SECURITY SOLUTIONS TODAY

SURVEILLANCE REIMAGINED

IN THIS ISSUE

In The News
Neurotechnology
Wins UIDAI
Biometrics SDK
Benchmarking
Challenge 2025 **| 06**

In The News
12 | Suprema's
BioStation 3
Achieves Record
Global Sales
and Industry
Recognition in
2025

In The News
Hong Kong
to Host 2026 **| 17**
INTERPOL
General
Assembly

CONTACT

JAN – MAR 2026

SECURITY SOLUTIONS TODAY

SURVEILLANCE REIMAGINED

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

NEUROTECHNOLOGY ACHIEVES ISO/IEC 30107-3 LEVEL 2 COMPLIANCE FOR ADVANCED FACE LIVENESS DETECTION

VILNIUS, Lithuania —Neurotechnology, a provider of deep learning–based biometric identification solutions, announced today that its face liveness detection technology has successfully passed a Level 2 (Level B) Presentation Attack Detection (PAD) evaluation, confirming compliance with the ISO/IEC 30107-3 international standard.

The independent assessment verifies that upcoming releases of MegaMatcher SDK and MegaMatcher ID demonstrate strong resilience against sophisticated biometric spoofing attacks, reinforcing their suitability for high-security and large-scale identity verification applications.

Presentation Attack Detection is a critical component of biometric systems, designed to distinguish between biometric data captured from a live individual and attempts using fraudulent artifacts. While Level 1 testing addresses basic attacks such as printed photographs or digital displays, Level 2 (Level B) evaluations assess resistance against advanced spoofing methods, including:

· 2D paper masks with cutouts
· Curved and 3D surface projections
· Shallow fakes and balaclava masks

"With the increasing adoption of facial biometrics in high-risk applications such as banking, digital onboarding, and automated identity verification, spoofing techniques continue to grow in sophistication," said Mantas Kundrotas, Liveness Project Lead at Neurotechnology. "Achieving ISO Level 2 compliance validates our commitment to staying ahead of these evolving threats and enables our customers to deploy biometric solutions with confidence without compromising user convenience."

The evaluation was conducted by BixeLab, an NVLAP-accredited biometric testing laboratory (NVLAP Lab Code: 600301-0). According to the test report, Neurotechnology's PAD algorithms successfully blocked the majority of advanced presentation attacks while maintaining a low False Rejection Rate (FRR) for legitimate users.

About MegaMatcher SDK and MegaMatcher ID

MegaMatcher SDK is a comprehensive multi-biometric software development kit designed for building large-scale and multimodal identification systems, supporting face, fingerprint, voice, and iris recognition. MegaMatcher

Image by Freepik

ID is a dedicated solution for streamlined digital identity management and authentication.

ISO/IEC 30107-3 Level 2 compliance confirms that both solutions meet the stringent requirements of high-security environments, including financial services, digital identity programs, and fraud-sensitive onboarding processes.

About Neurotechnology

Founded in 1990 and headquartered in Vilnius, Lithuania, Neurotechnology develops high-precision biometric algorithms and AI-powered software based on deep neural networks. Its technologies are deployed in more than 140 countries and support national-scale initiatives such as identity programs, elections, law enforcement, and border control. Notable implementations include India's Aadhaar program, national elections in Ghana and Liberia, and voter de-duplication initiatives in the Democratic Republic of the Congo collectively processing biometric data for nearly two billion people worldwide. ∎

THE SECRET LIFE OF PARKED DOMAINS: THE INTERNET'S FORGOTTEN REAL ESTATE IS NOW A PRESSING THREAT

Singapore, December 22, 2025 – New research from Infoblox Threat Intel reveals that parked domains, once widely considered harmless advertising pages, have become a significant and largely overlooked cybersecurity threat.

According to large-scale experiments conducted by Infoblox Threat Intel, more than 90 percent of visits to parked domains now redirect users to malicious destinations, including scams, scareware, illegal content, or malware. This marks a significant reversal from the risk profile observed a decade ago.

The research identifies abuse of so-called direct search or zero-click advertising systems as a key driver of this shift. Instead of displaying a simple advertising page, parked domains now frequently redirect visitors automatically to advertiser-selected websites, often without any user interaction or warning. In many cases, these destinations are controlled by malicious actors.

The findings also indicate that fraud protection mechanisms used by major domain parking platforms can unintentionally help cybercriminals conceal their activity from the security community. In addition, recent policy changes by Google appear to have further increased risk exposure for users.

Image by Freepik

> "A decade ago, research showed that parked domains were mostly harmless and rarely more than digital clutter. Today, our research shows they have become almost exclusively malicious. What was once internet background noise is now a largely unrecognized, persistent, and pervasive threat."
> – Dr. Renée Burton, Vice President, Infoblox Threat Intel.

Key Findings

- Direct search is a highly abused mechanism that sends users who visit a parked domain directly to advertising content.
- In many cases, these advertisers deliver scams or malware.
- The research identifies three major domain portfolio holders, often referred to as domainers, that use advanced techniques such as visitor profiling, lookalike domains, typo-based email collection, and advanced DNS tactics including Fast Flux.
- These actors selectively route users either to benign ad pages or directly to high-risk websites, targeting different brands and audiences.
- The complexity of the parked domain ecosystem makes abuse reporting extremely difficult.

The research highlights how a combination of advertising systems, automated redirection, and DNS-level manipulation has transformed parked domains into a persistent security threat that remains largely invisible to users and difficult for defenders to address. ∎

Vector by Freepik

Altronix®

RACK MOUNT　　　　HARDENED OUTDOOR　　　　WALL MOUNT

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™

NEUROTECHNOLOGY WINS UIDAI BIOMETRICS SDK BENCHMARKING CHALLENGE 2025

Neurotechnology secures first place for fingerprint matching performance in UIDAI's global benchmarking challenge Neurotechnology, a provider of deep learning based solutions and high precision biometric identification technologies, today announced that its fingerprint matching algorithm has been ranked first in the UIDAI Biometrics SDK Benchmarking Challenge 2025, organized by the Unique Identification Authority of India.

