

DETEKTOR



International

Publisher's comment:

**Europe's security industry at risk
when regulation becomes a barrier**

The security technology market:

**Global physical security market to
surpass 150 billion dollars by 2030**

The interview - Gerard Figols, I-Pro:

"Cameras will become AI agents"

SPECIAL EDITORIAL FEATURE:

ACCESS CONTROL

- cloud solutions drive the market

SPECIAL EDITORIAL FEATURE:

PERIMETER SECURITY

**- terrorism and cross-border
intrusions propel the market**



DETEKTOR
INTERNATIONAL
AWARD

Best Product 2025

THE SECURITY PRODUCTS OF THE YEAR

DETEKTOR INTERNATIONAL AWARD PRESENTS THE TOP 12 PRODUCTS IN 2025

Secure Your Success

Access Control • Intrusion Detection • Building Automation

ICT®

TSL Multi-Technology
Card Reader

With ICT, every door opens to **better outcomes.**

Behind every classroom door, there's a foundational story to be told - from protecting students and staff day-to-day, to streamlining school operations. ICT's customisable solutions provide built-in access control, intrusion detection, mobile credentials, and extensive integrations. Beyond security, ICT Protege helps you optimise operations, easily integrating with HR/ student and visitor management systems, and building automation so most resources can be spent on education.

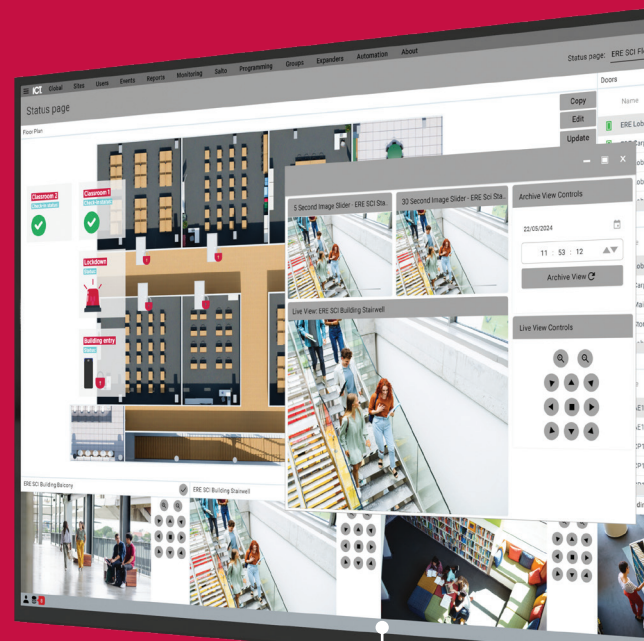
Secure your success with ICT.



Find out more

✉ emea-info@ict.co

🌐 info.ict.co/as-edu



Protege GX Interface



ISSN-1651-3800 published by **armedia**

Head office:

AR Media International AB
Elektravägen 14 • S-126 30 Hägersten
Sweden
Tel: +46 8 556 306 80
E-mail: info@armedia.se
www.detektor.com
www.armedia.se

Asia Office

Asha Chang
AR Media Marketing Corporation
Address: 3F., No. 197, Xinshih 3rd Road
Sec. 2, Tamsui District (251), New Taipei,
Taiwan
Office phone: +(886-2) 2622 1365,
+(886-2) 2622 1385
Mobile: +(886) 922 116272,
Email: asha@armediaint.com

General Information

- Detektor International is published twice a year.
- No part of this magazine may be reproduced without prior permission from the publisher.
- Detektor International welcomes manuscripts, news, releases and photographs, but cannot be held responsible for loss or damage incurred in transit or in possession.
- News releases can be sent to intnews@securityworldmarket.com

Subscriptions

Anette Friberg
+46 8 556 306 80
One-year subscription
Detektor International, 1 year/1 issue *,
printed edition. Price: € 15

Publisher

Lennart Alexandrie
lennart.alexandrie@armediaint.com

Editorial Team

Rachel Ward Owens, Markus Lahtinen,
Jonny Sjöberg, Lennart Alexandrie
info@armedia.se

Art Director

Linn A. Maddern
linn.maddern@armedia.se

Advertisements

Deniz Baykal
deniz.baykal@armedia.se

Printing

Stibo, 2025



Lennart Alexandrie, Publisher.

Europe's security industry at risk when regulation becomes a barrier

The European security industry finds itself at a crossroads, facing both extraordinary opportunities and profound challenges. Emerging technologies such as artificial intelligence, biometric authentication systems, and advanced surveillance solutions promise more effective protection against crime, cyber attacks, and terrorism. Yet it is precisely these innovations that risk being stifled by the dense web of regulation taking shape within the European Union.

Two legislative pillars are particularly significant: the General Data Protection Regulation (GDPR) and the forthcoming AI Act. Both aim to safeguard individual rights, strengthen privacy, and foster trust in digital technologies. However, for the security sector they also impose a heavy burden. GDPR restricts the use of sensitive personal data, such as biometric identifiers, to train and improve AI-based security systems. Meanwhile, the AI Act classifies many of the industry's most promising technologies as "high risk." This designation entails extensive requirements for documentation, transparency, risk assessments, and third-party audits—processes that slow innovation and place costs on companies, especially smaller players that may lack the necessary resources.

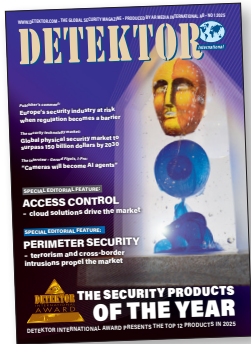
This is not merely a matter of economics or business growth. When European companies are limited in their ability to develop new security solutions as quickly as competitors in the United States or China, the consequences extend to public safety itself. Police forces, border agencies, and defence institutions face restrictions in deploying AI tools to combat organised crime or terrorism. Businesses already under constant threat from cyber attacks risk losing access to the most effective protective technologies. Ultimately, it is the citizens who pay the price. Regulations designed to protect privacy can, in practice, leave society more vulnerable to real-world threats.

The global comparison is stark. In the United States, regulation is fragmented and often market-driven, allowing companies to experiment and deploy new technologies at a much faster pace. China goes even further, with state-backed development and access to massive data sets enabling its companies to dominate surveillance technology and export it worldwide. Europe, by contrast, emphasises strict precautionary regulation, but at the cost of slower innovation cycles and reduced competitiveness.

In addition to GDPR and the AI Act, other EU laws shape the sector's landscape. The NIS2 Directive strengthens cyber security obligations for critical sectors such as energy, transport, and healthcare, while the CER Directive seeks to protect critical infrastructure against both physical and digital threats. These frameworks undoubtedly improve resilience, yet they also increase the regulatory burden and complexity faced by market actors.

The challenge for the European Union is thus to strike a delicate balance. On the one hand, there is a legitimate responsibility to uphold fundamental rights and ensure that technology is deployed ethically and lawfully. On the other, Europe must safeguard its capacity for innovation and competitiveness in a world where threats are escalating and where other global powers are far less hesitant to push boundaries. Failure to find this balance risks not only a loss of technological leadership, but also greater vulnerability for European societies.

It is a paradox that demands political courage: acknowledging that an excessive focus on privacy can, in practice, erode security. Europe's security industry has the potential to drive both economic growth and societal resilience—but only if regulation is shaped to enable innovation rather than suffocate it.



3 Publisher's Comment. Europe's security industry at risk when regulation becomes a barrier.

6 Security Technology Market.

Global physical security market to surpass 150 billion dollars by 2030.

8 AI video market set to grow 32 per cent annually through 2032.

10 Special Feature: Access Control

Cloud-based platforms and ACaaS drive the market for access control.

24 Special Feature: Perimeter Security

Terrorism and cross-border intrusions propel the perimeter security market.

32 Anniversary. AR Media International and Detektor celebrate 35 years.

34 Detektor International Award 2025.

36 Top 12 security products of the year.

46 The Interview.

Gerard Figols, I-Pro: "Cameras will become AI agents."

48 Sectech.

Sectech 2025 breaks record.

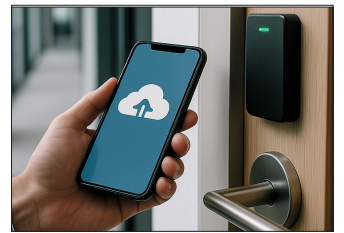
50 Security Events. The calendar of security fairs.



Security Technology Market

The global physical security market is projected to grow from 120.79 billion US dollars in 2025 to 151.50 billion US dollars by 2030.

Page 6



Special Feature: Access Control Systems

A new report suggests that the access control market is expected to grow from 10.62 billion US dollars in 2025 to 15.80 billion dollars by 2030, at a CAGR of 8.3 per cent.

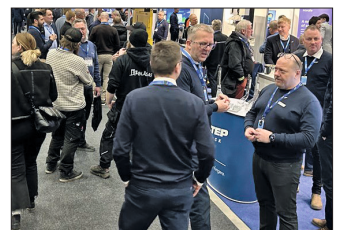
Page 10



Special Feature: Perimeter Security

The increasing threat of cross-border intrusions is expected to propel the growth of the perimeter security market going forward.

Page 24



Security Events: Sectech 2025
Sectech – the compact pan-Scandinavian security event – held in Stockholm on 14–15 October 2025 – was a huge success.

Page 48

DETEKTOR INTERNATIONAL AWARD



Detektor International Award 2025.

Detektor International Award 2025 – four overall winners and eight other award recipients.

Photo: Camilla Svensk

Page 34



Open-platform body worn solutions.



Solutions that work with yours.

Global physical security market to surpass 150 billion dollars by 2030

The global physical security market is projected to grow from 120.79 billion US dollars in 2025 to 151.50 billion US dollars by 2030, at a CAGR of 4.6 per cent during the forecast period, according to the latest findings from research company, Marketsandmarkets.

Delray Beach, FL (USA)

The rise in security breaches and malicious attacks in areas like transportation, healthcare, government, and commercial buildings is increasing the need for stronger physical security. Organisations are now focusing on real-time protection, from controlling access to preventing threats across their facilities, according to the report.

Investing in modern solutions

The threat landscape is becoming more complex, with attackers using a combination of physical intrusions and cyber techniques, along with insider threats, unauthorised drone activity, and coordinated break-ins at sensitive locations like hospitals and airports. To address these risks, businesses are investing in modern solutions such as integrated access control systems, smart sensors, and AI-powered surveillance that enhance safety without disrupting operations, Marketsandmarkets stresses.

Video surveillance still takes the major share

Expanding needs for real-time monitoring, crime prevention, and upgrading public safety across commercial, government, and infrastructure sectors are driving demand for video surveillance systems. IP cameras and video analytics now provide functionality much more advanced than mere recording, like providing actionable insight in the form of motion detection, face recognition, and behavioural analysis.

Integrated into smart infrastructure, these solutions provide real-time awareness of vehicles, machinery, and building perimeters. With increasing security threats and operational intelligence moving to the centre stage, deployment is increasingly taking place in high-risk locations such as banks, malls, transportation centres, and public spaces.

Despite advancements in smart and data-driven technologies, video surveillance still remains a vital component in preventing



Expanding needs for real-time monitoring, crime prevention, and upgrading public safety across commercial, government, and infrastructure sectors are driving demand for video surveillance systems.

security incidents and enhancing proactive threat management across sectors.

Deterrence, detection and rapid response capabilities

With expansive assets and complex infrastructure, large-sized businesses are more vulnerable to physical attacks, driving their strong reliance on advancing their physical security systems. To address these vulnerabilities, such as unauthorised access to data centres, insider threats, theft of valuable equipment, tampering with operational systems, or targeted attacks on executive facilities, large enter-

prises demand integrated physical security frameworks that combine deterrence, detection, and rapid response capabilities.

AI, IoT, and real-time analytics

Large enterprises typically allocate high budgets for security, enabling them to deploy integrated solutions powered by AI, IoT, and real-time analytics. Moreover, the need to meet regulatory requirements and protect brand reputation further drives their investment in robust, enterprise-grade physical security systems, according to the report.

The biggest video trends: AI and cloud technology

The transition to cloud technology and the rise of artificial intelligence in video surveillance are the two main macro trends identified in the "World Market for Video Surveillance Hardware and Software - 2025 Edition" report from Novaira Insights.

Newport Pagnell, Buckinghamshire (UK)

The US and Canadian markets are leading the shift towards cloud-based solutions, with significant growth in recurring cloud video management software revenues.

Better video analytics performance

Additionally, AI technologies are enhancing video analytics performance, approaching a

majority of new camera shipments to include deep learning powered video analytics capabilities on their embedded chipsets. This plus the renewed drive towards system wide intelligent automation is propagating AI use across surveillance systems, according to the report.

High growth in emerging markets

The report forecasts a compound annual growth rate (CAGR) of

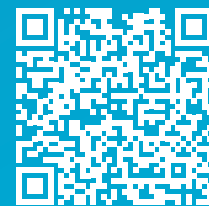
8.1 per cent for the global market excluding China from 2024 to 2029. This growth is driven by robust expansion in emerging markets such as India, Latin America, and the Middle East, along with increased demand for cloud solutions in established markets like North America and Western Europe. Novaira Insights estimated the global market for video surveillance equipment to be worth 25 billion dollars in 2024.

ASSA ABLOY

Your Go-To Resource for Industry Insight

6th
biennial
edition!

Discover
what's next
for wireless
access control.



Get your copy

Experience a safer
and more open world

AI video market set to grow 32 per cent annually through 2032

The global AI video market was valued at USD 3.86 billion in 2024 and is expected to grow to USD 42.29 billion by 2033, representing a compound annual growth rate (CAGR) of 32.2 per cent between 2025 and 2033, according to a new report by Grand View Research, Inc.

San Francisco, Ca (USA)

AI technologies enhance surveillance systems by providing advanced features such as facial recognition, anomaly detection, and automated alerts, which improve the effectiveness of monitoring efforts.

More efficient responses

These solutions enable faster identification of potential threats and more efficient responses to incidents, contributing to safer environments in public spaces and critical infrastructure. As security

challenges become more complex, the demand for sophisticated AI-driven tools that can offer real-time analysis and actionable insights continues to rise. This trend highlights the crucial role of AI in enhancing public safety and addressing evolving security needs, according to the report.

Highlights from the report:

- The cloud-based platforms segment led the market and accounted for over 50 per cent of the global revenue in 2024. Cloud-based plat-

forms are growing rapidly due to their scalability, cost-efficiency, and the increasing demand for flexible, remote access to AI video solutions and data management.

- The B2B (enterprise) segment accounted for the largest revenue share in 2024. The B2B (enterprise) sector is growing in the market as businesses increasingly adopt AI-driven solutions for enhanced video analytics, automation, and operational efficiency.

