in whole or in part without the written permission of the publisher.

For advertising interests, please email us at **info@tradelinkmedia.com.sg.**

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

TRENDAI™ APPOINTS SOFFENNY YAP AS COUNTRY MANAGER FOR SINGAPORE

Cybersecurity industry veteran and ecosystem leader to drive TrendAI™'s next phase of growth as AI reshapes Singapore's threat landscape

Singapore – Global AI security leader TrendAI™ has appointed Soffenny Yap as Country Manager for Singapore, effective September 1, 2026. Yap steps up from a senior leadership role within its Singapore business and will take charge of the company's strategy, growth, and customer and partner relationships in one of the region's most advanced cybersecurity markets.

At TrendAI™, Yap has led both Enterprise and Public Sector sales, deepening relationships with some of Singapore's largest organisations and government agencies. She joined the company after heading security services sales at IBM, where she worked with enterprises and public bodies to strengthen their security posture. That combination of commercial leadership and hands-on work with regulated, high-stakes customers gives her a clear view of what local organisations need to stay resilient as AI changes the security equation.

Beyond her corporate role, Yap is an active contributor to Singapore's cybersecurity community. She serves as Secretary of the Association of Information Security Professionals (AiSP), Chairman of the IoT Special Interest Group at the Centre for Strategic Cyberspace and International Studies (CSCIS), and Vice President for the DDAS PMEs and DDASCares initiatives at the Digital Defence Alliance Singapore (DDAS). Through these roles, she has championed cybersecurity awareness, digital defence, and the development of local cyber talent.

Singapore is among the region's most digitally advanced markets, and one of the fastest to put AI to work across financial services, government, and critical infrastructure. That progress comes with exposure: more than eight in 10 enterprises encounter a cybersecurity incident each year, according to the Cyber Security Agency of Singapore, and attackers are now using AI to move faster and operate at greater scale. This is the shift TrendAI™ is built for: giving organisations full visibility over their AI, consolidating security across identities, infrastructure, and data, and helping them cut risk and stop threats earlier. Under Yap's leadership, TrendAI™ will focus on helping Singapore organisations adopt AI with confidence while strengthening their resilience.

"Singapore's organisations are moving fast on AI, and attackers are moving just as fast. The task is not to slow that progress, but to secure it, so enterprises and public agencies can adopt AI with confidence," said Soffenny Yap,



Image by Magnific

Country Manager – Singapore, TrendAI™. "Having worked alongside Singapore's businesses, government agencies, and cybersecurity community for years, I know the appetite is there to get this right. I look forward to helping our customers and partners build the visibility and resilience they need to stay ahead of the threat."

"Soffenny's appointment reflects the strength of the leaders we grow from within. She pairs a deep understanding of Singapore's enterprises and public sector with genuine standing across the country's cybersecurity community. As AI reshapes both how organisations operate and how they are attacked, that combination of commercial insight and ecosystem trust is exactly what our customers and partners need. I am confident that under her leadership, our Singapore business will chart an even stronger growth trajectory," said Dhanya Thakkar, Senior Vice President – AMEA, TrendAI™.

About TrendAI™

TrendAI™, the global AI security leader and enterprise business unit of Trend Micro, empowers organizations with full AI visibility, governance, and consolidated security that inspires confidence, drives innovation, and eliminates risk. Trusted by the largest enterprises and governments across 185 countries, TrendAI™ secures the entire organization, from identities to infrastructure to data. Global Fortune 500 companies rely on TrendAI™ to cut risk and stop threats up to 115 days earlier, powered by world-leading threat and attack intelligence.

Through deep ecosystem partnerships with market leaders like NVIDIA, Anthropic, AWS, Google, and Microsoft, TrendAI™ empowers your organization to securely drive forward at the speed of AI. ■

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

SYNOLOGY® LAUNCHES ACTIVEPROTECT MANAGER 2.0, BRINGING EXPANDED PLATFORM SUPPORT AND ADVANCING AI-DRIVEN SECURITY

Singapore – Synology launched ActiveProtect Manager 2.0 (APM 2.0), the latest software update for its ActiveProtect data protection appliances. This release introduces expanded platform coverage, cross-platform recovery, and enhanced security, with future updates bringing AI-driven threat mitigation.



"Managing fragmented backup infrastructure drives up costs and slows recovery. The ActiveProtect appliance unites purpose-built storage with powerful data management software into a single, predictable investment. APM 2.0 builds on that value, enabling organizations to safeguard their entire hybrid infrastructure through one centralized, scalable solution."

– Jia-Yu Liu, Executive Vice President of the Synology Data Protection Group

ActiveProtect Manager 2.0 Expanded platform coverage

APM 2.0 extends protection to Amazon EC2, Azure VM, Proxmox VE, Nutanix AHV, and Google Workspace. Cross-platform recovery allows workloads to be backed up and restored across different environments, supporting both disaster recovery and seamless workload migration.

Backup destinations have also expanded. ActiveProtect Vault now supports a wider range of Synology NAS models, while Azure Blob Storage joins the list of supported copy and tiering targets. Backups stored in Amazon S3 Storage or Azure Blob Storage can be restored directly into either Amazon EC2 or Azure VM as a cloud disaster recovery strategy without routing through on-premises hardware, significantly reducing recovery times.

AI-driven proactive resiliency

ActiveProtect Manager 2.0 adds software-based storage encryption at the volume level to secure data at rest. Backup data and system configurations remain inaccessible in the event of drive theft or hardware loss.

The upcoming APM 2.1 update will add AI/ML anomaly detection, tracking each backup version for shifts in change rate, file modifications, mass deletions, and entropy. Suspicious backup copies will be moved to quarantine for administrators to investigate, limiting the risk of backup contamination. The model learns from those outcomes to improve accuracy and reduce false positives.

APM 2.1 will also scan backups for malware before restoration, using integrated third-party antivirus software such as Microsoft Defender, Bitdefender, and ESET. If malware is detected in the most recent backup, Auto Fallback restores the latest clean version instead.

Availability

ActiveProtect Manager 2.0 is available for all DP-Series appliances at no additional cost. For details, please refer to the product page.

About Synology

Founded in Taiwan in 2000, Synology is a technology company specializing in network-attached storage (NAS), data backup and recovery, video surveillance, and networking solutions for businesses and individuals worldwide. Over the past two decades, Synology has continuously expanded its ecosystem to help users manage, protect, and unlock the value of data more effectively in the era of cloud, AI, and big data.

Synology's core philosophy is to build a comprehensive hybrid-cloud ecosystem that enables businesses to protect, synchronize, and manage data through a centralized, intuitive, and easy-to-operate platform. From enterprise storage, data backup, file sharing, and collaboration to video surveillance and network infrastructure, Synology's solutions are designed to simplify IT management and accelerate digital transformation.

Alongside ongoing technology innovation, Synology also focuses strongly on long-term stability, security, and scalability for data infrastructure. More than half of Fortune 500 companies use Synology solutions, reflecting the brand's credibility and ability to support large-scale data operations worldwide. ■

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™

© 2026 Altronix Corporation – altronix.com

CYBERSECURITY AWARENESS MONTH PERSPECTIVES FROM KEEPER SECURITY

>> Darren Guccione, CEO And Co-Founder, Keeper Security

"Cybersecurity Awareness Month has traditionally focused on human behavior: recognizing phishing, protecting credentials, and making better decisions about access to an organization's network, data, and accounts. That conversation now needs to expand. As organizations rapidly deploy AI agents across their environments, they are creating an entirely new class of digital users, often without applying the same identity governance expected for employees, contractors, or administrators.

AI is transforming from intelligence to unremovable enterprise infrastructure. AI agents can now authenticate into systems, retrieve sensitive information, interact with applications, execute workflows, and make critical decisions – all at machine speed. If an agent has credentials and permissions, it represents an identity, and every identity creates risk when its access is excessive, persistent, or poorly monitored.

The biggest problem is scale. Organizations can deploy hundreds or thousands of non-human identities far faster than they onboard human employees. If those agents receive standing credentials, broad permissions, or long-lived secrets without appropriate governance, the attack surface expands just as quickly. A compromised AI agent with privileged access can give an attacker direct access to critical systems and data.

The security principles needed to secure these identities are not new. Organizations should apply the same zero-trust discipline to AI agents that they apply to people: verify every identity, enforce the principle of least privilege, eliminate unnecessary standing access, continuously monitor privileged activity, and protect and rotate credentials and secrets. Access should be granted only to the resources required for a specific task and only for as long as that access is necessary.

Cybersecurity awareness must evolve alongside technology. We have spent years teaching organizations that every employee identity requires governance. Now we need to extend that understanding to machines.

The next frontier of cybersecurity awareness is recognizing that AI agents are users too. Organizations that govern them accordingly will be far better positioned to capture the benefits of agentic AI without creating an unmanaged layer of privileged access."

>> Michael Marino, SVP Of Strategy, Identity Security, Keeper Security

"Cybersecurity Awareness Month is an opportunity to reflect not only on how cyber threats have evolved, but on how our defenses have had to evolve alongside them. Over my career in identity security, I've seen few areas change as significantly as Privileged Access Management (PAM).

PAM was once primarily about putting administrator passwords into a secure vault. That made sense when infrastructure was largely on-premises, privileged users were relatively easy to identify, and access occurred within clearly defined network boundaries. The objective was straightforward: protect powerful credentials and maintain an audit trail around their use.

The days of a contained network perimeter no longer exist. Organizations now operate across cloud, hybrid, and remote infrastructure, while employees, contractors, applications, service accounts, and automated systems all require different levels of access. Keeper research found that 94% of organizations operate in hybrid or cloud-first environments.* As access has become more distributed, the traditional concept of privilege has expanded with it.

