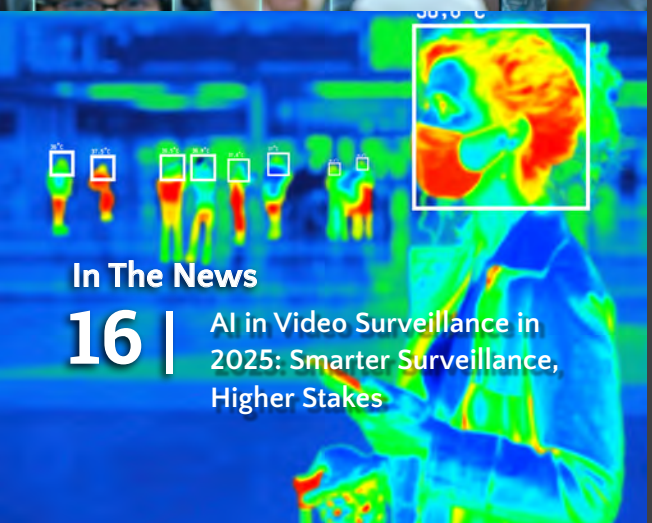
JUL – SEP 2025

SECURITY SOLUTIONS TODAY

ARTIFICIAL INTELLIGENCE IN VIDEO SURVEILLANCE AND ANALYSIS

IN THIS ISSUE



CONTACT

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

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

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

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

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

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

SECURITY SOLUTIONS TODAY
is published quarterly by Trade Link Media Pte Ltd (Co. Reg. No.: 199204277K)
1 Paya Lebar Link, #04-01, Paya Lebar Quarter 1 (PLQ 1), Singapore 408533
Tel: +65 6842 2580
ISSN 2345-7112 (E-periodical)

GLOBAL VIDEO SURVEILLANCE MARKET TO SURGE TO $204.5 BILLION BY 2032, DRIVEN BY AI AND SMART SECURITY INNOVATIONS

New York, NY – According to a new report published by Allied Market Research, the global video surveillance market is projected to grow from $61.8 billion in 2022 to a staggering $204.5 billion by 2032, registering a compound annual growth rate (CAGR) of 12.8% over the forecast period.

The report, titled "Video Surveillance Market by Component, Enterprise Size, System Type, Customer Type, and Application," highlights the critical role of artificial intelligence (AI), IoT integration, and cloud-based analytics in shaping the future of global surveillance infrastructure.

AI-Powered Security Driving the Next Generation of Surveillance

Modern video surveillance systems are evolving beyond passive monitoring, integrating AI-driven features such as real-time facial recognition, object tracking, anomaly detection, and behavioral analytics. These advancements are transforming security systems into intelligent, proactive tools capable of delivering operational insights across commercial, governmental, and critical infrastructure sectors.

"AI-enabled video analytics are redefining how organizations approach security—providing not just surveillance, but smart situational awareness," said a senior research analyst at Allied Market Research. "As global security concerns rise, this intelligence layer is becoming indispensable."

Key Market Drivers and Trends

- **Integration of IoT with surveillance cameras** is enabling smarter, connected ecosystems.
- **Demand for cloud-based video management systems (VMS)** is accelerating adoption across SMEs and large enterprises alike.
- **Asia-Pacific** is emerging as a dominant market, fueled by government initiatives and infrastructure modernization.

Challenges to Market Adoption

Despite the optimistic forecast, the market faces challenges, including high initial costs of cameras, storage, and analytics infrastructure. The need for skilled professionals for integration and maintenance also increases overall expenses.

These factors are particularly restrictive for smaller enterprises. Additionally, as technology evolves, frequent upgrades and long-term commitments add to financial pressures.

Market Segmentation Highlights

- **System Types:** Analog, IP, and hybrid surveillance
- **Components:** Hardware (camera, storage, accessories), software (video analytics, VMS), services
- **Applications:** Commercial, military & defense, infrastructure, residential
- **Customer Types:** B2B and B2C segments
- **Enterprise Size:** Small, medium, and large-scale organizations
- **Regions:** North America, Europe, Asia-Pacific, and LAMEA

Competitive Landscape

The report also features competitive analysis and profiles of key players such as:
Teledyne FLIR, Dahua Technology, Panasonic Corporation, Canon Inc., Motorola Solutions, Honeywell Commercial Security, Eagle Eye Networks, Verkada, and BCD International. These companies are investing heavily in product innovation, AI integration, and strategic acquisitions to gain market advantage.

About Allied Market Research

Allied Market Research (AMR) is a leading market intelligence firm providing business insights and consulting services across global markets. Thier reports deliver actionable data, deep industry analysis, and forecasted trends that enable organizations to stay competitive in dynamic industries. With a focus on emerging technologies and global transformation, AMR empowers decision-makers with evidence-based market strategies. ■

RETAIL REWIRED: HOW AI AND VIDEO ANALYTICS ARE TRANSFORMING STORE SECURITY AND STRATEGY

By Scott Thomas, National Director for Signature Brands, Sales at Genetec.

In an era where organized retail crime (ORC), inventory shrinkage, and staffing shortages have become persistent challenges, retailers are turning to artificial intelligence (AI) and intelligent automation (IA) to strengthen security and improve operational agility. More than just loss prevention tools, today's AI-enabled surveillance systems are helping businesses do more with less while elevating the customer experience along the way.

According to the 2025 Genetec State of Physical Security Report, 78% of retailers now use AI to trigger events of interest. From streamlining investigations to understanding shopper behavior, AI-powered solutions are redefining how physical stores operate.

From Surveillance to Smart Security

Retailers capture hundreds of hours of video per week, per location. But raw footage alone isn't enough. AI-enabled analytics allow security teams to automate alerting, filter false positives, and extract critical insights from massive volumes of data.

For instance, video systems can be trained to flag suspicious behavior of individuals loitering in high-value aisles. These alerts help store management proactively respond to potential threats without needing to monitor every camera at all times.

Beyond threat detection, AI-powered forensic tools now let investigators search recorded footage using natural language prompts like "man in blue shirt" or "red truck in the parking lot." What once took hours can now be achieved in minutes.

When paired with digital evidence management systems (DEMS), retailers can also securely share case files with law enforcement, speeding up investigations and prosecutions.