- The video analysis AI segment accounted for the largest revenue share in 2024. Video analysis AI is expanding in the market because it delivers actionable insights through real-time data processing and advanced analytics. The rising need for enhanced surveillance, quality control,

and customer behaviour insights is driving its broader adoption across multiple industries.

- Rising consumer and business demand for personalised and engaging video content is driving the adoption of AI technologies that offer tailored recommendations and automated content creation. According to the research, this trend is expanding the market as organisations seek to enhance user experiences.

- The market is growing rapidly due to advancements in machine learning and computer vision, which enhance the accuracy and capabilities of video analysis tools. These innovations enable more sophisticated applications in fields like security, media, and entertainment.

Rapid growth ahead for counter-drone technology

The global anti-drone market will reach 14.51 billion US dollars by 2030 from 4.48 billion dollars in 2025, registering a CAGR of 26.5 per cent from 2025 to 2030, according to the latest reports from Marketandmarkets. The global anti-drone market is primarily driven by escalating security concerns over the unauthorised and potentially malicious use of drones across military, critical infrastructure, and public spaces.

Delray Beach, Fl (USA)

Increasing incidents of drone-related threats, such as espionage, smuggling, and attacks, have compelled governments and organisations to adopt robust counter-drone technologies. Advances in detection and mitigation technologies, including AI-powered systems, multi-sensor integration, and directed energy weapons, further propel the market by enhancing the effectiveness and reliability of anti-drone solutions.

Ground-based solutions projected to dominate

The ground-based segment is expected to hold the largest

share of the anti-drone market in 2030 due to its versatility, ease of deployment, and ability to cover vast areas with integrated sensor arrays. These systems can incorporate multiple detection and disruption technologies, such as radar, RF jamming, and directed energy weapons, making them effective against diverse drone threats. Their suitability for protecting critical infrastructure, military installations, and public events further drives widespread adoption.

Additionally, they offer scalability and easier maintenance compared with airborne or naval



The rapid expansion of drone usage across industries such as logistics, agriculture, construction, and event management raises concerns over safety and security.

platforms, strengthening their dominance in the market.

Commercial sector the strongest vertical

The commercial segment is expected to exhibit the highest CAGR in the anti-drone market during the forecast period due to the rapid expansion of drone usage across industries such as logistics, agriculture, construction, and event management, which raises concerns over safety and security. Increasing investments by businesses to protect assets, comply with regulations,

and ensure operational continuity drives demand for effective counter-drone solutions.

Additionally, the growing awareness of drone-related risks in crowded urban environments and critical commercial facilities fuels the adoption of advanced detection and disruption technologies. The rising trend of integrating anti-drone systems with IoT and cloud-based platforms further accelerates market growth in this segment, making it a key revenue driver, according to Marketandmarkets.

MAKE YOUR ACCESS CONTROL INTUITIVE STID MOBILE ID



Intuitive technologies for a seamless world



BADGE MODE



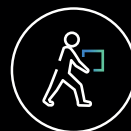
SLIDE MODE



TAP TAP MODE



REMOTE MODE



FREE HAND MODE



VOCAL COMMAND

SMARTER SECURITY ANSWERS



Cloud-based platforms and ACaaS drive the market for access control

A new report from Marketsandmarkets suggests that the access control market is expected to grow from 10.62 billion US dollars in 2025 to 15.80 billion dollars by 2030, at a Compound Annual Growth Rate (CAGR) of 8.3 per cent. The market is driven by the rising adoption of IoT-enabled security systems and cloud-based platforms.

IoT enhances automation efficiency by enabling secure, real-time data exchange, while cloud integration offers scalability, remote monitoring, and reduced maintenance costs. Together, they support advanced models like Access Control as a Service (ACaaS), providing businesses flexibility, visibility across sites, and seamless updates. This interconnected shift from traditional systems to IoT and cloud solutions fuels strong market growth, according to Marketsandmarkets.

Rapid growth of ACaaS

Hosted access control as a service (ACaaS) is expected to hold the largest market share in the overall access control market owing to its flexibility, scalability, and cost-effectiveness. Unlike traditional systems, ACaaS eliminates the need for heavy infrastructure or on-premises servers, as data is stored and managed at third-party locations. This allows users to gain complete control over access rights without incurring high maintenance costs.

Being cloud-based, it requires no client-side software and enables centralized monitoring of multiple facilities, offering seamless and maintenance-free experience. Hosted ACaaS also enhances security and efficiency by supporting remote access and management from any device. Solutions can provide robust, feature-rich, and always-available access control that businesses can rely on for uninterrupted operations. The ability to push security patches, updates, and troubleshooting remotely ensures

higher resilience compared to on-premises systems, Marketsandmarkets stresses.

More software centric

Another research company, Omdia, states in its 2025 Access Control Report that the access control software market has been the fastest growing global driver of access control equipment sales over the past decade as the industry has become more software centric.

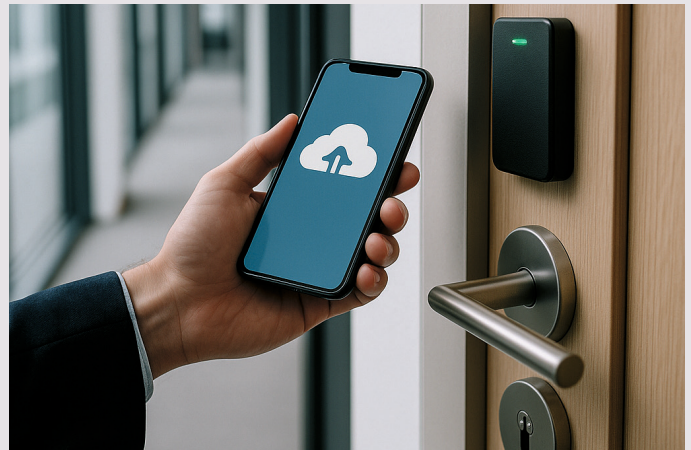
“Cloud-based solutions have emerged as a significant growth driver due to their scalability and their enhanced data processing capabilities”, says Bryan Montany, Principal Research Analyst, Physical Security at Omdia.

Critical infrastructure

Additionally, the growing need to safeguard critical infrastructure such as oil & gas, chemical, pharmaceutical, metal & mining, power, automotive, and water treatment sectors is fuelling adoption. With increasing concerns around unauthorized access and data security, enterprises are turning toward ACaaS for its ability to provide secure, scalable, and future-ready solutions.

ID verification and smart buildings

The ID verification market is growing faster than the access control market. Marketsandmarkets estimates that the sector is projected to grow from 14.34 billion dollars in 2025 to 29.32 billion dollars by 2030 at a CAGR of 15.4 per cent. And the smart buildings market grows



Cloud integration offers scalability, remote monitoring, and reduced maintenance costs.

more or less at the same pace with a CAGR of 15.6 per cent from 2025 to 2030.

Commercial smart buildings are at the forefront of the smart building segment within the smart cities market, largely due to their high adoption rates in office buildings, retail spaces, and corporate office parks. This trend is driven by the demand for increased operational efficiency and cost reduction. These buildings implement various solutions, including automated building management systems (BMS) that help to reduce HVAC, lighting, and energy consumption. Smart visitor and access systems enhance security and streamline entry processes. AI-driven space optimisation and data analysis maximize the use of space based on occupancy patterns, Marketsandmarkets stresses.

Residential market on the rise

Residential premises have witnessed an increased adoption of access control and video surveillance security systems. Residential properties have installed electronic lock-based access control systems to prevent invasion and burglary. One of the most important requirements regarding protecting personal belongings is to carry out rigorous and detailed control of

the people who enter and leave the residential premises. The entry gates are the doorways to residential communities and buildings. Without supervision, anyone can freely enter and exit the property. The demand for electronic products has surged with the growing home automation trend. Home security is a major concern for homeowners nowadays.

North America leads the market

North America holds the largest share in the global access control industry driven by rising demand for cloud-based services, mobile access control solutions, and advanced management software. Organisations across industries are increasingly adopting these technologies to enhance security and operational efficiency.

The region is also witnessing strong uptake of biometric authentication and multi-technology readers, particularly in the commercial and government sectors. For instance, the US Department of Defense and the Department of Homeland Security have long relied on fingerprint biometrics to facilitate both physical and digital access while addressing critical security concerns, according to Marketsandmarkets.

Cutting-Edge Access Control for Tough Environments



The **HID Signo Mechanical Keypad Reader** delivers cutting-edge access control in the toughest conditions. Whether it's freezing temperatures, rain, or low visibility, this reader is designed to perform.

- Resilient Performance: IP65-rated for rugged environments.
- Mechanical Input: Easy to use, even with gloves.
- Mobile Credentials: Supports HID Mobile Access® and credentials in Wallet.
- Advanced Security: Cryptographic key storage for enhanced protection.
- Remote Management: Hassle-free updates from anywhere.
- Sustainable Design: Energy-saving features validated by GreenCircle certification.



Learn More!

Scan the QR Code to
Discover HID Signo 40T



Powering **Trusted Identities**

Kelly Gill, Assa Abloy Opening Solutions:

Staying secure in today's digital landscape

In today's connected world, attacks are more likely to target digital rather than physical entry points, states Kelly Gill, SVP and CTO at Assa Abloy Opening Solutions EMEA.

In this article she shares her insights on today's regulatory environment — including NIS2 and the Cyber Resilience Act – and what the access control industry must do to remain digitally secure.

As the industry has shifted from mainly mechanical to increasingly digital solutions, the need to constantly monitor and assess risks has become crucial.

"This means not only meeting mandatory regulations but also voluntarily adopting international standards such as ISO 27001, which protects data and systems through a structured and independently audited framework," explains Kelly Gill.

To raise the bar for cyber security across Europe EU has introduced the Network and Information Security Directive 2 (NIS2) and the Cyber Resilience Act (CRA).

The new regulations

NIS2 is reshaping cyber security expectations by setting higher standards to reduce risk, improve transparency, and protect data and services. Alongside it, the CRA introduces mandatory requirements for products with digital components. This makes "secure by design," regular updates, and compliance checks essential before products can enter the EU market.

"For companies in our industry, responsibilities now extend well beyond internal systems," Gill notes. "Organisations must also ensure that suppliers and service providers comply, with regular risk assessments forming a central part of the process. The consequences of falling short are severe – from

significant fines and audits to the potential withdrawal of products from the market."

For customers, the message is clear: security must be built in from the start.

Competitive advantage

Gill is eager to stress that compliance is not just about meeting regulations — it is also a competitive advantage.

"At Assa Abloy Opening Solutions EMEA, security is part of our DNA," she says. "We embed these standards into everything we do, giving customers solutions they can trust to be compliant and resilient."

The rise of AI

AI is transforming the digital security landscape. It cannot be separated from the regulatory framework shaping the industry. With AI advancing rapidly and new regulations coming into force, Kelly Gill is convinced that Assa Abloy has established a digital compliance framework to stay ahead of the curve and use AI as an enabler to improve security and achieve compliance.

"AI brings powerful benefits, including more intelligent monitoring, faster anomaly detection, and smarter tools for operational efficiency," Gill explains. "These capabilities directly support NIS2 and the CRA, particularly in proac-

tive risk management and incident response."

"On the other hand, AI introduces new risks. The attack surface is expanding, and threats such as deepfakes and smarter phishing create serious challenges that regulators are determined to address. Both NIS2 and the CRA emphasise continuous monitoring, transparency and accountability — principles that must now also guide the responsible use of AI."

According to Gill, Assa Abloy Opening Solutions EMEA sees AI not just as a risk to mitigate, but as a capability to strengthen resilience and trust.

"That's why we are embedding strong governance practices around AI and building cyber security standards into every stage of product development," she says. "By doing so, we help our customers align with new regulations while ensuring AI serves as a tool for greater security and confidence."

Trust and compliance

Gill emphasises that Assa Abloy Opening Solutions EMEA is taking NIS2, the CRA and the rise of cyber threats seriously — ensuring compliance and enhancing trust with all customers.

"We have reinforced supplier oversight, streamlined incident reporting, and embedded cyber security into every stage of product development and lifecycle management," she explains. "Our teams also conduct ongoing risk assessments and post-incident reviews to ensure lessons are learned and improvements made."

By taking these steps, Assa Abloy Opening Solutions not only meets regulatory requirements but also strengthens the resilience of its supply chain — and the trust customers place in the company.



Kelly Gill, SVP and CTO at Assa Abloy Opening Solutions EMEA.

Another key commitment is supporting customers on their compliance journey. Recent initiatives include the newly released whitepaper "Enhancing Cyber-Physical Resilience with Digital Access Solutions" and a detailed NIS2 whitepaper from last year, both providing clear and practical guidance.

"By showing what these regulations mean in practice and how intelligent access solutions can directly support compliance, we aim to make the path forward less complex and more achievable for our customers," Gill says.

Looking ahead

The days when security threats to businesses and products were purely physical are long gone. Today, the digital realm poses even greater and constantly evolving challenges.

"It's crucial that, as an industry, we take the necessary steps to meet the directives of NIS2 and the CRA and continually monitor the rise of AI. Only by doing so can we protect our customers, preserve our reputations, and build the trust that defines true leadership in security," Gill concludes.



ACRE ACCESS CONTROL

Native cloud and on-premises solutions. We don't want you guessing if you're secure.
We want you to know.

RESHAPING SECURITY TOGETHER

The technology we choose, driven by the end user experience we desire, impacts the software we develop, and adheres to our go-to-market strategy of being a disruptor.



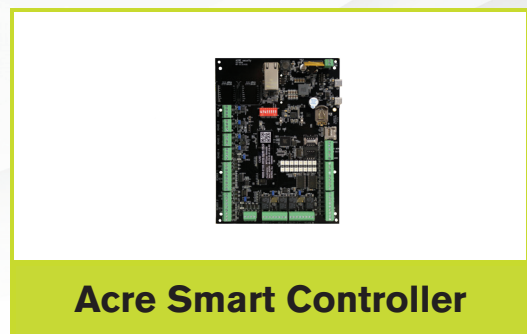
Acre Access Control



Acre Wallet



Acre Multi-Tech Readers



Acre Smart Controller



Scan Here
LEARN MORE

acresecurity.com

Robert Jansson, Stid Security:

With smart buildings, the tech

Smart buildings and smart cities are built on integration – systems that can communicate and function seamlessly together. Yet the access control market is still dominated by proprietary solutions, according to Robert Jansson at access control card technology company Stid Security.

“The industry needs to change. Open technology is crucial for both security and development,” he says.

Robert Jansson, Director of Sales for the Nordics, Eastern Europe and South Africa at Stid Security, has worked in security and access control for nearly 30 years. With unwavering persistence, he has emphasised the importance of using technology based on open standards – and he has no plans to stop.