Modern PAM, therefore, has to be about much more than protecting passwords. It must control when privileged access is granted, what someone or something can access, and what happens during that session. Principles such as least privilege, just-in-time access, and zero standing privilege help organizations replace persistent administrative rights with access that is intentional, temporary, and auditable.

The next stage of this evolution will be driven by automation and AI. Non-human identities and AI agents are creating privileged access at a scale that security teams cannot manage manually. At the same time, AI can help defenders analyze privileged activity and identify suspicious behavior much faster.

The lesson for Cybersecurity Awareness Month is that cybersecurity fundamentals don't disappear as technology changes; they evolve to meet the occasion. Privileged access will always represent concentrated risk. Effective PAM is about continually adapting how that risk is controlled as the identities, infrastructure, and technologies around it change."

continue on page 9

>> Anne Cutler, Cybersecurity Expert, Keeper Security

"For many people, deepfakes still feel like an internet novelty – a fake celebrity video, an altered image, or an amusing example of what AI can create. That perception needs to change. Deepfakes are increasingly relevant to personal cybersecurity because the same technology used for entertainment can be weaponized by cybercriminals to impersonate other people, manipulate trust, and steal sensitive information.

Cybercriminals have always relied on social engineering, but what AI changes is how convincing and scalable those attacks can become. An attacker no longer has to rely solely on a suspicious email pretending to be an organization or individual you know. AI can help imitate a person's voice, appearance, or communication style, creating a much more persuasive request for money, account credentials, or sensitive information.

Our natural instinct to trust familiarity has become a vulnerability. Cybersecurity Awareness Month is an opportunity to update the way we think about personal security. Recognizing phishing emails remains important, but awareness now also means questioning unexpected requests regardless of how authentic or personal they appear. A familiar face or voice should no longer be treated as proof of identity.

If a family member, colleague, or financial institution appears to contact you with an unusual or urgent request, verify it through another trusted channel. Call the person using a number you already have rather than one provided in the message. Never provide passwords or Multi-Factor Authentication (MFA) codes in response to an unsolicited request, and always use strong, unique credentials backed up with MFA to make accounts harder to compromise.

Deepfake awareness is personal cybersecurity awareness. Understanding how attackers can weaponize synthetic media is becoming an essential part of protecting our identities, accounts, and financial lives. ■



APAC ORGANISATIONS URGED TO ACCELERATE QUANTUM READINESS AS REGULATORY DEADLINES APPROACH

World Quantum Readiness Day 2026 highlights growing urgency around post-quantum cryptography migration across Asia Pacific.

Singapore – Organisations across Asia Pacific must move beyond planning and begin implementing post-quantum cryptography (PQC) strategies now, as governments introduce quantum-security roadmaps and migration timelines. Industry experts said the challenge is increasingly shifting from awareness to execution, with the scale and complexity of migration leaving some organisations unsure where to begin.

Speaking at World Quantum Readiness Day 2026, hosted by DigiCert, cybersecurity, regulatory and industry leaders said organisations can no longer afford to wait for perfect visibility, mature standards, or complete technology readiness before starting their PQC transition.

"Three years ago, many organisations were still in denial, believing quantum computers were years away. Today, most organisations have accepted that they need to act. The core trust fabric of the internet is due for a once-in-30-year upgrade, and if organisations do not start today, they are already out of time."

- Dr. Amit Sinha, CEO of DigiCert.



Amit Sinha, CEO of DigiCert, delivers the opening remarks at World Quantum Readiness Day 2026.

Australia sets an aggressive pace for post-quantum migration

A key theme throughout the event was the increasingly important role of regulation in shaping quantum readiness strategies.

According to Naomi Wynn, CEO of National Energy PKI (NEPKI), Australia is taking one of the most ambitious approaches globally to PQC migration: "Australia is typically a technology follower, but when it comes to post-quantum cryptography, we're leading the charge from a regulatory perspective," said Wynn. "The Australian Signals Directorate and Australian Cyber Security Centre have requested full PQC compliance and migration by 2030. Compared to other jurisdictions such as the US, Singapore or China that require only partial compliance by that timeframe, this represents a significant step change for Australian industry."



(From right) Dean Coughlin, Senior Director, Digital Trust Specialist, DigiCert; Wynn, Chief Executive Officer, National Energy PKI (NEPKI); and Jostein Stokkan, Product Manager, Service Offerings, Atea, discuss global post-quantum cryptography regulations, standards and interoperability during the"What, When, and Why: The Global Regulatory and Standards Landscape" session at World Quantum Readiness Day 2026.

Wynn also noted that while countries including China are developing their own approaches to quantum-safe cryptography, differing standards should not slow progress: "Different jurisdictions will naturally develop different approaches, but over time we expect greater global standardisation and interoperability," said Wynn. "The important thing is that everyone is getting started."

'Paralysis of analysis' is delaying action

Despite the progress in migration regulations and standards, experts said the scale of migration itself is creating a new barrier to action. Many organisations are facing a "paralysis of analysis" with teams confronted by vast amounts of information, potential migration paths, and the perceived need to establish a complete cryptographic inventory before taking action. For PKI and security teams that have historically been under-resourced, the prospect of large-scale, enterprise-wide transformation can make it difficult to know where to begin.

continue on page 12

NO CHALLENGE TOO TOUGH. NO SOLUTION TOO BOLD.



SIDEX - ACDR 2026

28 to 30 October 2026
Singapore Expo Hall 3
Booth H01

As threats become more complex, agencies need trusted technologies that enable faster decisions, stronger coordination and greater mission effectiveness.

Backed by operational expertise and deployments in more than 100 cities worldwide, ST Engineering delivers integrated public safety and security solutions that enhance situational awareness, protect critical infrastructure and strengthen national resilience.

At SIDEX 2026, discover our latest AI-enabled command systems, Manned-Unmanned Teaming capabilities, maritime safety and security solutions, and space-based intelligence technologies.

Join us to explore how we can help build safer, more secure and resilient communities.

ST Engineering

"I would take the word 'quantum' out of it entirely; organizations don't need a background in physics to begin preparing. This is fundamentally a risk-management and cybersecurity challenge. Many of the steps required to prepare are already known."

- Colin Soutar, Global Quantum Cyber Readiness Leader at Deloitte & Touche LLP.

Sadaaki Yamazaki, Senior Security Specialist at Daiwa Institute of Research Ltd. in Japan, shared lessons from the organisation's post-quantum proof of concept, offering an example of how organisations in APAC are beginning to move from awareness to practical testing.

"The biggest lesson from our proof of concept was that the technical impact of adopting post-quantum cryptography was more manageable than we initially expected. The larger challenge is organisational. Understanding where cryptography is used, managing dependencies and building governance across the enterprise are often more difficult than the technology itself."

- Sadaaki Yamazaki, Senior Security Specialist at Daiwa Institute of Research Ltd.

Yamazaki's experience highlights that quantum readiness extends beyond selecting and implementing new cryptographic algorithms. For organisations beginning their transition, establishing visibility into where cryptography is being used, understanding dependencies across systems and applications, and putting governance structures in place can be critical to moving from a proof of concept towards broader implementation.

Sharing lessons from LGT Financial Services Ltd.'s migration journey, Christian Pfister, Lead of the Quantum Safe Competence Center, said the company achieved its first meaningful milestone within six months by focusing on a targeted pilot rather than waiting for a perfect cryptographic inventory.

"Our advice is simple: don't wait. Start with a practical use case, build evidence, learn from the process, and expand from there."

DigiCert is also applying these principles internally through its own "Customer Zero" quantum readiness programme. Lakshmi Hanspal, Chief Trust Officer at DigiCert, shared that the company has structured its migration around clear milestones, beginning with cryptographic inventory, TLS 1.3 enablement and ensuring post-quantum cryptographic algorithms are available across its environment. Hanspal noted that DigiCert has already completed these foundational phases.

New quantum readiness capabilities: Quantum Central

During the event, DigiCert also announced Quantum Central, a new capability designed to help organisations inventory cryptographic assets, identify ownership, assess cryptographic posture and measure progress throughout their PQC migration journey. Quantum Central extends the visibility and automation capabilities within the DigiCert ONE platform to support enterprise-wide quantum readiness initiatives.

"Quantum readiness is not just a technology project. It's an organisational transformation effort. Organisations need visibility into their cryptographic assets, ownership of risk and a clear roadmap for migration."

- Deepika Chauhan, Chief Product Officer at DigiCert.



Deepika Chauhan, Chief Product Officer at DigiCert, introduces the latest innovations in quantum readiness, including Quantum Central, during World Quantum Readiness Day 2026.

As governments accelerate quantum-safe migration guidance and organisations face growing pressure to modernise their cryptographic infrastructure, speakers agreed that the biggest risk is no longer uncertainty around quantum computing itself, but postponing preparation. The message from World Quantum Readiness Day 2026 was clear: organisations do not need to have every answer before they begin, but they do need to start building their quantum readiness roadmap now. Did you miss the event? Watch on demand here.

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.** ■

THE SECURITY EVENT ASIA

10 – 12 NOVEMBER 2026

SANDS EXPO & CONVENTION CENTRE, SINGAPORE

SAFETYSECURITYASIA.COM/SECURITY-EVENT

A PREMIER MARKETPLACE FOR SECURITY PROFESSIONALS

125+

WORLD-LEADING SUPPLIERS & MANUFACTURERS

4,000+

SECURITY VISITORS & PROFESSIONALS

10,000+

SOLUTIONS & PRODUCTS



REGISTER YOUR COMPLIMENTARY VISITOR PASS NOW!

TAP INTO OUR WORLD-CLASS SECURITY NETWORK

TELTRONIC TO PROVIDE THE BROADBAND COMMUNICATIONS SYSTEM FOR EFE TRENES DE CHILE'S NEW LINES.

