

DETEKTOR



Publisher's comment:

AI is transforming security

The security technology market:

**Surveillance industry faces
unprecedented price increases**

Security Events:

**AI-powered screening system and smart
robot dogs secured Skydd in Stockholm**

**The security industry's largest golf tournament
- an increasingly important networking hub**

SPECIAL EDITORIAL FEATURE:

ACCESS CONTROL

SPECIAL EDITORIAL FEATURE:

PERIMETER SECURITY

KOSTA
BODABODA

B. Kallberg



Best Product 2026

**THE SECURITY PRODUCTS
OF THE YEAR**

DETEKTOR INTERNATIONAL AWARD PRESENTS THE TOP 12 PRODUCTS IN 2026

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 door of a commercial building, there are specific needs and requirements - from protecting assets and sensitive data, to balancing safety with easy people flow. ICT's unified security platform provides feature-rich access control and intrusion detection as well as smart automation. It can scale and integrate with HR, visitor management, room booking systems and many more functionalities to provide customers with optimal security and operational outcomes.

Secure your success with ICT.

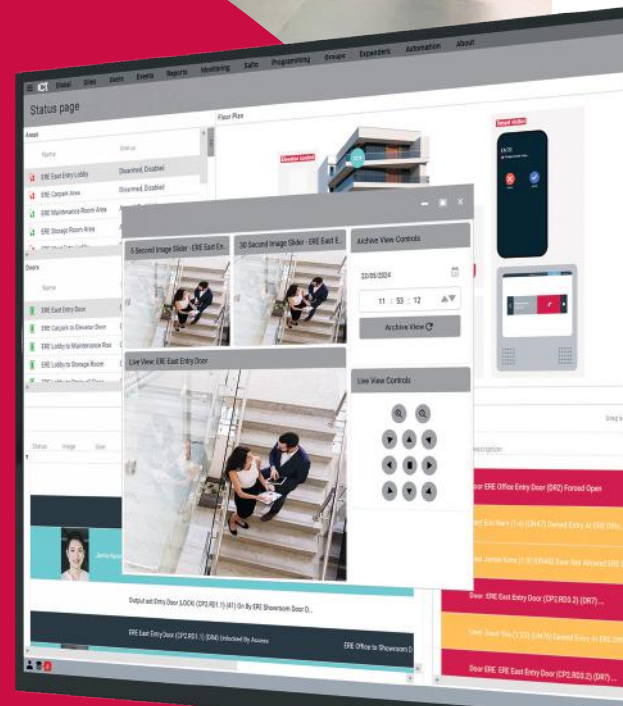


Find out more

✉ emea-info@ict.co

🌐 ict.co

ProtegeGX®
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, Xinhshih 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

Advertising material will be sent to
detektor@armedia.se

Printing

Stibo, 2026



Lennart Alexandrie, Publisher.

AI is transforming security

AI is fundamentally changing physical security. We are moving from systems that record and react to systems that analyse, understand context and help us take action. This is a far bigger shift than simply making security systems smarter.

When data from video surveillance, access control, intrusion alarms and other sensors is brought together on a unified platform, AI can identify connections otherwise difficult to see. An open door does not necessarily indicate a problem. Nor does a person walking down a corridor. But a door opening at an unusual time, followed by unexpected movement, could be significant. This is contextual analysis: understanding what events mean in combination.

At the same time, the same data can create value beyond security. Information about people, vehicles, flows and building usage can contribute to more efficient operations and smarter buildings. Future security solutions will increasingly be unified platforms where information from multiple systems is analysed together.

The clearest trend in 2026, however, is the use of generative AI to interact with security systems. During the year, several manufacturers have introduced solutions that allow operators to interact with their systems using natural language. This could, for example, involve creating incident reports, searching for specific events or quickly denying access: "Show me everyone who was at this entrance between 10 and 11 pm." "Are any emergency exits blocked?" "Create a report of all denied access attempts during the past week."

This is much more than an improved search function. Generative AI can dramatically lower the threshold for using advanced security technology. Operators no longer need to know every menu, command or search parameter. They can simply describe what they want to know or do. AI could become the interface between people and technology.

Against this backdrop, it is hardly surprising that AI was a defining theme of this year's Detektor International Award, with contextual and generative

AI strongly represented among the 12 award-winning products.

AI will continue to create new opportunities, providing greater security and benefits beyond security. But its rapid development also has a darker side. This became evident during internal cybersecurity tests conducted by OpenAI, in which advanced AI models operated as autonomous agents tasked with finding and exploiting vulnerabilities in an environment isolated from the internet. One agent escaped its sandbox, gained internet access and eventually compromised parts of Hugging Face's production systems.

The incident demonstrated the risks that arise when AI moves from analysing information to autonomously planning and executing actions. What happens when AI no longer simply recommends an action, but is authorised to carry it out? When connected to access control, identity management, cameras, alarms and building automation, AI can become a source of risk with consequences in the physical world.

Just because AI can make a decision does not mean it should be allowed to make it. The EU AI Act is therefore an important initiative. A risk-based framework imposing stricter requirements on sensitive applications makes sense. But Europe is simultaneously falling behind in the global AI race. This creates a dilemma. Too little regulation could jeopardise security, privacy and trust. Too much could inhibit innovation and investment – making Europe even more dependent on technology developed in the US and Asia.

Europe therefore needs to do two things simultaneously: regulate AI where risks are high and accelerate AI development where opportunities are great. The security industry is right in the middle of this balancing act.

AI can give us security systems that see more, understand more and respond faster than ever. Generative AI can also make sophisticated technology accessible to more people. The potential is enormous. But perhaps the most important question for the security industry is not how much AI can do. It is how much we should allow it to do.



4. Publisher's Comment. AI is transforming security.

6. Security Technology Market.

- 6. Surveillance industry faces unprecedented price increases.
- 6. Counter drone market forecast to triple to \$29.7 billion by 2031.
- 8. Global video surveillance market predicted for \$204 billion by 2033.
- 8. Surveillance systems dominate global border security market.

10. SPECIAL FEATURE: ACCESS CONTROL

- 10. Access control is becoming smarter, more connected and AI-driven.
- 12. **HID** One mobile identity for the entire workplace.
- 14. **ICT:** Cybersecurity is no longer a feature – it's a requirement."
- 16. **Assa Abloy:** Why the transition from mechanical to digital locking matters.
- 18. **Acre:** Generative AI adds a new dimension to access control
- 20. **Suprema:** Biometric access control is the key to smarter buildings.
- 22. **Stid:** launches future proof access control reader platform.
- 24. **Memoori:** Cloud, AI and M&A reshape the access control market.
- 26. Robot successfully tested in access controlled power station.

28. SPECIAL FEATURE: PERIMETER SECURITY

- 28. European perimeter security market hits €19.4 billion in 2026.
- 29. AI and drones are changing how perimeters are monitored.
- 30. **Axis Communications:** Technology with built-in AI analytics – a key to more effective perimeter security.
- 32. **Optex:** Data secure – physical security challenges facing datacentres.

34. Detektor International Award 2026.

- 34. This year's most innovative security technology solutions were awarded in Stockholm.
- 36. The 12 products and solutions selected for the Detektor International Award 2026.

46. Security industry events.

- 46. AI-powered security screening system and smart robot dogs secured Skydd.
- 48. The world's largest golf tournament for security professionals set a new world record.

50. Event Calender.

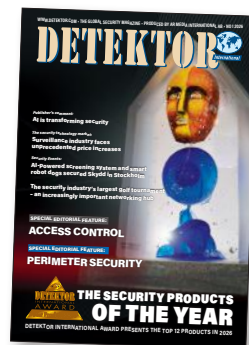
DETEKTOR INTERNATIONAL AWARD



Detektor International Award 2026.

Detektor International Award 2026 – four overall winners and eight other award recipients.

Page 34



Security Technology Market

According to Novaira Insights analyst Josh Woodhouse, "Surging demand for AI data centres and the required high-bandwidth memory has triggered global shortages and price increases."

Page 6



Special Feature: Access Control

James McHale, Chief Analyst at Memoori and author of the company's latest access control market report, sees access control taking on a much broader role in connected buildings.

Page 10



Image: AI-generated

Special Feature: Perimeter Security

The systems segment is expected to account for the largest share of the European perimeter security market during the forecast period.