“An open access control system is built on standardised protocols and interfaces. It should easily integrate with other systems, such

SSCP, and RFID/NFC, and can be easily integrated with other systems via API and SDK. This allows partners to develop tailored solutions for everything from access control to advanced applications.

“We practise what we preach and share our technology with players who want to use it. That’s the right path if the security industry’s solutions are to keep evolving with the times and with customers’ growing needs.”

” With open systems, buildings can create a connected ecosystem where all components work together. That makes managing both operations and security significantly easier”

as video surveillance, alarms, lighting, and energy management,” he explains firmly.

“For smart buildings, this is a fundamental requirement: operations become more efficient, security is higher, and the entire system is easier to manage.”

Open standards – in Stid’s DNA

It’s no coincidence that Robert Jansson advocates so strongly for open technology. Stid has made openness part of its DNA. The company’s reader technology is built on standards such as OSDP,

Flexibility and scalability

Another key advantage is flexibility. Technology evolves rapidly, and systems must be expandable and adaptable over time – without locking organisations into a single supplier.

“New functions and systems should be able to be added without replacing the entire infrastructure. That’s the only way to future-proof buildings,” says Robert Jansson.

Security in focus

The strongest argument for open platforms, however, is security.



Robert Jansson, Director of Sales for the Nordics, Eastern Europe and South Africa at Stid Security, has worked in security and access control for nearly 30 years.



Stid Mobile ID – a digital access control solution that lets users unlock doors with their smartphone instead of a physical badge, using secure Bluetooth, NFC, or cloud-based credentials. Of course, based on open technology.

Cyber security threats are increasing, and regulations are tightening – making open systems a necessity.

“Security is a cornerstone of both smart buildings and cities. Given today’s threat landscape, there’s no sustainable future for proprietary systems. They quickly become insecure because technology develops too fast,” Jansson observes.

Working towards standardisation

Stid Security is also involved in

the Smart Physical Access Control Alliance (SPAC Alliance), where leading players in physical and logical security collaborate to strengthen European infrastructure. The goal is to promote open, interoperable standards and certification within access control – for example, regarding encryption and biometric methods.

“With open systems, buildings can create a connected ecosystem where all components work together. That makes managing both operations and security

nology of the future is open

significantly easier,” says Robert Jansson.

Secure card technology

An important aspect of access control systems is the reader technology itself – Stid’s area of expertise. Jansson emphasises that organisations should avoid older 125 kHz technology and instead use the globally established 13.56 MHz radio frequency for contactless communication, as used in modern RFID and NFC solutions.

“It enables fast data transfer, strong security, and encryption. The older 125 kHz technology

Act (CRA) are putting increasing pressure on suppliers and organisations. Systems that handle sensitive data or are connected to critical infrastructure must be continuously updated and adaptable.

“Many existing access control systems will need to be replaced. That creates opportunities for suppliers who build their solutions on open standards,” says Robert Jansson.

The future is open

Robert Jansson is convinced that the security industry, too, is moving towards open technol-

“We practise what we preach and share our technology with players who want to use it.”

should be avoided,” he advises.

When it comes to secure cards, Jansson recommends Desfire EV3.

“If all security attributes are activated, Desfire EV3 provides maximum security. If not, security is compromised.”

Regulations driving change

The EU’s NIS2 Directive, the existing GDPR framework, and the upcoming Cyber Resilience

ogy platforms. The development of smart buildings and growing integration needs support this trend.

“Smart buildings require open systems. Without standardised, flexible, and secure platforms, it’s impossible to meet the increasing demands for integration, cybersecurity, and future-proofing,” he says, concluding:

“Proprietary systems belong to the past. The future is open.”



Stid designs and manufactures high-security identification and access control solutions, including RFID readers, credentials, and mobile access systems for physical and logical security.



With unwavering persistence, Robert Jansson has emphasised the importance of using technology based on open standards – and he has no plans to stop.

Jaroslav Barton, HID:

Three signs it's time to upgrade

The card reader mounted by your office entrance has been faithfully serving your organisation for years – perhaps even decades. Employees tap their cards, the door opens, and people gain access. From a basic functionality standpoint, everything seems to be working. But is it?

In this article, Jaroslav Barton of HID shares his views on when it's time to upgrade your access control system.

As security threats evolve and organisational needs become more complex, the question isn't just whether your access control system works – it's whether it still fits your organisation's current and future requirements.

"The reality is that many facility managers assume their existing access control technology is meeting their security needs simply because it's still granting entry to authorised personnel," says Jaroslav Barton, Director of Product Marketing, Physical Access Control, at HID.

"However, functional and optimal are two very different things, especially when it comes to security, compliance, and operational efficiency."

Reassessing your access control foundation

For many organisations, the access control systems installed years ago were perfectly adequate for their needs at the time. These systems reliably controlled who could enter which areas and, for environments with basic security requirements, they may continue to serve that purpose effectively.

However, as organisations grow, face new regulatory requirements, or operate in environments where security is critical, the limitations of older access control technology become more apparent.

"Legacy systems that rely on basic proximity cards and out-

dated communication protocols may not provide the level of security, auditability, or integration capabilities that present-day organisations require," Barton explains.

This distinction is particularly important for organisations handling sensitive data, operating in regulated industries, or managing facilities where unauthorised access could have serious consequences.

"In these environments, access control isn't just about convenience – it's a critical component of the overall security infrastructure."

Three clear signs it's time to upgrade

Jaroslav Barton highlights three key signs that it's time to modernise your access control system:

1. Security requirements have outgrown your technology

If security is critical to your organisation's operations, legacy access control technology may no longer provide adequate protection. Older systems that rely on unencrypted credentials and outdated protocols, such as Wiegand, were designed for a very different threat landscape than today's.

Organisations handling sensitive data, operating in high-security environments, or managing facilities where unauthorised access could have serious consequences need systems that can



Employees and visitors expect the same convenience they get from their smartphones everywhere else – including work, states Jaroslav Barton.

withstand sophisticated attacks. This means encrypted credentials, secure communication between readers and controllers, and comprehensive audit trails.

The key question isn't whether your current system has security flaws – it's whether its vulnerabilities align with your organisation's risk tolerance and security requirements.

2. Keeping up with regulatory requirements

Regulatory frameworks across Europe are increasingly recognising the link between physical and digital security. The EU's NIS2 Directive, which came into effect in October 2024, requires organisations in critical sectors to implement comprehensive cyber security measures – including assessments of their physical access control systems and supply chain security.

Similarly, the UK's Govpass programme aims to replace the patchwork of different credentials government employees have



Jaroslav Barton, Director of Product Marketing, Physical Access Control, at HID.

historically carried with standardised, encrypted credentials. For the hundreds of UK departments and agencies that must comply with Govpass, this means upgrading legacy access control systems.

Beyond these initiatives, industry-specific regulations are also driving demand for more secure, auditable solutions. Organisations subject to these requirements need systems that provide detailed access logs and demonstrate sufficient security to

your access control system



The question isn't just whether your access control system works – it's whether it still fits your organisation's current and future requirements.

ensure credentials cannot be easily duplicated or tampered with.

3. Missing out on operational opportunities

Legacy access control systems are often single-purpose tools in a multi-purpose world. Modern smart cards and mobile access solutions can do far more than

create a more seamless experience for employees and visitors.

Triggers for migration decisions

So, what typically prompts organisations to make the switch? Based on HID's experience, Barton identifies and comments on five common scenarios that

“Organisations that experience a security breach often fast-track their migration plans, recognising that their system wasn't protecting them as well as it should have.”

just open doors – they can integrate with building automation systems, manage parking access, handle cafeteria payments, and even control printer usage.

By sticking with basic proximity cards, organisations not only accept security risks but also miss opportunities to streamline operations, reduce costs, and

serve as eye-openers for end users to upgrade:

Security incidents

“Nothing motivates immediate action quite like discovering that someone gained unauthorised access to your facility or data. Organisations that experience a security breach often fast-track



Younger employees, often view traditional key cards as outdated and inconvenient.

their migration plans, recognising that their system wasn't protecting them as well as it should have,” Barton says.

Proactive security assessments

“Forward-thinking organisations don't wait for a breach to reveal weaknesses,” Barton notes. “Regular security audits and risk assessments can uncover outdated technologies that no longer meet today's threat landscape. By identifying vulnerabilities early, these organisations can plan upgrades on their own terms—rather than reacting under pressure after an incident.”

User-driven demand

“Increasingly, employees and visitors expect the same convenience they get from their smartphones everywhere else – including work. Why should they carry both a phone and a separate access card? This expectation is particularly strong among younger employees, who view traditional key cards as

outdated and inconvenient,” he adds.

The aesthetic awakening

“Sometimes the catalyst is as simple as realising that a 30-year-old reader looks out of place in a modern, professional environment. Organisations investing in updated office spaces often realise their access control technology should reflect the same attention to design and functionality.”

Smart building readiness

Finally, many organisations pursuing smart building initiatives discover that their legacy systems cannot integrate with modern building automation, energy management, or sustainability platforms.

“When outdated physical access control systems become the bottleneck preventing occupancy-based HVAC optimisation or environmental reporting, migration becomes essential for meeting operational efficiency goals,” Barton concludes.

Neil Foster, ICT:

Moving towards smarter access control – means more than just security

Access control systems have a long lifespan, often remaining in operation for 15–20 years. But with increasing demands for security, integration, regulatory compliance and sustainability goals, a technology update becomes essential. A modern access control system can also contribute to improved operational efficiency and energy savings – benefits that, according to Neil Foster at ICT, should not be overlooked.

Modern access control and alarm systems can do more than secure a facility – they can also enhance efficiency and productivity, says Neil Foster, Regional Sales Director for Northern Europe at ICT, a developer and manufacturer of unified and intelligent access control and security solutions.

“By consolidating different systems into a central platform and automating events – for example switching off air conditioning, turning off lights or arming an area when no one is present – you can go beyond security,” he explains.

“The access control system also becomes a tool for driving operational efficiency and reducing energy costs, which should be factored into any investment decision.”

Productivity in practice

Neil Foster illustrates this with an example:

“If the access control platform

their destination floor. Saving just a few minutes for hundreds or even thousands of people every working day leads to significant productivity gains. In high-demand environments such as healthcare, those minutes can be absolutely critical.”

Smarter step by step

Modernising equipment on a limited budget can be challenging and requires strategic planning. By carefully reviewing the existing technical infrastructure, it is often possible to identify older, compatible equipment for integration, enabling a phased and systematic migration to smarter systems.

“At ICT we have worked with many customers who have carried out phased migrations, significantly reducing project costs while maintaining operational continuity by retaining parts of the old system and complementing it with ICT Protege Access Control,” explains Neil Foster.

“Replacing hundreds of readers, door controllers and an entire credential base all at once is a major undertaking and can cause major disruption, particularly in 24/7 operations”

is integrated with turnstiles and elevator systems in a high-rise building, it can manage people flow and direct users to the fastest lift to

“This gives customers immediate access to new features and third-party integrations supported by Protege GX – ICT’s access control



Modern access control and alarm systems can do more than secure a facility – they can also enhance efficiency and productivity

and intrusion detection platform – while keeping initial investments and disruptions to a minimum.”

“Replacing hundreds of readers, door controllers and an entire credential base all at once is a major undertaking and can cause major disruption, particularly in 24/7 operations.”

Continuous synchronisation

A critical point in migration is ensuring that legacy and new access control servers continuously synchronise data to avoid discrepancies in the user database. For this purpose, ICT offers the DataSync software, which enables gradual equipment upgrades tailored to customer needs and budgets.

Balancing cost, sustainability and security

Both private and public sectors face the challenge of optimising space utilisation while balancing cost, sustainability and security. The choice of technology has a major impact on both CAPEX (Capital Expenditures) – investments in fixed assets – and ongoing operational costs (OPEX), such as license subscriptions, service agreements and upgrades.

Neil Foster emphasises that



Neil Foster, Regional Sales Director for Northern Europe at ICT.

access control is a core, embedded element of a building’s functionality, delivering both security and operational benefits.

“An open technology that can integrate with legacy equipment and third-party solutions – and can be adapted and scaled to meet new requirements via its flexible infrastructure – provides both risk minimization and economic benefits, in terms of both initial investment and future maintenance.”

“This is also the philosophy behind ICT and our open Protege platform,” he concludes.



PROTECTION FROM EVERY SIDE

Long range detection with REDSCAN Pro

The award-winning REDSCAN Pro LiDAR series can accurately detect intruders and moving objects up to 50 x 100m away – making it particularly well suited for protecting the highest security sites. And by creating rectangular, high resolution detection patterns, there are no ‘gaps’, so everything from facades to fences, ceilings to roofs can be covered. For the installer, the sensor’s intelligent multiple zones logic means each detection zone can be independently configured, while its camera module brings visual assistance for configuration and post-alarm analysis. The alarms and video stream can all be configured via ONVIF.

www.optex-europe.com



Onvif® | 
ONVIF is a trademark of Onvif, Inc.

Daniel Persson, Acre Security:

How AI can transform Access

In January 2025, Acre Security acquired Reks.AI – a company that have developed a large language model designed specifically for access control.

“AI can, for example, analyse workflows and act as a kind of watchdog within the system, responding to abnormal behaviour,” explains Daniel Persson, Business Development Director – EMEA/APAC-at Acre Security.

Persson compares Reks to Chat-GPT, as both are large language models, but Reks has been trained specifically for access control applications. The company’s founders now work within Acre Security.

“AI isn’t yet widely used in access control,” he says, “but we’re now implementing it into our Acre Access Control platform. The aim is to simplify processes so users can receive both report-based and real-time insights into system activity – such as identifying irregular behaviour.”

Debut in Las Vegas

Acre Security’s first AI demonstrations in public took place at the major security trade show ISC West in Las Vegas in April in 2024, followed by a showcase at The Security Event in Birmingham, UK. In both cases, it was a success. The interest in AI and its usefulness in access control systems is evident.

Enhanced usability

Today’s access control systems can already issue alerts for suspicious behaviour – for example, when an authorised user opens a door at an unusual time.

“But currently, this has to be configured for each individual door,” Persson explains. “With AI, you can imagine a system that continuously analyses event

logs, learns what’s normal, and automatically raises alerts when something unusual occurs.”

He believes AI will make access control systems both simpler and more intuitive. A typical example is in reception, when a visitor arrives and needs temporary access.