- *Siemens Mobility, which has been awarded the project, has selected the Spanish company to deploy a private 4G network and equip the trains with its onboard solution for train-to-ground data transmission services.*
- *The network will support the Level 2 ETCS signalling system and will be integrated with the Passenger Information System, public address system and CCTV.*
- *The communications infrastructure is 5G-ready and could therefore evolve to 5G through a simple software upgrade.*

Zaragoza – Teltronic, a Spanish company with more than 50 years of experience in the critical communications sector, will be responsible for supplying the broadband communications network that will provide data transmission services for the two new lines of EFE Trenes de Chile, which will connect the capital city, Santiago de Chile, with the towns of Melipilla and Batuco, as part of the project awarded by the Chilean railway operator to Siemens Mobility for the implementation of the country's first ETCS Level 2 system.

In this regard, Siemens Mobility has entrusted Teltronic with the deployment of a private 4G network that will provide coverage along the 87 kilometres of new railway lines. The system is 5G-ready, meaning that it can evolve to 5G technology through a simple software upgrade. In addition, the infrastructure includes two control nodes, one primary and one redundant, to ensure system robustness.

"This project strengthens Teltronic's leadership position in the deployment of broadband communications networks for railway environments, with a solution that is ready to evolve to 5G, which would enable a future migration towards FRMCS implementation".

– Felipe Sanjuán, Transport Business Development Director.



Teltronic will also equip the 32 new trains that will operate on the lines with its RTP-800, a state-of-the-art radio that will enable continuous train-to-ground data transmission. The onboard solution is completed by the DCD7 touch-screen console, which has been designed to meet the stringent requirements of railway environments and allows train drivers to operate the radio controls.

The system, which is also prepared to support voice communications, will be integrated with the Passenger Information System, the public address system and the CCTV network, whose images will be transmitted in real time. It will also support the Level 2 ETCS railway signalling system and will therefore play a key role in the safe and efficient operation of the trains.

New Efe Trenes De Chile Lines

Empresa de los Ferrocarriles del Estado (EFE Trenes de Chile) is the state-owned railway company responsible for passenger transport and railway infrastructure for passenger and freight rail services across 10 regions of the country.

As part of its commitment to improving the quality of life of the communities it serves by reducing travel times and promoting sustainable connectivity, the company will expand its services with two new lines, Melipilla–Estación Central and Santiago–Batuco, comprising nearly 90 kilometres of high-standard railway infrastructure in the Metropolitan Region.

Both lines will generate significant journey time savings for approximately 92 million passengers per year. In total, EFE Trenes de Chile will bring 32 new trains into service, and the new routes will include a total of 19 stations. ■

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

AIRTEL BUSINESS LAUNCHES IQ GATEWAY – INDIA'S FIRST BUSINESS COMMUNICATIONS PLATFORM WITH TELCO-GRADE NETWORK INTELLIGENCE FOR SAFE ENTERPRISE MESSAGING.

- *The DPDP-compliant unified platform combines Airtel's industry-leading fraud protection solutions with network insights to make every customer conversation safer and more trusted.*
- *To enable enterprises to manage multiple service providers and customer communication channels (SMS, WhatsApp, RCS, and business voice) on a single, sovereign control plane, reducing delivery failures, spam risks, and regulatory challenges.*
- *Enterprises can now easily optimize their customer conversation channels (including fallback options), ensure easy identity verification, and curb artificially inflated traffic costs.*

Airtel Business, India's leading provider of secure and reliable connectivity, technology, and communications solutions, today launched Airtel IQ Gateway, India's first-ever telco-grade network intelligence platform that brings different customer communication channels onto one safe control plane.

Enterprises now won't need to manage multiple vendors separately if they opt for Airtel IQ Gateway, a DPDP-compliant platform that combines SMS, WhatsApp, RCS, voice communications, and number verification (silent authentication) together in one place. It will enable enterprises to easily manage their business communications at scale, while protecting customer trust and making safety foundational to every customer interaction.

This offering from Airtel Business is of critical importance today, when businesses have to manage fragmented customer communication stacks across multiple service providers and tools to reach their customers, with limited visibility into the real delivery of messages. Messages are often reported as delivered even when they fail, while International OTP pumping by bots inflates bills. Moreover, managing pre-approved message templates is manual and often leads to mistakes. For enterprises, especially in sectors like BFSI, government, e-commerce and logistics, this not only hurts customer trust when consumers are targeted by scams; it also damages their brand reputation.

Airtel IQ Gateway solves this with a single control center for all business communications. It brings together Airtel's fraud protection with automatic integrations of the native message template system (DLT), automatic switching to backup service providers, and intelligent routing across SMS, WhatsApp, RCS, and voice.

By leveraging Airtel's built-in network intelligence and trust layers for enterprise use, such as IQ Verify for fraud protection and Silent Authentication for SIM-based login, with capabilities like spotting fraudulent account creations and takeovers and artificial traffic spikes, Airtel IQ Gateway protects enterprises from fraud losses and billing spikes caused by industry-wide SMS pumping.

Launched nationwide today after successful trial deployments across select banks, financial institutions and other relevant industry collaborations, the platform extends Airtel's proven expertise in fraud prevention for end customers to enterprises, enabling them to build customer trust at scale through safe communications.

"As India accelerates towards a safe, inclusive digital economy, trust must become the foundation of every digital interaction. Secure-by-design customer engagement is today the bedrock on which enterprises can scale with confidence. At Airtel, we have already demonstrated the power of network-grade fraud prevention in protecting millions of consumers across our mobile and digital services. With IQ Gateway, we are extending this proven expertise to enterprises, enabling them to build brand trust while ensuring every customer conversation is safe, authenticated, and resilient. By embedding trust at the network layer, we are enabling our enterprise customers, especially banks, government departments and logistics firms, to reduce cybercrime losses and strengthen the credibility of every customer interaction. This is a decisive step towards a safer digital future for India, where citizens and businesses can transact and engage with equal confidence."

– Sharat Sinha, CEO Airtel Business

Key capabilities of Airtel IQ Gateway

- **Flexible deployment:** It can be integrated with existing communication workflows and vendor ecosystems. It can be installed on the enterprise's premises or hosted on Airtel's cloud as SaaS, based on customer preference and security requirements.

continue on page 17


Image by Magnific

- **Unified platform with end-to-end control:** Enterprises can manage all their customer communications on a single dashboard with real-time analytics and transparent delivery reporting
- **Protection from financial loss:** Safeguard against fraud losses and billing spikes from fraudulent SMS pumping that are prevalent in the industry
- **Network-grade intelligent features:** Airtel's industry-leading fraud protection is combined with native DLT integration, automated vendor failover, and intelligent multi-channel routing for built-in trust and safety
- **Airtel IQ Verify (network-first fraud scoring)** evaluates network, device, and usage signals to prevent fraudulent accounts from being onboarded and safeguard authentic customers from getting defrauded.
- **Delivery transparency** with network-level delivery reports
- **Silent Authentication (network-first login/SIM binding)** replaces OTP SMS for login and SIM-binding flows by validating that the entered number matches the active SIM in-device, reducing SIM-swap and social-engineering risks.

For more details on Airtel IQ Gateway, log on to **www.airtel.in/b2b/iq-gateway**

About Bharti Airtel

Headquartered in India, Airtel is a global communications solutions provider with over 650 million customers in 15 countries across India and Africa. The company also has a presence in Bangladesh and Sri Lanka through its associate entities. The company is ranked second amongst mobile operators globally, and its networks cover over two billion people. Airtel is India's largest integrated communications solutions provider and the second largest mobile operator in Africa.

Airtel's retail portfolio includes high-speed 4G/5G mobile, Wi-Fi (FTTH+ FWA) that promises speeds up to 1 Gbps, with convergence across linear and on-demand entertainment, video streaming services, digital payments and financial services. For enterprise customers, Airtel offers a gamut of solutions that includes secure connectivity, cloud and data center services, cyber security, IoT, and cloud-based communication. Airtel's digital arm – Xtelify- empowers telcos globally to leverage the power of AI, data, and technology to accelerate their digital transformation and drive growth.

Xtelify also offers Airtel Cloud in India, enabling enterprises with a sovereign, telco-grade cloud platform that guarantees secure migration, effortless scaling, lower costs, and no vendor lock-in. Within its diversified portfolio, Airtel also offers passive infrastructure services through its subsidiary Indus Towers Ltd.

For more details, visit **www.airtel.com** ■

ATNORTH TO DEVELOP A NEW DATA CENTER IN SALO, FINLAND

The planned site will support critical digital infrastructure while creating opportunities for local collaboration, energy partnerships and heat reuse.

Helsinki, Finland – atNorth, the leading Nordic high-density colocation and built-to-suit data center provider, today announced plans to develop a new data center, FIN05, in Salo, Finland, as part of its ongoing objective to meet the demand for high-performance digital infrastructure in a responsible way.

Salo offers a strong location for critical infrastructure serving customers with demanding requirements for connectivity and resilience. Its proximity to Helsinki and Finland's digital talent pool also supports the development of the site.

FIN05 will be developed on a 28.6-hectare site. Power for the first phase, planned at 75 MW, is secured, with a path to power of up to 230 MW for the wider development. The site will connect through a Fingrid substation.

atNorth's investment in the Salo site is expected to be approximately €2 billion. This estimate does not include servers owned by customers, or their installation, which could represent a further investment of up to an estimated €10 billion.

atNorth plans to enter into long-term power purchase agreements with local energy suppliers to support energy production in the region, as well as flexibility solutions that

continue on page 18

"FIN05 is an opportunity to develop critical digital infrastructure while working with the region to create lasting local value. We are exploring how local energy partnerships, flexibility solutions and heat reuse can contribute to the wider energy system and community. We look forward to working with Salo and regional partners as the project develops."

- Eyjólfur Magnús Kristinsson, CEO atNorth

"We are delighted to welcome this investment to our region. The new data center will create valuable employment opportunities during both construction and ongoing operations, while generating wider economic benefits for local businesses. This development strengthens our position as an attractive destination for innovative industries and supports sustainable long-term growth for our community."