The benchmarking challenge invited global technology providers and research institutions to submit 1:1 fingerprint matching solutions to evaluate performance under real world conditions. The evaluation was designed to replicate the Aadhaar ID renewal process for children, measuring how accurately fingerprint verification systems perform over extended periods as children grow.

Neurotechnology's solution achieved the highest performance results among all participants, demonstrating strong accuracy and long term stability. Neurotechnology, in consortium with Tata Consultancy

"We are proud to be ranked first by the UIDAI for our fingerprint verification algorithm. This recognition reflects our commitment to providing industry leading biometric solutions. We are grateful for this acknowledgement and look forward to new evaluations and challenges."
– Evaldas Borcovas, Head of Biometrics Research at Neurotechnology.

Image by Freepik

Services (TCS), is one of three biometric providers supporting India's Aadhaar ID program. The company's Automated Biometric Identification System (ABIS) currently manages more than 1.8 billion identities, using fingerprint, face, and iris biometric modalities. The system is designed to support national scale identity programs by processing, searching, and matching large volumes of biometric data efficiently and securely.

UIDAI Biometrics SDK Benchmarking Challenge 2025

The UIDAI launched the Biometrics SDK Benchmarking Challenge 2025 to identify high performing fingerprint verification technologies for large scale identity systems. The challenge attracted 2,106 applications globally and placed strong emphasis on the long term reliability of biometric matching solutions.

A key component of the evaluation was a unique long term dataset of children aged 5 to 10 years, with a 5 to 10 year gap between fingerprint samples. This dataset was used to assess age invariance and determine how well fingerprint verification

systems maintain accuracy over time.

The results of the challenge highlight the importance of stable and reliable biometric technologies for national digital identity programs such as Aadhaar.

About Neurotechnology

Founded in 1990 in Vilnius, Lithuania, Neurotechnology develops high precision algorithms and software based on deep neural networks and artificial intelligence technologies. The company's expertise spans biometric person identification, computer vision, natural language processing, and AI driven systems.

Neurotechnology's solutions are used in more than 140 countries and support numerous national scale projects, including national ID systems, passports, elections, law enforcement, and border control initiatives. Notable deployments include India's Aadhaar program, general elections in Ghana and Liberia, voter de-duplication for the Democratic Republic of the Congo, and other projects that collectively process biometric data for nearly two billion people worldwide. ∎

ZBETA APPOINTS LEARNING AND DEVELOPMENT EXPERT TO SHAPE THE FUTURE OF TALENT DEVELOPMENT

San Francisco– ZBeta, a pioneer in delivering comprehensive physical security consulting services, today announced the appointment of Jim McCormack as Learning and Development Manager. In this role, McCormack will focus on strengthening the company's commitment to learning, technical excellence, and collaboration across the organization.

McCormack will lead and oversee ZBeta's learning and development initiatives, including onboarding, career growth, and internal knowledge sharing. His work will center on building scalable programs that help new hires quickly become effective, support continuous professional development, and deepen expertise across all teams. "At ZBeta, our greatest asset is the collective knowledge and drive of our people," said Anna Yates, Vice President of Talent and Culture at ZBeta. "Jim's approach to learning and development will further strengthen our foundation and help us continue to set new standards for client

Image by Freepik

service and performance, while reinforcing ZBeta's ongoing commitment to both our people and our clients."

Investing in people and growth is central to ZBeta's mission. McCormack's appointment builds on this commitment and sharpens the company's focus on developing talent and

driving operational excellence. By fostering a culture of continuous learning, ZBeta continues to redefine modern consulting as forward thinking, collaborative, and focused on exceeding client expectations.

A strategic and results driven leader, McCormack brings more than 13 years of experience designing, implementing, and evolving learning, training, and quality programs across global organizations. His expertise spans the full learning lifecycle, including curriculum design, global learning management system implementation, leadership development, and embedding Diversity, Equity, and Inclusion principles into organizational cultures.

Prior to joining ZBeta, McCormack served as Global Learning and Development Lead for SMB at Accenture, where he managed teams across six global locations and implemented standardized learning assets to support collaboration and performance excellence.

He previously held senior training leadership roles at Indeed.com, where he led financial operations training strategy. McCormack is also the founder of RKW Training, a consultancy specializing in onboarding, management development, and learning strategy design.

"ZBeta's focus on people and its culture of continuous learning and collaboration aligns perfectly with my passion for building educational and training ecosystems that empower organizations to grow and thrive," said McCormack. "By focusing on capability building and knowledge sharing, we can elevate how our teams deliver for clients and for one another."

About ZBeta

ZBeta is a world class physical security design and managed services firm supporting some of the most dynamic and high profile organizations and individuals in the world. The company applies a data driven, technology led, and human centered approach to help clients architect and engineer superior physical security solutions, implement them seamlessly, and operate them at peak efficiency.

ZBeta supports projects ranging from new corporate campuses and data center mega campuses to future ready technology roadmaps and internal team augmentation. The company operates at scale, moves at the pace of today's projects, represents client programs as its own, and delivers where others cannot. **Learn more at ZBeta.com.** ∎

NEUROTECHNOLOGY SETS INDUSTRY BENCHMARK IN BIOMETRIC SECURITY WITH FACE LIVENESS DETECTION AND FINGERPRINT ACCURACY

Vilnius, Lithuania – Neurotechnology, a leader in deep learning–based biometric solutions, today announced two major achievements demonstrating its continued leadership in high–precision identification technologies.