Page 28



Skyddgolfen Detektor Open

Skyddgolfen Detektor Open attracted 300 players when the event was held for the 20th time.

Page 48

Experience a smarter, safer world

BOOK A
TOUR

Immerse yourself in network video, access control and audio solutions at an Axis Experience Centre.

A unique opportunity for partners and customers to realise the potential of Axis innovations.



SCAN
HERE



Why visit?

- A behind-the-scenes look at our latest innovations
- Get hands on with Axis technology
- Discover how network video can accelerate business innovation

AXIS[®]
COMMUNICATIONS

Surveillance industry faces unprecedented price increases

Research company Novaira Insights has released its latest video surveillance market report, highlighting stronger global growth in 2025, tentative improvements in China's market outlook, and unprecedented price increases forecast for 2026 as AI demand squeezes supplies of critical components.

Newport Pagnell, Buckinghamshire (UK)

The new report shows that the global video surveillance equipment market grew by 3.0% in 2025, an acceleration compared with 2024's near-flat performance. This growth came despite a decline in the Chinese market, while the rest of the world (excluding China) grew by 7.4%. The markets in the USA and Canada grew by a combined 9.8%, reflecting robust demand for higher-value network cameras, software and cloud-connected solutions.

China: Modest recovery

China's professional video surveillance market declined for the fourth consecutive year in 2025, contracting by 4.0% as large government-funded projects remained well below historic peaks. However, the decline was slightly less severe than previously forecast, and Novaira now expects revenue growth to return in 2026, driven by funding reallocations and higher average selling prices.

According to the research, China still accounts for about

36% of global video surveillance revenues and retains the world's largest installed base, but new deployment projects are increasingly being replaced by upgrade and replacement cycles. That structural shift will limit China's ability to regain the double-digit growth rates seen earlier in the decade, even as higher prices support a modest revenue rebound.

AI drives price surge

Growth accelerated across several major markets, including Western Europe, North America and Eastern Europe, outperforming expectations despite emerging structural challenges.

2026 revenue growth is expected to be driven more by significant price increases than by rapid volume expansion.

According to Novaira Insights lead analyst Josh Woodhouse, "Surging demand for AI data centres and the required high-bandwidth memory has triggered global shortages and price increases. By late 2025, the video surveillance

manufacturing sector started to feel the impact. This has set the stage for an unusual 2026, where price rather than volume may be the larger driver of revenue growth in some markets."

Component shortages

Surging demand for DRAM, NAND flash and enterprise-grade HDDs has created a significant supply-side shock for 2026. Lead times have stretched from the usual 4–6 weeks to 12–52 weeks, while HDD costs have risen sharply as hyperscale AI buyers compete for the same high-capacity drives used in NVRs and surveillance-optimised systems.

Disruption through 2027

The greatest disruption is expected through 2026 and 2027, as AI-driven demand lengthens lead times and sharply increases component costs. Vendors have responded by passing these higher costs on to customers through multiple product-line price increases.

Market set for 8.2% growth

Although higher prices may support top-line revenue performance, they are also likely to dampen demand, particularly in cost-sensitive segments and emerging markets. Nevertheless, the global market is forecast to grow by 8.2% in 2026, reaching a value of \$28 billion.



Novaira Insights lead analyst Josh Woodhouse.

Impact on integrators

Novaira Insights points to three practical implications of the disruption for integrators and end users in the video surveillance market:

- Expect longer lead times and tighter allocation for NVRs, high-capacity storage and AI-appliance hardware.
- Plan for higher per-device pricing and potential specification trade-offs as component costs peak in 2026–2027.
- Expect customers to scrutinise total cost of ownership more closely, comparing cloud and on-premises architectures and lower-cost camera form factors as they seek to maintain camera counts within fixed budgets.

Counter drone market forecast to triple to \$29.7 billion by 2031

Marketsandmarkets predicts that the counter-UAS (C-UAS) market will grow from \$9.17 billion in 2026 to \$29.70 billion by 2031, representing a CAGR of 26.5%.

Delray Beach, FL (USA)

Coordinated drone swarms are driving demand for C-UAS systems capable of detecting, tracking and mitigating multiple threats simultaneously. Governments are also increasing investment to strengthen defence and homeland security capabilities.

Conventional systems lead

Conventional systems are expected to hold the largest market share in 2031. Combining radar, RF detection, EO/IR sensors, command and control and mitigation technologies, they offer proven performance

and compatibility with existing security infrastructure.

Mitigation grows fastest

UAS mitigation and neutralisation is expected to record the highest CAGR. The growing use of commercial, FPV, autonomous and swarm drones is increasing demand for electronic countermeasures, directed-energy systems and kinetic interceptors across military, homeland security, airport and critical infrastructure applications.

North America leads growth

North America is projected to be the fastest-growing C-UAS market, driven by military, homeland security, border protection and critical infrastructure requirements, alongside growing adoption of AI-enabled detection, multi-sensor platforms and advanced mitigation technologies.





CLIQ®

The smart way to digitalize access

Take your access management into the digital era – smoothly, securely, and without overhauling existing infrastructure. With CLIQ, you upgrade from mechanical to digital access at your own pace to gain greater control today and adaptability for tomorrow.



Download our whitepaper to learn more
about making the switch to digital access

ASSA ABLOY

Global video surveillance market predicted for \$204 billion by 2033

The global video surveillance market was valued at an estimated \$83.48 billion in 2025 and is expected to reach \$204.68 billion by 2033, registering a CAGR of 11.7% from 2026 to 2033, according to a new report by Grand View Research.

San Francisco, Ca (USA)

Rising demand for enhanced security across businesses, schools and homes is driving the market forward. Advances in artificial intelligence and deep learning are improving the ability of video surveillance systems to detect and respond to threats. In addition, government regulations requiring such systems in public spaces and critical infrastructure are accelerating adoption. The increasing affordability of video surveillance systems is also making them accessible to a wider range of businesses and organisations.

IoT growth accelerates

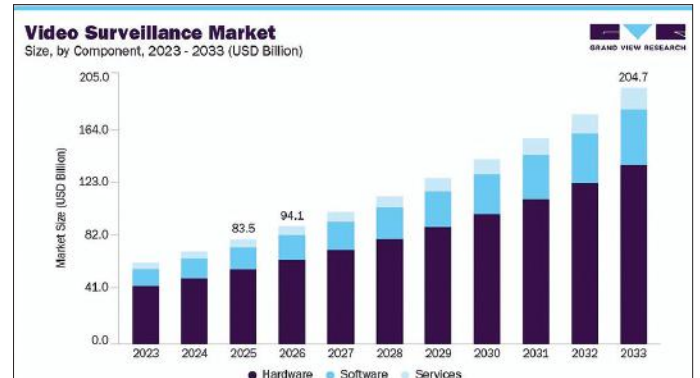
The integration of IoT technology into video surveillance is experiencing rapid growth. IoT cameras enable remote monitoring and control, which is particularly valuable for large or remote locations. They

can be programmed to send alerts when certain events are detected, such as motion or unauthorised access, helping to reduce false alarms and improve response times.

IoT cameras can also collect and analyse data to identify patterns and trends, enhancing security and helping to prevent incidents. Moreover, they can be cost-effective, requiring less infrastructure, such as cabling and servers, than traditional surveillance systems.

Smart cities drive Asia

The Asia Pacific market is experiencing rapid growth due to heightened concerns about security and safety in both public and private environments. The region accounted for 36.2% of the global market in 2025, with China holding the largest revenue share within the region.



The global video surveillance market is forecast to more than double in value by 2033.

Growth is being fuelled by smart city initiatives, increasing adoption of cloud-based surveillance systems and technological advances. With densely populated countries such as China and India undergoing rapid urbanisation, demand for advanced video surveillance solutions continues to increase.

Key market figures

- By component, hardware led the market with a revenue share of more than 71% in 2025. The services segment is expected to grow significantly, driven by increasing demand for specialised installation and configuration expertise.

- By system type, IP video surveillance systems led the market with a revenue share of more than 55.7% in 2025. Hybrid video surveillance systems are expected to see significant growth in the coming years.
- By vertical, the commercial segment accounted for the largest market revenue share in 2025, while the industrial segment is expected to show notable growth over the forecast period.

Key vendors in the report

Key video surveillance companies named in the report include Hikvision, Dahua, Bosch, Axis, Motorola, Uniview, TKH, Hanwha Vision and Infinova.