Coordinated Defense Against Organized Crime

As ORC becomes increasingly sophisticated, many retail chains are deploying license plate recognition (LPR) cameras across locations to build community-driven intelligence. When a suspicious vehicle is flagged at one store, the alert can instantly be shared across nearby stores,

Image by Freepik

continue on page 6

altronix.com


Image by Freepik

turning individual retailers into a networked defense system.

This shared visibility not only helps in preventing repeat offenses but also strengthens legal cases with consistent, multi-location evidence.

Beyond Security: Retail Insights that Drive Revenue

Today's AI surveillance tools also double as operational intelligence platforms. By layering video data with analytics like heat mapping and people counting, retailers can gain a clearer picture of customer flow, display effectiveness, and staffing needs.

- **Foot Traffic & Store Layouts:** One national coffee chain used video analytics to redesign store layouts, repositioning self-serve stations for better flow and accessibility.
- **Marketing & Promotions:** AI helps assess the success of campaigns by comparing traffic and conversion rates before, during, and after promotions, down to the day and hour.
- **Stocking & Cleanliness:** AI now has power alerts for restocking empty shelves or addressing cluttered aisles—improving both appearance and efficiency.
- **Queue Detection:** When checkout lines grow long, systems can trigger alerts for additional registers to be opened, helping prevent lost sales and improve customer satisfaction.

Intelligent Automation, Not Autopilot

While AI adds powerful capabilities, retailers must remember that technology should augment—


Image by Freepik

continue on page 7

not replace—human decision-making. This is where Intelligent Automation (IA) enters: a human-in-the-loop approach that combines AI with intuitive user design, rule-based logic, and transparent decision support.

With this framework, machines handle repetitive or data-heavy tasks while security professionals make the final calls, ensuring both efficiency and accountability.

Responsible AI Adoption: What to Look For

Adopting AI in retail security and operations requires careful planning.

Retailers should prioritize:
Privacy & Compliance: Ensure systems respect data protection laws and apply proper access controls.

Transparency & Accuracy: Choose vendors who test for bias and offer explainable AI outputs.

Future-Readiness: Embrace open-architecture platforms that support future integrations and evolving analytics capabilities.

The Bottom Line

AI and video analytics are no longer futuristic concepts; they're essential tools in modern retail strategy. From deterring theft to redesigning store layouts, these technologies deliver tangible ROI across security, efficiency, and customer satisfaction. Retailers who approach AI adoption thoughtfully and keep humans in the loop are best positioned to thrive in this new, intelligent era of physical commerce.

About the Author

Scott Thomas is the National Director of Sales for Signature Brands at Genetec, where he leads retail, financial, hospitality, gaming, and cannabis verticals in the U.S. With over 30 years in the physical security industry, Scott has helped shape security strategies for some of the world's most recognized brands. ■

WILDFIRE WATCH 2.0: HOW AI AND SATELLITE CAMERAS ARE REIMAGINING DISASTER DETECTION

UBCO, Rogers, and Pano AI join forces to deploy intelligent surveillance in B.C.'s wildfire zones.

In the parched hills and fire-prone forests of British Columbia, the future of wildfire surveillance is taking shape, and it's powered by artificial intelligence, 5G, and satellites.

In a pilot project led by UBC Okanagan (UBCO) in partnership with Rogers Communications and Pano AI, a network of AI-powered cameras and low-cost weather stations is being deployed to spot wildfires early, often before human observers can.

The system leverages SpaceX's Swarm low-bandwidth satellite service and Rogers' 5G network, allowing real-time detection and alerts — even in remote, infrastructure-starved regions.


Image by Freepik

"Early detection of wildfires is critical in preventing their spread to help protect communities and our forests."
– Sonia Kastner, CEO of Pano AI

Rethinking Risk: From Reactive to Real-Time

For decades, wildfire detection relied on lookout towers, citizen reports, and a patchwork of weather stations. While functional, these methods often lagged behind the fire itself. That lag can mean the difference between containment and catastrophe.

Now, UBCO researchers are augmenting the system with real-time AI surveillance.

"The way we model fire risk is traditionally based on weather station data," says Dr. Mathieu Bourbonnais, assistant professor in UBCO's Department of Earth, Environmental and Geographic Sciences and a former wildland firefighter.

"But we're moving toward a system where we can see and respond to fire as it starts, not hours later."

The pilot expands on Bourbonnais' earlier work developing low-cost weather stations capable of monitoring wind, humidity, and fuel conditions. These devices were deployed throughout the Okanagan, 80 units in total, but 14 were lost in the McDougall Creek wildfire in 2023. Remarkably, they continued transmitting data until the final seconds before burning.

AI That Sees Smoke Before It Spreads

What sets this project apart is its use of AI-equipped cameras capable of detecting smoke from as far as 20 kilometers away. These are not your average security cameras. Built with high-resolution optics and machine learning algorithms, they analyze live video feeds to identify the telltale signs of wildfire ignition — even when it's just a faint plume on the horizon.

Still, the tech is not without challenges.

"A fire doesn't often start out dramatically," Bourbonnais explains. "It might be a wisp of smoke that's easy to confuse with truck exhaust or morning fog. That's where the AI needs to be smart and where human oversight remains critical."

The AI cameras will initially be installed on wireless towers near Fort St. James, Smithers, and Chetwynd, extending surveillance reach into regions where ground-based detection systems are sparse.

Cloud, Space, and Safety

The pilot's backbone is its connectivity: SpaceX Swarm satellites provide low-bandwidth data transmission from isolated terrain, while Rogers' 5G network handles high-speed video from closer-in areas. Together, they enable live dashboards for first responders and forest managers, even from the edge of the fire zone.

It's part of a broader effort by Rogers to enhance emergency infrastructure. The company is also donating satellite

continue on page 10

YOUR PHYSICAL SECURITY IS NOW A CYBER RISK — ACT BEFORE IT'S TOO LATE.

Your cameras, access control systems, and facility sensors are now connected – and exposed. Most weren't built for today's threat landscape. That makes them ideal targets for cybercriminals.

The Cost of Inaction

- **Disruption & Downtime:** Doors don't open. Cameras go dark. Control systems freeze.
- **Ransom Demands:** Hijacked devices used to extort millions.
- **Privacy Violations:** Leaked access logs and video feeds = Lawsuits + Fines.
- **Reputational Fallout:** Clients and partners lose trust fast.

Disarm the Threat. Secure the Future.