The company's face liveness detection technology has successfully passed a rigorous Level 2 (Level B) Presentation Attack Detection (PAD) evaluation, confirming compliance with the ISO/IEC 30107–3 standard. The evaluation, conducted by BixeLab, an NVLAP–accredited biometric testing laboratory, assessed the system's resilience against advanced spoofing techniques, including 2D paper masks, 3D surface projections, shallow fakes, and balaclava masks. The results confirm that Neurotechnology's upcoming MegaMatcher SDK and

Image by Freepik

MegaMatcher ID solutions provide high security for critical applications such as digital onboarding, financial services, and automated identity verification.

In addition, Neurotechnology achieved first place in the National Institute of Standards and Technology (NIST) FRIF TE E1N evaluation for one–to–many fingerprint identification.

HOTEL & SHOP PLUS
Shanghai

China's Leading Trade Show for Hospitality Construction and Operation

Hotel and Shop Plus

31 MARCH - 3 APRIL 2026 | SNIEC, Shanghai

Organizer **sinoexpo**
informa markets

Discover
hotel security solutions
at Hall E6.

Contact us: jade.liao@imsinoexpo.com
Explore more: www.expohsp.com

Follow Us On

#HotelandShopPlus

Visitor Free Registration

The company's fingerprint algorithm demonstrated top-tier accuracy across all testing categories, including single-finger, multi-finger, and full ten-finger operational scenarios. The evaluation highlights the robustness and suitability of Neurotechnology's solutions for demanding law enforcement and national-scale identity programs.

"These recognitions underscore our commitment to developing cutting-edge biometric technologies that combine security, reliability, and user convenience," said Evaldas Borcovas, Head of Biometrics Research at Neurotechnology. "From advanced fingerprint algorithms to next-generation face liveness detection, our solutions are designed to meet the highest international standards and withstand sophisticated spoofing attempts."

About MegaMatcher SDK and MegaMatcher ID

MegaMatcher SDK is a comprehensive multi-biometric software development kit for large-scale and multi-modal face, fingerprint, voice, and iris identification systems. MegaMatcher ID is designed for streamlined digital identity management and authentication.

Both solutions are suitable for high-security applications where protection against advanced fraud techniques is essential.

About Neurotechnology

Founded in 1990 in Vilnius, Lithuania, Neurotechnology develops high-precision algorithms and software based on deep neural networks and AI technologies. Its solutions are deployed in over 140 countries and national-scale projects, including passports, elections, law enforcement, and border control, processing nearly two billion biometric records worldwide. ∎

DATA BREACHES HIGHLIGHT THE CRITICAL ROLE OF ZERO TRUST AND PRIVILEGED ACCESS CONTROLS

By Darren Guccione, CEO & Co-founder, Keeper Security

Healthcare data is among the most sensitive forms of information. It must be accessible precisely when and where care is delivered, which makes securing it especially complex. This same requirement also makes healthcare data a highly attractive target for cybercriminals. When patient information is exposed, the consequences extend far beyond a single system or platform, directly affecting individual privacy and eroding trust in the healthcare services people depend on.

As digital health platforms continue to scale, access expands rapidly across users, systems, and third-party partners, often faster than security controls are reassessed. Over time, this creates access pathways that are broader, more persistent, or less visible than originally intended. In many major data breaches, the root cause is not a single technical failure, but access that lasted longer, extended further, or was more difficult to monitor than it should have been.

Image by Freepik

This is where zero-trust architecture and privileged access controls play a critical role. In complex healthcare environments, elevated access is unavoidable, but it must be intentional, tightly governed, and fully visible. When privileged access is distributed across disconnected systems, organizations struggle to understand who has access to what, or to identify when access conditions change. Managing privileged access through a modern, unified platform provides clearer visibility, stronger control, and a greater ability to contain incidents before they escalate.

While investigations can help explain how a breach occurred, they do not prevent future incidents on their own. What matters is whether organizations use these events as an opportunity to reassess how access is managed in practice and whether protections evolve alongside the systems they are designed to secure. At the same time, individuals should recognize that no system is immune and take advantage of tools such as dark web monitoring services like BreachWatch, which alert users when personal information appears in known data breaches.

Trust in digital healthcare is fragile. Preserving it requires continuous attention and clear accountability around who can access sensitive data and why. Security is effective only when it is actively maintained, not assumed. ∎

MTX (Milipol TechX) 2026

28 - 30 April 2026
Sands Expo & Convention Centre, Singapore

Supercharging Innovation for Our Safer Tomorrow

REGISTER FOR YOUR FREE VISITOR PASS

www.mtx.sg

SUPREMA'S BIOSTATION 3 ACHIEVES RECORD GLOBAL SALES AND INDUSTRY RECOGNITION IN 2025

Seoul, Korea – Suprema, a global leader in AI-powered security solutions, today announced that its flagship biometric device, BioStation 3, is on track to set a new annual global sales record by the end of 2025. This milestone represents Suprema's highest annual sales for its biometric solutions and highlights the growing international demand for advanced facial authentication technology.

The growth reflects sustained momentum across multiple regions, including the United Kingdom, the Americas, Japan, and the Middle East, rather than a temporary spike in a single market. Deployments of 600 to over 1,000 units at high-security sites, such as public institutions, financial organizations, and large-scale residential complexes, have further reinforced BioStation 3's position as a leading solution in the global security market.

Key Drivers of BioStation 3's Global Competitiveness

1. AI-Powered Facial Authentication – BioStation 3 delivers high accuracy and stable performance, ensuring seamless access control for administrators and end users across real-world environments.
2. Optimized User Experience – Designed for diverse and complex operating conditions, BioStation 3 enhances both security and convenience in daily operations.
3. Robust Data Protection – The device complies with GDPR and successfully passed iBeta's ISO/IEC 30107-3 Presentation Attack Detection (PAD) test, safeguarding against facial spoofing. Suprema's Template on Mobile

(ToM) technology allows users to securely manage their own data, strengthening trust in markets with strict regulatory requirements, including the United States and the United Kingdom.