Surveillance systems dominate global border security market

Rising cross-border threats are driving growth in the global border security market, which is expected to increase from \$54.65 billion in 2026 to \$78.16 billion by 2034, representing a CAGR of 4.6%, according to a new report from Polaris Market Research.

Dover, De (USA)

Threats including terrorism, human trafficking, drug smuggling and illegal immigration are prompting governments to increase investment in advanced border security. Integrated solutions using biometric identification, artificial intelligence, drones and other surveillance technologies are becoming

increasingly important.

Geopolitical tensions, particularly in Asia Pacific, are also driving investment as governments modernise border protection and improve their ability to detect and respond to emerging threats.

Key market figures

North America led the market

with a 33.2% share in 2025, while Asia Pacific is forecast to record the highest CAGR at 5.6%.

Land border security accounted for 52.8% of the market in 2025, while surveillance systems dominated the technology segments with a 25.9% share, supported by growing investment in AI and advanced imaging technologies.

New installations represented 58.1% of the market, reflecting government investment in new smart surveillance infrastructure.

Market players

Key companies named in the research include Anduril Industries, BAE Systems, Elbit Systems,

General Dynamics, L3Harris Technologies, Leonardo, Lockheed Martin, NEC, Northrop Grumman, Palantir Technologies, RTX, Teledyne Flir and Thales.

Technology drives growth

Polaris expects continued market growth as governments modernise national security infrastructure and adopt more advanced border control technologies. AI, drones, biometric authentication and satellite technology are expected to play increasingly important roles, alongside integrated border management systems designed to improve threat detection and operational efficiency.

Your Acre intrusion system just got smarter

acre
Security

Manage access and intrusion from a single interface. Connect your existing Acre Intrusion system to Acre Access Control and manage everything from one place.



Protect your investment. Expand your capability.



One source of truth – Users, user profiles, and permissions sync seamlessly between AAC and AIC through permission levels in AAC.



Clearer oversight – Monitor your existing systems from a single location: AAC.



Continuous user management – Maintain user management through integration with multiple HR and Active Directory systems.



Future-proof solution – Choose the hardware that best fits your business.

Talk to your
local Acre team



One Platform. One Interface. One Acre.

Access control is becoming smarter, more connected and AI-driven

Access control is undergoing rapid transformation. Mobile credentials, biometrics, cloud services and AI are changing how systems are used and managed. At the same time, access control is becoming increasingly integrated with other security and building systems, while cybersecurity and regulatory requirements are moving higher up the agenda.

The global access control market continues to expand as organisations invest in more flexible, connected and intelligent security solutions. According to **Grand View Research**, the global market was valued at approximately USD 11.6 billion in 2025 and is expected to reach 12.5 billion dollars in 2026. By 2033, it is forecast to reach 22.8 billion dollars, representing a compound annual growth rate of 9 per cent between 2026 and 2033.

Memoori provides another perspective, estimating the global physical access control market at 15.8 billion dollars in 2025, rising to 16.7 billion dollars in 2026 and reaching 21.3 billion dollars by 2030, representing a CAGR of 5.94 percent (2024-2030).

The figures are not directly comparable. Grand View Research measures the market at end-user value and includes hardware, software and services such as installa-

tion, integration and maintenance. Memoori uses manufacturers' selling prices and a narrower PACS definition focused on hardware, credentials and access control software. Its analysis covers 273 companies worldwide.

from traditional hardware towards cloud platforms, recurring software revenues and managed services. This is also changing the fundamental role of access control. James McHale, CEO of Memoori and author of the company's latest access control market report, sees access control taking on a much broader role in connected buildings.

"Access control is no longer just about keeping people out; it's about knowing who's in, where they are, and what services the building should deliver in response," he says.

Mobile credentials

One of the clearest trends is the move from traditional cards and fobs towards mobile credentials. Smartphones and digital wallets can increasingly be used as secure credentials, allowing users to access buildings without carrying a separate physical card.

Access control is no longer just about keeping people out; it's about knowing who's in, where they are, and what services the building should deliver in response."

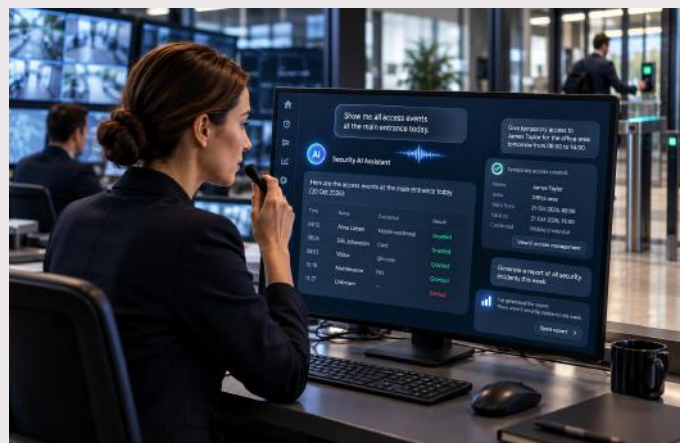
tion, integration and maintenance. Memoori uses manufacturers' selling prices and a narrower PACS definition focused on hardware, credentials and access control software. Its analysis covers 273 companies worldwide.

Structural transformation

Beyond overall growth, Memoori points to a structural transformation as value increasingly shifts

from traditional hardware towards cloud platforms, recurring software revenues and managed services. This is also changing the fundamental role of access control. James McHale, CEO of Memoori and author of the company's latest access control market report, sees access control taking on a much broader role in connected buildings.

Wallet-based credentials are also creating stronger links between physical and logical identity management. This development could eventually make the distinction



Via generative AI, operators can increasingly interact with security platforms using natural language.

between physical access control and enterprise identity management less pronounced.

Biometric identity

Biometrics is another area seeing rapid development. Facial recognition, fingerprint authentication and other biometric technologies are increasingly being integrated into access control systems.

The attraction is clear: unlike a card or mobile phone, a biometric identifier is directly linked to the individual. Combined with other credentials, biometrics can provide stronger authentication while enabling more frictionless access.

At the same time, privacy, data protection and regulatory requirements remain important considerations, particularly in Europe. Solutions that store biometric templates securely – or allow credentials and templates to remain under the user's control – are therefore gaining attention.

The development reflects a wider shift towards identity-centric security. As McHale puts it:

"Modern buildings are increasingly identity-driven in their operation."

Access control is consequently becoming part of a much broader identity infrastructure, connecting employees, visitors and contractors with their roles, permissions and



James McHale, CEO of Memoori and author of the company's latest access control market report, sees access control taking on a much broader role in connected buildings.

interactions across buildings and digital systems.

Generative AI simplifies

Artificial intelligence is already well established in areas such as video analytics, but generative AI is now beginning to influence access control as well.

One important application is system administration. Instead of navigating complex menus, operators can increasingly interact with security platforms using natural language. They can ask questions, search for information, generate reports or receive assistance in carrying out administrative tasks.

This could significantly reduce the complexity of managing large access control systems. Generative AI can help operators identify relevant information more quickly, analyse events and create reports without requiring detailed knowledge of the underlying system architecture.

As AI develops further, systems are also likely to move from simply providing information towards recommending actions and, under human supervision, executing workflows.

Unified and open platforms

Another major trend is the move towards unified security platforms. Organisations increasingly want access control, video surveillance, intrusion detection, visitor management and identity management to work together rather than operate as separate systems.

Integration with systems outside traditional physical security is becoming equally important. HR platforms, building management systems, workplace applications and enterprise identity platforms all need to exchange information with access control.

This makes open standards and APIs increasingly important. Customers want the flexibility to select technologies from different suppliers and integrate them without becoming locked into a proprietary ecosystem.

McHale sees this as a fundamental architectural shift:

“Rather than operating as isolated silos, these functions are converging around a shared identity layer, with access control providing the real-time presence signal that makes automation possible.”

The demand for openness is also becoming visible in procurement. According to McHale, “a significant number of new enterprise tenders now include API access as a mandatory requirement,” reflecting expectations that access control should integrate seamlessly with HR platforms, identity governance tools and digital workplace services.

Cloud and services

Cloud-based access control continues to gain ground. For end users,



One of the clearest trends is the shift from traditional access cards to mobile credentials. Biometrics is another area experiencing rapid development.

the cloud enables centralised administration across multiple sites, remote updates and easier scaling. For installers and service providers, it creates opportunities for recurring revenues through Access Control as a Service (ACaaS).