Join the leaders building the region's most secure, AI-ready facilities.

Register now:
arcmediaglobal.com/datacenters

Trusted by DC CISOs & Facilities Leads

20% OFF FOR SST READERS
USE PROMO CODE **SST20**

BUILDING & OPERATING AI-READY DATA CENTERS ASIA-PACIFIC EXECUTIVE CONFERENCE 2025

UNLOCKING INNOVATION AND GROWTH TO SEIZE LEADERSHIP OF THE FUTURE

DEC. 3, 2025 · MANILA, PH

PART OF AI WEEK ASIA

CALL +63 2 8785 1977
EMAIL DATACENTERS@ARCMEDIAGLOBAL.COM
VISIT ARCMEDIAGLOBAL.COM/DATACENTERS

ORGANIZED BY
PROMOTED BY
OFFICIAL MEDIA PARTNERS
OFFICIAL TRADE ASSOCIATION PARTNER

"Communications are critical in search and rescue operations,". "This technology directly impacts the safety of everyone involved."
- Dwight Yochim, CEO of BCSRA

phones to the B.C. Search and Rescue Association (BCSRA), aiding more than 3,400 SAR personnel across the province.

A National Model in the Making?

While similar AI wildfire systems have already been adopted in California, this project marks one of Canada's first at-scale integrations of AI, satellite, and 5G for wildfire prevention.

"Climate change is a global issue that requires urgent action," said Tony Staffieri, CEO of Rogers. "Communities across the country are facing the effects of unprecedented wildfires. Technology like this is critical to future readiness."

The pilot could eventually scale across provincial and national borders, forming the basis for a climate-resilient AI surveillance grid, one that sees the first signs of disaster and empowers responders to act before flames take hold.

Watching the Watchers: The Ethics of AI in the Wild

The project also brings important lessons for any AI surveillance deployment — whether for wildfire detection, critical infrastructure, or public safety.

Accuracy, privacy, and human validation remain paramount. False positives — mistaking a tractor's exhaust for wildfire smoke could lead to unnecessary panic or wasted resources. But missed detections could be worse.

For Bourbonnais, it's about balance: "The AI doesn't replace people. It gives them better tools faster, smarter, and more scalable than anything we've had before."

Final Frame

As Canada confronts longer, hotter fire seasons, this project is more than a tech trial. It's a vision for a proactive, AI-powered public safety system, one that sees smoke on the horizon and sounds the alarm before it's too late.

With Pano AI's cameras, Rogers' infrastructure, and UBCO's research, the future of wildfire detection may no longer be a watchtower but a smart lens in the sky. ■

LIVEREACH AI AND BLUE EYE PARTNER TO DELIVER AI-POWERED AFTER-HOURS VIRTUAL GUARDING

The collaboration brings real-time deterrence and cloud-based monitoring to businesses seeking smarter, cost-effective nighttime security.

As businesses increasingly seek intelligent security solutions that work around the clock, LiveReach AI has announced a strategic partnership with Blue Eye to introduce after-hours virtual guarding. The joint offering, branded LiveReach RVM powered by Blue Eye, combines AI-driven detection with human-verified response, allowing organizations to proactively protect their sites during nights, weekends, and other off-hours.

LiveReach AI is recognized for its enterprise-grade video analytics, real-time alerts, and unified cloud video management platform. With the addition of Blue Eye's live monitoring capabilities, the solution goes beyond passive surveillance by providing active intervention that helps prevent incidents before they escalate.

According to LiveReach AI Co-Founder and CEO Abhi Jain, the partnership enables customers to extend their protection without added complexity. "Blue Eye gives us the ability to act on alerts in real time, helping prevent

Image by Freepik

continue on page 12

secutech

THAILAND

messe frankfurt NCC

5 - 7 Nov 2025 | QSNCC, Bangkok

400 Exhibitors | 11,600 Sqm | 14,000 Visitors

Ideal For

- Smart small city and city infrastructure
- IoT solution for commercial and high-end residential building
- Smart fire solution for industrial zones
- Disaster prevention and rescue

Unique Strengths

- Thailand is SEA's second largest economy with large scale investment in smart & safe city and EEC projects.
- The show is concurrent with the Thailand Smart City Expo and EdTex. This will allow the show to achieve maximum synergy between visitors.
- Opportunities to present your solutions to professionals across the industrial, commercial, residential, smart living, telecom, energy, mobility, healthcare, retail, environmental, and education sectors.

Concurrent shows

fire & safety presented by Secutech Thailand

Thailand Smart City Expo 2025

EdTeX THAILAND'S EDUCATION TECHNOLOGY EXPO

Download Show Info

Contact us

Ms. Michelle Chu +886 2 8729 1099 ext 768
Michelle.chu@taiwan.messefrankfurt.com

problems instead of just recording them," he said.

Real-Time Response, Not Just Recording

Unlike traditional security guards who are costly and limited in coverage or basic video verification systems that react only after an incident occurs, Blue Eye offers a proactive deterrence model. The system uses AI to detect activity during restricted hours. From there, trained professionals assess the situation, issue live voice warnings to intruders, and coordinate with law enforcement when a threat is verified. This human-in-the-loop process is designed to reduce false alarms, accelerate response, and enhance overall protection.

Steve Jackson, CEO of Blue Eye, emphasized that businesses today expect more than alerts. "Customers aren't looking for more notifications. They want fewer incidents, faster resolutions, and a solution that actually works when their properties are most vulnerable," he said.

Market Growth and Rapid Deployment

The partnership comes at a time when the remote video monitoring (RVM) market is experiencing rapid expansion. A Raymond James report from April 2025 highlights a 23% annual growth rate in the sector as more enterprises replace or supplement traditional guards and outdated alarm systems.

Deployment of LiveReach RVM can often be completed within a few days, with predictable pricing that covers detection, verification, deterrence, and full access to a secure reporting portal. Clients receive incident summaries, audio evidence, camera analytics, and site-level trend reports, enabling both security and strategic decision-making.

Tailored for High-Exposure Sites

The solution is especially well-suited to properties that face consistent after-hours exposure or risks. Common applications include:

- Construction sites
- Automotive dealerships
- Industrial yards
- Multifamily housing complexes
- Commercial real estate portfolios

For such sites, LiveReach RVM offers a reliable, scalable, and cost-effective alternative to 24/7 physical patrols. Jain noted that both companies are aligned in their goal of making enterprise-grade security more accessible. "Together, we are delivering the kind of real-time protection today's customers expect," he said.