The device's innovation and reliability have been recognized by the security industry. BioStation 3 was awarded Best Product in the Biometrics category at the 2025 Readers' Choice Awards, hosted by Security Buyer magazine, a leading global publication covering emerging trends and technologies in security.

"The record-breaking sales and international recognition of BioStation 3 highlight the growing adoption of AI-powered facial authentication in the global security market," said Hanchul Kim, CEO of Suprema Inc. "It is especially significant that major clients with stringent security requirements trust BioStation 3 for real-world deployments. Suprema will continue to drive innovation, ensuring that security and convenience evolve hand-in-hand."

About Suprema Inc.

Suprema is a global leader in biometric and security solutions, specializing in AI-powered access control, time and attendance, and identity management systems. With a strong focus on innovation, data protection, and user-centric design, Suprema delivers solutions that meet the highest standards of security and privacy across international markets. ■

Image by Freepik

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

3 SHOWS
39,720 SQM
45,000 VISITORS

secutech

22 - 24 April 2026
Taipei, Taiwan

500 Exhibiting Brands
15,120 Sqm
15,000 Visitors

Concurrent with

fire & safety
presented by Secutech

SMAbuilding
presented by Secutech

Download
Info Pack

www.secutech.com

secutech⁺
VIETNAM
AI, IOT & ICT FOR SMART SOLUTIONS

9 - 12 September 2026
Hanoi, Vietnam

480 Exhibiting Brands
13,000 Sqm
17,000 Visitors

Concurrent with

fire & safety
presented by Secutech Vietnam

SMAbuilding
presented by Secutech Vietnam

Download
Info Pack

www.secutechvietnam.com

secutech
THAILAND

18 - 20 November 2026
Bangkok, Thailand

400 Exhibiting Brands
11,600 Sqm
13,000 Visitors

Concurrent with

fire & safety
presented by Secutech Thailand

Thailand Smart City Expo

Download
Info Pack

www.secutechthailand.com

CONTACT US

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

messe frankfurt

DETECTION TECHNOLOGY CELEBRATES THE OFFICIAL OPENING OF ITS NEW INDIA SITE

Espoo, Finland, 9 December 2025, 13:00 EET – Detection Technology Plc, a global leader in X-ray detector solutions, today marked a significant milestone in its global growth journey with the official opening of its new service and production facility in the greater Delhi area of India.

The inauguration ceremony was attended by the Ambassador of Finland to India, Mr. Kimmo Lähdevirta, alongside company representatives and invited guests.

The establishment of the India site strengthens Detection Technology's presence in one of the world's fastest-growing markets. The investment brings operations closer to customers, enabling locally delivered services, shorter lead times, and more cost-effective solutions, while maintaining the company's established quality standards.

"We see significant long-term potential in India, and this new facility enables us to support customers locally with the same dedication that guides our global operations," said Hannu Martola, President and CEO of Detection Technology.

"India is positioned for major advancements in infrastructure development, particularly in healthcare, the movement of people and goods through airports, seaports, rail stations, and border points, as well as in manufacturing

inspection. We intend to play an active role in supporting these developments through our expertise in X-ray technologies. Our comprehensive portfolio of modular detector building blocks is now also produced under the Made in India label, which is an important milestone for us."

Arve Lukander, President of EMEIA and Americas Business Units, added that shipments of Made in India products will begin immediately. During the initial operational phase, the site will focus on end assembly and final testing of detector boards designed for security X-ray imaging. The roadmap includes a rapid scale-up to incorporate the assembly of TFT flat panel detectors to support India's industrial and medical imaging requirements.

Lukander also highlighted the site's technical capabilities, noting that Detection Technology has invested in advanced equipment and built a skilled local team. In addition to production, the facility will host product demonstrations to support customers in selecting detectors suited to their imaging applications.

Located at Cyberwalk Tech Park in the greater Delhi area, the site benefits from strong connectivity across India and international markets. Operations in India are conducted through the company's fully owned subsidiary, DT Detection Technology India Private Ltd. ∎

SUPREMA'S BIOSTATION 3 SETS NEW GLOBAL SALES RECORD, HIGHLIGHTING RAPID GROWTH IN AI-POWERED FACIAL AUTHENTICATION

Seoul, South Korea – Suprema, a global leader in AI-powered security solutions, today announced that its flagship facial authentication device, BioStation 3, is on track to achieve the highest annual global sales record in the company's biometric device portfolio by the end of 2025. This milestone reflects accelerating global demand for facial authentication technologies across regulated and high-security environments.
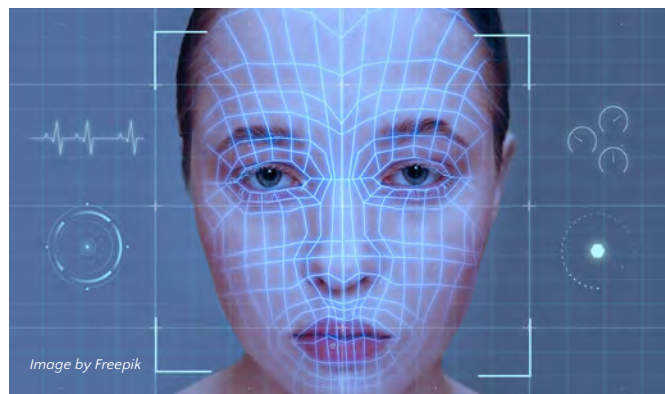
Unlike growth driven by a single-region surge, BioStation 3's performance demonstrates balanced, sustained momentum across multiple global markets. The solution has recorded over 30% year-over-year sales growth in key regions including the United Kingdom, the Americas, Japan, and the Middle East. Large-scale deployments—ranging from 600 to more than 1,000 units have been completed at high-security sites such as public institutions, financial organizations, and large residential complexes, further reinforcing its position in the global security market.