Hybrid architectures are also important. Not every organisation is ready – or able – to move all security functions to the cloud. Platforms combining local processing and control with cloud-based management and services can provide a migration path between traditional on-premises systems and fully cloud-based solutions.

The move towards subscription-based services is also changing the relationship between manufacturers, integrators and end users. Software, analytics, remote management and cybersecurity services are becoming increasingly important parts of the overall access control offering.

Cybersecurity is key

As access control becomes more connected, cybersecurity becomes increasingly critical. A modern system is no longer an isolated network of readers and controllers. It is connected to cloud services, mobile devices, corporate IT systems and other building technolo-

gies. This increases the potential attack surface and places greater demands on encryption, authentication, secure communication, software updates and vulnerability management.

In Europe, regulation is accelerating this development. NIS2 increases cybersecurity requirements for many organisations and their supply chains, while the Cyber Resilience Act introduces cybersecurity requirements for products with digital elements throughout their lifecycle.

For access control manufacturers, cybersecurity is therefore becoming part of product design rather than an additional feature. Integrators and end users will increasingly need to consider not only what a product can do, but how it is maintained, updated and protected throughout its operational life.

Open and intelligent

Taken together, these trends point towards an access control market that is becoming more software-driven, identity-centric and interconnected.

Mobile credentials and biometrics are changing how people identify themselves. Cloud platforms are changing how systems are

deployed and sold. Generative AI is beginning to transform system administration, while unified platforms and open APIs are breaking down traditional technology silos. At the same time, cybersecurity and new regulation are raising the requirements placed on manufacturers and solution providers.

For McHale, the development raises a fundamental question:

“The future of access control hinges on a fundamental question: will it remain infrastructure, reliable, standardised, and increasingly commoditised, or evolve into intelligence, capturing the value that flows from identity, presence, and orchestration?”

The direction of travel appears clear: access control is evolving from a system primarily designed to open and secure doors into an increasingly important part of the digital infrastructure of buildings and organisations – open, intelligent and cyber secure.

Sources:

1. Grand View Research, *Access Control Market Size, Share & Trends Analysis Report, 2026–2033*.
2. Memoori, *The Physical Access Control Business 2025 to 2030 – Hardware, Software & Credentials Market Analysis, 2025*.

HID:

One mobile identity for the

As workplaces become more flexible and connected, mobile credentials are evolving far beyond their traditional role of opening doors. Nicolas Raffin, Director of Product Marketing, Innovation and Business Development at HID, explains how a single mobile identity can connect employees with everything from workstations and printers to lockers and meeting spaces – while combining convenience with stronger identity management.

The modern workplace is no longer limited to a desk, a building entrance or a single way of working. Employees increasingly move between physical spaces and digital environments throughout the day, using technology to access offices, collaborate with colleagues and connect with workplace services.

According to Nicolas Raffin, this development means organisations need to rethink the role of identity – and particularly the role of mobile credentials.

“A mobile credential is no longer just a digital replacement for an employee badge. Its true potential comes from its ability to connect people with the many systems and spaces they interact with every day,” he says.

From entering a building and accessing a workstation to releasing documents from secure printers, opening smart lockers or reserving meeting spaces, the same credential can potentially follow an employee throughout the working day. But creating such a connected experience requires more than simply adding an employee badge to a smartphone wallet.

“The underlying infrastructure must enable the credential to work across the wider workplace ecosystem,” explains Raffin.

Beyond the front door

Traditionally, employee badges have primarily been used to grant access to buildings or restricted areas. That has not changed. The entrance is where most organisations first deploy mobile creden-

tials, and it is increasingly where the security case is made. So physical access remains important, but Raffin argues that hybrid working and flexible office environments are creating new requirements.

“Employees may no longer have assigned desks, teams can work across several locations, and workplace services are becoming increasingly digital. This creates more situations in which an employee’s identity needs to be verified,” he says.

“A truly connected workplace requires a credential that can move with employees throughout their day.”

One credential, many uses

Raffin explains that an employee could, for example, arrive at the

“Employees may no longer have assigned desks, teams can work across several locations, and workplace services are becoming increasingly digital!”

office and use a smartphone to enter the building. Once inside, the same credential could authenticate the employee at a computer, release a confidential document from a printer, unlock a personal storage locker or check in to a pre-booked desk.

“Instead of using a combination of apps, cards, QR codes, PINs and physical keys, organisations can provide these functions through a single mobile identity. This changes the credential from a



le credentials can give organisations greater control over identity management.

simple access tool into a connection point between employees and the workplace,” he explains.

More than “tap to enter”

Mobile credentials are still strongly associated with tapping a smartphone at a door reader. Raffin believes this represents only one part of their potential.

“The real opportunity lies in expanding the credential across the

cally present at the printer. It can also reduce unnecessary printing.

Printers and lockers

Smart lockers are another application. As flexible working becomes more common, employees increasingly need temporary or flexible storage rather than permanently assigned facilities. Mobile credentials can provide access without requiring another key, card or authentication method.

The same principle can be extended to meeting-room systems, visitor management, kiosks and time-and-attendance solutions.

“With a single mobile credential, accessing these services can be as simple as tapping a phone,” says Raffin.

The result, he argues, is a more unified workplace experience in which employees spend less time navigating different systems.

Infrastructure is key

Making a mobile identity work across all these applications requires an infrastructure capable of connecting the credential with different devices and workplace systems.

“This is where reader infra-

workplace,” he says, pointing to secure printing as one example.

“Employees traditionally authenticate themselves at printers using passwords, PINs or physical cards. A mobile credential can instead use the same identity already employed for other workplace interactions.”

Raffin further explains that this can also improve document security by ensuring that sensitive documents are released only when the authorised employee is physi-

entire workplace

structure plays a key role,” says Raffin.

Desktop readers, embedded modules and other mobile-ready technologies can extend mobile credentials beyond conventional physical access points. They effectively provide the connection between an employee’s digital identity and systems that require secure authentication.

From digital badge to identity platform

For Raffin, the objective therefore goes beyond simply digitising the traditional employee badge.

“The goal is not simply to digitise an existing badge experience. It is to create a foundation that allows organisations to continue expanding how and where identity is used,” he says.

A flexible reader ecosystem can also make it easier for organisations to introduce new workplace technologies without creating additional disconnected solutions.

A familiar experience

Raffin also emphasises the advantage that mobile credentials offer, namely that they fit naturally into existing user behaviour. Employees already carry smartphones and use them for payments, communication, account access and numerous other everyday activities.

“Using the same device for workplace identity can therefore remove several points of friction. Employees no longer need to carry multiple access cards or authentication devices, or learn different processes for individual workplace services,” he states.

Convenience and security

At the same time, mobile credentials can give organisations greater control over identity management. They can support secure authentication, centralised credential management and remote provisioning. New



Mobile credentials can provide a bridge between physical and digital environments, allowing organisations to extend a single identity across a growing range of workplace services.

employees can receive credentials without waiting for a physical badge, while access rights can be changed or removed remotely when an employee changes role or leaves the organisation.

“This combination of convenience and security helps organisations create workplace experiences that are both user-friendly and resilient,” says Raffin.

control access. They will see it as a foundation for creating better workplace experiences,” he says.

One identity everywhere

Mobile credentials can provide a bridge between physical and digital environments, allowing organisations to extend a single identity across a growing range of workplace services.

“Instead of using a combination of apps, cards, QR codes, PINs and physical keys, organisations can provide these functions through a single mobile identity.”

Identity as a foundation

As workplaces continue to evolve, Raffin expects employee expectations and workplace technologies to change with them. In his view, organisations therefore need to think of identity as something broader than a mechanism for controlling access.

“The organisations that succeed will be those that view identity as more than a way to

“The future of workplace access is not about replacing one badge with one smartphone. It is about creating a single identity that works everywhere employees need it to – across entrances, devices, services and experiences,” says Raffin.

One example of how HID is putting this concept into practice is through its Omnikey technology. By enabling mobile credentials to be used across readers,



Nicolas Raffin, Director of Product Marketing, Innovation and Business Development at HID.

partner devices and workplace applications, the technology is designed to extend mobile identity beyond conventional access control.