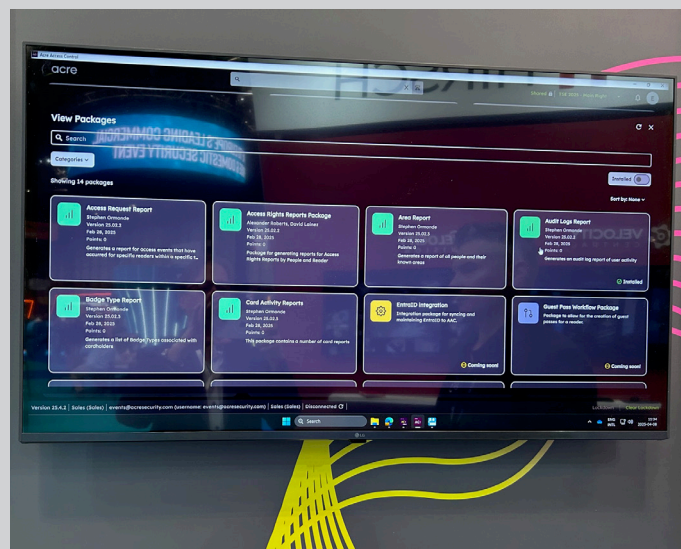
“Currently, the receptionist has to check the calendar, decide when the person should have access, and determine which doors to open – a multi-step process. Access control systems are rarely user-friendly, often designed by engineers for engineers,” Persson says.

With AI, such tasks could become effortless.

“For instance, if you tell the AI that a visitor should have access

” You might ask the AI to show who has accessed certain buildings during a given period – or, conversely, identify users who haven’t accessed specific areas for months, indicating their credentials might need to be revoked.”

to the lobby and conference room for the next two days, it can instantly generate the required script and implement it in



Acre Access Control is Acre Security’s latest major launch – a cloud-based access control platform offering a comprehensive suite of packaged SaaS services.

real time – no technical training required.”

Faster, smarter reporting

One of AI’s strongest advantages in access control is its ability to quickly generate customised reports.

“You might ask the AI to show who has accessed certain buildings during a given period – or, conversely, identify users who haven’t accessed specific areas for

months. You could, for example, ask for a list of everyone over 35 who entered a specific door within the last 52 weeks – and the AI will instantly provide it in your preferred report format.”

AI as a Security Consultant

Persson also envisions AI acting as a virtual security consultant – analysing the entire access control infrastructure and suggesting improvements.

“You could ask the AI to review how the system is structured compared to how it’s actually being used, and then recommend enhancements,” he says. “It might identify that too many employees have access to unnecessary areas, or that a high number of temporary visitors and contractors are entering the site. Based on this, it could suggest creating new user groups, adjusting access levels, or other security improvements.”

He believes the potential of large language models in access control is still largely untapped.

“Because it’s an AI, new pos-

Control Systems



Daniel Persson, Business Development Director – EMEA/APAC at Acre Security, is convinced that AI will make access control systems more user-friendly.

” With AI, you can imagine a system that continuously analyses event logs, learns what’s normal, and automatically raises alerts when something unusual occurs.”

sibilities will emerge – and users themselves will likely discover use cases we haven’t even thought of yet.”

Human oversight still essential

Persson is careful to stress that AI

does not make decisions on its own.

“It must be told what to do – whether that’s to trigger an alert, send a message, or initiate a lockdown,” he explains. “These escalation chains require human decision-making. AI doesn’t replace that.”

He continues:

“We can’t assume AI will solve everything. You still have to tell it what to look for. If someone who normally comes to the office five days a week suddenly stops showing up, the AI can detect it – but it won’t know if it’s something

that needs reporting. You have to define what’s important. You could say AI knows everything, but it doesn’t know what you want to know. Just like with ChatGPT, it’s all about asking the right questions.”

The role of physical security systems

Smart buildings are no longer defined solely by energy efficiency, automation or connectivity. At their core lies another crucial component: physical security systems. Access control, video surveillance and related technologies are evolving from being standalone protective measures into integrated parts of the smart building ecosystem.

According to a report from market analysis firm Memoori, the global market for the Building Internet of Things (BIoT) is expected to grow from USD 64.1 billion in 2024 to USD 101.0 billion in 2030, representing a compound annual growth rate of 7.87 per cent – significantly lower than the historical growth rates of 10–16 per cent.

A software-oriented trend

According to James McHale, market analyst and founder of Memoori, the category Data Integration, Analytics & Software represents the largest and fastest-growing segment, with a growth rate of 9.53 per cent.

“This shows that the market is increasingly focusing on software-defined value rather than hardware,” he comments.

The importance of security

As properties adopt IoT, cloud and AI technologies to create safer and more efficient environments, physical security systems ensure these digital ecosystems remain robust. They protect people, assets and operations – while also providing data that enhances building performance. Without strong access control and video surveillance, the promise of ‘smartness’ risks being undermined by vulnerabilities.

A business resource

James McHale, founder and CEO of Memoori, stresses that security has long been seen as a necessary evil rather than a strategic tool – but that is changing.

“Security has largely been viewed as something you must have to gather evidence when something happens, and therefore not directly contributing to ROI.

But with IoT, security providers now have the opportunity to be more involved in the organisation’s operational processes.

This reflects a shift where security in smart buildings is no longer seen merely as a protective tool, but as a resource for business value creation.”

Security as a major component

Although energy optimisation and automation often dominate the discussion around smart buildings, the physical security industry actually accounts for one of the largest shares of investment. According to Market.us, 50–60 per cent of the installed technology in smart buildings consists of physical security systems – mainly access control and video surveillance.

Services make up an even larger part of the ecosystem: the Security Industry Association estimates that the value of services such as remote monitoring and maintenance reached nearly USD 300 billion as early as 2022 – underlining how central security is to both operations and budgets in smart buildings.

Gatekeeper and data source

Modern access control is far more than keys and locks. Digital identities – ranging from mobile apps to biometric solutions – enable property owners and operators to grant, revoke and monitor access in real time.

- **Operational efficiency:** Logs provide insights into space utilisation and occupancy.
- **Security and resilience:** Lost credentials can be immediately deactivated.



Without robust access control, video surveillance and intrusion detection, a building’s ‘smartness’ risks being undermined by vulnerabilities.

- **User experience:** Smooth, contactless solutions increase convenience, particularly in high-traffic environments.

In smart buildings, access control is therefore not only a security feature – but also a tool for optimising resource use and improving user experience.

From surveillance to intelligence

Video surveillance is evolving rapidly. According to Memoori’s 2023 market report, the global video surveillance market was worth USD 30.4 billion in 2022 and is expected to reach nearly USD 45 billion by 2028.

Growth is largely driven by AI and edge analytics, which make systems more proactive and intelligent. Memoori predicts that by 2028, more than half of all network cameras will have built-in AI capabilities. This enables real-time detection of anomalies, intrusions or safety risks. When integrated with access control, every entry event can also be visually verified – enhancing accountability and reducing false alarms.

Integration with other building systems

The real strength of physical security in smart buildings lies in interoperability. When security systems are linked with, for example, ventilation, lighting, visitor management or alarms, they become part of a co-ordinated and responsive ecosystem. For instance:

- Lighting and ventilation can automatically adjust based on occupancy data from the access control system.
- In an emergency, lockdowns or evacuation procedures can be automatically triggered through the



James McHale, market analyst and founder of Memoori.

in smart buildings



Physical security systems are enablers of smarter, safer and more efficient buildings.

surveillance system.

- Visitor management can be made smoother without compromising security.

According to James McHale, it is important for security system vendors to “blur the boundaries” between physical security and smart building IoT to fully capture the opportunities that smart buildings present.

“Those who fail to adapt risk being left behind,” he says.

Open standards as a prerequisite

A key factor in this development is the use of open standards. Proprietary systems may offer short-term functionality but often lead to lock-in, high lifecycle costs and limited integration.

- **Future-proofing:** Technologies based on open standards – such as ONVIF for video surveillance, BACnet for building automation and OPC UA for secure, platform-independent communication between machines, sensors and IT systems.

- **Flexibility and scalability:** Property owners can replace or expand parts of the system without being tied to a single vendor.

- **Innovation and security:** Open ecosystems drive development and allow vulnerabilities to be identified and addressed more quickly.

With the growing cyber threat, standardisation and security have become inherent components of smart building infrastructure.

IoT and increased security requirements

In Memoori's report IoT Platforms in Smart Commercial Buildings

2025 to 2030, the number of IoT devices in commercial buildings is estimated to grow from 2 billion today to over 4 billion by 2030. With this rapid growth come risks: over 80 per cent of organisations report IoT-related security incidents.

As more devices become connected and physical security becomes increasingly intertwined with IT and IoT infrastructure, robust frameworks – such as Zero Trust, NIST and ISO/IEC 27001 – are critical to safeguarding smart building ecosystems.

Security and trust

While integration and intelligence bring significant benefits, privacy and data protection must not be overlooked. Clear policies, secure data management and compliance with regulations – such as GDPR, the EU's NIS2 Directive, and the upcoming Cyber Resilience Act (CRA) and AI Act – are essential to building trust in smart environments.

Contributing beyond security

Physical security systems are no longer just “guards at the door” – they are enablers of smarter, safer and more efficient buildings. Access control and video surveillance not only provide protection but also deliver insights, interoperability and resilience.

As Memoori and other market analysts emphasise, the convergence of physical security and smart building IoT is both inevitable and necessary. But for this vision to become reality, the industry must fully embrace open standards. Only then can physical security evolve into the backbone of the smart building era – securing not only places, but the very intelligence that makes them ‘smart’.

Note: The Memoori report “IoT Platforms in Smart Commercial Buildings 2025 to 2030” can be ordered from www.armedia.se (click on **Reports**).

What's on in the Security Industry?

– We keep track of what's happening!



security
WORLDMARKET.COM

– a world-class information source
for the security industry since 1998

www.securityworldmarket.com

armedia
...we are security

AR Media International AB
www.securityworldmarket.com, www.armedia.se

Terrorism and cross-border intrusions



Perimeter protection has become three-dimensional – threats can now also come from the air. In recent months, countries such as Poland, Denmark, and Norway have reported problems with unidentified drones flying over airports and other critical infrastructure.

The perimeter security market size is expected to grow from 78.27 billion US dollars in 2025 to 118.33 billion dollars in 2029, at a compound annual growth rate (CAGR) of 10.9 per cent. The increasing threat of cross-border intrusions is expected to propel the growth of the perimeter security market going forward.

According to The Business Research Company's report Perimeter Security Global Market Report 2025, the market is forecast to grow strongly from 2025 onwards – expanding by 7.9 per cent this year, followed by a CAGR of 10.9 per cent through 2029.

The Perimeter Security Global Market Report 2025 includes revenues earned from providing intrusion detection systems, threat identification, surveillance detection, pattern analysis, barrier systems, and professional security services.

Major trends

Growth during the forecast period can be attributed to the increasing

demand for cyber-physical security integration, cloud-based solutions, scalable systems, and environmental sensors. Major trends include interoperability and integration, predictive maintenance, energy efficiency and sustainability, mobile integration and control, as well as environmental sensors and anomaly detection, according to the report.

Market drivers

The increasing threat of terrorism and cross-border intrusions is expected to propel the growth of the perimeter security market going forward. Cross-border intrusions refer to the movement of a unit, force, or military asset into another country's designated

operational area, territorial waters, or airspace for surveillance or intelligence gathering. These threats are rising as various countries and groups seek to gain power and fulfil their demands. Perimeter security serves as the first line of defence in securing critical assets, information, and people through the use of cutting-edge technology, the report stresses.

Critical infrastructure

According to MarketsandMarkets, the physical security segment accounts for the largest share of the critical infrastructure security mar-

ket and assets against physical threats such as intrusions, theft, and terrorist activities.

Increasing urbanization

According to The Business Research Company's report, increasing urbanisation is also expected to propel the growth of the perimeter security market going forward. Urbanisation refers to the process by which rural areas become urbanized as a result of economic development and industrialisation. Perimeter security enhances safety by establishing protective boundaries and utilising technologies such

” Cross-border intrusions refer to the movement of a unit, force, or military asset into another country's designated operational area, territorial waters, or airspace for surveillance or intelligence gathering”

ket. The dominance of this segment is attributed to the increasing need to safeguard facilities, personnel,

as sensors and surveillance systems to monitor and control access to urban areas.



propel the perimeter security market

Mix of technologies

Perimeter security is often described as a multi-layered system – much like the layers of an onion. Each layer may require different technical solutions, and the need for comprehensive,

reliable data with video surveillance systems that can verify and confirm events.

Laser, lidar, thermal sensors, fence-mounted sensors, infrared sensors, integrated fibre-optic perimeter intrusion detection

tion about an object's location, speed, and trajectory; moving targets can be classified as, for example, a person, car, or truck, and used to visually verify what other technologies have detected.

Anti-drone systems

With the introduction of drones, perimeter protection has become three-dimensional – threats can now also come from the air. This issue has become even more relevant during the war in Ukraine, and in recent months, countries such as Poland, Denmark, and Norway have reported problems with unidentified drones flying over airports and other critical infrastructure.

The global anti-drone market is growing rapidly, with an expected CAGR of 26.5 per cent from 2025 to 2030, primarily driven by escalating security concerns over the unauthorised and potentially malicious use of drones across military, critical infrastructure, and public spaces.

AI and machine learning also enable systems to differentiate between genuine threats and false alarms with greater accuracy"

multi-tier perimeter protection has grown significantly. There is no single solution that fits all applications. In many cases, effective perimeter security combines high-quality sensors that deliver

systems, and perimeter fence detection systems can be used to detect people or objects approaching or breaching the perimeter. Cameras with video analytics can generate informa-

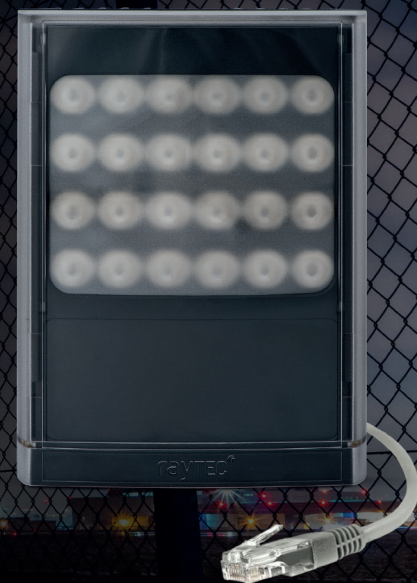
More effective detection with AI

The integration of AI and machine-learning technologies is enhancing market potential, making security systems more adaptable and effective in threat detection and response. AI and machine learning also enable systems to differentiate between genuine threats and false alarms with greater accuracy. As a result, response times are faster, and overall security is more robust.

Intelligent Network Lighting

VARIO2^{iP} PoE

A comprehensive range of Infra-Red, White-Light and Hybrid LED network illuminators



Fully
Programmable

Real-Time
Response

Remote Set-up
and Maintenance

rayTEC[®]
www.raytecled.com

Jimmy Ek, Axis Communications:

Network audio can be used to enhance security

Network audio can have a strong impact on industrial applications according to Jimmy Ek, Nordic Sales Manager at Axis Communications.

"From enhancing security to aiding day-to-day operations, and even improving safety across your factories and plants. This goes for hazardous areas as well, where explosion-protected audio equipment is required", he says.