About the Companies

LiveReach AI is a provider of cloud-based video security and analytics solutions, offering real-time alerts, AI-powered detection, and centralized video management to help enterprises protect people, property, and operations.More information: **www.livereach.ai.**

Blue Eye specializes in remote video monitoring and real-time deterrence through virtual guarding. Its approach blends AI detection with live human verification to reduce crime and improve situational awareness. More information: **www.goblueeye.com.** ■

SEEING SMARTER: OAKLEY AND META DEBUT AI-ENHANCED SMART GLASSES WITH 3K VIDEO

AI-Powered Eyewear Redefines Mobile Surveillance with 3K Video and Real-Time Visual Intelligence

Oakley's latest innovation doesn't just sharpen your vision—it augments it. In a headline-making collaboration with Meta, the performance eyewear brand has launched a new generation of smart glasses equipped with built-in Meta AI and a 3K front-facing camera. The result is a wearable device that straddles the line between consumer gadget and enterprise-grade visual intelligence. These aren't your average connected glasses. At the core of the Oakley Meta Smart Glasses is a real-time AI assistant, powered by Meta's conversational intelligence, capable of identifying objects, interpreting visual context, and responding to natural voice commands. It's the kind of always-on situational awareness that was once confined to science fiction and high-security environments.

From Vision Enhancement to Surveillance Capability

What makes this launch particularly notable for the security and surveillance industry is how

continue on page 13


Image by Freepik

seamlessly it fuses cutting-edge optics with intelligent analytics. The 3K camera embedded in the frame captures high-resolution video on demand, opening the door to advanced use cases in mobile surveillance, incident documentation, and even remote AI-driven forensics.

Unlike traditional CCTV or body-worn cameras, these smart glasses offer hands-free video intelligence ideal for professionals in security, first response, inspections, and frontline logistics. Real-time insights are no longer tethered to a control room or dashboard; they're delivered directly to the user's field of vision.

Wearable Intelligence at the Edge

The promise of AI at the edge, analyzed and acted upon in the moment, is what truly distinguishes this device. By layering intelligent video processing directly into a wearable form factor, Oakley and Meta are reshaping how we think about surveillance systems. This is not simply about recording what happened; it's about understanding what's happening right now.

While privacy and ethical considerations around wearables continue to evolve, there's no denying the potential impact of this technology. As environments grow more complex and risks more dynamic, the ability to carry AI-powered perception into the field is not just a luxury; it's fast becoming a strategic necessity.

A Glimpse Into the Future

For a device that looks deceptively simple, the Oakley Meta Glasses signal a turning point. They represent a shift from static infrastructure to mobile, intelligent endpoints, where surveillance, support, and situational intelligence converge in real time.

As AI-driven video continues to define the future of safety, operations, and security, this is one product that deserves to be on the radar of every forward-looking enterprise. ■

EDGE AI AT WORK: NEXCOM'S AIEDGE-X®310 POWERS THE NEXT GENERATION OF RETAIL SURVEILLANCE AND CUSTOMER INTELLIGENCE

As AI becomes more deeply embedded in real-world environments, edge computing is no longer a futuristic concept; it's a strategic necessity. In high-traffic spaces such as retail stores, malls, and commercial complexes, latency, bandwidth, and data privacy considerations render cloud-only AI surveillance models impractical. Enter the AIEdge-X®310 from NEXCOM: a high-performance edge AI platform purpose-built for real-time video analytics and intelligent decision-making at the source.

At the heart of the AIEdge-X310 is a robust architecture powered by Intel 12th to 14th Gen Core processors and up to an NVIDIA RTX 6000 Ada GPU. This powerhouse combination enables on-premise execution of deep learning models, delivering rapid inference for critical applications such as facial recognition, behavior analysis,


Image by Freepik

crowd detection, and loss prevention, all without the latency of cloud relay.

continue on page 14

Real-Time Insight, Where It Matters Most

Retailers are increasingly deploying AI for more than just security. With the AIEdge-X®310, stores can combine real-time video feeds with AI algorithms to track shopper movement, optimize store layouts, and respond instantly to anomalies such as theft or unattended items. By localizing processing, businesses gain the ability to analyze and respond to events in milliseconds, essential for situations where reaction time equals risk mitigation.

Security operators benefit from the system's ability to process multiple high-resolution video streams simultaneously, enabling advanced functions such as license plate recognition, virtual perimeter fencing, and the detection of suspicious behavior. These are all run at the edge, ensuring continuity of service even in limited or unreliable network conditions.

Built for Demanding Environments

What sets the AIEdge-X®310 apart is not just power, but its flexibility. It's equipped with multiple PCIe slots for expansion, supports high-bandwidth I/O, and is ruggedized for 24/7 deployment in demanding environments. Whether integrated into a security command center or tucked behind retail walls, the system is built to handle mission-critical AI workloads with minimal maintenance.

The Future of Surveillance Is Local and Intelligent

As the boundaries between physical security, customer experience, and operational intelligence continue to blur, the need for real-time, edge-based AI becomes clear. NEXCOM's AIEdge-X®310 addresses this need head-on, delivering performance, scalability, and precision in a single, deployable solution.

In a landscape where every second and every data point counts, this edge AI platform provides not just surveillance but actionable intelligence. For security professionals, retail strategists, and systems integrators alike, it's a glimpse into the future of intelligent, localized vision. ■

THE SILENT WATCHERS: HOW GEORGIA IS USING CAMERAS TO QUELL PROTEST

Each night in Tbilisi, a steady tide of demonstrators floods Rustaveli Avenue, protesting what they see as the steady erosion of democratic freedoms in Georgia. But while police batons and tear gas have largely retreated from view, a different form of control now looms over the crowds, one mounted high above, fixed to light poles and rooftops.

These aren't ordinary surveillance cameras. They rotate, zoom, and lock on individuals with unnerving precision. Protesters know them well. Many now arrive masked—not just to hide from view, but to shield their identities from lenses capable of tracking faces, reading body language, and picking out individuals from a sea of moving people.

Over the past six months, this quiet, technological clampdown has replaced street confrontations with something more calculating. The message is clear: the government is still watching, even if its presence feels invisible.