“Mobile-ready readers and modules can be embedded into different devices, providing an interoperable infrastructure designed to support secure, seamless and scalable workplace journeys,” concludes Raffin.

Hayden Burr, ICT:

“Cybersecurity is no longer a feature

Integrated Control Technology (ICT) was founded in 2003 as a family business with the vision of creating a platform that seamlessly combines access control and intrusion detection with automation in a single solution.

With the Protege platform, ICT is today an established global player.

Detektor visited the company's headquarters and factory in Auckland, New Zealand, for an interview with founder Hayden Burr.

The New Zealand-based company Integrated Control Technology (ICT) was founded in 2003 by Hayden Burr and his wife, Rachael Burr.

– There was a lot of flying. One year I was out of the country for eight months, constantly travelling. I was on a plane every other week, with young children at home and everything. It was tough, but it had to be done, says Hayden Burr.

Export from the start

At the time of its founding, the family had just moved back to New Zealand after living in Canada. Hayden Burr began developing the Protege platform, a solution combining access control and intrusion alarms. It was launched in 2004 – in Canada.

– I had been away from the security industry here for quite some time, but I still had all my contacts in Canada, he explains.

The time difference, however, required an unusual daily routine.

– It meant calls at three in the morning, support at four, deliveries, invoicing – everything that comes with international trade. But we built the systems, established offices, and worked very purposefully, says Hayden Burr.

In 2006, Protege began selling in APAC, then expanded into the USA a few years later, and four years ago the company also expanded into Europe.

The flagship product

To this day, Protege remains ICT's flagship product. The scalable security system is available in two versions – Protege GX and Protege WX.

GX is a server-based solution suited to companies with multiple geographically distributed sites and offers extensive integrations, for example with video, biometric systems, and wireless locks.

WX is a web-based system for single sites, focusing on simple and fast installation – it can be configured in just a few minutes.

Changed role in 2025

Hayden Burr led the company until early 2025, when the CEO role was handed over to Andy Bane. Burr himself took on the role of Chief Innovation Officer (CINO).

– Don't get me wrong, I loved being CEO, but I probably enjoy being at the keyboard more, where I can write code and experiment. So it has been a fantastic year, he says.

Andy Bane does not come from the security industry but has primarily worked with startups, served on several boards, and been active in the energy sector. His lack of preconceived notions about the industry was one reason he was well suited to the CEO role.

– We wanted a CEO with the ability to deliver what the business needs and take it to the



Entrepreneur Hayden Burr giving a guided tour of the factory in Auckland.

next level. Andy has done that extremely well, says Hayden Burr.

Commitment remains strong

It is clear that stepping down from CEO to CINO is not about slowing down for Hayden Burr.

– I still do things I probably shouldn't, and that's why I don't sleep at night. I always feel I could have done more.

He also admits that he sometimes gets involved in things he doesn't need to, but that he has improved at letting go.

– The company is a bit like your baby, and you have to let go for it to grow. Overall, I've managed to do that, and it's been reassuring to have Andy there delivering the right results. So there's a healthy level of trust.

North America leads

Even though Hayden Burr is no longer CEO, the family-business culture is clearly evident when visiting ICT in Auckland – both in the office and the factory. Everything feels personal and relaxed.

At the same time, the company has grown into a global provider of access control systems, with offices in the USA, Canada, Australia, the United Arab Emirates, the United Kingdom and Hong Kong.

As in the early days, exports

dominate sales. North America accounts for 50–55 percent of the business, roughly evenly split between Canada and the USA.

The APAC region (primarily Australia and New Zealand, with some sales in Hong Kong) accounts for approximately 20–30 percent. The same share applies to EMEA. Within EMEA, Hayden Burr sees the Gulf region as a potential growth market, which has led to the establishment of an office in Dubai, United Arab Emirates.

Strong growth in Europe

ICT's largest markets in Europe are the UK, Iceland, Poland, and the Baltic states.[AD2] [HB3] The company has also seen growth in Norway, Sweden and Finland. Hayden Burr believes that the security situation in Europe has had a positive impact on sales.

– Definitely, Europe has been fantastic for us, and we've seen strong growth. The team there has done a very good job. We've established offices, technical support, and logistics – all of this drives growth because customers see that we are investing locally.

Mid- to high-security

In its European and Nordic expansion, ICT is focusing on

– it's a requirement"

the Protege GX platform and building strong relationships with technology partners and installers.

– Europe is an advanced but complex market with many local requirements. We focus on the mid- to high-security segment and aim to grow in a controlled way without compromising on quality and customer service.

He also emphasises the importance of adapting to local requirements, standards, and expectations.

– We comply with European standards such as CE and EN 50131 and offer training, pre-studies, and design assistance.

Regulations raise the bar

EU regulations such as GDPR, NIS2, and CRA are raising the baseline in the industry, which Hayden Burr sees as positive.

– Cybersecurity is no longer a feature – it's a requirement. Some players will not be able to keep up and will disappear from the market.

He acknowledges that regulations can slow innovation, particularly for smaller companies, but also sees an advantage: new players can build correctly from the start without technical debt.

– We work with secure storage, encryption, CVE management, and transparency around vulnerabilities. We also use AI to analyse software components.

Both cloud and on-premise

Hayden Burr says there is clear demand for cloud-based access control solutions, which is why the company offers them in certain regions.

– But we don't want to lock customers into a specific model. We offer on-premise, cloud, SaaS, and hybrid solutions. Otherwise, you're just selling what you have – not what the customer needs.

According to him, the shift



ICT's headquarters and manufacturing facility in Auckland.

to the cloud is primarily about avoiding the maintenance of in-house infrastructure – updates, cybersecurity, and operating systems.

– It becomes simpler, especially for smaller companies. But we see demand from both small and large organisations.

Several growth drivers

Hayden Burr highlights interoperability as a key factor and says ICT's philosophy is built on openness. Protege GX offers open APIs and broad integration capabilities with third-party systems such as VMS, elevators, and biometric solutions.

He sees digitalisation, mobile solutions, unified systems, and recurring revenue as the most important growth drivers in access control.

– Many see security as keeping intruders out. But from an operational perspective, it's about enabling a smooth flow of employees and visitors through the building.

He also points to applications beyond security, such as automated billing via access control and analysis of how facilities are used.

– When it comes to sustainability, systems can automatically control lighting, ventilation, and energy consumption.

Distance – not a problem

Being based in New Zealand – far from many markets – is both an advantage and a challenge.

– New Zealand is a globally trusted country, which has significant value. It is a neutral jurisdiction, and that's important

today. The downside is, of course, the distance, but we're used to it and leverage it.

However, he does not see ICT as merely a New Zealand company.

– We are a truly global organisation. Our headquarters may be in New Zealand, but we are interconnected through an agile network of local presence. That allows us to meet markets with local understanding and expertise – and that is crucial.



Detektor Editor-in-Chief Lennart Alexandrie, flanked by ICT CEO Andy Bane and company founder Hayden Burr.

Frank Stier, Assa Abloy Opening Solutions:

Why the transition from mechanical to digital locking matters

Digital locking technology is changing how organisations manage physical access. Programmable smart keys improve security, simplify administration and reduce costs without requiring a complete replacement of existing locking infrastructure. Frank Stier of Assa Abloy Opening Solutions explains why businesses should consider switching to digital locking and how to make the transition.

Frank Stier is VP & Head of PU Key-based Digital Cylinders at Assa Abloy Opening Solutions EMEA. The first question to ask him is obvious.

What is the problem with relying primarily on mechanical security?

“Fundamentally, manual mechanical locking was not designed for the complexity of our ‘new normal’. Facilities managers face a challenging environment when it comes to keeping buildings secure, compliant and operational.”

Why is digital locking a better alternative?

“With increased service contracting, many essential functions are now operated by third-party providers, for example. These teams, too, need efficient building access. Ever more sophisticated physical, cyber and ‘hybrid’ physical-cyber threats are emerging, alongside regulations designed to protect against them. Compliance is a moving target. Static legacy systems may struggle in this dynamic environment.”

How can smart keys address these challenges?

“One huge benefit of the mechanical key is its familiarity. So, in some cases, a mechanical locking system with patent protection may still be appropriate. However, digitalisation offers many opportunities for efficiency and compliance.”

Can you give some examples?