Key Drivers of Global Competitiveness

BioStation 3's expanding adoption is underpinned by three core strengths:

1. **AI-Powered Facial** Authentication Accuracy BioStation 3 delivers high-precision facial authentication with stable performance in real-world environments, supporting secure and seamless access control across diverse operational conditions.

2. **Optimized User Experience for Real-World Operations**
   Designed for complex and varied security settings, the device enhances both convenience and reliability, ensuring consistent performance even in demanding environments.

3. **Robust Data Protection and Privacy Compliance**
   BioStation 3 complies with GDPR, one of the world's most stringent data protection regulations, and has successfully passed iBeta's ISO/IEC 30107-3 Presentation Attack Detection (PAD) testing for facial spoofing. The solution incorporates advanced encryption technologies and Suprema's Template on Mobile (ToM) authentication method, enabling users to directly manage their own biometric data.

These data protection and privacy capabilities have contributed to strong adoption in markets such as the United States and the United Kingdom, where regulatory

Image by Freepik

scrutiny around facial authentication remains high. As a result, BioStation 3 is now being actively deployed in major projects, with broader cross-industry adoption expected in the coming year.

Industry Recognition

In addition to its commercial performance, BioStation 3 has received industry-wide recognition for its innovation and market impact. The device was awarded Best Product in the Biometrics category at the 2025 Readers' Choice Awards, hosted by Security Buyer magazine. The award is determined through voting by security professionals and recognizes products with proven innovation and real-world applicability.

Executive Perspective

"The record-breaking sales performance and global award recognition of BioStation 3 demonstrate how AI-powered facial authentication is rapidly establishing itself as a trusted security standard worldwide," said Hanchul Kim, CEO of Suprema Inc. "It is especially meaningful that international clients with stringent security and regulatory requirements have validated BioStation 3's accuracy and reliability through real-world deployments. Suprema will continue to drive innovation that strengthens security while enhancing convenience."

About Suprema

Suprema is a global leader in AI-based security solutions, specializing in biometric authentication, access control, and intelligent surveillance technologies. With a strong focus on innovation, privacy, and regulatory compliance, Suprema delivers advanced security solutions trusted by organizations worldwide. ∎

WORLD POLICE SUMMIT 2026 TO SHOWCASE AI, ADVANCED SECURITY TECHNOLOGIES, AND GLOBAL COLLABORATION

Dubai, UAE – Under the patronage of His Highness Sheikh Mohammed bin Rashid Al Maktoum, Vice President and Prime Minister of the UAE and Ruler of Dubai, the fifth edition of the World Police Summit will take place from 23–25 June 2026 at the Dubai World Trade Centre. Held under the theme Connected for Impact: Uniting Global Policing to Safeguard Future Generations, the Summit is set to bring together law enforcement agencies, INTERPOL, Europol, the United Nations, and top global experts to address the evolving challenges in security, digital policing, and AI-enabled crime prevention.

Colonel Dr. Rashid Hamdan Al Ghafri, Secretary-General of the World Police Summit, highlighted the Summit's growing importance as a platform for knowledge exchange and international collaboration: "The Summit represents a unique opportunity to showcase successful global policing models, explore advanced technologies, and build strategic partnerships that enhance the capabilities of police agencies worldwide.

The fifth edition will address emerging themes, including AI-assisted surveillance, digital crime response, crisis management, and the use of advanced technologies to protect communities and critical infrastructure." Khalid Al Hammadi, Executive Vice President of DXB LIVE, emphasized the Summit's role in reinforcing Dubai's reputation as a global hub for security innovation and policing expertise: "The World Police Summit highlights the UAE's leadership in hosting major international events and demonstrates the global community's commitment to advancing security technologies, AI applications, and best practices in policing. Through this platform, technology providers, law enforcement, and policy makers come together to explore innovative solutions for the challenges facing modern societies."

The Summit will feature high-level panel discussions, workshops, and exhibitions showcasing cutting-edge policing technologies, including AI-driven surveillance, cybersecurity solutions, and integrated command-and-control systems. Participants will have opportunities to engage with technology providers, collaborate on global security initiatives, and explore partnerships to strengthen policing effectiveness.

The previous edition of the Summit recorded participation from over 53,000 delegates across more than 110 countries, including Ministers of Interior, Police Chiefs, diplomats, and security specialists. It featured 140 panel sessions and facilitated 38 strategic partnerships between international security agencies, technology providers, and academic institutions. Building on this success, the 2026 edition aims to expand its focus on advanced technologies, AI-enabled law enforcement solutions, and global collaboration to address the rapidly evolving security landscape. ∎

Image by Freepik

HONG KONG TO HOST 2026 INTERPOL GENERAL ASSEMBLY

Hong Kong SAR will host the 94th INTERPOL General Assembly in 2026, marking a significant milestone for the city and reinforcing its role in global law enforcement cooperation. The event will bring police chiefs and senior security officials from INTERPOL's 196 member states to Hong Kong for high-level discussions on transnational crime and international security.

It will be the first time the INTERPOL General Assembly is held in the Hong Kong Special Administrative Region and the third time in China, following previous assemblies in Beijing in 1995 and 2017.

Image by Freepik

The announcement was formalised at the closing ceremony of the 93rd INTERPOL General Assembly in Morocco last November, where Vice Minister of Public Security of the People's Republic of China, Mr Xu Datong, presented the INTERPOL flag to Hong Kong Police Force (HKPF) Commissioner, Mr Chow Yat-ming, symbolising Hong Kong's role as the next host city.