- Anna-Kristiina Korhonen Mayor of Salo

"This project demonstrates Salo's potential as a location for major digital infrastructure investment. We have worked closely with atNorth and the municipality to provide a development-ready site, with the scale, planning readiness and power roadmap needed for large data center projects."

- Matti-Juho Ervasti, Partner at Regant Oy

could support the efficient operation of Fingrid's transmission grid. The company will also work with local stakeholders to explore opportunities to make use of heat generated by the data center, helping create value beyond the facility itself. This builds on existing heat reuse collaborations with Kesko Corporation in Finland, Stockholm Exergi in Sweden, as well as Vestforbrænding and Selected Group in Denmark.

FIN05 is part of atNorth's continued investment across the Nordics, alongside developments in Stockholm and Sollefteå in Sweden, Haugaland in Norway, Ølgod in Denmark and Kouvola in Finland. Across its projects, atNorth works with local communities and partners to develop infrastructure that supports customers and contributes to the regions where it operates.

About atNorth

atNorth is a leading Nordic data center company that offers cost-effective, scalable high-density colocation and built-to-suit services trusted by industry-leading organizations. With sustainability at its core, atNorth's data centers run on renewable energy resources and support circular economy principles. All atNorth sites leverage innovative design, power efficiency, and intelligent operations to provide long-term infrastructure and flexible colocation deployments.

atNorth is headquartered in Reykjavik, Iceland, and operates seven data centers in strategic locations across the Nordics, as well as four mega sites under development across Kouvola, Finland, Ølgod, Denmark, Sollefteå, Sweden, and Haugaland, Norway. The business also has an additional metro site under development in Stockholm, Sweden. ■



Image by Magnific

NEW HID SIGNO DÉCOR READER COMBINES SECURE ACCESS AND DESIGN AESTHETIC

The flush-mount reader brings Signo's trusted security architecture to high-design, high-traffic spaces, giving architects and specifiers a reader that complements the spaces it protects

Singapore – HID, a worldwide leader in trusted identity and physical access control solutions, has launched HID Signo Décor in response to a request that architects, specifiers and integrators have repeatedly raised: a Signo-grade reader built for high-design spaces, without a compromise on the security behind it.

The Signo Décor Reader 30 model mounts flush on European- and China-style back boxes and sits behind a robust glass face, rated IK10 for impact resistance and IP65 for indoor and outdoor use, fitting naturally into design-led lobbies, hotels, transport hubs and mixed-use developments while standing up to demanding daily use.

"Security should not force a choice between how a space looks and how well it is protected," said Prabhuraj Patil, Senior Director, Physical Access Control Solutions (PACS) for ASEAN and India Subcontinent, HID. "This belief is what drives HID's product development: to give customers choice without asking them to trade away the trust they have placed in our Signo line."



Décor runs on the same architecture as the rest of the Signo family, so specifiers and integrators can bring it into a design-led project with the same confidence as any other Signo reader. It uses EAL5+ certified secure element hardware and supports the SIO data model for trusted authentication, and it communicates with control panels over Open Supervised Device Protocol for encrypted two-way monitoring. Native Bluetooth and NFC support means end users can present a phone as easily as a card, using HID® Mobile Access® and digital wallet credentials alongside existing access cards.

For teams managing readers across a portfolio of buildings, that consistency extends to operations. Signo Décor can be updated and monitored through HID Reader Manager, or remotely using HID Linq, so firmware and configuration stay current without a technician visiting every door. It is also available as a module for integration into intercoms, elevators, turnstiles, and other access hardware, giving OEM partners a consistent design language across their product lines.

The Signo Décor Reader 30 model, available in black or white in a 90x90 mm form, is available to order now in Europe, China, Hong Kong, Singapore, and the UAE. Additional Signo Décor model variants will become available in other regions later this year. For more information, visit the website.



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.** ■

I-PRO MARKS SEVEN YEARS OF INNOVATION AND TRANSFORMATION

Tokyo, Japan – i-PRO Co., Ltd., a global leader in professional security and public safety solutions, today marks seven years of innovation and transformation since becoming an independent company in 2019.

Seven years ago, i-PRO began its journey as an independent company with an opportunity to build a new kind of organization: one that could make its own technology and business decisions, operate with greater agility and respond more directly to the changing needs of the security market.

Since separating from Panasonic in 2019, i-PRO has steadily built the technology strategy, operations, partnerships and culture to support that vision. This year marked another important step in that journey. In March 2026, i-PRO completed the transition of wholesale and marketing functions for its products in Japan from Panasonic Connect, bringing these activities directly under the i-PRO organization. With development, manufacturing, sales and marketing now more fully connected under the i-PRO name in its home market, the company has brought more of its core business functions together to support its strategic direction and future growth.

That evolution reflects a broader transformation that has taken place over the past seven years. Investments in manufacturing, AI, cybersecurity, open technology, education, and people are helping i-PRO operate with greater agility and bring innovation to customers faster. As the company enters its eighth year, that foundation is positioning i-PRO for its next stage of growth and continued progress toward market leadership.

Building the Organization for Greater Speed and Agility

In October 2025, i-PRO began operations at its Saga Factory in Japan, which now serves as a core i-PRO manufacturing facility, supplying Made-in-Japan products globally. As i-PRO transitions to an integrated production system spanning component manufacturing, assembly, and inspection, the factory is advancing digitalization and automation. This investment further strengthens i-PRO's manufacturing capabilities, alongside those of its Suzhou plant, while enhancing flexibility and resilience across the global supply chain.

Combined with the relocation of sales and marketing functions in Japan, these investments are helping to create a more integrated organizational structure by strengthening collaboration across development, manufacturing, and sales teams. This enables i-PRO to respond more effectively



to continuously changing market needs through faster decision-making, closer collaboration, and greater agility.

Turning Agility Into Innovation

The progress i-PRO has made across its operations is also reflected in the pace of its technology development. Its advances in AI are a case in point, reflecting the technology's central role in i-PRO's business strategy. After introducing generative AI for forensic video analysis in 2025, i-PRO expanded the technology into real-time video operations in 2026 with its X-series Fisheye Cameras featuring generative AI running fully at the edge. Capabilities such as AI On-Site Learning are also making it possible to adapt analytics to individual environments, giving customers greater flexibility to address specific operational requirements.

Rather than treating AI as a standalone feature, i-PRO has focused on making advanced capabilities practical for customers to deploy within the infrastructure they already use. Its open-platform strategy and growing technology ecosystem give organizations greater choice in how they build and evolve their security systems. This approach has been reinforced through closer collaboration with technology partners such as Milestone Systems, which named i-PRO its Innovation & AI Solution Partner of the Year for the U.S. region. The recognition reflects i-PRO's continued investment in edge AI and open technology, and its focus on making these innovations accessible across the wider security ecosystem. One example is its growing range of camera models compatible with leading cloud providers, giving customers greater flexibility to choose the infrastructure that best meets their needs.

continue on page 21

Preparing for Evolving Security Requirements

Innovation also means anticipating how customer needs and requirements will evolve. Cybersecurity has therefore become an increasingly important part of i-PRO's product strategy. Through initiatives such as its Security Update Initiative, the company is strengthening hardware, firmware, and product architecture to address emerging cybersecurity standards and regulations across major global markets and help customers prepare for changing security requirements.

Investing in People and Knowledge

As i-PRO has transformed its technology and operations, it has also invested in building the knowledge needed to support a rapidly changing security industry.

i-PRO University plays an important role in that effort. For the broader industry, technical and sales learning tracks provide education in areas including AI-enabled edge systems, cybersecurity, network configuration, and consultative selling. Internally, the same emphasis on continued learning helps i-PRO employees develop the skills needed to keep pace with new technologies and changing customer requirements.

The investment in people is also reflected in i-PRO's workplace culture. The company achieved Great Place to Work® certification for the second consecutive year across every region where it operates, including Japan, the Americas, EMEA, Asia Pacific and China. The global recognition reflects the culture i-PRO has continued to build alongside its business since becoming independent.

Making Sustainability Part of Long-Term Growth

As i-PRO grows, sustainability is also becoming more deeply integrated into how the company plans for the future.


Image by Magnific

The appointment of Shohei Ozaki as Chief Sustainability Officer made sustainability a C-level responsibility, helping integrate it more closely into company decision-making and long-term business strategy.

i-PRO has also strengthened its commitment through membership in the United Nations Global Compact, aligning the company with a global framework for responsible business practices. Together, these steps strengthen the role of sustainability as the company continues to grow.

Looking Ahead

As i-PRO enters its eighth year, the investments made since becoming independent are helping position the company for its next stage of growth. With greater agility to respond to changing customer needs and advance new ideas, i-PRO will continue strengthening its position in the global security market.

"As i-PRO marks its seventh anniversary, I would like to thank our customers, partners, and employees for their continued trust and support. This milestone represents not only how far we have come, but also the beginning of our next stage of growth. Over the past years, we have strengthened our manufacturing, sales, and global business foundations while investing in a culture where people can thrive. Growth requires us not only to build on our strengths, but also to rethink conventional assumptions, embrace new perspectives, and drive meaningful transformation. We will continue creating value for our customers and advancing our global growth with confidence."

-Masato Nakao, President & CEO i-PRO Co., Ltd.

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 we provide our partners, customers, and users with innovative and sustainable technologies. i-PRO joined the United Nations Global Compact in 2023. ■

DIGICERT QUANTUM CENTRAL NOW AVAILABLE TO HELP ORGANIZATIONS TURN PQC PLANS INTO ACTION

Expanded capabilities turn fragmented cryptographic data into a prioritized plan, coordinated action, and measurable progress toward post-quantum readiness.