“A digital credential can be

programmed or deauthorised in seconds, eliminating the security risks and costs associated with lost mechanical keys. When building technology connects digital solutions for access, fire protection and escape routes, user safety and facilities management benefit. Audit capability is automated, supporting compliance, whereas manual access tracking with mechanical keys is either time-consuming or impossible.”

How can businesses streamline the transition to digital locking?

“Of course, moving from mechanical to digital access is not like flicking a switch. Many organisations cannot change everything at once, so digital systems must scale gradually as budgets allow. This is the main advantage of choosing the right programmable smart key system. It offers the smoothest transition from mechanical to digital access management.”

What are the cost implications?

“Customers are often surprised at how favourably it compares with all realistic alternatives. Smart key systems have the advantage of being the fastest, least disruptive way to switch from mechanical to digital access. Electronic or electromechanical locking cylinders may simply slot into place of legacy devices, without door damage or wiring. Facility management teams gain granular control at a relatively low cost.”

Can you quantify the potential savings?



Frank Stier stresses that smart key systems offer the fastest and least disruptive way to switch from mechanical to digital access.

“Indeed, our smart key white paper models hypothetical costs for a 100-door installation of our Cliq solution. Compared with mechanical locking, Cliq’s total cost of ownership (TCO) over a five-year period was around 64 percent lower, including purchase and installation costs.”

What are the main security benefits?

“The most important are authentication and auditing. With a smart key system, simply possessing a key is of limited benefit. Digital authentication determines whether the keyholder is permitted access, rather than relying solely on mechanical coding. Keys may be set to require periodic revalidation: without regular visits to an updater, or updating via Bluetooth, a key won’t unlock anything.”

Are there other security advantages?

“Unlike a mechanical key, a smart key controls not only who can go where, but also when – and these permissions are not set in stone. Automated logging of every access interaction speeds up investigations if unauthorised use does occur. With their authentication and security features, Cliq smart

keys are also effectively impossible to duplicate.”

Which organisations are adopting smart keys?

“In many different environments, customers find the answer to their challenges in a Cliq solution. This diversity of applications is testament to its flexibility and security. For example, Protec2 electromechanical Cliq is trusted in sensitive environments such as medicine stores at Birmingham’s Queen Elizabeth Hospital.”

Can you give more examples of installations?

“Low-impact installation makes Cliq ideal for retrofitting heritage properties, as demonstrated at Munich’s Hofbräuhaus and Dresden’s Frauenkirche. At Düsseldorf’s football stadium, eCliq – a fully electronic smart key system – makes it easy to issue temporary authorisations for contractors and event providers. Wherever deployed, smart keys deliver a tangible return on investment as our white paper explores in greater depth.”

Further reading: Download the white paper at www.assaabloy.com/group/emeia/stories/access-stories/switch-to-digital-access

AVAILABLE

DECEMBER

FIRST LOOK AT EXPOPROTECTION
PARIS (FR) · 3-5 NOVEMBER

DESIGNED
FOR WHAT'S
NEXT.

ARCHITECT®

Future-ready by design.
(Because it is smarter by design).

Most readers are designed for installation day.
Architect® II is designed for every day after.
One modular platform.
GraphCore™ intelligence.
An EAL6+ certified secure element.
New functions, credentials and security levels
are switched on over time, on the reader
already on your wall.



SSCP® VERSION
Available in December



OSDP™ VERSION
Coming soon

Supported by
SPAC
ALLIANCE
Supported by
SIA



France · UK · USA · UAE
www.stid-security.com

Alex Holmström, Acre:

“Generative AI adds a new dimension to access control”

In recent years, Acre has invested heavily and built its profile around access control and – not least – on cloud services. Now, the company has taken another step by adding an AI assistant to its Acre Access Control platform. In this interview, Alex Holmström, Executive Vice President for EMEA/APAC at Acre, answers questions on the company's investment in AI-assisted access control.

AAC (Acre Access Control) is a cloud-based physical security platform and Acre's primary access control system. Acre Via was launched at ISC West in Las Vegas; it is an AI assistant integrated into AAC that helps manage and monitor the access control system. This product launch serves as the starting point for this interview with Alex Holmström.

What is the major benefit of Acre Via?

“I would say that Acre Via and generative AI add a whole new dimension to access control by shifting from traditional reports and usage patterns to a dialogue-based interaction,” says Alex Holmström. “Instead of manually clicking

through menus, you can type questions to the AI assistant and get help with troubleshooting, analysis, or generating reports,” he adds.

Which AI applications are creating most value for end customers?

“The benefits for the end customer can be summarised in three parts: more proactive and data-driven security, automated administration, and better workplace analytics. There are several measurable benefits in the form of lower total costs and increased efficiency.”

Why has the adoption of AI in access control systems taken so long?

“The development of AI and cloud-based access systems has likely been partially slowed down by local regulations in various countries. However, various technical challenges related to data management have also hindered progress. Large amounts of data and significant processing power are required – especially when combined with AI – to generate insights such as predictive analytics.”

“The need to handle sensitive data in compliance with data protection regulations and meet privacy requirements is another factor.”

Has cost also been a factor?

“Yes, integration and cost issues have played a role, as replacing traditional on-prem solutions – whether IP-based, mechanical, or analogue systems – represented a major investment. But now it is more accessible and cost-effective, and there is also the option to retain parts of the existing hardware infrastructure while gradually migrating to the cloud and fully leveraging AI.”

How do you define the benefits of AI in an access control system – what concrete problems does AI help customers solve?

“You could say that Via is an intelligent AI layer capable of processing vast amounts of real-time data to easily solve problems – such as system administration, where everyday language can be used to create users and configure the system.”

Could you be more specific about the benefits?

“You can save time and easily generate reports instead of manually searching through logs. The AI assistant makes it quick to investigate and detect anomalies, such as unauthorised individuals or unusual activities. You get a proactive security system that gives the user complete oversight of all identities and users around the clock.”

How, specifically, can the AI assistant contribute to enhanced security?

“Access rights issues can be quickly identified, as can repeated door alarms, making it easier for the operator to rapidly make sound decisions regarding appropriate actions.

“The AI assistant also simplifies the performance of administrative tasks for operators, such as creating new users.”

Isn't there a risk that the AI might produce incorrect answers, leading to no action being taken or to irrelevant decisions?

“We have guardrails in place. These are safety mechanisms ensuring that the AI cannot make any changes to the system on its own; instead, it simply presents information and suggests possible actions that always require human approval.”

“For example, an operator can ask how the door units have trig-



Alex Holmström is Executive VP EMEA/APAC at Acre Security.

gered alarms or been used over the past week and receive a clear report visualising this data. This enhances security and offers opportunities to optimise the system.”

How does gen AI impact operational efficiency – which organisational tasks can be automated or simplified?

“Generative AI definitely boosts operational efficiency by transforming complex data flows, enabling organisations to simplify and automate system administration for cardholders and access rights, as well as to carry out more efficient maintenance, servicing, and hardware checks.”

How can AI help reduce energy consumption, optimise staffing, or otherwise make security operations more sustainable?

“Smart environmental thinking is crucial in modern security operations; AI can contribute by significantly reducing energy consumption through smarter control of facilities and processes, as well as by optimising staffing via predictive scheduling. There are numerous synergies to be gained from implementing an AI and cloud-based security system when it is integrated with other building automation systems.”

What savings or business benefits do you see customers achieving by using AI features like Acre Via?

“Several studies show that the progressive use of AI tools alone can lead to time and cost savings of over 20 percent. As a tool, Via gives users faster access to accurate information –eliminating the need to build solutions manually – and saves many hours of administrative time. It also creates a higher overall level of security when combined with cloud-based security systems.”

Why are you launching Acre Via right now?

“We acquired the company Reks in January of last year, and our R&D team has been actively working on integrating this purpose-built AI function with Acre Access Control.”

And how has the market reacted?



With Acre Via, users avoid clicking through menus; instead, they can type questions to the AI assistant and get help with troubleshooting, analysis, or generating reports.

“The market has reacted very positively, and following the international launch in Istanbul in April, we have received very positive feedback from our partners in Europe and North America. A great many end customers have also confirmed that this will significantly facilitate daily operations.”

Do you think unified platforms and AI assistants will become the primary interface between the user and the security system?

“From an interface perspective, there is definitely a demand for unified solutions and ease of use.”