The Fine That Changed Everything

Medea Turashvili, a mother of two and a long-time human rights advocate, never imagined that standing on a public street could result in a ₾5,000 fine—nearly double Georgia's average monthly wage. Her offense? Appearing in a protest crowd that momentarily blocked a road.

"There were no police there to tell us to move," she says. "Just cameras. And a week later, a letter came with

continue on page 15

a photo of me and a fine that could wipe out my family's monthly budget."

She's not alone. Activists estimate thousands have received similar fines, often with no chance to contest them unless they initiate costly court appeals.

A New Kind of Enforcement

What makes this campaign different isn't just the size of the fines or the number of people penalized. It's how it's being done.

Officially, the Ministry of Internal Affairs hasn't confirmed the exact process. But the pattern is too consistent to ignore. Protesters are identified through overhead video stills—often taken from newly installed, high-definition cameras positioned strategically around key protest zones like Rustaveli Avenue.

Some of these cameras have the capability to follow individuals as they move, zoom in to capture the details of what someone is reading, or isolate people based on physical characteristics. Civil rights groups say this is a marked departure from Georgia's prior use of surveillance, which typically focused on vehicle plates or monitoring criminal suspects.

"What we're seeing is a shift," says Giorgi Davituri from the Institute for Development of Freedom of Information (IDFI). "Before, the state might have looked for a specific person. Now it's using surveillance to find out who you are—on a mass scale."

Surveillance Without Oversight

The legal foundations for this kind of surveillance are murky at best. Under Georgian law, collecting personal information—especially images used for identification—should require strong justification. But in practice, the state appears to be stretching the rules, using administrative fines as a way to sidestep due process.


Image by Freepik

Groups like the Georgian Young Lawyers' Association (GYLA) have documented numerous irregularities: people fined for simply standing on an already blocked road, footage being used without court approval, and cameras used to track not just public gatherings, but individual movements after protests have ended.

Worse, protest funds created to help pay fines have been frozen, and police have reportedly delivered notices to people's family homes late at night—an intimidation tactic that many say echoes the country's authoritarian past.

"This isn't about law enforcement," says Tamaz Kirtava from GYLA. "It's about sending a message: we see you, and we'll make you pay for speaking out."

An Imported Infrastructure of Control

Many of the most powerful surveillance tools now in use in Tbilisi were manufactured abroad, particularly by companies in China. Camera models recently installed around protest sites can distinguish facial expressions, detect physical traits, and capture sharp images from long distances.

While officials claim these systems are meant to ensure public safety, their deployment closely mirrors methods used in more repressive regimes—from tracking religious minorities in China to monitoring political dissidents in Russia.

"Technology isn't neutral," says Tina Khidasheli, a former Minister of Defense. "The decision to use these systems says something about the kind of country we're becoming. Especially when many of our democratic allies are banning the very same tools."

Where Protest Meets Resistance

Despite the pressure, protests in Tbilisi continue now well past their 180th day. Marchers wear carnival masks, surgical coverings, or simply keep their heads down. But many, like Luka, say the surveillance has only strengthened their resolve.

"I used to just attend quietly," he says. "But the moment they fined me, without warning, without explanation, I felt part of something bigger. They tried to scare me. Instead, they made me stay."

For many in Georgia, the fear is no longer of confrontation, but of being slowly pushed out of the public square one camera at a time. ■

AI IN VIDEO SURVEILLANCE IN 2025: SMARTER SURVEILLANCE, HIGHER STAKES

From threat detection to behavioral analysis, AI brings both power and controversy to modern surveillance.

By 2025, artificial intelligence is expected to have fundamentally reshaped the video surveillance landscape. Once reactive and manual, today's systems are predictive, autonomous, and deeply integrated into security infrastructure. AI now enables real-time threat detection, behavioral analysis, and multi-source data fusion, raising both operational capabilities and ethical concerns.

Key Applications and Capabilities

1. Behavioral Anomaly Detection
Advanced computer vision models analyze individual and group behavior to detect abnormal activities such as loitering, sudden directional changes, crowd formation, or object abandonment. These systems are used in transport hubs, stadiums, and urban centers to proactively flag incidents before escalation.

2. Facial Recognition and Re-Identification
AI now supports low-light, off-angle, and motion-tolerant facial recognition. It can track individuals across multiple cameras and locations using re-identification algorithms. These systems are widely deployed in airports, border control, and high-security zones.

3. Automated License Plate Recognition (ALPR)
AI-enhanced vehicle identification is used in law enforcement, smart traffic systems, and toll management. Improvements in motion blur handling and character recognition accuracy allow for vehicle tracking in real time, even at high speeds or in adverse weather.

4. Edge AI and Cloud Hybrid Processing
Modern surveillance cameras use on-device AI to process and filter data locally, reducing latency and minimizing bandwidth. Only relevant footage or alerts are transmitted to central servers for deeper analysis or archiving, making large-scale deployments more efficient.

Image by Freepik

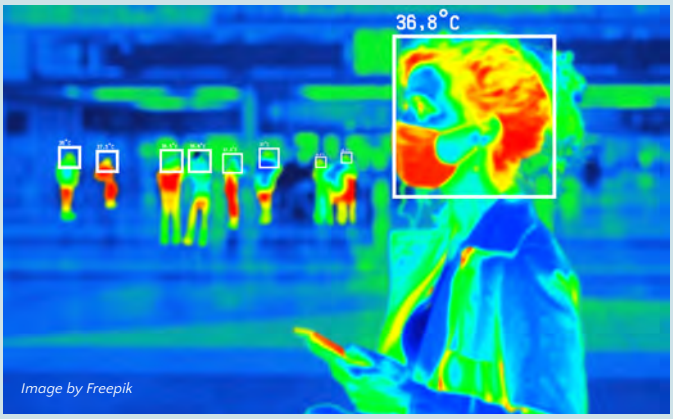


Image by Freepik

5. Multimodal Surveillance Systems
AI systems now fuse video with thermal imaging, acoustic sensors (e.g., gunshot detection), and chemical or radiation sensors. This layered approach enhances situational awareness, especially in critical infrastructure, defense installations, and public event security.

2025 Trends Shaping the Industry

Predictive Surveillance and Incident Forecasting
AI tools analyze historical video data, crime patterns, and environmental cues to predict potential security incidents. Used during large-scale events or political demonstrations, these systems help pre-position law enforcement or alert emergency services.