"China has previously hosted the INTERPOL General Assembly in Beijing, and in 2026, Hong Kong, China will take on this important responsibility," Mr Xu said, underscoring the significance of the decision.

A Strategic Vote of Confidence

Commissioner Chow described the selection as a strong endorsement of both the Hong Kong SAR and the Hong Kong Police Force, highlighting the city's growing importance as an international law enforcement hub.

"Having attended multiple INTERPOL General Assemblies overseas, I never imagined that Hong Kong would one day host this prestigious event," Mr Chow said. "When our country proposed Hong Kong as the host, I felt deeply honoured."

He added that the General Assembly offers an opportunity to demonstrate Hong Kong's role as a global 'super connector', linking international policing efforts across regions while operating under the 'One Country, Two Systems' framework.

Hong Kong's Longstanding Role Within INTERPOL

Hong Kong has maintained a close and active relationship with INTERPOL for decades. The HKPF operates as a sub-bureau under China, contributing expertise in areas such as cybercrime, financial crime, and major transnational investigations.

HKPF officers are regularly seconded to INTERPOL's headquarters in Lyon, France, and the Global Complex for Innovation in Singapore. At present, three officers are serving in key roles one focusing on financial crime coordination in Lyon, and two supporting technology crime management initiatives in Singapore.

These international postings reflect Hong Kong's growing involvement in shaping global responses to emerging crime trends.

Expanding Regional and Global Collaboration

In parallel, the HKPF is refining its international engagement strategy, with increased focus on strengthening ties across ASEAN and Belt and Road Initiative jurisdictions. The aim is to improve coordination against increasingly complex forms of cross-border crime, particularly financial fraud.

A key development is FRONTIER+, a global intelligence-sharing platform launched in October 2024. Now connecting 13 jurisdictions, the platform enables real-time exchange of information and rapid interception of fraudulent funds moving across borders.

Ethics and Governance in Modern Policing

As policing becomes more data-driven and technologically complex, governance and ethics have taken on renewed importance. In November 2025, the HKPF hosted its first Ethics Governance Roundtable in Hong Kong, bringing together representatives from INTERPOL, the Independent Commission Against

Corruption (ICAC), and law enforcement agencies from multiple countries. INTERPOL's delegation was led by Mr Eugênio Ricas, Director of the Office of Internal Oversight. Discussions focused on ethics governance, integrity frameworks, and personal financial risk management for law enforcement leaders—reflecting the growing emphasis on accountability in international policing.

Preparations Underway

Commissioner Chow confirmed that preparations for the 2026 General Assembly are already progressing, with close coordination between the HKSAR Government, the HKPF, INTERPOL, and China's National Central Bureau. "Hosting the General Assembly is a top priority," he said. "We are

committed to ensuring a smooth and successful event." Beyond formal proceedings, Hong Kong aims to offer delegates a broader experience of the city its energy, hospitality, and culture.

"We want every delegation to have an unforgettable experience from the moment they arrive at Hong Kong International Airport," Mr Chow added.

About the INTERPOL General Assembly

The General Assembly is INTERPOL's highest governing body, convened annually to set strategic priorities, approve policies, and strengthen cooperation among member states in addressing global security challenges. ∎

KHON KAEN AIRPORT ENHANCES AIRSIDE SECURITY WITH NAVTECH ADVANCEGUARD

Oxfordshire, UK – Navtech Radar has delivered a new radar-based airside surveillance and detection solution at Khon Kaen Airport, one of the busiest aviation hubs in Thailand's Isan region. The installation supports the airport's ongoing programme to enhance operational safety and resilience as passenger traffic continues to increase.

Ranked among the top three airports in Thailand's Isan region, Khon Kaen Airport handles approximately 1.5 million passengers annually. The airport's expansive airside environment, combined with frequent changes in weather and visibility, posed challenges for conventional camera-based security systems, which struggled to provide consistent monitoring. Airport operators required a solution capable of delivering continuous, reliable detection regardless of lighting or weather conditions.
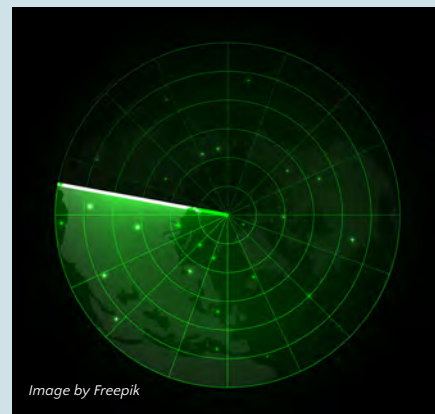
Working in collaboration with local technology consultant Chotipon Bunyarat, Navtech Radar deployed its AdvanceGuard wide-area surveillance solution. The installation includes two HDR311 radar sensors, providing full 360-degree detection

"For the cost, compared to the performance, Navtech Radar's solution can overwhelmingly win over other solutions" – *Chotipon Bunyarat.*

across the active airside.

AdvanceGuard's rules-based software continuously monitors all movement in real time and generates alerts whenever predefined security rules are breached. Integrated cameras are automatically directed to the point of interest, enabling immediate visual verification and supporting fast, informed operational responses.

The new system has strengthened Khon Kaen Airport's security capabilities while avoiding additional infrastructure complexity. With reliable, real-time, site-wide information accessible through a single interface, operators now benefit from a clear and consistent view of all airside activity. This enhanced situational awareness enables teams to respond quickly and confidently to unauthorised movement, improving both safety and operational efficiency.