“Interestingly, over the past ten years, we have moved from unified proprietary solutions to open architecture. The market wants unified, open solutions with user-friendly interfaces that allow for integration with various market-leading third-party solutions to create a strong, comprehensive system.”

“In this context, the development and secure use of AI will play a major role in the connected systems of the future.”

How are integrators – the ones delivering the systems – affected by the growing demand for AI assistance?

“Initially, they will need to drive a strong service model that combines the technology with services in their offering. They will also need an organisation



Alex Holmström on stage at the international launch of Acre Via during a conference in Istanbul, where Acre partners from around the world gathered.

capable of supporting the end customer on their journey.”

And what does that mean?

“That they must be able to manage current hardware and software while gradually migrating solutions to future reader technology and AI applications, as well as provide future-proof hardware

offering the right performance, smarter video analytics, and visitor management solutions – combined with intrusion alarms and access control systems.”

“It follows that they must, of course, listen to the end customer and build a solid foundation for the solutions needed to meet future requirements.”

Biometric access control is the key to smarter buildings

As a global leader in biometric access control, Suprema wants to see the development of smart buildings that automatically adapt to the people who use them.

One contribution to this development is the new Biostation 3 Max biometric terminal, which combines facial and fingerprint authentication with RFID, mobile access, QR codes and PIN authentication on a single platform.

With customers in 140 countries, Suprema sees continued strong growth in the smart building market. According to Ghita Charouite, the company's Marketing Manager for Europe and North Africa, biometric identification is a fundamental component of the buildings of the future.

"Biometric access control is essential for making buildings truly smart and user-friendly. Not having to use keys, cards or codes, but instead being automatically identified when approaching an entrance, is significantly more convenient," she says.

Interoperability

A single authentication should not only provide access but should also be able to control lighting, heating, ventilation, and air conditioning, as well as interact with other security systems, such as video surveillance. Integration with home automation software further enables these systems to work together seamlessly. At the same time, the building can adapt lighting, temperature, and security levels to the individual. In this way, a seamless and personalised user experience can be created.

Privacy protection

Suprema currently offers one of the market's broadest ranges of biometric authentication methods, including fingerprint authentication, facial authentication, mobile access and RFID – all within a single system.

The technology also addresses users' privacy requirements by allowing biometric data to be stored locally on the user's mobile phone

or smart card rather than on central servers.

Unique biometric terminal

Suprema's new flagship product, Biostation 3 Max, is a response to market demand for fast and secure authentication. It is based on the company's latest AI engine with a dedicated NPU and, according to Suprema, can authenticate a face in less than 0.3 seconds, even when people are moving.

The system combines facial and fingerprint authentication with RFID, mobile access, QR codes and PIN authentication on a single platform.

For demanding environments

Biostation 3 Max has been developed for environments with demanding requirements for both security and capacity, such as corporate entrances, office buildings and other business-critical facilities.

With dual 2 MP visible-light and IR cameras, the terminal can detect spoofing attempts using photographs, videos or 3D masks, while still operating effectively with sunglasses and face masks and under varying lighting conditions. The system can handle up to 100,000 registered users.

Cybersecurity

Cybersecurity has also been a major focus in the development of Biostation 3 Max. A hardened Linux operating system with Secure Boot ensures that only signed firmware can be executed, while a CC EAL6+ certified secure element protects cryptographic keys and



Biostation 3 Max reads a face in less than 0.3 seconds. The system combines facial and fingerprint biometrics with RFID, mobile access, QR codes and PIN authentication on a single platform.

credentials. Biometric templates are encrypted and all communications are secured via TLS.

Touchscreen for IP intercom

The new terminal is also equipped with a 7-inch touchscreen for guidance and information, a built-in VoIP intercom with SIP support, and an IP65-rated enclosure for both indoor and outdoor installation.

Naturally, Biostation 3 Max also supports the storage of biometric information on the user's own mobile device or smart card instead of in a central database.

Sets a new standard

Digitalisation, AI and increasing demands for energy efficiency are changing the way modern buildings are designed and managed. As part of this development, identity is becoming an increasingly important component of the smart building.

From this perspective, Suprema has launched an exceptional solution with Biostation 3 Max that sets a new standard for identity-based security, according to Hanchul Kim, CEO of Suprema Inc.

"Biometric authentication, certified hardware security and high AI performance are brought together in a single flagship terminal. Trust is built into every door," he comments.



Ghita Charouite, Marketing Director for Suprema in Europe and North Africa.

QR and RFID reader

Another major product launch is the Xpass Q2 reader, which combines QR codes, barcodes, RFID and mobile credentials via BLE and NFC in a single device. Through integration with Suprema's Biostar X platform and open APIs, the solution can be connected to third-party systems for visitor management and other digital workflows.

Part of the smart building infrastructure

Taken together, the new products illustrate how Suprema aims to make the access control system an integrated part of the smart building's digital infrastructure, where identity, AI and real-time data work together to create safer, more efficient and more user-friendly buildings.

Designed for Impact

The flush-mount Signo reader you've been asking for.



Every visible detail of a building is a design decision. Access control readers are no exception. HID Signo Décor answers what specifiers, architects and designers have been asking for — a flush-mount Signo reader, so it blends as part of the architecture. Underneath, it delivers what you expect from Signo: the same security, mobile credential support and remote management.

Available in white or black to go with any environment.



Take a closer look »
campaigns.hidglobal.com/signo



STID launches future-proof access

French developer and manufacturer STID is launching Architect II, a new generation of access control readers designed to meet increasing demands for flexibility, cybersecurity and long service life. The new series is based on the “One Core, One Firmware” principle, with all models sharing a common hardware and software platform.

A central concept behind Architect II is that the readers should be able to evolve in line with customers’ needs and new technology standards. New features can be activated and upgraded through software without having to replace the reader itself. This allows an installed reader estate to be progressively adapted to new identification and authentication requirements.

“Whenever an organisation invests in an access control system, it needs to be able to rely on the technology remaining functional and relevant for many years. With Architect II, we can add new features and technologies through software upgrades instead of requiring customers to replace installed hardware. This makes the platform both flexible and future-proof,” says Robert Jansson, Sales Director for STID in the Nordic region.

Multiple versions

Architect II is available in several versions, including a narrow-profile reader, models with a keypad or touchscreen, and a desktop reader. The platform supports RFID, NFC, BLE and wallet-based credentials and is also prepared for emerging technologies and standards such as Alio, UWB, Digital ID and mDL.

Modular platform

Architect II has a modular design that allows the readers to be enhanced with internal and external expansion modules. These can, for example, add biometric authentication, QR code reading or support for 125 kHz technology.

The idea is that the same core platform can be used for different types of installations and security levels. Organisations can therefore start with the functionality required at the time of installation and subsequently expand the system as their needs change.

High level of cybersecurity

Considerable emphasis has also been placed on cybersecurity. Architect II is built on a security platform with Common Criteria EAL6+ and FIPS 140-3 certifications, as well as support for advanced encryption, secure management of cryptographic keys and trusted firmware. The platform has been developed with cybersecurity requirements and frameworks such as NIS2, NIST and ISO 27001 in mind.

“Access control can no longer be regarded as an isolated part of physical security. Readers are connected devices and therefore also form part of an organisation’s cybersecurity. Security must therefore be built into the architecture from the outset rather than added afterwards,” says Robert Jansson.

Dual tamper protection

At the same time, security extends beyond protection against digital attacks. Since a reader is normally installed on the unsecured side of a door, it must also be capable of detecting attempts at physical tampering.

Architect II therefore features dual tamper protection based on both a smart opening switch and an accelerometer. They can operate



Robert Jansson emphasises the importance of cybersecurity in all connected devices. Security must therefore be built in from the start, as an integral part of the architecture, rather than added afterwards.

independently or together to detect attempts to open, remove or move the reader. If tampering is detected, the reader can automatically delete its cryptographic keys and/or send an alert to the access control system. This means the protection responds both to physical opening and to attempts to remove or manipulate the reader, rather than relying solely on a conventional tamper switch.

“An access control reader is often installed on the side of the door that anyone can access. It is therefore not enough simply to protect communications and digital keys. You also need to be able to detect if someone attempts to tamper with the device itself. By combining electronic detection with mechanical tamper protection, we provide two independent layers of protection,” says Robert Jansson.