By now most people are aware of the various ways network audio can be used to bring value to different environments. This could be prerecorded announcements reminding commuters of safety procedures on train stations, messages to shoppers about the latest discounts, or even reassuring students that help is on the way following an incident on a school or university campus. However, Axis Communications

physical speaker wiring (circuits) there is less risk of complications when trying to identify an issue. In a network audio system, every individual speaker is addressable and monitored over the network. This means, end users can use IP based health monitoring and configuration of the complete system. If there is a problem, there is an easy way to find out and have the tools to take immediate action.

Jimmy Ek says: "Your operators

Thermal cameras equipped with analytics spot intruders as soon as they enter the scene. A horn speaker is triggered to play a prerecorded message warning the perpetrators that law enforcement is on the way, causing them to retreat"

emphasises there are just as strong and impactful use cases for audio in critical infrastructure and industrial plants.

Differences between network audio and traditional systems

Network speakers are all-in-one audio systems, 100 per cent IP end points and connect to the standard network, which makes installation, configuration and management simple – without the need for dedicated audio cabling. You only need a single cable for both power and connectivity. Without

can remotely monitor the entire system more efficiently and quickly identify and address any issues which arise, resulting in a system you know works as intended. In turn, this helps reduce downtime and improves solution efficiency, positively contributing to your business' success."

A surveillance system can be set up to activate a pre-recorded message when it detects indications of undesirable activity. Additionally, it can be configured to trigger alerts that tell operators to visually assess a situation and then speak directly to the individuals involved via the



Jimmy Ek, Nordic Sales Manager at Axis Communications.

speakers. Network audio solutions can also be set up to divide premises into zones. Instead of broadcasting a message to all areas, messages can be tailored depending on the location. This is all handled within the audio management software.

Defending the perimeter against intrusion

According to Axis Communications, audio solutions are only one part of the arsenal implemented to ensure the security of a critical site: Network cameras equipped with analytics also play an important role in spotting and investigating adverse activity, but audio can support by actively deterring intruders' intent on causing damage or theft.

Jimmy Ek says: "Thermal cameras equipped with analytics spot intruders as soon as they enter the scene. A horn speaker is triggered to play a prerecorded message warning the perpetrators that law

enforcement is on the way, causing them to retreat. As a result, damage to company property has been avoided, saving not only money and time, but also ensuring production continuity."

Audio helps enhance operational efficiency

Although intrusion deterrence is a main use case for audio, there are other areas within the industrial environment which can also benefit, Jimmy Ek stresses.

"For example, minimizing disruption to your production line is crucial to ensuring that there are no delays in delivering products to customers. You can use audio solutions, such as voice messages to notify relevant staff of overheating or malfunctioning equipment or process errors like jammed products on conveyor belts, enabling them to quickly intervene", he says.

If the environment is noisy, it

and operations in industrial sites



Network audio can be configured to trigger alerts that tell operators to visually assess a situation and then speak directly to the individuals involved via the speakers.

can be hard to hear speaker messages; in these cases a strobe siren could act as a visual alert to notify staff that an anomaly has been detected.

Jimmy Ek says: "Adding audio to your toolkit ultimately means less unwanted downtime, more efficient and ongoing production processes and less material loss."

Minimizing incidents by supporting safety procedures

Maintaining the safety of workers in an industrial environment is an absolute priority, with every process and area closely evaluated to identify and minimize risks. Even trained and experienced personnel can be involved in accidents, and according to Axis Communications, the use of network audio can help remind the workforce of

safety procedures.

"For example, you can set automated messages to alert people that they are entering restricted or dangerous areas after they have been detected by a camera equipped with intelligent analyt-

” Ultimately, the beauty of this solution lies in its functionality in a variety of scenarios eliminating the need for compromise or investment in separate system.”

ics. This quick intervention can make all the difference by avoiding accidents, supporting workers' health and reducing downtime", Jimmy Ek says.

Also, health and safety reminders, such as wearing the correct PPE can ensure that their health is being prioritised.

Complement the certified evacuation system

However, accidents and emergencies do occur in industrial sites, and these can have disastrous consequences. The main priority is evacuating all personnel to

where permitted.

Jimmy Ek says: "This offers the agility needed to guide personnel if the situation changes or rapidly declines, improving efficiencies and potentially saving lives. However, it should be noted that these systems act to complement the certified evacuation system in place."

Network audio adds value

Considering the complexity of industrial environments, Axis Communications believes network audio solutions can be used to bolster security, streamline processes, improve efficiencies and ensure worker well-being.

"Ultimately, the beauty of this solution lies in its functionality in a variety of scenarios eliminating the need for compromise or investment in separate system", Jimmy Ek concludes.

safety as quickly as possible, and surveillance technology can be useful in these critical situations, Axis Communications stresses. A combination of speakers and cameras can be valuable in assessing the situation while broadcasting live or prerecorded messages to support the evacuation efforts,

How modern technology safeguards

Train derailments and accidents cost both money and lives. That is why companies and governments across Europe are keen to make transport tunnels safer.

“Modern laser detection sensors can see in complete darkness, strong sunlight, and artificial light, and are unaffected by the train’s bright headlights, reflections on tunnel walls, or other trains passing through”, says Eelko Griepink, Area Sales Manager for Benelux and Northern Europe at Optex.

Tunnels are a vital part of Europe’s transport infrastructure, connect communities, and contribute to the overall economy and competitiveness of the single European market. And as tunnels have become more complex, so too has the technology required to protect them, according to Eelko Griepink.

Tunnels are getting longer and deeper

More transport systems are being built in underground tunnels each year in order to reduce the effect of noise and pollution on people’s lives and the environment. And these tunnels are getting longer and deeper. For instance, the tunnel from Randabreg to Bokn in Rogaland County, Norway, is 26.7km long and 392 metres deep under water, and the Fehmarnbelt tunnel between Germany and Denmark, once complete in 2029, will be the world’s longest underwater tunnel and create a direct corridor from Northern to central Europe.

“Without these tunnel networks, economies may falter. Railway incidents, for example, can be costly. In December 2023, a fully loaded iron ore train derailed at Vassijaure Station near the Swedish-Norwegian border on the Malmabanen line, a critical route for Sweden’s largest mining company, LKAB. The line was not reopened until 20 February 2024, but it closed again just days later,

following a second derailment, and remained closed until early March”, says Eelko Griepink.

This disruption had a significant impact, with LKAB reporting daily revenue losses of 8.8 million Euro during the closures. Similarly, when part of the Alpine network, the Mont Blanc tunnel, closed following a fire in 1990, the Italian economy lost an estimated 300 to 450 million Euro per annum until it reopened three years later.

More than 800 deaths each year

Whilst such large-scale incidents are rare, smaller ones are not. European Railway safety statistics reveal there were 1,567 significant railway accidents in 2023 with 841 lives lost and 569 people seriously injured. Over half (58.4 per cent) of fatalities were trespassers – typically vagrants (setting up tents in tunnels), vandals, or graffiti artists, according to Eelko Griepink.

Even if there is no injury or loss of life, vandalism can cause derailments, collisions and fires, all of which is costly. In one year alone there were 3,559 acts of vandalism and graffiti on Spanish railways, of which 729 attempts were stopped. Such incidents cost Spanish Renfe roughly 25 million Euro annually, Deutsche Bahn spends 12.1 million Euro, and Brussels’ SNBC around 6 million Euro cleaning graffiti off rolling stock.



Eelko Griepink, Area Sales Manager for Benelux and Northern Europe at Optex.

“These incidents are not as economically damaging as the Mont Blanc fire, but show that protecting the railways and the trespassers is both expensive and challenging”, says Eelko Griepink.

From CCTV to smart surveillance

Accurately detecting a person in the confines of a tunnel is challenging enough by itself and is only made more difficult when several trains are using the tunnels at the same time.

For around 50 years, CCTV has been used to monitor tunnel entrances and exits. But early systems needed security teams to constantly watch between 12 to 24 camera feeds on a single screen. Thankfully, video analytics was created and overcame some of these challenges. A trespasser will instantly trigger an alert which directs the security teams to the appropriate camera feed, who can then immediately decide what action to take.

“The technology, though, has to keep evolving. Trespassers have learnt that they can go undetected by moving towards or entering the tunnel as the train is passing or deliberately alter their appearance to fool the analytics software. The heat and humidity inside tunnels can adversely affect many older technologies, and radar or microwave technology struggles to filter the noise and false alarms generated



by the train, and so they fail to provide adequate detection”, says Eelko Griepink.

He points out that Optex’s Redscan sensors operate reliably at temperatures as low as -40°C and modern laser detection sensors are unaffected by humidity, temperature, or lighting conditions.

Eelko Griepink says: “Equipped with intelligent sensing analytics, the Lidar technology does not depend on visible light or thermal spectrums, which is useful when tracking a person or animal from the lit tunnel entrance to inside and further along the tracks or in the shadows. They perform remarkably well even during heavy snowfall that alters the apparent ground height and light levels.”

Accurate detection

Tunnels located in isolated regions need accurate detection because a false alarm is costly in time and effort if security services are called out unnecessarily. More advanced detection sensors, such as Optex’s Redscan series, use dynamic event filtering to accurately identify human trespassers.

Europe's transport tunnels



With intelligent sensor analysis, lidar technology is not dependent on visible or thermal light, making the method effective for detecting people or animals in the illuminated tunnel mouth as well as further into the tunnel and along the track.

When monitoring a tunnel entrance, specific detection criteria or logic is applied to establish different detection zones, the sequence of alarm triggers, and the size of an object, which in combination can determine whether a train, a person, or a group of people is entering the tunnel.

"Redscan Lidar sensors can detect objects across eight different zones and an area of 100 metres. They can be configured to recognise objects larger or smaller than a defined size; for example, they can ignore trains while detecting people or overlook small rocks but identify boulders", says Eelko Griepink.

If a person or group is detected, the control centre and train driver are alerted, allowing the train to slow down or stop to avoid a striking a person, a large wild animal or an obstruction. Additionally, since the sensors continuously scan the area, security teams receive the precise x,y coordinates of any detected object, enabling a rapid response.

Dark and dirty

Train tracks, when cleaned, throw up a considerable amount of metal and oil into the air, which, like pollution from diesel fumes, can coat or potentially damage the cameras and sensors. Dirty cameras or sensors cannot detect intruders or incidents, so they need to be cleaned.

Eelko Griepink says: "The latest sensors from Optex feature an algorithm that continuously meas-

ures the return or reflection of the laser signal, tracking the percentage of the unit's window that is soiled. Once a certain level of soiling is reached, security personnel are notified."

Optex has also developed a special self-healing foil for laser sensors used in underground tunnels, which protects the laser window from dust, metal fragments, oil, and other pollutants. These sensors can reduce the frequency of security personnel's trips to tunnels in remote locations, helping to lower operating and maintenance costs.

“Trespassers have learnt that they can go undetected by moving towards or entering the tunnel as the train is passing or deliberately alter their appearance to fool the analytics software”

Eelko Griepink says: "Sensors are often adapted for different environments and various uses, so the

correct choice of sensor is essential to the design of any tunnel security system."

Designing the right system
Designing the right security

system begins with a survey of the site and an estimate of how many cameras and sensors are needed for the size of the tunnel to ensure sufficient coverage. The quality and amount of light at the openings and along the tunnel will help determine whether dynamic filtering sensors are needed because they will be unaffected by trains passing or light bouncing.

In most average European rail tunnels, for example, laser sensors are installed on both sides of the track. With larger tunnels, there is usually a third set of sensors in the middle between the tracks. Ultimately, finding the right solutions and combination of technologies that are fit for purpose will vary from tunnel to tunnel, according to Optex.

Eelko Griepink concludes: "But continued development and advancement of new technologies can only help to enhance safety and ensure Europe's critical tunnels remain open."

Callum Ryder, Product Manager at Raytec:

The right lighting is crucial for perimeter protection

For perimeter applications using for example IP cameras, PIR sensors, laser detectors and fibre optic fence sensors, specifying an IP enabled illuminator capable of providing an automated lighting response, is essential, according to Callum Ryder, Product Manager at Raytec.

“If a PIR sensor detects movement from an intruder, an alarm could be raised to automatically turn on the white-light or put the lamps into deterrent mode”, he says.

From critical infrastructure to private property, perimeter protection systems are used in a wide variety of applications. According to Raytec, all tend to have common security goals: they are deployed to restrict access, detect and deter crime and protect important assets. And there are key things to consider when specifying an illuminator for use as part of a perimeter protection system.

Infrared and white light

Infrared (IR) illumination is the most common type of light used around a perimeter fence line. IR emits zero light pollution (so not to disturb the surrounding area), but crucially, it allows the camera to capture night-time images covertly, without alerting potential intruders or giving them light to work by, Raytec stresses.

Callum Ryder says: “Once the camera has detected an intruder, the site may choose to raise an alarm. This is where white-light is often deployed; automatically triggered as a flashing deterrent to ward off an intruder, or used to provide accurate positive identification of the intruder.”

He emphasises only using white-light when it is needed ensures light pollution is kept to a minimum while still providing optimum levels of security. In some instances, white-light may still be chosen to illuminate the entire perimeter, but due to light pollution, and the fact that the camera is more receptive to IR, means

white-light is often preferred as a deterrent.

Hybrid

Hybrid illuminators provide an all-in-one solution, combining both IR and white-light into a single unit. This means one illuminator can be used for both covert surveillance, and as a white-light deterrent. Hybrid allows the user to control the wavelength and switch seamlessly between IR and white-light.

Quality and distance

Perimeter fence lines often cover large areas, so distance and coverage of an illuminator is one of the main things for a specifier to consider. However, it is also equally important to consider how the illuminator will assist the camera in obtaining the highest quality images, Callum Ryder stresses.

“Illuminators able to deliver longer distances may allow cost savings by reducing the total number of illuminators across the site. It may also allow the user to reduce costs in terms of the numbers of cameras, lighting columns, cabling and other ancillary equipment needed as part of the installation”, he says.

Hardware integration

For perimeter applications using IP cameras, passive infrared sensors, laser detectors and fibre optic fence sensors, specifying an IP enabled illuminator capable of providing an automated lighting response, is



Vario2 is Raytec's range of LED illuminators designed to enhance the performance of any security system.

essential, according to Raytec.

“For example, if a PIR sensor detects movement from an intruder, an alarm could be raised to automatically turn on the white-light (so the intruder can be positively identified) or put the lamps into deterrent mode (to ward off the intruder)”, Callum Ryder says.

Software integration

Raytec believes it is important to choose an illuminator which can be integrated with the security management platform in use by the site.