Singapore – DigiCert, a global leader in intelligent trust, today announced the general availability of DigiCert Quantum Central, part of the DigiCert ONE platform, that helps organizations manage and demonstrate progress toward post-quantum cryptography (PQC) readiness.

First introduced in preview in July, Quantum Central offers expanded capabilities that help organizations move from finding cryptographic risks to managing them. Teams can bring together cryptographic data from multiple sources, apply their own security policies, initiate remediation workflows, assign ownership, and track progress from a central location.

The launch comes as organizations struggle to turn PQC planning into execution. According to the 2026 DigiCert Quantum Readiness Outlook, 87% of organizations are planning, testing or implementing PQC initiatives, yet only 7% have deployed quantum-safe or hybrid cryptography.

"Most organizations understand the quantum risk. Their challenge is coordinating action across legacy systems, fragmented data, and multiple technology owners," said Kevin Hilscher, Senior Director of Product Management at DigiCert. "Quantum Central turns cryptographic visibility into a prioritized and trackable readiness program. Teams can begin with a critical environment, act on what they find and expand over time, while giving leadership, auditors and regulators clear evidence of progress."



Quantum Central helps security, IT, risk, and compliance teams:

- **Create a unified cryptographic inventory:** Consolidate and normalize data from DigiCert ONE, network scans, certificate lifecycle management platforms, key vaults, uploaded CSV files, and software or cryptographic bills of materials.
- **Establish policies and priorities:** Define cryptographic policies based on organizational requirements, industry standards, and regulatory guidance. Quantum Central evaluates inventory data, identifies policy violations, and alerts teams when action is needed.
- **Turn findings into remediation:** Translate policy violations into recommended actions and create change requests through established workflows, including Jira. Integration with DigiCert Trust Lifecycle Manager enables teams to initiate certificate lifecycle actions directly from their readiness program.
- **Interpret inventory data faster:** Use an inventory-aware AI assistant to understand findings, explore cryptographic exposure, and identify practical next steps.
- **Measure and report progress**: Track remediation status, policy compliance, and overall cryptographic posture through centralized dashboards. Organizations can also export inventory data as cryptographic bills of materials for audits, assessments, and reporting.
- **Connect external systems:** Import cryptographic data programmatically through an API, allowing organizations to continue expanding their inventory as their readiness programs mature.

"The market is entering the operational phase of post-quantum readiness, and enterprises need a way to connect cryptographic discovery with business context, policy and remediation," said Jennifer Glenn, Research Director for Information and Data Security at IDC. "Tying inventory, workflows, and

continue on page 23

reporting to that policy in a single view gives organizations a practical operating model for the complex, multiyear transition to quantum-safe cryptography."

Quantum readiness requires organizations to manage a multiyear technology transition while standards, vendor capabilities, and regulatory expectations continue to evolve. Organizations can make practical progress now by assigning accountable owners, establishing enough cryptographic visibility to set priorities, adopting PQC where supported, and documenting results. An incremental approach allows teams to begin with a critical application environment or infrastructure layer and expand their program without waiting for a complete enterprise-wide inventory.

Quantum Central is the management layer for enterprise quantum readiness, spanning cryptographic use cases beyond PKI. DigiCert ONE managers provide the automation layer for certificates, software, devices, and content, while DigiCert Private CA and CertCentral provide the trust and issuance foundation needed to put new cryptography into production. That combination helps organizations manage the broader readiness program while preparing for the more complex PKI transition that will unfold over time.

DigiCert Quantum Central is available now. Organizations can start a free trial, request a demonstration, or contact DigiCert to discuss an enterprise deployment.

Resources:

- Organizations can deploy PQC today to protect their network traffic from harvest-now, decrypt-later attacks. Read our white paper, Recommendations for Quantum Safe TLS, for more details.
- Check the quantum readiness of your organization's and others' websites with our online PQC Checker.
- Learn the basics about post-quantum cryptography and understand the urgency to start quantum readiness now in DigiCert's PQC for Dummies Guide.

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.** ■

KEEPER SECURITY FRESHSERVICE WORKFLOW APP STREAMLINES VAULT AND PRIVILEGED ACCESS REQUEST PROCESS

New integration enables IT and security teams to search the Keeper vault and submit access requests directly from the Freshservice ticket sidebar.

Singapore – Keeper Security, the leading zero-trust and zero-knowledge identity security and Privileged Access Management (PAM) platform, today announces a Freshservice Workflow integration that connects vault and privileged access requests to the ticketing systems IT and security teams already use.

The integration lets agents fulfill Keeper vault access and approval requests, including Endpoint Privilege Manager and Cloud SSO device approvals, directly from a Freshservice ticket. The workflow bottleneck experienced with other solutions is eliminated by removing the need for agents to leave tickets for approvals, log into a separate system, or move decisions through unaudited side channels like email or chat.


Image by Magnific

Streamlining Ticket Management and Approval

Access approvals often stall after the initial request

continue on page 24



"The cryptographic boundary cannot move outside Keeper. This integration processes every approval through Commander ServiceMode on infrastructure owned and controlled by the customer, so the attack surface doesn't expand when you wire Freshservice into your approval workflow. Freshservice is the interface for the request, never the place where secrets are stored."

- Craig Lurey, CTO and Co-founder of Keeper Security



"Every access request is an identity decision, and the further those decisions drift from a governed system, the weaker the audit trail becomes. Integrating Keeper into Freshservice keeps approval decisions inside a ticketing system that security teams already trust, which means zero standing privilege and full audit control stay intact. This becomes increasingly important in the agentic era, as access requests multiply across both human and machine identities."

- Darren Guccione, CEO and Co-founder of Keeper Security

creation. A user submits a helpdesk ticket, but the person fulfilling it has to leave that ticket, log into a separate system, track down the right record or folder, and manually grant permission before reporting back. Each handoff introduces delays and moves access decisions outside of the audit trail.

The Keeper Security Freshservice Workflow App removes that handoff. When an employee submits a request through a Freshservice service catalog item, the assigned agent can search through Keeper content, configure permissions, and approve or deny the request from a Keeper Vault tab inside the ticket itself.

Every action runs through a customer-hosted Keeper Commander ServiceMode endpoint, so Keeper's zero-knowledge encryption and access controls stay intact, and Keeper never stores credentials inside Freshservice's IT Service Management (ITSM) and Enterprise Service Management (ESM) platform.

The integration also supports Endpoint Privilege Manager and Cloud SSO device approvals when paired with Keeper's ITSM for Freshservice app, so security admins maintain a single ticketing interface for both incident-driven access requests and routine approval workflows.

Availability

The Keeper Security Freshservice Workflow App is available now in the Freshworks Marketplace for organisations with an active Keeper Commander deployment. To learn more about the integration, visit **docs.keeper.io.**

About Keeper Security

Keeper Security is the leading zero-trust and zero-knowledge identity security solution, trusted by millions of people and thousands of organizations globally. KeeperPAM® is Keeper's privileged access management platform that unifies password and passkey management, secrets management, privileged session management, and endpoint privilege management in a single cloud-native platform, protected with quantum-resistant encryption. KeeperAI delivers real-time, AI-native threat detection across every privileged session. As AI agents proliferate and identity becomes the defining attack surface, Keeper governs access for humans, machines, non-human identities, and AI agents, serving as the unified control plane for access, compliance, and visibility across the enterprise. For more information, visit **KeeperSecurity.com.** ■

DIGITECH ASEAN THAILAND & AI CONNECT 2026

Returns to Connect Technology Leaders, AI Innovators, and Business Decision-Makers across ASEAN



Bangkok, Thailand– DigiTech ASEAN Thailand & AI Connect 2026, the premier international exhibition and business networking platform for digital business solutions, is making a grand return. The event will take place from 25-27 November 2026 at Hall 7-8, IMPACT Exhibition & Convention Center, Bangkok, Thailand

With a focus on helping businesses navigate today's economic challenges and rapid technological shifts, this year's event has expanded its exhibition space. It will showcase a comprehensive range of digital and AI solutions aimed at driving business growth and promoting sustainability across various industries. Attendees will discover how to leverage tech to reduce costs, boost efficiency, and keep pace with the fast-evolving business landscape.

This year's event is expected to attract over 400 leading global tech brands and companies catering to enterprises, mid-sized businesses, and SMEs alike, and welcome more than 12,000 tech buyers and visitors.

The event serves as a direct bridge connecting tech providers with high-potential buyers. The exhibition will span six key technology sectors, which are Business Software, Cybersecurity, E-commerce & Digital Marketing,
Data & Cloud, Smart Solutions & IoT, and Artificial Intelligence (AI).

Visitors can stay ahead of the curve with technology trend updates and practical business workshops led by industry experts at the Global Tech Stage and The Future of AI Stage. The event will also feature face-to-face product demonstrations, allowing attendees to experience solutions firsthand and see how they work in real-world business scenarios. In addition, a pre-arranged Business Matching Program will be available to help drive digital transformation and create opportunities for targeted strategic partnerships.



Ms. Peerayaphan Ponganam, Assistant Director of the Exhibition Project Department at IMPACT Exhibition Management Co., Ltd., shared: "DigiTech ASEAN Thailand & AI Connect reflects the continuously rising demand for digital and AI solutions as businesses look to stay competitive in a volatile economy. IMPACT is dedicated to making this event a powerful regional business and knowledge hub. It offers tech providers of all sizes the chance to connect face-to-face and strengthens Thailand's position as a vital digital and AI hub for ASEAN."

This landmark event is proudly supported by its Silver Sponsors, whose innovation drives the region's digital transformation forward: 9 Dots Consulting Co., Ltd., Adobe, Axons, DCSS (Thailand) Co., Ltd., SambaNova Systems Inc., Socket 9, Wholix, and Zoho Corporation.

continue on page 26

Kelly Chong, Sales Executive, Southeast Asia at Adobe, added: "At Adobe, we believe creativity and productivity are the heart of success in the modern business era. We are thrilled to support DigiTech ASEAN Thailand & AI Connect 2026 as a Silver Sponsor. As the ASEAN market rapidly adopts advanced digital marketing strategies and tech-driven frameworks, this event is the perfect opportunity to showcase Adobe's AI-powered smart solutions to businesses in Thailand and across the region."