Image by Freepik

About Navtech Radar

Navtech Radar is a global leader in high-definition radar solutions for critical infrastructure security. Its AdvanceGuard system delivers wide-area surveillance for complex environments, providing full situational awareness and improving operational efficiency. Navtech's technology is deployed worldwide across airports, ports, oil and gas facilities, and industrial sites. ∎

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.

Scan QR code below to read our news.
Sign up for free subscription.

Connect with us on social media!

f

in

Y

@securesolutionstoday   @tradelinkmedia   @tradelinkmedia

Surveillance Reimagined:
AI, Ethics, and the Future of Security

- *Modern surveillance is evolving from passive cameras to AI-driven systems that detect anomalies, predict risks, and respond faster across cities, airports, retail, and law enforcement.*
- *At the same time, ethics, privacy, and accountability are crucial, as facial recognition and behavioral analytics raise questions of bias, consent, and explainability.*
- *The future depends on edge AI, connected systems, and privacy-by-design, with public trust, transparency, and human oversight determining whether technology protects or intrudes.*

Surveillance is no longer just about cameras watching silently, it's evolving into a smart, proactive, and ethical system. Today, AI-driven analytics, facial recognition, and advanced data tools are transforming how we monitor cities, airports, and workplaces.

These technologies can detect unusual patterns, predict potential risks, and respond faster than ever before. But innovation brings challenges. Questions of privacy, bias, and data protection are central to this new landscape.

How can organizations harness AI for safety without compromising personal freedoms? This issue of Security Solutions Today explores how technology, ethics, and regulation converge to redefine surveillance.

Images by Freepik

AI Revolution in Surveillance

Globally, the AI in video surveillance market was valued at several billion dollars in the mid-2020s and is projected to grow explosively over the next decade. Depending on the analysis, market size forecasts range from roughly USD 6.5–7.0 billion today to between USD 28–58 billion by 2030-35, expanding at CAGRs of 16 %–24 % or more as organizations adopt AI for threat detection, facial recognition, and behavioral analytics.

AI-enhanced systems can process thousands of hours of footage in minutes, detect anomalies with far greater speed and accuracy than manual review, and reduce false alarms by significant percentages compared with traditional systems. Facial recognition algorithms in controlled settings have achieved high accuracy rates, and video analytics are rapidly becoming central to smart-city and enterprise security solutions.

Challenges in Modern Surveillance

While AI and advanced analytics are revolutionizing surveillance, they also bring complex technical, ethical, and operational challenges that

Image by Freepik

organizations must address:

Data Overload:
Modern surveillance generates massive volumes of video, biometric, and behavioral data often thousands of hours of footage per day. Processing this data requires sophisticated AI algorithms, cloud infrastructure, and storage solutions. Without proper systems, critical events may be missed, and valuable insights remain buried in raw data.

Privacy and Consent Concerns:
Capturing personal information, from facial features to movement patterns, raises legal and societal questions. Citizens increasingly demand transparency on how their data is collected and used. Overreach, such as constant monitoring in public spaces, can erode trust and provoke public backlash.

Bias and Ethical Risks:
AI systems rely on historical datasets,

Sector	Use Case	AI Functionality
Airports	Passenger and baggage screening	Facial recognition, anomaly detection, predictive threat alerts
Smart Cities	Traffic monitoring & crowd management	Real-time video analytics, object and behavior detection
Retail	Theft prevention & customer flow	Behavioral analytics, anomaly detection, automated alerts
Industrial Sites	Perimeter security & safety compliance	Object tracking, intrusion detection, alerting
Law Enforcement	Public safety monitoring	Facial recognition, predictive policing models, automated alerts

Insight: These applications show how AI transforms surveillance from passive monitoring to proactive security, enabling faster response, smarter resource allocation, and predictive capabilities.

which may contain racial, gender, or socioeconomic biases. Misidentification in law enforcement or security contexts can lead to wrongful alerts, arrests, or discriminatory profiling, undermining fairness and accountability. Organizations must continuously audit algorithms to ensure equity and minimize harm. As one industry expert notes.

Cybersecurity Vulnerabilities:
Surveillance networks, especially those connected to the cloud, are high-value targets for cyberattacks. Breaches of sensitive biometric or behavioral data can lead to identity theft, espionage, or regulatory penalties. Strong encryption, access controls, and continuous monitoring are essential to protect both data and public trust.

Regulatory Compliance and Legal Risks:
Global privacy regulations, including GDPR, CCPA, BIPA, and emerging biometric laws, impose strict rules on data handling. Non-compliance can result in multi-million-dollar fines, lawsuits, and reputational damage, making governance as important as the technology itself.

Integration and Technical Limitations:
Many organizations operate legacy surveillance systems that do not easily integrate with AI analytics, IoT sensors, or predictive tools. Fragmented systems create blind spots, reduce efficiency, and limit the ability to act proactively.

Human Oversight and Accountability:
AI can automate detection, but human interpretation remains critical. Decisions such as whether to alert law enforcement, intervene in a public space, or investigate anomalies require context, judgment, and accountability. Overreliance on automation without human checks can erode transparency, fairness, and public confidence.

Emerging Technologies Shaping the Future of Surveillance

As traditional surveillance systems reach their limits, a new generation of technologies is redefining how security is delivered: faster, smarter, and more accountable.

Intelligence at the Edge
Rather than streaming raw footage to centralized servers, edge AI processes data directly at the camera. This dramatically reduces latency, cuts bandwidth costs, and strengthens privacy by minimizing unnecessary data movement. The result is instant detection of intrusions, unattended objects, and unsafe behavior essential for high-risk environments such as airports, transit networks, and industrial zones.

From Detection to Understanding
Surveillance has moved beyond motion alerts. Advanced video analytics now bring context awareness, enabling systems to interpret behavior instead of merely recording it. By distinguishing between routine activity and genuine threats, AI reduces false alarms and delivers more precise, decision-ready insights.