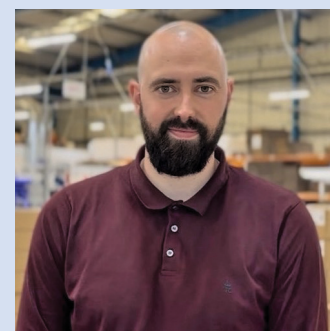
Callum Ryder says: “For example, if a site is using Milestone’s Xprotect platform, the chosen illuminator should be capable of being integrated into that system, so it can be controlled easily and lighting responses set-up to be triggered by other detection devices.”

Camera analytics

Cameras with video analytics are often used as part of a perimeter surveillance system. Lighting plays an important role in helping the cameras to provide a consistent, clear image.

One way to help ensure a good image is to select an illuminator which uses technology which reduces hot spots and provides an even image across the entire scene.

“Camera analytics will often require increased light levels



Callum Ryder, Product Manager at Raytec.

compared to standard applications. Even the best cameras will still produce noisy images in darkness that will seriously impact the performance of camera analytics and create false alarms. No light, no camera analytics”, says Callum Ryder.

Lighting design

According to Raytec, lighting design should be considered an essential part of specifying lighting for a perimeter security application.

“Undertaking a lighting design helps to ensure the correct light levels are achieved across the site and are essential for cameras to be able to capture high quality images. For an installer, a lighting design also provides a useful reference which becomes an important document during the installation and commissioning process”, Callum Ryder concludes.

www.skydd.net

SKYDD 2026

The Nordic region's largest trade fair for the security industry
Don't miss the chance to be a part of the biggest security event of
the year!

SKYDD



**TOTAL
FÖRSVARSMÄSSAN**

OCTOBER 20-22 2026

TOTALFÖRSVARSMÄSSAN

Gathers Sweden's leading stakeholders in civil
and military defence – from authorities and companies
to voluntary organisations – to showcase solutions, create
dialogue and build resilience.

● ||| ◀ ▶ **STHLM SMÄSSAN**

AR Media International and Detektor celebrate 35 years



AR Media International was founded in 1990 – the same year the first issue of Detektor magazine was launched for the Swedish market. Founder Lennart Alexandrie reflects on three and a half decades of innovation, challenges and milestones.

When asked about this 35-year journey, the publisher answers almost instinctively:

“Being part of such a dynamic industry has been incredibly exciting. I’ve also had the privilege of working with a fantastic team whose competence and dedication have continuously driven AR Media’s development forward.”

“I’ve been fortunate to work together with our Sales Manager, Deniz Baykal, for 27 years and with our Production Manager, Marika Thelenius, for 32 years. Continuity and stability are so important for a company – especially in an ever-changing world.”

Early challenges and breakthroughs

AR Media began during an economic recession but survived by attracting international manufacturers who were willing to support their Swedish distributors’ advertising in Detektor, which at that time focused solely on the Swedish market.

“It meant a lot of travelling across Europe to fill the distributors’ advertising budgets – usually by train, which was by far the cheapest way to travel back then,” recalls Lennart Alexandrie.

Educational book and digital expansion

Among the company’s early achievements was the publication of the educational book *Svensk Säkerhet* (Swedish Security), which was used in security training for over a decade, as well as the launch of the digital news portal *Securityworldmarket.com* in 1998.

Securityworldmarket was the first online publication in the security industry providing daily

news updates.

In 2001, the compact security event Sectech was introduced in Sweden, further strengthening the company’s position within the industry.

Pioneering publications

Detektor was also the first publication to report on network-based video surveillance after a visit from Axis founder Martin Gren, who demonstrated the world’s first network camera.

“Many in the industry were upset when we predicted a bright future for IP-based technology – but we were right,” Alexandrie recalls.

The company also coined the term Security as a Service (SECaaS) in 2007 – a concept that is now widely used across both the digital and physical security markets.

Advocacy and influence

Through their think tank SNOS, founded in 2011, AR Media worked to promote more liberal camera surveillance laws in Sweden. They introduced new terminology such as security camera and safety camera to replace surveillance camera, helping to shift both public and political perceptions of the technology.

The conference The Safety Camera Day brought together industry leaders and politicians to discuss privacy and public safety.

“The event played a key role in influencing legislation,” says Alexandrie.

SNOS also commissioned independent meta-studies demonstrating the crime-preventive effects of cameras – research that was later used as a foundation for government reforms.

When the government intro-



The founder and publisher of AR Media International – Lennart Alexandrie – looks back on 35 years in the security trade publishing and events business.



A well-known face. Sales Manager Deniz Baykal has been with AR Media for 27 years.



Production Manager, Marika Thelenius, the backbone of AR Media, since 32 years.

duced a new, much more permit-friendly law on the use of camera surveillance, SNOS was appointed as one of the consultation bodies.

Recognition and industry leadership

In 2005, *Securityworldmarket.com* and Detektor were ranked as the most recognised and regularly used security trade media in EMEA and Scandinavia. Behind the report was the highly respected market analysis firm IMS Research. The results were based on a global survey sent to 600 security professionals.

“Our media brands were also ranked among the top in the UK and North America, which made us incredibly proud. To achieve that level of recognition within just a

few years exceeded all our expectations,” says Lennart Alexandrie.

AR Media was also a driving force behind the creation of a unified Swedish security industry organisation. Through their media platforms, they strongly advocated replacing the former trade body with a more proactive organisation. When that transition took place, Alexandrie became one of three independent industry experts in the reference group that – together with leaders in the security industry – went on to found *Säkerhetsbranschen* (the Security Industry Association).

“It was a very exciting time – to be part of shaping a stronger voice for the Swedish security industry,” he concludes.

IoT Platforms in Smart Commercial Buildings 2025 to 2030

– get the latest market research and investment analysis report



**Order the report online
from AR Media NOW**

This new 2025 report from Memoori provides an in-depth and objective analysis of the Internet of Things (IoT) Platforms market for Smart Commercial Buildings from 2022 to 2030. It offers detailed insights into the evolving ecosystem of IoT platforms, architectural trends, vendor positioning, and strategic roadmaps across key market segments.

Why do you need this report?

- Explore the fragmented and rapidly evolving smart building IoT platform landscape, with clear market forecasts under three scenarios to 2030.
- Understand competitive dynamics and platform functionality through a unique ecosystem mapping and detailed vendor comparison.
- Gain actionable recommendations tailored for various stakeholder groups to help align technology investments with measurable business outcomes.
- Access comprehensive data resources including high-resolution charts and spreadsheets that support strategic decision-making in deploying IoT platforms in commercial real estate.

Order the report on www.armedia.se – click on Reports – or contact us at info@armedia.se

armedia
...we are security

AR Media International AB, Elektravägen 14, 126 30 Hägersten, Sweden, Tel: +46 8 556 306 80, info@armedia.se, www.armedia.se

ASSA ABLOY

Your Go-To Resource for Industry Insight

**6th
biennial
edition!**



Discover what's next for wireless access control.



Get your copy

Experience a safer
and more open world



Photo: Camilla Svensk

The Detektor magazine's editor-in-chief, Lennart Alexandrie (left in the picture), congratulated the first prize winners: Niclas Gustafsson (Apstec Systems), Philip Svensson (HID), Frida Hjortronsteen (Axis Communications), and Maryam Moassesi (Suprema).

Detektor International Award 2025

Celebrating four top winners and eight outstanding achievers

On October 14, the winners of the 2025 Detektor International Award were announced during a gala dinner at Stockholmsmässan, coinciding with the opening day of Sectech, the compact pan-Scandinavian trade fair event.

Established in 2000, the Detektor International Award is one of the most prestigious and recognised prizes in the security industry.

"With this award, we aim to highlight solutions that represent true innovation and deliver significant customer benefits," said Lennart Alexandrie, editor-in-chief and founder of Detektor magazine.

Independent award

The Detektor International Award is not an accolade that manufacturers can apply for. The selection process is entirely independent, conducted by the editorial team at Detektor, who actively search for innovative products and solutions through their news reporting and attendance at industry trade shows. Submitted products are evaluated

before deciding which 12 solutions are nominated as finalists.

Four product categories

The Detektor International Award features four categories:

- Alarm & Detection
- ID & Access Control
- Video Surveillance
- IoT & Security Solutions

Members of the award jury from five countries

The winners are selected by a jury consisting of eight members from Detektor's editorial board. The jury includes editors from Sweden, Norway, Denmark, the UK, and Taiwan.

Alarm & Detection – the overall winner

The first prize in the Alarm &

Detection category was awarded to **Apstec Systems** from Sweden for their *HSS Falcon*, a solution for real-time screening and threat detection of people and items, protecting crowded spaces without disrupting the natural flow of people.

ID & Access Control – the overall winner

The first prize in the ID & Access Control category went to **HID Global** from USA for *HID Amico* – biometric facial recognition readers that delivers secure, fast, and contactless access.

Video Surveillance – the overall winner

In the Video Surveillance category, **Axis Communications** from Sweden took the first prize for their *Axis Q1728-LE Block Camera*. It is the world's first ARTPEC-9 chip-powered camera and offers superior image quality, advanced AI analytics, efficient AV1 compression, and robust cyber security.

IoT & Security Solutions – the overall winner

Suprema, a South Korean company, received first prize in the IoT & Security Solutions category for their *Q-Vision Pro*, the world's first AI module on-device to prevent financial crimes at ATMs.

Innovative Achievement Award

In addition to the first prize winners, eight other companies received the Innovative Achievement Award during the ceremony.

In the Alarm & Detection category, **Artifel** from France was recognised for its *Check'In Infra*, a smart alarm system that protects isolated technical infrastructure sites. They shared the award with Swedish manufacturer **Alarmtech**, recognised for their *MCX 270* – a high-security intrusion detection solution for explosive environments.

In the ID & Access Control category, **Salto Systems** from Spain was awarded for the *Salto XS4 Face*, alongside **Pacom Group** from Sweden which received rec-

Alarm & Detection



Photo: Camilla Svensk

Artifeel Alain Staron, Apstec Systems Niclas Gustafsson and Alarmtech Anders Henning were the award recipients in the Alarm & Detection category.

ID & Access Control



Photo: Camilla Svensk

The three winners in the ID & Access Control category were from Pacom, Mårten Gunnarsson, HID, Philip Svensson and Salto Dennis Postol.

IoT & Security Solutions



Photo: Camilla Svensk

Stefan Albertsson, Addsecure, Maryam Moassesi, Suprema and Tor Kenneth Gibbs Bergland from Hanwha Vision represented the award winners in the IoT & Security Solutions category.

ognition for the Vigil Core v.11.0 platform.

In the Video Surveillance category, German manufacturer **Keenfinity Group** received the award for their Bosch Dinion thermal 8100i thermal camera, while **I-Pro** (from Japan) shared the honour for their High Zoom Bullet Camera.

Finally, in the IoT & Security Solutions category, **Addsecure** from Sweden was honoured for its unified platform that streamlines transport operations, Fleetvision, alongside **Hanwha Vision** from South Korea, which received recognition for the Dual-Lens Barcode Reader Camera – a 4K dual-sensor camera with AI-

Video Surveillance



Photo: Camilla Svensk

The winners from I-Pro Brian Møller, Axis, Frida Hjortronsteen and Keenfinity Björn Admés won the Video Surveillance category.

powered barcode scanning.

Twelve great solutions

Even though the Detektor International Award selects an overall winner, Detektor International's editor-in-chief Lennart Alexandrie emphasised that all three nominated manufacturers in each category should be seen as winners.

"Every year, we report on hundreds of product innovations in our media. We have selected twelve products and solutions that meet our criteria for innovation and customer benefits. Therefore, all twelve nominated manufacturers are winners and rightful recipients of the Detektor International Award," he noted.

Detektor International Award 2025

– The winning products and solutions

Alarm & Detection

The overall winner 2025

HSS Falcon by Apstec Systems (Sweden)



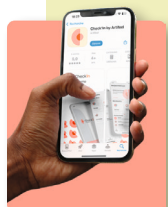
HSS Falcon is a security screening system enabling high-capacity, real-time screening of both people and handheld items. The system stands out by detecting a wide range of threats – including explosives, weapons, pyrotechnics, narcotics, and cash – while ensuring a fast and seamless process. It identifies and distinguishes knives, long-bladed weapons, and various metallic or semi-polymer firearms from everyday objects.

THE JURY'S MOTIVATION: "HSS Falcon's speed and accuracy in protecting crowded spaces – without disrupting the natural flow of people – sets a new benchmark for threat detection. It proves how innovation can both enhance security and safeguard the openness of society."

The Innovative Achievement Award 2025

Check'In Infra by Artifeel (France)

MCX 270 by Alarmtech (Sweden)



Check'In Infra from Artifeel is a compact autonomous alarm system developed to protect technical infrastructure from intrusion, particularly installations located in exposed environments (for example, remote sites or underground). No Wifi or power connection is required, Check'In Infra uses a battery-powered sensor with built-in AI that distinguishes real threats from false alarms and responds with instant notifications and loud alarms.

THE JURY'S MOTIVATION: "With its AI-driven threat detection and resilient dual-SIM connectivity, Check'In Infra enables alarm alerts even for remote and vulnerable technical infrastructure sites. This battery-powered security system stands out as a unique solution."



Alarmtech's MCX 270 is a robust high-security magnetic contact designed to protect, for example, garage and industrial doors, particularly in environments with explosion

risks. ATEX-certified and engineered to resist tampering and external magnetic fields, makes it especially suitable for installations where high operational reliability is required.

THE JURY'S MOTIVATION: "This intrusion detection solution, built for explosive environments, once again proves Alarmtech's robust engineering capability. With its unrivalled reliability in high-risk applications, the MCX 270 demonstrates true innovation, safety, and trust."

ID & Access Control

The overall winner 2025

HID Amico by HID Global (USA)



HID Amico is an advanced biometric facial recognition reader for access control, developed to provide high security, fast recognition, and contactless access. In addition to facial recognition (for distances of up to 2 metres), HID Amico supports cards, PIN codes, QR codes, and HID Mobile Access and offers a web-based registration platform.

THE JURY'S MOTIVATION: "This facial recognition reader delivers secure, fast, and contactless access. By supporting cards, PIN codes, QR codes, HID Mobile Access and wallets, it combines robust multi-factor authentication and raises the standard for modern access control solutions."

The Innovative Achievement Award 2025

Salto XS4 Face by Salto (Spain)

Vigil Core v.11.by Pacom Group (Sweden)



Salto XS4 Face is a biometric access control terminal with facial recognition. The system includes a built-in algorithm, liveness detection which ensures that the system only recognises a live face, not a photo or mask, and it is optimised for both privacy and quick verification. It is available as a cloud-based service.

THE JURY'S MOTIVATION: "This cutting-edge facial recognition solution, featuring built-in algorithms and liveness detection, delivers an outstanding, user-friendly, and fast innovation-driven approach to access control."