Join us at DigiTech ASEAN Thailand & AI Connect 2026, taking place **25-27 November 2026** at **Hall 7-8, IMPACT Exhibition & Convention Center, Bangkok, Thailand,** where leading technology providers, AI innovators, business leaders, and industry professionals will come together to explore the future of digital business.

For more information, please visit **www.digitechasean.com.**

Free visitor registration: **https://digitechasean.com/visitor-registration/?campaign=Intmedia**

For inquiries, call **+66 (0) 2-833-5370** or email **info@digitechasean.com**

About the organiser

IMPACT Exhibition Management Co. Ltd.
IMPACT Exhibition Management Co., Ltd. is the leading exhibition organiser in Thailand. We organise and manage professional trade and public exhibitions, conferences, meetings and training, working hand in hand with international trade associations, organisers, and corporations across a broad spectrum of industries.
For more information, please visit **https://impactorganizer.com/** ■

SECURITY ESSEN AND EUDEX 2026: A STRONG SIGNAL FOR CIVIL-MILITARY COOPERATION

High share of decision-makers and international reach

Four days, around 900 exhibitors from 49 countries and 30,000 trade visitors: the very first EURO DEFENCE EXPO (EUDEX) and Security Essen, held at Messe Essen, have ended with excellent results. Trade visitors from 96 countries attended both events to find out about new technologies and solutions for defence and civil security.

Exhibitors and visitors alike were highly satisfied with the combination of the new trade fair for the defence industry and the established security trade fair.

"With this dual trade fair event 'made in Germany', we have broken new ground in linking civil-military cooperation. This unique platform offered participants visibility and new opportunities"
- Oliver P. Kuhrt, CEO of Messe Essen.

He particularly highlighted the calibre of the trade visitors: 83 per cent of EUDEX trade visitors are decision-makers in purchasing and procurement, while the figure for Security Essen is 76 per cent.

Drones, AI and connectivity were the defining topics at both trade fairs

Key topics at both events were AI, the interconnection of systems, robotics and unmanned aerial systems.

"We held many high-quality discussions and arranged specific meetings to further develop business opportunities. We are very satisfied with the footfall and response at our stand. The organisation and compact structure of the trade fair also contributed to our positive overall assessment of the event."

Another increase in visitor numbers at Security Essen

With a rise in visitor numbers of around ten per cent, Security Essen once again underlined its strong position as the leading international trade fair for the civilian security industry.

A total of 522 exhibitors from 41 countries presented the full range of modern security technology to trade visitors – from access control, fire and burglary protection, video and perimeter security, to risk management, services and civil protection.

The exhibitors' innovations included AI agents for control centres, solutions for new programming interfaces in hazard management systems and the centralised management of various access technologies, as well as new developments for improved protection of critical infrastructure.

To this end, companies presented, among other things, enhanced biometric identification options, high-performance photoelectric barriers for perimeter protection and

continue on page 27

The overlap in content was particularly evident when it came to drones. At EUDEX, remote-controlled systems for reconnaissance, resupply and other military applications were on display. One exhibitor unveiled its new long-range reconnaissance drone for the first time, with a flight time of up to eight hours.

At Security Essen, companies showcased solutions for surveillance, inspection and the protection of critical infrastructure, as well as for the detection and defence against unauthorised aerial vehicles.

One in four trade visitors at Security Essen was particularly interested in the drone sector, while at EUDEX, unmanned systems and robotics were the most important topic for 40 per cent of trade visitors.

EUDEX celebrated a successful launch

EUDEX kicked off for the first time with 365 exhibitors from 28 countries. Trade visitors came primarily from industry and the armed forces, but also from government bodies, research, politics and diplomacy.

They made the most of the new trade fair format to engage in direct dialogue. The products and services on offer ranged from unmanned systems and robots, AI and software, through to personal protective equipment, transport containers, mobile protective infrastructure, supply and packaging solutions, command and communication technologies, reconnaissance and surveillance solutions, as well as vehicles and heavy equipment.

EUDEX specifically sought to forge links between the defence industry and companies from other industrial sectors.

Dr Jens Bodo Koch, CEO of Heckler & Koch GmbH, said: "In our view, the inaugural EUDEX was a success. It is good and right that Messe Essen here in Germany took the lead early on in establishing a defence trade fair alongside its Security Essen event. We encountered an international trade audience here and held numerous discussions with end-users, suppliers and decision-makers. Even in its very first edition, EUDEX has thus demonstrated that it can be an interesting platform for professional exchange within the security and defence industry. We were also particularly pleased with the very positive response to our products and solutions."

Stefan Houben, Key Account Manager for Defence and Public Affairs at SCANIA, said: "EUDEX provided us with an effective platform to present our transport and mobility solutions for the defence sector to a high-calibre specialist audience. We found the exchange with representatives from industry and politics, as well as with military users from both Germany and abroad, particularly valuable.

centralised alarm systems.

Dipl.-Ing. Markus Kock, Managing Director of WAGNER Deutschland GmbH, said: "Security 2026 provided us with an excellent platform for engaging with customers and prospective clients. The attractive stand location and high footfall enabled us to hold numerous meaningful discussions.

"In particular, the presentation of our new TITANUS REX® aspirating smoke detector attracted a great deal of attention. The response to our solutions for fire prevention, firefighting and risk management showed that these topics are of great relevance to many of the trade fair visitors. Overall, we consider our participation in the trade fair to have been a success."

Klaus Hirzel, Director Sales DACH, Honeywell Technologies, said: "Security Essen once again showed how important connected solutions are for our customers. For us, it is a strong signal to bring fire and life safety, security and access solutions, and building automation together as one integrated offering."

Stefanie Goetz, Director Sales DACH, Honeywell Technologies, added: "The many positive conversations at Security Essen showed that connected Building Automation solutions continue to play an important role for our customers – from fire detection and alarm systems to access control, video surveillance, intrusion detection and building automation. For us, it is therefore especially important to bring these areas together and present them as integrated solutions."

Visitors were satisfied with their participation

Nine out of ten visitors to Security Essen were satisfied with their visit, would recommend the trade fair to others and intend to attend the next event as well.

Visitors to both trade fairs praised the international character of the events, the presence of market leaders and the range of new products on offer.

The combination of the two events was also taken full advantage of: one in two visitors to EUDEX also visited Security Essen.

A total of 30,000 trade visitors attended the twin trade fairs. In addition, numerous members of the press, political delegations and guests of honour were in attendance.

Next exhibition dates: **19 to 22 September 2028**

The next Security Essen and the next EUDEX will take place from **19 to 22 September 2028** at Messe Essen. ■

Delve into strategies and technologies protecting power plants, transport systems, and data centres from both physical and cyber threats

Introduction

Critical infrastructure refers to the systems, assets, equipment, networks, etc., whose disruption would have a severe impact on an organization to deliver its primary daily services, where in turn will jeopardize national development and/or national security of a country. These include power grids, water treatment facilities, transportation networks, telecommunications, data centres, financial services, etc, just to name a few. Today, critical infrastructure operators encounter dual challenge: protecting against physical and cyber security threats. In the recent years, these threats are unfortunately converging as what is now known as hybrid attacks, and they can no longer to be treated as separate domains.



Image by Magnific

The Evolving Threat Landscape



Image by Magnific

Cyber threats to critical infrastructure have grown in sophistication and frequency, and such kind of threat is no longer generic in nature. Malwares are highly customized and specifically designed nowadays for industrial control systems. Some of the malwares are engineered to attack power grids by leveraging native industrial communication protocols to directly interact with and control grid equipment remotely. Unlike traditional IT attacks, such malwares can cause direct physical disruption, rendering critical equipment unresponsive and therefore compromise power plant's daily operations. Other emerging cyber threats may include false data injection attacks like manipulating sensor data to deceive control systems, using AI-generated voices for vishing and automated exploit generation, exploiting third-party providers with deep system access, etc.

Physical threats, on the other hand, remain equally concerning over the years. Since 2020, power grid operators have suffered hundreds of incidents ranging from shootings to intrusions and vandalism. Data centres confronted by theft, vandalism, arson, and non-hostile incidents like power failures or overheating. Whereas for transport systems, they are deemed to be vulnerable to Global Navigation Satellite System (GNSS) interference, where navigation can be misled due to jamming and spoofing.



Terrorist organizations view critical infrastructure as a prime target due to its symbolic value, potential for mass disruption, and the high media attention an attack would generate. These are the most common objectives which terrorists around the world want to achieve in their mission oriented attacks. This type of physical threats are diverse, ranging from simple sabotage to sophisticated, coordinated and catastrophic assaults such as launching vehicle-borne improvised explosive device (VBIED), person-borne improvised explosive device (PBIED), Unmanned Aerial System (UAS), vehicle-as-weapon (VAW), vessel improvised explosive device (VIED), etc., chemical, biological & radiological (CBR) agents, attacks. Although these threats which are launched by outsiders and reasonably mitigated by critical infrastructure operators, insider threats which exploiting disgruntle employees (both existing or ex-staff) and/or contractors with authorized access to cause damage to critical assets of the critical infrastructure is widely overlooked or worst being ignored.

Modus operandi of attacks against critical infrastructures may include but not limited to are deliberately damaging critical assets like transformers or control systems of power plants and electrical grids, by using VBIED, PBIED, sabotage &

assault, using projectiles or explosives from a distance to avoid ground-level security, etc. Disrupting rail networks by using fire, placing obstructions on tracks, or sabotaging brake hoses, signal systems, and train couplers, targeting airports, train stations, and vehicles with VBIED or PBIED, using VAW to ram into facilities or crowds, jamming or spoofing satellite navigation to disrupt aviation and shipping, etc., to launch attacks against transport systems.