Rise of Connected Security Ecosystems
Modern surveillance no longer operates in isolation. Cameras are increasingly integrated into IoT-driven ecosystems, linked with access control, environmental sensors, alarms, and building management systems. In smart cities and large campuses, this connectivity enables automated, coordinated responses whether redirecting traffic, issuing alerts, or dispatching security teams in real time.

Eyes in the Sky
AI-powered drones are expanding surveillance beyond fixed infrastructure. Deployed for perimeter protection, large public events, and emergency response, autonomous aerial systems provide rapid, flexible coverage and situational awareness in locations where

static cameras cannot reach.

Designing for Privacy by Default
As scrutiny around surveillance grows, privacy-enhancing technologies are becoming standard. Features such as automated face blurring, data anonymization, encryption, and role-based access controls help organizations balance operational security with regulatory compliance and public trust.

Ethics, Accountability, and the Trust Deficit

As surveillance systems grow more intelligent, they also become more controversial. The power to identify faces, track movements, and predict behavior raises a fundamental question: who is being protected and at what cost?

Privacy in an Always-On World
AI-driven surveillance often relies on continuous data collection, blurring the line between safety and intrusion. Without clear limits on data retention, purpose, and access, surveillance risks becoming pervasive rather than protective. Public acceptance increasingly depends on transparency: what data is collected, how long it is stored, and who controls it.

Bias, Accuracy, and Algorithmic Fairness
Facial recognition and behavioral

analytics are only as reliable as the data used to train them. Studies have shown performance disparities across demographics, leading to concerns about misidentification and unequal enforcement. In high-stakes environments such as law enforcement and border control, even small error rates can have serious consequences.

Black Boxes to Explainable AI
Many AI surveillance systems operate as "black boxes," offering decisions without clear reasoning. This lack of explainability makes accountability difficult when systems fail or produce biased outcomes. Regulators and enterprises alike are now pushing for auditable, explainable AI models that can justify alerts, classifications, and predictions.

Regulation Catching Up with Innovation
Governments worldwide are racing to define guardrails for AI surveillance. Frameworks such as the EU AI Act, evolving data protection laws, and sector-specific guidelines are shaping how and where these technologies can be deployed. Compliance is no longer optional—it is becoming a core design requirement.

Trust as the New Security Metric
Ultimately, the effectiveness of surveillance depends on public trust. Systems that prioritize ethics, oversight, and proportional use are more likely to gain acceptance and deliver long-term value. The future of surveillance will not be defined by technology alone, but by how responsibly it is governed.

Designing Surveillance Systems People Can Trust

Solving today's surveillance challenges requires more than better algorithms—it demands a strategic shift in how systems are designed, governed, and deployed. Organizations must treat trust as

"Identity security needs to evolve so that every identity, whether human or machine, can be trusted to work together. Businesses that get this right will position themselves as standard-setters, turning a vulnerability into an advantage and giving their industries the foundation to thrive."

a core security outcome, not a byproduct.

At the technical level, this means embedding privacy-by-design into surveillance architectures. Edge processing, data minimization, encryption, and identity-based access controls should be default features, not optional add-ons. AI systems must be auditable, explainable, and continuously tested for bias and accuracy, particularly in high-risk environments such as law enforcement and border control.

Equally important is human oversight. Clear escalation protocols, documented decision-making, and accountable operators ensure AI augments judgment rather than replaces it. Finally, transparent communication with regulators and the public through policies, disclosures, and independent audits helps bridge the trust gap. ∎

COMING SOON

JAN 12 – 14 2026	**Intersec 2026** 📍 Dubai, UAE 🌐 https://intersec.ae.messefrankfurt.com/dubai/en.html
FEB 4 – 5 2026	**Cybersec Asia 2026** 📍 Bangkok, Thailand 🌐 https://cybersec-asia.net/
MAR 18 – 20 2026	**SECON 2026** 📍 KINTEX, South Korea 🌐 www.seconexpo.com
MAR 3 – 6 2026	**Security Show 2026** 📍 Tokyo, Japan 🌐 https://messe.nikkei.co.jp/
MAR 25 – 27 2026	**ISC West 2026** 📍 Las Vegas, USA 🌐 https://www.discoverisc.com/west/en-us.html
MAR/APR 31 Mar – 3 Apr 2026	**Hotel & Shop Plus 2025** *(Page 9)* 📍 SNIEC, Shanghai 🌐 www.expohsp.com
APR 28 – 30 2026	**Milipol Asia Pacific 2026** *(Page 11)* 📍 Singapore 🌐 https://www.mtx.sg/
APR 22 – 24 2026	**Secutech International 2026** *(Page 13)* 📍 Taipei, Taiwan 🌐 https://secutech.tw.messefrankfurt.com/taipei/en.html
MAY 7 – 9 2026	**Intersec Shanghai 2026** 📍 Shanghai, China 🌐 https://intersec-shanghai.hk.messefrankfurt.com/shanghai/en.html
MAY 19 – 21 2026	**ISNR 2026** 📍 Abu Dhabi, UAE 🌐 https://www.isnrabudhabi.com/
AUG 11 – 13 2026	**Indo Security & Forum 2026** 📍 Jakarta, Indonesia 🌐 https://indosecurity.com/
SEP 2 – 4 2026	**Security Exhibition 2026** 📍 Sydney, Australia 🌐 https://www.securityexpo.com.au/
SEP 9 – 12 2026	**Secutech Vietnam 2026** *(Page 13)* 📍 Hanoi, Vietnam 🌐 https://secutechvietnam.tw.messefrankfurt.com/hanoi/en.html
SEP 22 – 25 2026	**Security Essen 2026** 📍 Essen, Germany 🌐 www.security-essen.de

SUBSCRIPTION FORM

■ 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)