The Vigil Core v.11.0 from Pacom Group is a scalable cloud-based security platform combining access control, intrusion detection, video verification, and BMS management. It features role-based access, multi-credential support, elevator control, and visitor management and the user

can instantly access live video feeds for accurate alarm management and real-time event responses.

THE JURY'S MOTIVATION: "By uniting access control, intrusion detection, video verification, and BMS in a powerful, scalable, cloud-based platform, Vigil Core sets a new benchmark for future-ready access control and integrated security management."



Innovation and usability are key priorities for the editorial board of Detektor, when selecting products and solutions for nomination to the Detektor International Award. Here are the 12 products, living up to these criteria in 2025.

Stockholm, Sweden

Video Surveillance

The overall winner 2025

Axis Q1728-LE Block Camera by Axis Communications (Sweden)

Axis Q1728-LE Block Camera is an advanced 4K outdoor block camera and is based on Axis' proprietary Artpec-9 (system on chip) and delivers 8MP resolution and 60fps in 4K. The large 1/1.2" sensor offers extreme light sensitivity, and the camera includes edge-AI analytics and efficient video compression (with support for the open video coding standard AV1), reducing bandwidth and storage requirements.



THE JURY'S MOTIVATION: "This 4K camera sets a new benchmark in outdoor surveillance. Powered by the ARTPEC-9 chip, it offers superior image quality, advanced AI analytics, efficient AV1 compression, and robust cyber security – making it a convincing winning solution."

The Innovative Achievement Award 2025

Bosch Dinion thermal 8100i by Keenfinity Group (Germany) High Zoom Bullet Camera by I-Pro (Japan)

Bosch Dinion thermal 8100i from Keenfinity Group is a thermal camera designed for 24/7 surveillance, also under challenging conditions such as fog, smoke, rain, or snow. It combines high-resolution thermal imaging with built-in AI capacity through IVA Pro Perimeter, which offers AI-based 3D auto-calibration of the detection area and enables detection of moving, crawling, or camouflaged objects at distances of up to 586 metres.



THE JURY'S MOTIVATION: "By combining high-resolution thermal imaging with AI-powered IVA Pro Perimeter analytics, the Bosch Dinion Thermal 8100i delivers remarkable performance even in the most challenging conditions, making it a groundbreaking tool for perimeter surveillance."



High Zoom Bullet Camera, from I-Pro in an outdoor 4K camera with up to 30x optical zoom and powerful infrared illumination reaching up to 250 metres. It is equipped with built-in AI analytics (edge) to automatically identify objects and situations on-site and some models are optimised for

license plate recognition at speeds of up to 130 km/h, while also detecting vehicle model, colour, and country of origin.

THE JURY'S MOTIVATION: "With its 30x optical zoom and an infrared range of 250 metres, the High Zoom Bullet Camera elevates outdoor surveillance to new heights. By combining edge AI analytics with high-speed ANPR, it stands as a true example of innovation excellence."

IoT Security Solutions

The overall winner 2025

Q-Vision Pro by Suprema (South Korea)



Q-Vision Pro is a device with a built-in AI module designed to predict and prevent financial crimes at standalone units such as ATMs. It combines facial recognition with behavioural analysis to detect suspicious actions in real time – without requiring a network connection. It operates autonomously and supports up to 50,000 users and offers robust multi-layer data encryption.

THE JURY'S MOTIVATION: "With its embedded AI module to predict and prevent financial crimes at ATMs in real time, Q-Vision Pro marks a new milestone for Suprema. The combination of facial recognition, behavioural analysis, and robust encryption makes it a truly winning concept."

The Innovative Achievement Award 2025

Dual-Lens Barcode Reader Camera by Hanwha Vision (South Korea) Fleetvision by Addsecure (Sweden)



Dual-Lens Barcode Reader Camera, from Hanwha Vision combines barcode reading and video surveillance in a single device. It is equipped with two sensors (mono and colour, in 4K resolution) and can read multiple barcodes in one frame while simultaneously recording video. With AI-powered label detection, the camera can distinguish codes even on fast-moving conveyor belts, at speeds of up to 2 m/s.

THE JURY'S MOTIVATION: "The Dual-Lens Barcode Reader Camera pioneers the fusion of barcode scanning and video surveillance in a single device. With dual 4K sensors, AI-powered label detection, and excellent performance, this solution sets a new standard for smart industrial operations."

Fleetvision from Addsecure is a unified platform for vehicle and logistics management that helps transport companies handle complexity with clarity and control. By collecting real-time data from vehicles, drivers, and various systems, users gain powerful insights and smoother operations. The platform provides control over vehicles, drivers, and transport operations, including positioning of vehicle locations and working hours reporting.



THE JURY'S MOTIVATION: "By unifying real-time data from vehicles, drivers, and logistics in a single transport management platform, Fleetvision provides actionable insights that enhance efficiency, safety, sustainability, and overall clarity and control of complex fleet operations."



THE OVERALL **WINNER**

ALARM & DETECTION



HSS Falcon

– the solution for real-time screening and threat detection of people and items

The jury's motivation:

*“HSS Falcon’s speed and accuracy in protecting crowded spaces
– without disrupting the natural flow of people – set a new benchmark for threat detection.
It proves how innovation can both enhance security and safeguard the openness of society.”*



www.apstecsystems.com



INNOVATIVE ACHIEVEMENT AWARD
within the category of
ALARM & DETECTION



MCX 270

– the high-security intrusion detection solution for explosive environments

The jury's motivation:

““This intrusion detection solution, built for explosive environments, once again proves Alarmtech’s robust engineering capability. With its unrivaled reliability in high-risk applications, the MCX 270 demonstrates true innovation, safety, and trust.”



www.alarmtechglobal.com



INNOVATIVE ACHIEVEMENT AWARD
within the category of
ALARM & DETECTION



Check'In Infra

– the smart and autonomous alarm system to protect isolated technical infrastructure sites

The jury's motivation:

“With AI-driven threat detection and resilient dual-SIM connectivity, Check'In Infra ensures alarm alerts even at the most remote and vulnerable infrastructure sites. This battery-powered security system truly stands out as a unique solution.”



www.artifeel.com



THE OVERALL WINNER

ID & ACCESS CONTROL



HID Amico
– biometric facial
recognition readers



The jury's motivation:

"This facial recognition reader delivers secure, fast, and contactless access. By supporting cards, PIN codes, QR codes, HID Mobile Access and wallets, it combines robust multi-factor authentication and raises the standard for modern access control solutions."



www.hidglobal.com



INNOVATIVE ACHIEVEMENT AWARD
within the category of
ID & ACCESS CONTROL



Vigil Core v.11.0
– the unified, scalable platform
for security and BMS integration

The jury's motivation:

"By uniting access control, intrusion detection, video verification, and BMS in a powerful, scalable, cloud-based platform, Vigil Core sets a new benchmark for future-ready access control and integrated security management."

PACOM

www.pacom.com



INNOVATIVE ACHIEVEMENT AWARD
within the category of
ID & ACCESS CONTROL



Salto XS4 Face
– the single-source facial
recognition access control solution

The jury's motivation:

"This cutting-edge facial recognition solution, featuring built-in algorithms and liveness detection, delivers an outstanding, user-friendly, and fast innovation-driven approach to access control."

salto 
INSPIRED ACCESS

www.saltosystems.com



THE OVERALL
WINNER
VIDEO SURVEILLANCE



The jury's motivation:

““This 4K camera sets a new benchmark in outdoor surveillance.

Powered by the ARTPEC-9 chip, it offers superior image quality, advanced AI analytics, efficient AV1 compression, and robust cybersecurity – making it a convincing winning solution.”



www.axis.com



INNOVATIVE ACHIEVEMENT AWARD
within the category of
VIDEO SURVEILLANCE



i-PRO High Zoom Bullet Camera
– advanced long-range security with
edge-processed analytics and powerful IR

The jury's motivation:

"With its 30x optical zoom and an infrared range of 250 meters, the High Zoom Bullet Camera elevates outdoor surveillance to new heights.

By combining on-edge AI analytics with high-speed ANPR, it stands as a true example of innovation excellence."

i-PRO

i-PRO.com



INNOVATIVE ACHIEVEMENT AWARD
within the category of
VIDEO SURVEILLANCE



Bosch Dinion thermal 8100i
– the thermal camera featuring
AI-powered perimeter detection analytics

The jury's motivation:

"By combining high-resolution thermal imaging with AI-powered IVA Pro Perimeter analytics, the Bosch Dinion Thermal 8100i delivers remarkable performance even in the most challenging conditions, making it a groundbreaking tool for perimeter surveillance."

KEENFINITY

www.keenfinity-group.com



THE OVERALL
WINNER
IoT & SECURITY SOLUTIONS



Q-Vision Pro

– the world's first AI module
on-device to prevent financial crimes at ATMs

The jury's motivation:

"With its embedded AI module to predict and prevent financial crimes at ATMs in real time, Q-Vision Pro marks a new milestone for Suprema. The combination of facial recognition, behavioral analysis, and robust encryption makes it a truly winning concept."

suprema

www.supremainc.com



Innovative Achievement 2025

INNOVATIVE ACHIEVEMENT AWARD
within the category of
IoT & SECURITY SOLUTIONS



AddSecure FleetVision
– the unified platform that
streamlines transport operations

The jury's motivation:

“By unifying real-time data from vehicles, drivers, and logistics in a single transport management platform, FleetVision provides actionable insights that enhance efficiency, safety, sustainability, and overall clarity and control of complex fleet operations.”

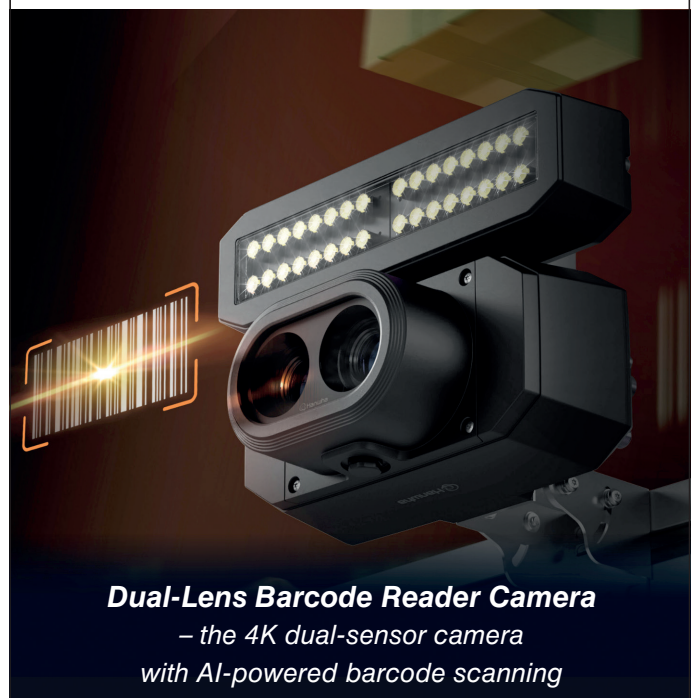
ADD:SECURE®

www.addsecure.se



Innovative Achievement 2025

INNOVATIVE ACHIEVEMENT AWARD
within the category of
IoT & SECURITY SOLUTIONS



Dual-Lens Barcode Reader Camera
– the 4K dual-sensor camera
with AI-powered barcode scanning

The jury's motivation:

“The Dual-Lens Barcode Reader Camera pioneers the fusion of barcode scanning and video surveillance in a single device. With dual 4K sensors, AI-powered label detection, and excellent performance, this solution sets a new standard for smart industrial operations.”

 **Hanwha Vision**

www.hanwhavision.eu

Gerard Figols, I-Pro:

"Cameras will become

Intelligent edge-based video surveillance allows the system to become faster, more scalable and more customer friendly, according to I-Pro Chief Operating Officer, Gerard Figols.

- In the future we will regard cameras as AI agents. They will have power to be able to see, listen, and to understand what is going on. It is important they are continually trained, enhancing their intelligence, which means their algorithms are becoming smarter, he says.

Gerard Figols joined Panasonic in 2007 and was leading curve-out to establish I-Pro in the EMEA Region in 2021. His role has evolved from EMEA to global responsibilities being now Chief Operating Officer.

Can you explain what intelligent edge-based video surveillance means?

"Intelligent edge-based system surveillance means that the camera itself can process and analyse the video data in real time. And that is important. So basically, what it does is analysing the data where the data is created itself. And this is a big difference from traditional systems where video is sent to a server or a cloud platform to be processed. Edge computing not only boosts speed and scalability but also reduces energy consumption and infrastructure requirements. Importantly, it strengthens

privacy by minimizing the transmission of personal data to centralised systems, making GDPR compliance easier."

What is the biggest difference from traditional systems?

"So in those traditional setups, you often need a lot of network bandwidth, and you need a very powerful backend system. Sometimes the response can be delayed because there is latency between the data being sent to the data being analysed. With the edge-based systems like I-Pro is developing, all the AI applications and processes run inside the camera, enabled by a strong AI processor. This allows for real-time alerts and actions – faster, more secure, and more efficient. We believe it is a shift from passive to proactive devices."

Does on-device processing of raw data enhance the precision of analytics?

"Yes, when you analyse the data at the edge, it is the raw data. It allows you to be more accurate, because the image is not compressed. When you compress data, you always lose something. It would be too heavy and costly to transfer all this data to a server and process all the data for many different devices at the same time. What is really important is that by analysing the data directly at the edge, our cameras can send



In 2019, I-Pro became independent from Panasonic.

only the metadata – the key information – rather than the full video stream. This allows the system and the operator to focus immediately on what matters and to make faster, more informed decisions."

What other benefits does at the edge bring?

"It allows the system to become faster, more scalable and more customer friendly – including better privacy and ethical AI use. We are proud to be the first in the physical security industry to achieve ISO/IEC 42001 certification, ensuring our technology is ethically governed by design. Edge computing also increases customer flexibility, letting them scale from one to thousands of devices without needing massive server capacity."

How are AI and machine learning being integrated into your edge surveillance devices?

"We integrate deep learning AI entirely into the camera using a powerful built-in AI processor.

This means that the camera can do more than just record video. It can understand what it sees. For example, I-Pro cameras can detect and classify up to 98 different attributes – the highest in the industry. Users can also customise the camera to their needs, meaning that they can train the camera to detect specific objects or behaviours which are important for them."

How does that work?

"The great thing about this training is that it can be done easily: thanks to our unique on-site learning feature, it can be done by the customer, and it takes just a few minutes. The camera will remember what it has learned, and it will become even better over time. The algorithm is going to be renovated continuously to make sure that the accuracy will keep improving and improving. So, in short, what we are doing is turning the camera into a smart learning device. It understands and helps the operators to make faster and better decisions."



"Edge computing not only increases speed and scalability, but also reduces energy consumption and the need for extensive infrastructure," says Gerard Figols.