Methods of attacks deployed by attackers against data centres are using weaponized drones and missiles which will cause fires and power outages, using VBIED or hostile vehicles to breach perimeter defences, etc. These physical threats are increasingly combined with cyber-attacks to maximize damage, creating a dangerous "cyber-physical" threat.

Sector-Specific Strategies and Technologies

For power plants and electrical grids, the key strategies and technologies which operators can possibly deployed to mitigate the emerging cyber-physical threats are unifying cybersecurity and physical security strategies. This means breaking down silos between IT and Operational Technology (OT) teams. Moving beyond perimeter defence to focus on users, assets, and resources. For instances, implement network segmentation, access proxies, and next-generation firewalls, integrate with hierarchical layering and active-deception honeypots, and build security into the engineering process from the outset, rather than treating it as an afterthought.

Whereas for transport systems, continuous monitoring of GNSS signals and other navigation systems to detect and respond to interference is paramount. Other methods of protecting such critical infrastructure against cyber-physical threats which operators may consider are to incorporate incident response mechanisms and threat intelligence sharing across transport operators, ensure data quality and security, system interoperability, and the reliability of algorithms used within critical transport infrastructure, and participate in industry drills and exercises that simulate cyber-physical attacks on transport systems.

For data centres, hardware-enforced isolation is needed to allow operators to instantly disconnect compute, storage, and network segments with secure, out-of-band commands that sit outside the attack surface. IP-based CCTV surveillance cameras equip with video content analytics and AI-centric technology, IP-based electronic access control system, and building management system should be further hardened and assured as operational technology against security threats. Security strategies must bridge physical and digital worlds, eliminating vulnerabilities on either side.



Image by Magnific

Conclusions with recommendations

Securing critical infrastructure requires a paradigm shift from siloed, reactive approaches to integrated, and proactive strategies. The convergence of physical and cyber threats demands unified security frameworks that bridge traditional organisational boundaries.

Security-by-Design (SBD) is the practice of integrating protective measures from the earliest stages of planning and design, rather than retrofitting them as an afterthought. For critical infrastructures, this means weaving security into the physical architecture, digital systems, operational procedures, and even maintenance schedules from the very beginning as a cost-effective security strategy. Retrofitting security onto legacy systems is notoriously expensive and often ineffective.

For power plants & electrical grids, operators are recommended to implement sets of cybersecurity measures like enforce IT/OT segmentation and use OT-aware threat detection systems. Transport systems, on the other hand, operators

are recommended to adopt secure boot standards and zero trust for connected rolling stock and control systems, embed security in maintenance and system updates across the asset lifecycle, design infrastructure to "design out" criminal and acts of terrorism opportunities, use geospatial tools to map and secure critical connections, and plan for cross-domain intelligence sharing against hybrid threats. Whereas for data centres, operators are recommended to enforce hardware isolation for sensitive workloads, segment power and cooling systems, and mandate data encryption at rest and in transit.

To mitigate criminal and terrorist threats through physical security measures, operators of these critical infrastructures must adopt Risk-Based & All-Hazards Approach and Physical Security Defence In-Depth Model. This means operators are ought to tailor the following recommended measures based on specific threat, vulnerability, and risk assessments, and considering all potential hazards.

Measures include but not limited to are Physical Barriers (e.g., crash-rated and anti-climb perimeter fences, crash-rated hostile vehicle measures, etc., to deter unauthorized access and VBIED threats), Strategic Site Layout Plans (e.g., minimize entry points, eliminate blind spots, create stand-off distances between public areas and sensitive assets, etc.), Access Controls (i.e., restrict access via authentication systems like 2FA electronic access control system), Personnel Security (i.e., conduct screening on vehicles, persons and bags using screening equipment like Walk-Through Metal Detector / Handheld Metal Detector, X-Ray Machine, Explosive Trace Detectors, etc., at all entry points), Detection Systems (e.g., infrared beams, fence intrusion detectors, motion detectors, etc.), Surveillance System (i.e., CCTV surveillance cameras with video content analytics and AI-centric capability for 24/7 monitoring that integrate with intrusion alarms for immediate security officers' respond), and Security Lighting (i.e., ensure adequate lighting to deter adversaries and enhance camera visibility), and Redundancy (e.g., build in redundant power sources, network paths, and utility feeds to maintain operations during an attack).
To mitigate insider threats, it is recommended that operators are to conduct rigorous insider threat mitigation programs for employees and contractors. These programs may include but not limited to Rigorous Screening (i.e., verify identity, conduct criminal checks, and validate references especially for high-risk roles), Role-based Access Control (i.e., grant access strictly on a need-to-know basis), Two-Deeph Work (i.e., requires two authorized individuals for sensitive operations), Vigilant Culture (e.g., train staff to spot "compelling events" like disgruntlement or financial distress and provide confidential reporting channels), Identify Anomalous Behaviour (i.e., detect deviations from normal behaviour and analyse abnormal access logs), and Behavioural Indicators (i.e., watch out for large data transfers, or attempts to bypass security controls).

The threat landscape will continue to evolve. Nation-state actors, ransomware gangs, and hybrid adversaries are constantly developing new tactics. Critical infrastructure operators must remain vigilant, adaptive, and collaborative, building resilience not as a one-time project but as an ongoing commitment. ■

Writer: Mr. Joshua Kwai



From 1997 to 2007, ***Mr. Joshua Kwai*** served in Singapore's Police Force and Ministry of Home Affairs, specialising in homeland security and law enforcement, while advising private-sector management on hardening physical security for key facilities. He then transitioned to security consulting (2007–2011), delivering high-value protection master plans, risk assessments, and custom in-house training programmes for Singaporean firms.

In 2011, 2013, and 2021, he founded JK Consultancy Holdings Pte Ltd (Singapore), JK Consultancy Services (Malaysia) Sdn Bhd, and Nanning JK Consultancy Services Limited (China) respectively, aiming to expand security risk management and training services across the Asia-Pacific region.

An international conference speaker and principal trainer, ***Mr. Joshua Kwai*** shares operational expertise with global security professionals and frequently contributes articles on threat analysis to prestigious journals. He has been interviewed by Malaysia's Bernama on emerging local threats and by Singapore's The Straits Times on the transformation challenges facing Chinese security firms.

He recently completed his Doctor of Business Administration (DBA) at ENAE Business School (University of Murcia, Spain), with a thesis entitled "Analysis of the Economic Viability of Physical Security Investment" that he graduated with a notable score and expects to receive his doctoral title by end-2026.

Beyond the Firewall: Securing Critical Infrastructure in the Age of AI

As critical infrastructure becomes more connected, AI is changing not only how these environments are defended, but where the security perimeter actually sits.

Key Takeaways

- *The security perimeter has expanded: Critical infrastructure now depends on interconnected IT, OT, cloud platforms, suppliers, and remote access, making identity and trust as important as network boundaries.*
- *AI is both a defence and a new risk: AI can help security teams detect threats faster, but AI-enabled systems also introduce new dependencies that must be governed, monitored, and tested.*
- *Resilience matters as much as prevention: Operators need visibility, controlled access, consequence-based risk management and tested recovery plans to keep essential services running when prevention fails.*