AI-Enabled Surveillance Drones
Autonomous drones equipped with AI perform routine perimeter scans, detect intrusions, and track moving targets across large properties. Widely adopted in logistics hubs, energy plants, and border zones, these systems offer aerial intelligence in real time.

Synthetic Data for AI Training
To reduce bias and improve accuracy, many AI models are trained on synthetic datasets that simulate extreme lighting, various ethnic profiles, crowd densities, and rare incidents. This helps overcome the limitations of real-world data scarcity.

continue on page 17

Emotion and Threat State Recognition
Some systems now attempt to identify potential aggression, fear, or panic by analyzing facial microexpressions and body language. While marketed for crowd safety and conflict prevention, these capabilities raise significant ethical and scientific concerns.

Challenges and Ethical Risks

Privacy and Mass Surveillance
With AI-powered cameras deployed across cities, concerns over privacy, consent, and data ownership have intensified. Critics argue that continuous biometric surveillance can lead to chilling effects on public assembly and freedom of movement.

Bias and Discrimination
Despite improvements in training data diversity, surveillance AI can still reflect or amplify societal biases, leading to disproportionate targeting or false positives, especially for marginalized groups.

Spoofing and Deepfake Evasion
Malicious actors now use deepfake technology to spoof faces, license plates, or voices. Surveillance systems are being hardened against such spoofing attacks using liveness detection and multi-modal verification methods.

Data Volume and Governance
With cameras generating terabytes of data daily, managing, storing, and securing this footage poses major challenges. Organizations must balance data retention needs with cybersecurity, compliance, and transparency obligations.

Future Outlook

AI in video surveillance will continue to expand in both capability and controversy. The push toward autonomous, predictive security must be balanced with robust governance frameworks, transparent AI models, and robust protections for civil liberties.

In high-stakes environments such as national borders, critical infrastructure, and large public gatherings, AI surveillance will remain indispensable. However, in civil society, its unchecked expansion may trigger legal challenges and public resistance. ■

CLOUDASTRUCTURE WINS "IMAGE PROCESSING SOLUTION OF THE YEAR" FOR REAL-TIME AI SECURITY

AI Breakthrough Awards Recognize Game-Changing Video Intelligence Platform from Cloudastructure

PALO ALTO, Calif. — June 25, 2025. Cloudastructure, a fast-rising force in AI-powered surveillance, has just been awarded the prestigious "Image Processing Solution of the Year" by the AI Breakthrough Awards 2025. The win highlights not only its cutting-edge threat detection technology but also its growing impact on real-world crime prevention.

A Proactive Approach to Crime Prevention

Unlike traditional forensic video review systems, Cloudastructure's solution is purpose-built for real-time security response. It combines high-speed image processing, AI-powered threat detection, and human-in-the-loop oversight, offering customers something rare in the security industry: actual deterrence. According to the company, their platform helped customers achieve a 98%+ deterrence rate against threatening activity in 2024.

> *"Our goal has always been simple—make AI useful in real-time, not just after the fact," said Abhik Sarkar, Director of Machine Learning. "This award is proof that we're on the right path."*

Powering AI at Scale — Without the Cloud Bloat

One of Cloudastructure's most impressive achievements is its complete control over the stack. Its bare-metal infrastructure avoids costly third-party cloud dependence, instead allowing the system to dynamically retrain models, scale inference workloads, and fine-tune GPU usage—all in-house.

- Processes over 300,000 videos per hour
- Achieves sub-500ms latency from input to alert
- Maintains ultra-high availability for the critical environment

In Sarkar's words, "We own every layer—from hardware to AI. That's how we deliver speed, accuracy, and cost-efficiency at scale."

Built for High-Stakes Environments

Cloudastructure's system is already

continue on page 18

gaining traction across multifamily housing, enterprise campuses, and remote industrial sites—locations where live deterrence, not just evidence, is essential.

With features like:

- **Modular architecture** that grows with client needs
- **Continuous AI improvement** with every deployment
- **Low TCO** (Total Cost of Ownership), reducing operational spend by up to 75%

...it's no surprise the company is being seen as a serious competitor to traditional surveillance giants.

Leadership That Delivers

CEO James McCormick summed up the company's vision with clarity:

> *"AI should do more than analyze—it should act. That's what we've built. A platform that protects real people, in real time."*
> ***- James McCormick***

About the Award

The AI Breakthrough Awards, part of Tech Breakthrough, spotlight leaders in AI, machine learning, computer vision, and more. Winners are selected by an expert judging panel based on innovation, performance, and real-world impact.

About Cloudastructure

Headquartered in Palo Alto, Cloudastructure delivers an advanced cloud-based security platform that pairs video surveillance, AI/ML analytics, and remote guarding in a single, scalable solution. Its contract-free model, 24/7 support, and focus on measurable outcomes make it an increasingly popular choice for enterprises seeking proactive security. ■

VERITONE'S 'TRACK' LETS LAW ENFORCEMENT FOLLOW YOU—WITHOUT FACIAL RECOGNITION

New AI tool tracks people using physical traits, sidestepping facial recognition laws.

As facial recognition bans spread, a new AI surveillance tool raises fresh questions about privacy and accountability.

With facial recognition facing legal pushback across the United States, law enforcement agencies are turning to an alternative AI tool that may be just as powerful—and just as controversial.

Track, developed by California-based AI company Veritone, allows authorities to identify and follow individuals across multiple video feeds using attributes like body size, clothing, hair style, accessories, and more. It does not rely on biometric facial data, meaning it can operate in jurisdictions where facial recognition is restricted or banned.

The system is already in use by over 400 organizations, including local and state police departments, universities, and federal agencies such as the Department of Justice. According to Veritone, Track has also been adopted by units under the Department of Homeland Security and the Department of Defense.