AI agents"

What types of video analytics insights can cameras deliver instantly on-site?

"I-Pro AI analytics includes features among others AI video motion detection, speed detection, sound classification, for example gunshots or glass breaking, people counting and occupancy detection. All of these are serverless capabilities and all of them are available free of charge and are helping customers to make faster decisions. This is especially useful in busy environments such as airports, stadiums, venues and retail stores where speed and accuracy are important."

Is there any specific feature that the end users are demanding more often?

"It varies a lot, but we are seeing that the trend is moving into operational efficiency. In the past, it was more related to security itself, but nowadays the cameras are used more and more out of security, in many other fields that can help to improve the operational efficiency by just analysing the video. But it very much depends on the customer and on the vertical. That is why we believe in the open platform. We have our own analytics that we bring in for free, but we have an open platform so any developer can bring their applications into our camera. In addition, we support Docker container environments, giving developers the flexibility to deploy custom AI solutions quickly and efficiently."

Which industries or sectors are seeing the fastest adoption of intelligent edge surveillance, and why?

"There is a bunch of sectors, but if I need to select some, I will say retail, transport, public safety and critical infrastructure. The

main reason is in these industries; you need to respond in real time. In retail, we detect theft, track customer behaviours and manage the store layouts. In transportation, edge devices help monitoring the traffic, identify crowding or suspicious activity and improve the passenger safety and experience. Hospitals use our on-site AI learning to detect ambulance arriving and trigger gate automation. Smart cities and infrastructure projects also benefit from edge technology, as they need systems that are scalable, privacy-friendly and efficient."

Can existing video surveillance systems be upgraded to AI without changing every single camera?

"Yes, and that is a very common request we have been getting since we introduced our first AI-powered cameras. With our AI Processing Relay Application, non-AI cameras do not need to be replaced but can become smart. This application is available for cameras from our X-Series range and can add AI functions to non-AI cameras. In fact, each X-series unit can upgrade up to three additional non-AI cameras, even from other manufacturers. This gives customers a step-by-step, financially efficient upgrade path, preserving their existing investment while adding powerful AI features such as vehicle classification, intrusion detection, or scene change detection. We also offer tools like I-Pro Active Guard, which works with leading VMS to let operators quickly search video using AI metadata – making legacy systems smarter and more efficient."

Finally, which trends do you believe will shape the next generation of intelligent surveillance solutions?



I-Pro's Chief Operating Officer, Gerard Figols.

"One of the most exciting trends we see is generative AI. Until now AI in surveillance has mostly been about detection and classification, like identifying people, vehicles and behaviours. But with generative AI, we are entering a new era where AI can help us understand complex situations, simulate possible scenarios and improve system performance and training accuracy. At I-Pro, we are exploring how generative AI can support incident reconstruction, predictive analysis, and even assist operators by

summarising large volumes of video into meaningful insights. This can significantly speed up the decision making in real time even further. Looking towards the future, we no longer perceive I-Pro cameras merely as cameras. We will regard them as AI agents. They will have power to be able to see, to listen, and to understand what is going on. And for these AI agents, it is important that they are continually trained, enhancing their intelligence, which means their algorithms are becoming smarter."



More visitors, more exhibitors, and more seminar participants – all quantitative boxes were ticked at Sectech 2025 in Stockholm.

Sectech 2025 breaks record

Stockholm, Sweden

Sectech – the compact pan-Scandinavian security event took place on the International Stockholm Fair (Stockholm) – which was held on the 14-15 October – was a huge success, attracting 3,324 visitors and 746 representatives from 124 exhibiting companies. Seminars featuring panel discussions on technology trends in the security market attracted 1,157 participants – also a new record.

More visitors, more exhibitors, and more seminar participants – all quantitative boxes were ticked, just as in 2023. But according to Sectech's project manager Deniz Baykal, from AR Media International, what truly stands out is the positive response from exhibitors and visitors alike.

"There have been so many people, and all the customers and exhibitors who have been here have done a fantastic job with their stands. We are very satisfied with Sectech," she says.

Kertil Stenberg, CEO of Heras, calls Sectech his favourite security exhibition in Scandinavia.

"From the very beginning, we have had a lot of customers and

industry colleagues at our stand. Here, the stands are relatively small, but everyone who is here is an industry professional, both those who are exhibiting and the visitors. This is a fantastic fair", he says.

Record number of seminar visitors

A record number of participants attended the seminar programme. The previous high of 1,090 from 2023 was surpassed, with 1,157 registered this year.

"It is particularly interesting as our programme is anything but broad. It is mainly based on panel discussions around niche technology areas," says Lennart Alexandrie,

CEO of AR Media International and responsible for the seminar programme at Sectech.

The panel on ID management and access control – the opportunities and challenges of digitalisation – attracted the largest audience (148 participants), featuring Daniel Hjort (Nexus Group), Freddie Parrman (Seriline), Märten Gunnarsson (Pacom Group) and Daniel Persson (Acre Security). Other panels also drew large audiences, such as the AI-powered security systems session (128 participants), perimeter protection (118 participants), and biometrics for ID management and access control (115 participants).

More exhibitors

The number of exhibitors also reached a new record. In 2023

there were 115, while this year 124 companies took part.

"We could have accepted even more exhibitors, but we are sticking to our strategy of growing slowly, ensuring the number of exhibitors harmonises with the number of trade visitors. That is one of the core ideas behind the event," states Lennart Alexandrie.

He highlights the fair's compact format as its main strength.

"Sectech 2025 was bigger than ever, but our goal is not to have as many people as possible – it is to have the right quality of visitors, and that has certainly been the case."

AI, cloud solutions, and cybersecurity were the key megatrends on display. From a product perspective, lidar technology showed strong progress, and mobile access

The need for knowledge about security technology is substantial – not only among suppliers but also among end users, who were strongly represented among the seminar participants."



The demand for knowledge about security technology is substantial – not least among end users, who were strongly represented at Sectech.

” There have been so many people, and all the customers and exhibitors who have been here have done a fantastic job with their stands. We are very satisfied with Sectech.”

solutions were also highly visible on the exhibition floor.

Many end customers

Exhibitors gave highly positive feedback, particularly regarding the quality of visitors.

“It has been really busy. We have seen a lot of different types of customers come to our stand –

many channel partners we already work with and new interest from partners across the northern region. In addition, we have seen more end users here this year, and it has been great to engage directly with them,” says Spencer Marshall, Executive Vice President for the UK and Europe at Gallagher Security.

Over 4,000 people on site

Including both visitors and exhibitor staff, the total number of people on site reached 4,070, surpassing the previous record of 3,861 from 2023 (of which 740 were stand staff). This year, 746 were stand representatives.

“Sectech, with its niche profile, plays an important role. The demand for knowledge about security technology is substantial – not only among suppliers but also among end users, who were strongly represented among the seminar participants,” concludes Lennart Alexandrie.



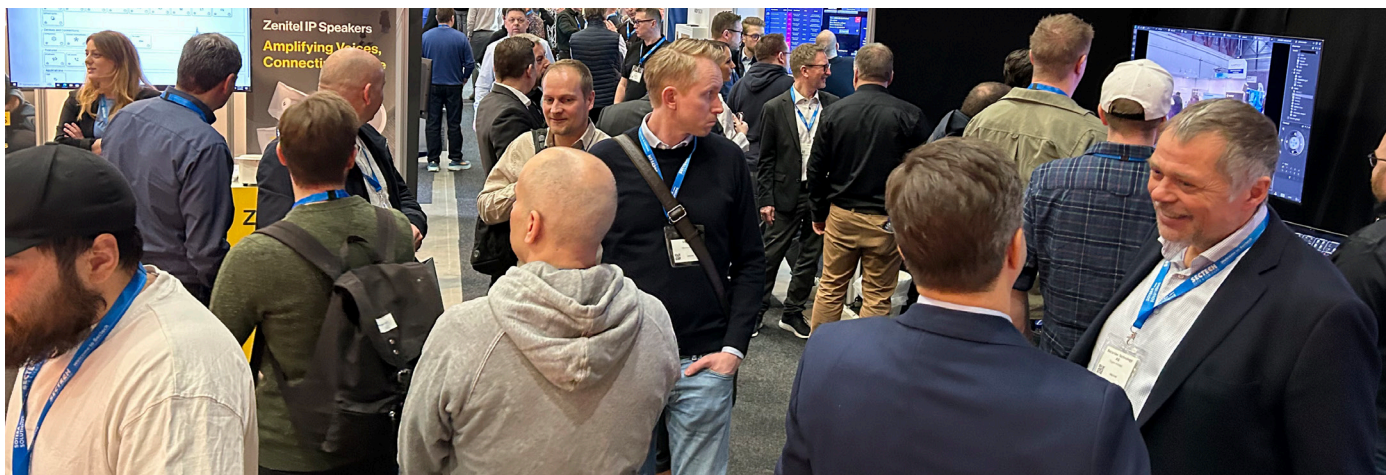
Jaroslav Barton, Product Marketing Director at HID, participated in a panel discussion about biometric access control.



Including both visitors and exhibitor staff, the total number of people on site reached 4,070.



A record number of participants attended the seminar programme. The previous high of 1,090 from 2023 was surpassed, with 1,157 registered this year.


2025
November

**11-12 November
OFSEC 2025 | Muscat, Oman**

Venue: Oman Convention & Exhibition Centre
Organiser: Muscat Expo LLC
Tel: +968 24788476
Email: info@muscat-expo.com
Website: www.ofsecevent.com


**11-13 November
The Security Event Asia |
Singapore, Singapore**

Venue: Sands Expo & Convention Centre
Organiser: Nineteen APAC Pte Ltd
Tel: +65 6031 1342
Email: team@safetysecurityasia.com
Website: www.safetysecurityasia.com


**18-20 November
ISC East - New York, United States**

Venue: Javits Center
Organiser: RX
Tel: 203.840.5602
Email: inquiry@isc.reedexpo.com
Website: www.discoverisc.com/east/en-us.html


**9-21 November
Sicurezza, Milan, Italy**

Venue: Fieramilano (Rho)
Organiser: Fiera Milano
Tel: +39 02.49976822
Email: visitatori.sicurezza@fieramilano.it
Website: https://www.sicurezza.it/en/

December

**9-11 December
Security Expo - Nadarzyn,
Warsaw, Poland**

Venue: Ptak Warsaw Expo
Organiser: Ptak Warsaw Expo
Tel: +48 518 739 124
Email: biuro.podawcze2@warsawexpo.eu
Website: warsawsecurityexpo.com/en


**11-13 December
IFSEC India | New Delhi, India**

Venue: Dubai World Trade Centre
Organiser: Messe Frankfurt
Tel: +971 4 3894 500
Email: intersec@uae.messefrankfurt.com
Website: www.intersec.ae.messefrankfurt.com

2026
January

**12-14 January
Intersec Dubai, Dubai UAE**

Venue: Dubai World Trade Centre
Organiser: Messe Frankfurt
Email: intersec@uae.messefrankfurt.com
Website: www.intersec.ae.messefrankfurt.com

March

**23-27 March
ISC West | Las Vegas, United States**

Venue: The Venetian Expo
Organiser: RX
Tel: +1 203 840 5602
Email: inquiry@isc.reedexpo.com
Website: www.discoverisc.com/west/en-us.html

April

**14-16 April
Security Expo - Nadarzyn,
Warsaw, Poland**

Venue: MTP Poznań EXPO
Organiser: Grupa MTP
Tel: + 48 61 869 2000
Email: info@grupamtp.pl
Website: securex.pl/e


**22 April
#TrygghetNu | Stockholm, Sweden**

Venue: Clarion Hotel Stockholm
Organiser: AR Media International AB
Tel: +46 8 556 306 80
Email: deniz.baykal@armedia.se
Website: www.trygghetnu.se
Visit AR Media at #TrygghetNu

May

**27-29 May
Eliaden - Lillestrøm, Norway**

Venue: Nova Spektrum
Organiser: Eliaden
Tel: +47 23087700
Email: post@eliaden.no
Website: www.eliaden.no

June

**2-4 June
Expo Seguridad México
Mexico City, Mexico**

Venue: Centro Banamex
Organiser: RX
Tel: +52 (55) 8852 6000
Email: info@exposeguridad.com
Website: www.exposeguridadmexico.com/en-gb.html

July

**1-2 July
SicherheitsExpo | Munich, Germany**

Venue: MOC Munich
Organiser: AFAG Messen und Ausstellungen
Tel: +49 (0)89-88 94 93 7777
Email: info[@]sicherheitsexpo.de
Website: www.sicherheitsexpo.de/en/munich/

August

**25 August
SkyddGolfen Detektor Open 2026
Nykvarn, Sweden**

Venue: Golf South Sthlm (Vidbynäs GC)
Organiser: AR Media International AB
Tel: +46 8 556 306 80
Email: deniz.baykal@armedia.se
Website: www.armedia.se/detektor/scandinavia/sv/
SkyddGolfen.asp
Visit AR Media at SkyddGolfen Detektor
Open 2026

October

**20-22 October
Skydd - Stockholm , Sweden**

Venue: Stockholmsmässan
Organiser: Stockholmsmässan
Tel: +46 8 7494100
Email: info@stockholmsmassan.se
Website: www.skydd.net
Visit AR Media at Skydd

November

**3-5 November
Expoprotection | Paris, France**

Venue: Porte de Versailles - Pav 1
Organiser: RX
Tel: (+33) 1 47 56 21 00
Email: communication.france@rxglobal.com
Website: www.expoprotection.com

Changes may occur. Visit www.securityworldmarket.com for the latest updates.

Can your company contribute to the Scandinavian security market?

If so, **don't miss** the opportunity to showcase your solutions at the premier security technology events in Norway and Sweden in 2027. Spaces are filling up fast – book your stand now to **secure your spot!**



Upcoming Events:

SECTECH Norway March 17–18, 2027
Nova Spektrum/Lilleström

SECTECH Sweden October 26–27, 2027
Stockholmsmässan/Stockholm

SECTECH
EXPO & SEMINARS

www.sectech-expo.com

**B****Posttidning**

Ej retur



Avs. AR Media International,
Elektravägen 14,
S-126 30 HÄGERSTEN



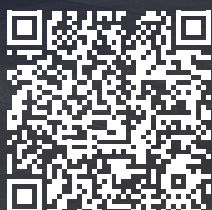
The Future of Security Screening

HSS Falcon's comprehensive, smart solution uses advanced AI-driven, high-throughput screening technology to detect explosives, weapons and narcotics on people and in bags.

- Advanced Technology
- Powerful Capabilities
- Premium Experience



HSS Falcon won the Detektor International Award 2025 in the category Alarm & Detection!



Scan the QR-code
to learn more about
HSS Falcon.

apstecsystems.com