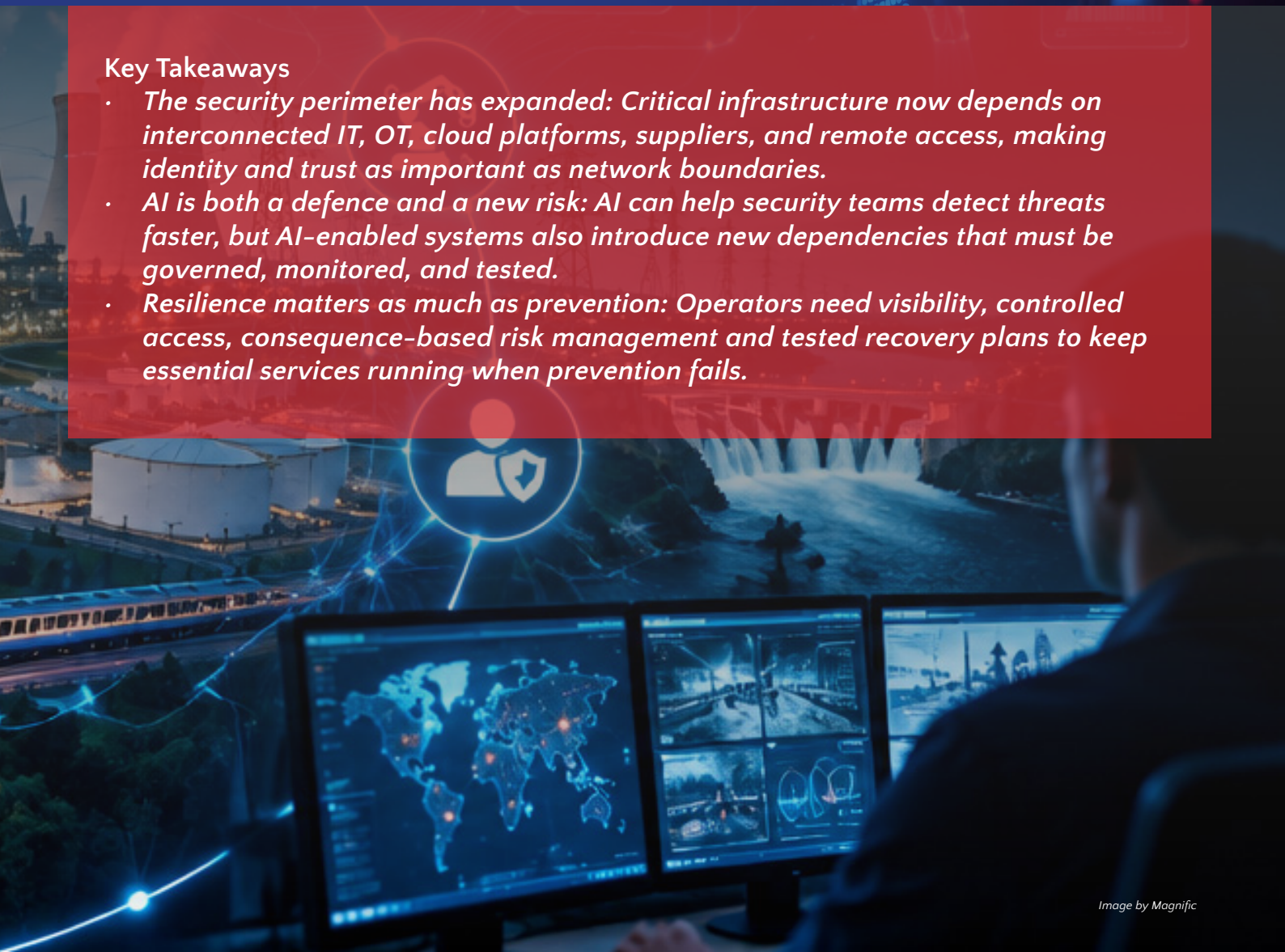


Image by Magnific

"Cybercriminals are most often breaking in without breaking anything — capitalizing on identity gaps overflowing from complex hybrid cloud environments that offer attackers multiple access points. Businesses need to shift away from an ad-hoc prevention mindset and focus on proactive measures such as modernizing authentication management, plugging multi-factor authentication holes and conducting real-time threat hunting to uncover hidden threats before they expose sensitive data."

- Mark Hughes, Global Managing Partner of Cybersecurity Services IBM

Nothing breaks. No alarm sounds, no file is encrypted, no screen flashes red. A "trusted account" simply does what trusted accounts do, which is reach into systems that run power, trains and data. By the time anyone asks who is behind it, the access has already travelled a long way.

IBM X-Force found that critical infrastructure organisations accounted for 70% of the attacks it responded to in 2024, with more than a quarter involving vulnerability exploitation.

For a power station, railway or data centre, the question is not only whether someone got in. It is how far that access can go. Security teams can know which systems are critical and still struggle to see everything those systems depend on. That is the blind spot, and the traditional perimeter does not cover it.

The Infrastructure Is More Connected Than the Security Model

For decades, operational systems were protected on the assumption that they were separated from the outside world. Today, operational technology (OT) connects to enterprise IT, remote engineering platforms, cloud services, sensors and third-party systems.

A power facility may depend on a vendor's remote maintenance platform. A railway may rely on communications linking several operational environments. A data centre may pair servers with connected cooling, power and building systems.

A weakness in one layer matters because of what it can reach in another. A compromised engineering workstation has very different consequences from a compromised office laptop if it holds privileged access to operational systems.

Many operators also struggle with a basic question: what is actually connected to our network, and why? Legacy equipment, temporary vendor links that became permanent, and cloud monitoring added by another team all leave connections nobody remembers approving.

The Perimeter Now Includes People and Suppliers

Equipment manufacturers, systems integrators and specialist contractors often need privileged access to diagnose faults or perform maintenance, frequently without visiting the site. A compromised vendor account can open a path into systems never designed to be internet-facing.

Verizon's 2026 Data Breach Investigations Report found third-party involvement in 48% of breaches, up from 30% in the previous year's dataset. The figure covers Verizon's broader dataset rather than critical infrastructure

specifically, but it shows the growing weight of supply-chain relationships.

Segmentation alone cannot solve this.

A segmented network can still be compromised if a trusted account holds excessive privileges or a vendor connection bypasses controls. Identity has become as important a boundary as the network.

Where the Risk Becomes Operational

The same compromise can have very different consequences depending on where it lands.

- **Power.** Access to an engineering workstation or trusted connection can create a path towards systems that influence physical operations. The worst outcomes are generation disruption or grid instability.
- **Transport.** Signalling, communications, surveillance and access control are spread across many locations, so an incident in one layer can ripple through connected operations. A compromised access-control system can change who reaches a facility, and compromised cameras can blind operators during an incident.
- **Data centres.** Compute and networking sit beside cooling, power distribution and building-management systems. An incident in a supporting layer becomes an availability problem that can affect services far beyond the building.

The 2021 Colonial Pipeline incident showed how an IT problem becomes an operational one. A ransomware attack on business systems led the company to halt pipeline operations anyway, because it could not be sure what was safe to run.

Patching cannot always close the gap. Equipment may have strict uptime requirements, vendor patches need testing, and older systems may run unsupported software. IBM identified 670 vulnerabilities disclosed in the first half of 2025 that could affect OT environments. Of those, 11% were rated Critical, and one-fifth of the critical ones had public exploit code.

AI Cuts Both Ways

For defenders, AI can process telemetry that human teams cannot examine manually, flagging communications that break an established baseline and helping analysts decide what to investigate first.

But AI is also becoming part of the infrastructure. A monitoring platform may shape what an operator investigates, and a maintenance system may influence when equipment is serviced. That raises hard questions: what if the data feeding a model is manipulated, or operators trust its recommendations too much? NIST is developing a Trustworthy AI in Critical Infrastructure Profile to address AI across IT, OT, and industrial control environments.

Attackers are using AI too. IBM's 2026 X-Force research reported a 44% increase in attacks beginning with exploitation of public-facing applications, while highlighting how AI accelerates vulnerability discovery. Faster attack cycles raise the pressure to find exposed systems before someone else does.

The Security Solutions Taking Shape

The shift beyond the traditional perimeter is also changing



Image by Magnific


Image by Magnific

what effective protection looks like. Security is moving towards greater visibility, tighter control over trust, and the ability to contain disruption when prevention fails.

Visibility Across the Infrastructure

Operators need to see more than individual assets. They need to understand the connections between IT, OT, cloud services, legacy equipment, and third-party systems. Passive monitoring can help identify these relationships without actively probing sensitive operational equipment.



That visibility also provides context. Knowing what an asset supports and what can reach it makes it easier to judge which weaknesses could have real operational consequences.

Identity and Controlled Access

Remote engineering and supplier access have become part of modern infrastructure operations. They also create potential paths into environments that were never designed for broad external access.

Identity controls therefore sit alongside network security. Strong authentication, least-privilege access, and tightly controlled vendor pathways can limit what a compromised account can reach and reduce opportunities for lateral movement.

Segmentation and Isolation

Segmentation remains an important layer, particularly where enterprise IT connects with operational environments. The objective is not simply to divide networks, but to limit how far a compromise can travel.

Where vulnerable systems cannot be patched immediately, isolation and restricted access can provide additional protection while operators plan a safer maintenance window.

AI-Driven Detection and Response

AI can help security teams process large volumes of telemetry, identify unusual behaviour and prioritise investigations. But AI systems themselves are becoming part of the infrastructure they are expected to protect.

Their data, interfaces and permissions therefore need security controls of their own. The greater the system's ability to influence operational decisions, the more important human oversight and defined boundaries become.

Resilience and Recovery

No security architecture can guarantee prevention. Critical infrastructure must also be able to contain an incident and recover without turning a cyber event into a prolonged operational failure.

That means testing isolation, trusted backups, manual procedures and recovery sequences before they are needed. In these environments, resilience is not separate from cybersecurity. It is part of the security architecture itself.

Beyond the Firewall

Security maturity was once measured by what an organisation had built: the walls, the tools, the controls. In critical infrastructure, that measure is running out of road. These environments are now networks of trust, and trust is either governed deliberately or inherited by accident.

The question is no longer how to keep attackers out, but what happens when something trusted turns out not to deserve it. Vendor accounts, engineering workstations, and AI systems are all trust decisions, and each should be mapped, bounded, and rehearsed before an adversary tests it. The firewall still has a role. It is simply no longer where the security story ends. ■

COMING SOON

OCT 28 – 30 2026

SIDEX-ACDR 2026 *(Page 5)*
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

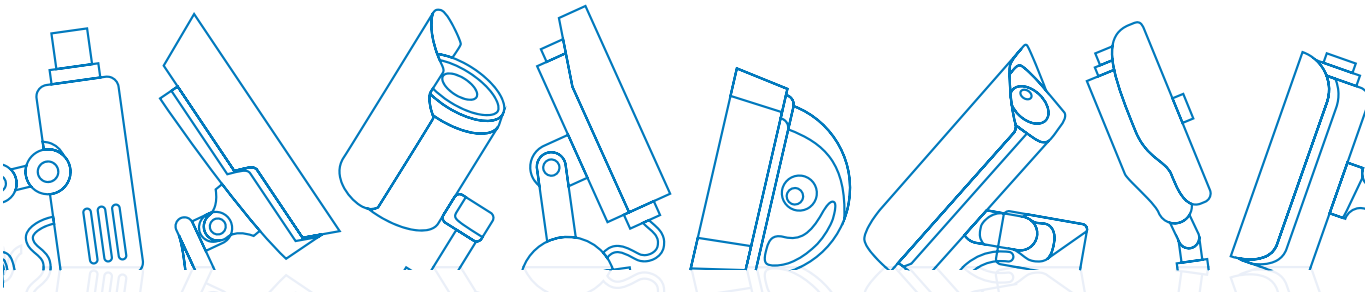
Secutech Thailand 2026 *(Page 3)*
Bangkok, Thailand
www.secutechthailand.com

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



Scan to visit our website

SECURITY SOLUTIONS TODAY

Security Solutions Today (SST) is a leading publication on the latest security information, trends and technology, and products that include Access Control, CCTV/IP Surveillance, Intrusion Detection and Integrated Security Systems.

SST is packed with the latest developments in security technologies and trends, events, previews and reviews of major global trade shows, product launches and security installations worldwide.

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