Track currently analyzes recorded footage from sources including body cameras, drones, Ring doorbells, and citizen-submitted videos. Users can input a set of

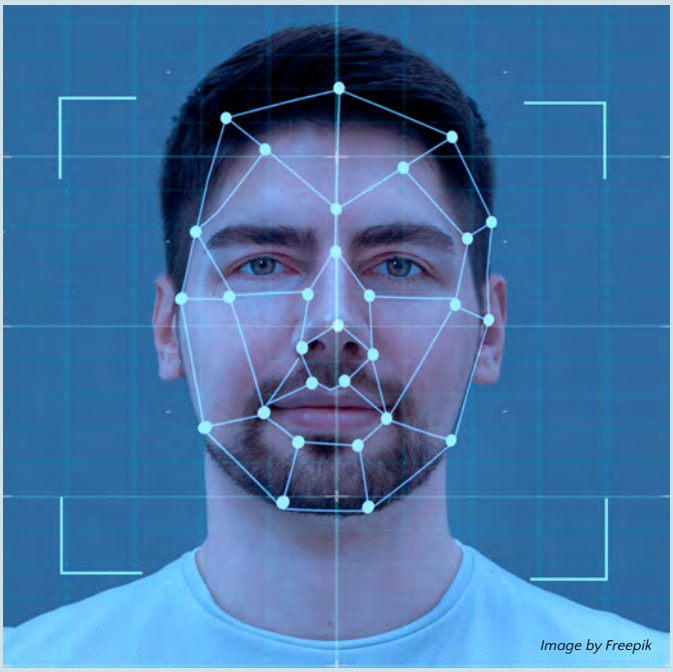


Image by Freepik

> *"If we're not allowed to track people's faces, how do we assist in trying to potentially identify criminals?"*
> ***- Ryan Steelberg, CEO, Veritone***

continue on page 19

attributes to isolate and follow individuals across different environments. A cloud-based version is available through both Amazon and Microsoft platforms. Veritone expects Track to support real-time video within the next year.

A Legal Loophole?

Track is gaining traction as cities and states adopt laws that limit facial recognition due to concerns about bias, wrongful arrests, and lack of transparency. However, because it does not use facial features, Track is not classified as a biometric system under most legal definitions.

This has raised alarm among civil rights advocates. The American Civil Liberties Union (ACLU), which became aware of the tool through a media investigation, said this is the first known example of non-biometric person-tracking at scale in the U.S.

"This is a potentially authoritarian technology," said Jay Stanley, Senior Policy Analyst at the ACLU.

"It enables a kind of mass surveillance that simply wasn't possible before."

While biometric laws often focus on permanent identifiers like faces and fingerprints, Track uses transient traits such as clothing or gait. Still, critics argue that repeat use of the same coat, backpack, or hairstyle makes it possible to track individuals in ways functionally similar to facial recognition.

Technical Scale, Operational Reach

Veritone claims Track can process over 300,000 videos per hour, with sub-500ms latency between footage input and alert generation. The company credits its performance to in-house infrastructure, including GPU-optimized inference and dynamic scheduling—giving it a cost and control advantage over cloud-reliant platforms.

"We own every part of the stack," said Abhik Sarkar, Director of Machine Learning at Veritone.
"That's what makes real-time tracking with high accuracy possible."

The company positions Track as a "culling tool" meant to speed up investigations by narrowing down footage, not as a dragnet surveillance system. Still, it is being used in active federal criminal cases, according to the company, though Veritone has not disclosed specific jurisdictions or outcomes.

A Turning Point for Surveillance Policy?

Track's deployment arrives at a moment when public trust in law enforcement surveillance is fragile, and when government interest in protest and immigration monitoring is rising. The Department of Homeland Security has recently increased its use of social media data to vet visa applicants, and reports suggest agencies have monitored activist activities.

Critics argue that tools like Track present a new category of surveillance power—one that blurs technical boundaries while evading current legal oversight.

"This isn't just automation—it's amplification," said Nathan Wessler, attorney at the ACLU.

"It creates a new kind of visibility law enforcement has never had."

As AI-driven surveillance evolves, tools like Track highlight a growing tension between technological capability and regulatory clarity. Whether laws meant to restrict facial recognition will expand to cover attribute-based tracking remains an open and pressing question. ■

How *Artificial Intelligence* Is Transforming National Surveillance and Threat Response

Short Summary

- Homeland security teams use AI to monitor air, land, and digital borders with greater speed and precision.
- Facial recognition and drone detection tools help officers act faster at checkpoints, disaster zones, and restricted airspace.
- Agencies address rising concerns around data ethics, AI explainability, and surveillance overreach through human-AI collaboration.

Images by Freepik

For years, homeland video surveillance relied on manual monitoring of surveillance camera feeds across borders, transportation hubs, and government buildings. However, this method has often failed during crucial moments. For instance, in several cases, security cameras captured suspects before and after attacks, but the huge amount of footage was too much for analysts to review quickly, causing delays in spotting threats.

These incidents show a clear problem: manual methods can't process video data fast enough or notice subtle but important behaviors in real-time.

Coming to 2025, external threats will become more complex, from FPV (First-Person View) and insider sabotage drone attacks to DIY swarms. Hence, homeland security needs more than just passive monitoring. It needs smart systems that can analyze video instantly, detect unusual activity, and send immediate alerts.

AI-powered video surveillance automates threat detection, enhances situational awareness, and fills the gaps left by manual monitoring, transforming video from a mere record into an active defense tool.

"Traditional systems used pixel-based motion, which led to a higher number of false positives and created excessive bandwidth and storage space constraints. Surveillance camera operators can easily get bombarded with too much information and too many false event alarms caused by lighting changes, shadows, or leaves blowing in the wind."

– Aaron Saks, Director of Sales Enablement, Hanwha Vision America, Teaneck, N.J.

Inside AI's Video Surveillance Shift

Artificial Intelligence is embedded in daily homeland security operations. From scanning airspace for rogue drones to analyzing cyber threats in real-time, AI is helping agencies act faster, see clearly, and stay ahead of evolving risks.

DHS is now speaking openly about where they're using AI, from disaster response to financial threat detection. Here's a look at how AI is reshaping surveillance and threat response on the ground.

1. Counter-Drone Surveillance: Solving the Low-Altitude Threat Challenge

Small, fast, and low-flying drones have become a real headache for traditional surveillance and radar systems, especially in crowded cities or complex environments. From hobbyist FPV drones to improvised swarms, these flying devices pose growing risks to airports, critical infrastructure, and public safety.

AI-powered video surveillance steps in to solve this challenge. It watches live video feeds closely, using deep learning training on countless drone behaviors to tell the difference between harmless objects and potential threats often before human eyes can.

Plus, this video analysis doesn't work alone. It teams up with radio frequency and acoustic sensors to create a smart, automated shield detecting, tracking, and responding to aerial threats faster and more accurately than ever before.

2. AI for Autonomous Situational Awareness (DHS-P2 Use Case)

Border security in remote, rugged areas has always been a tough job, often relying on limited human patrols and outdated tech. The DHS-P2 system changes that by a combination of smart IoT motion sensors with AI-powered video cameras to quietly watch over these challenging situations.

When motion is detected, the cameras spring to life, capturing clear, high-resolution images. Behind the scenes, AI quickly identifies whether it's a vehicle or a person, tracks their movement direction, and even matches them across multiple locations. This means fewer missed threats and less guesswork for border agents.

With its low power needs and discreet presence, the system acts like a vigilant digital sentinel, helping secure borders more efficiently.

3. Rapid Assessment of Satellite and Aerial Video for Disaster Response

In times of natural disasters, homeland security agencies rely on AI-powered satellite and drone video surveillance to gain fast, comprehensive situational awareness. Traditional ground assessments can be slow and hazardous, especially in large or inaccessible areas. AI accelerates this process by analyzing video footage to quickly identify damage, flooding, and other risks.

These aerial surveillance systems provide continuous or periodic monitoring of vast regions, allowing agencies to spot emerging threats and prioritize response efforts. AI models detect damaged infrastructure, blocked routes, and vulnerable populations, enabling homeland security teams to make informed, timely decisions.

4. Facial Recognition in Homeland Security

The Department of Homeland Security (DHS) even uses facial recognition technology to enhance security and speed up identity verification at key checkpoints. This AI-driven system helps reduce manual work and supports critical law enforcement efforts.

"As AI-based object detection and classification become more efficient on edge devices like IP cameras, false positives compared to basic video motion detection are greatly reduced. The environmental factors that resulted in false positives in pixel-based video motion detection are minimized with these types of AI models, since they are built solely to detect and classify people and vehicles."

– Quang Trinh, Business Development Manager, Platform technologies, Axis Communications.

Images by Freepik

Streamlining Traveler Identity Checks:
Travelers' photos are matched against daily passenger galleries or travel documents at air and land borders, speeding up processing and allowing officers to focus on higher-risk cases.

Supporting Critical Investigations:
Homeland Security Investigations (HSI) employs facial recognition, including Clearview AI, to identify victims and offenders in child exploitation cases, enabling rescues that might not have been possible otherwise. Use of Clearview AI is limited to these investigations.

Enhancing TSA Security and Convenience:
At TSA checkpoints, facial recognition verifies travelers' IDs and flight reservations. Opt-in TSA PreCheck members can also use touchless screening for faster access.

Images by Freepik

When Smart Surveillance Raises Tough Questions

As AI and video surveillance take on a bigger role in homeland security, they're helping teams work faster and cover more ground. But alongside these gains come tough questions—about fairness, transparency, and whether the public can really trust how these systems make decisions.

Black Box Decision-Making

Many AI systems used in surveillance operate opaquely—security officers may know what the system flagged, but not why it flagged it. This lack of transparency fuels public skepticism, especially when decisions impact civil rights. This problem may even be worse during external conflicts. Without explainability, it becomes harder to challenge errors or build trust in how surveillance decisions are made.

Bias and Discrimination

AI systems trained on skewed datasets may misidentify individuals, particularly from minority groups, leading to wrongful suspicion or detention. In security settings, even a single false match can trigger serious consequences, from unnecessary questioning to missed real threats. Without diverse, representative data and regular audits, these biases can quietly persist at scale.

Privacy Concerns

Expanding surveillance with AI-powered video often means capturing more personal data, sometimes without clear public knowledge or consent. This raises fears about constant monitoring and the potential misuse of sensitive information, especially in public spaces where people expect a degree of anonymity. There's also concern about how long this data is stored, who has access to it, and whether it could be shared with other agencies or private companies. Without strong privacy safeguards and clear policies, the use of AI surveillance risks eroding public trust and infringing on civil liberties.

Adversarial Attacks and System Vulnerability

In military and homeland defense operations, AI-powered video surveillance systems face sophisticated adversaries who actively try to deceive or disrupt them. Techniques like spoofing, where attackers use fake images, signals, or drones designed to confuse AI algorithms, can cause critical failures in threat detection.

These adversarial attacks exploit the vulnerabilities of AI models, potentially leading to missed threats or false alarms in sensitive defense scenarios.

Closing Comments

AI is turning video surveillance from passive recording to active threat detection in homeland security but it's not a standalone solution. While algorithms can spot patterns and flag anomalies in real time, human operators are still needed to interpret intent, apply judgement and ensure actions comply with legal and ethical standards. The future of surveillance isn't just smarter but safer. ■

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!

@securesolutionstoday

@tradelinkmedia

@tradelinkmedia

COMING SOON

SEP/OCT
30 Sep – 1 Oct
2025

International Security Expo 2025
London, United Kingdom
www.internationalsecurityexpo.com

OCT
8 – 9
2025

DataCentre World Asia 2025
Singapore
www.datacentreworldasia.com

OCT
28 – 31
2025

CPSE 2025
Shenzhen, China
http://cpse.com.cn/en-us

NOV
5 – 7
2025

Secutech Thailand 2025 *(Page 11)*
Bangkok, Thailand
https://secutechthailand.tw.messefrankfurt.com/

NOV
11 – 13
2025

Safety & Security Asia 2025
Singapore
www.safetysecurityasia.com

NOV
19 – 21
2025

SIDEX 2025
Singapore
https://sidex.sg/

NOV
18 – 20
2025

ISC East 2025
NYC, USA)
https://www.discoverisc.com/east/en-us.html

NOV
19 – 21
2025

Digitech ASEAN Thailand 2025
Bangkok, Thailand
https://digitechasean.com/

DEC
3
2025

AI Ready Data Centers Asia 2025 *(Page 9)*
Manila, Philippines
https://arcmediaglobal.com/datacenters/

JAN
12 – 14
2026

Intersec 2026
Dubai, UAE
https://intersec.ae.messefrankfurt.com/dubai/en.html

MAR
18 – 20
2026

SECON 2026
KINTEX, South Korea
www.seconexpo.com

MAR
23 – 27
2026

ISC West 2026
Las Vegas, USA
https://www.discoverisc.com/west/en-us.html

SEP
22 – 25
2026

Security Essen 2026
Essen, Germany
www.security-essen.de

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