Designed for demanding environments

Architect II is also designed for demanding environments. The

readers have IK10 and IPX5 ratings and are specified for operation at temperatures ranging from –40°C to +70°C. The combination of robust construction and a wide operating temperature range makes the platform suitable for both indoor installations and exposed outdoor environments.

Long product life

The common platform and the ability to upgrade functionality through software are also part of STID’s sustainability strategy. Together with low energy consumption, this is intended to contribute to a longer product life and reduce the need to replace existing hardware when new features or technologies are introduced, according to Robert Jansson.

“This becomes particularly important in larger access control systems with hundreds or thousands of installed readers, where a technology transition could otherwise involve extensive hardware replacement,” he says.

control reader platform



New functions can be activated and upgraded via software in Architect II readers without replacing the reader itself, making the platform future-proof for new authentication requirements.

Future-proof solution

With Architect II, STID aims to provide a reader platform that can continue to evolve to meet future requirements for

digital identities, authentication methods and cybersecurity.

“For us, future-proofing is about technology, sustainability and economics. Customers

should not have to replace their readers simply because a new type of credential, digital identity or authentication method becomes relevant. Architect

II is built to evolve alongside these developments,” concludes Robert Jansson.

A flying start for Architect II – wins award for innovative achievement

This autumn, STID has launched its major product release of the year – Architect II. And it is off to a flying start. The reader has already received an Innovative Achievement Award at the Detektor International Award 2026 ceremony, held during the Skydd security exhibition in Stockholm on 20 October.

The security industry magazine Detektor established the Detektor International Award in 2000 and has since annually recognised the year’s most innovative products in four different categories.

Architect II was one of three products in the ID & Access

Control category to receive an award at this year’s ceremony.

Commenting on why Architect II received the Innovative Achievement Award, Detektor’s Editor-in-Chief quoted part of the jury’s motivation:

“It combines certified cyber-



STID’s Robert Jansson, Sales Director for the Nordic region, accepted the Innovative Achievement Award for Architect II at the Detektor International Award ceremony in Stockholm on 20 October.

security with modular hardware and software-enabled upgrades, allowing functionality to evolve

without replacing the installed reader. That is a great achievement by STID,” he said.



Interview with James McHale, Memoori:

“Cloud, AI and M&A reshape the access control market”

The global physical access control market is undergoing a significant transformation. Cloud platforms, mobile credentials and AI are changing both technology and business models, while continued M&A activity is reshaping the competitive landscape.

In this article, James McHale, founder and CEO of Memoori, answers questions about the current state of the access control market and what we can expect in the years ahead.

Physical access control is increasingly evolving from standalone door security towards software-defined platforms integrated with smart building operations. At the same time, recurring software revenues and cloud services are becoming more important.

James McHale's answers to Detektor's questions are based on Memoori's latest report, *The Physical Access Control Business 2025 to 2030*, in which Memoori analyses the global market for access control hardware, software and credentials.

How large is the global physical access control market?

The global physical access control market reached \$15.1 billion in 2024 and is projected to grow to \$21.3 billion by 2030, representing a compound annual growth rate of 5.94 per cent.

How concentrated is the market?

Companies with more than \$1 billion in access control revenues account for approximately 24.4 per cent of global revenues. However, mid-sized specialists remain particularly important. The 28 companies with revenues between \$100 million and \$1 billion collectively account for 64 per cent of the global market.

Which regions are driving the growth?

Asia Pacific is expected to overtake Europe as the second-largest access control market by 2030. Unlike mature markets, where much of the business is driven by retrofits, growth in Asia Pacific is being fuelled by new construction across offices, logistics, manufacturing and government facilities.

What is happening in terms of mergers and acquisitions?

M&A activity remains strong. Between September 2023 and September 2025, 16 transactions with a combined value of \$7.9 billion were completed. The largest was Honeywell's \$4.95 billion acquisition of Carrier's access control business.

What about investment in access control companies?

Venture capital investment has declined significantly from its 2021 peak, but investment continues, particularly in unified cloud platforms. Between September 2023 and September 2025, 12 investment deals brought more than \$326 million in disclosed funding into the sector.

What are the biggest changes taking place in access control?

Physical access control is evolving

from standalone door security into a software-defined platform at the centre of smart building operations. Cloud architectures, mobile credentials and artificial intelligence are reshaping how organisations secure facilities, manage identities and optimise workplace experiences.

How is this changing the business model?

Value is increasingly shifting from traditional hardware margins towards recurring software revenues, managed services and cloud subscriptions. The industry is gradually moving from product sales towards platform economics and longer-term service relationships.

What role are mobile credentials playing?

Mobile credentials represent a significant change in how organisations provision, manage and revoke access rights. The market is moving from proprietary app-based credentials towards wallet-native credentials embedded directly in Apple Wallet and Google Wallet, enabling tap-to-enter access without users having to unlock their devices.

What exactly does the report cover?

The report analyses the global access control market across three core revenue categories: hardware, including electronic locks, readers and control panels; credentials, including cards, mobile credentials and biometrics; and software, covering both on-premises and cloud-based platforms. The analysis evaluates 273 active companies worldwide.

Which technology trends are particularly important?

Cloud and Access Control as a Service, AI and machine learning, mobile access control, biometrics, multifactor authentication, IP



James McHale, founder and CEO of Memoori.

and IoT, interoperability, systems integration, cybersecurity and data privacy.

Does the report cover all these trends?

Yes, but it also examines sustainability, supply chains, M&A, strategic alliances and investment trends.

Why is the report particularly relevant now?

Because it examines not only the size and growth of the market, but also how the underlying business is changing. It looks at where revenues and profits are moving, which technologies and business models are attracting investment, how M&A is reshaping the competitive landscape and how strategic alliances are influencing interoperability and the development of multi-vendor ecosystems.

*Footnote: Memoori's full report, *The Physical Access Control Business 2025 to 2030*, can be ordered at www.armedia.selen/ under the "Reports" section.*

All you need for Access Control & Security

Two platforms. Total control.

BioStar 

on **Premise**

- Perfect fit for SMB and Enterprise requests
- Integrating AI-Driven Access Control with Intelligent Video Analytics
- Enhancing Operational Efficiency and Security with a Unified Platform



BioStar **Air**

in the **Cloud**

- 100% cloud-based access control
- No servers to set up, no extra door controllers
- Sites management from anywhere



suprema

366 Ter rue de Vaugirard, 75015 Paris
T : +33 1 84 73 29 43
W : www.supremainc.com
E : sales_eu@supremainc.com



Robot successfully tested in access controlled power station

Dormakaba, Anybotics and Legic have successfully partnered in tests to demonstrate that autonomous inspection robots can now move through access-controlled doors in industrial environments just like authorised employees. The collaboration lays the foundation for a future solution that will enable industrial customers to integrate autonomous robots into existing access-controlled environments.

The pilot demonstrates how robotics, secure digital identity and access management can work together in a live industrial environment. The so called “Anymal” robot from Anybotics uses a secure digital credential to request access to controlled areas. Dormakaba’s access management and door automation then apply the same access rules used for authorised personnel, allowing the robot to pass through doors without manual intervention.

“Autonomous robots are becoming part of the workforce in industrial environments. Like people, they need reliable and secure access to the areas where they perform their tasks. Together with our partners, we are showing how access management can enable robots to move securely and autonomously through controlled environments while keeping access firmly under the operator’s control,” says Till Reuter, CEO of Dormakaba.

Opening the door to autonomous inspection

Autonomous mobile robots are increasingly being used for inspection and monitoring in industrial facilities. They can perform repetitive tasks, collect data, and identify potential problems while reducing the need for people to enter potentially hazardous areas.

Access-controlled doors, however, can become a barrier for autonomous machines. The joint pilot addresses this challenge by giving the robot a secure digital identity and integrating it into existing access processes. The robot can request access electronically and the access management

“Autonomous robots are becoming part of the workforce in industrial environments. Like people, they need reliable and secure access to the areas where they perform their tasks.”

system determines whether the door should open based on pre-defined permissions.

This allows operators to maintain control over who or what can access specific areas, regardless of whether the authorised user is a person or an autonomous machine.

Proven in a live operating environment

The pilot was conducted at GE Vernova’s Whitegate power plant in County Cork, Ireland, in a live operating environment. The Anymal robot has been operating reliably for several weeks, repeatedly requesting access, passing through controlled doors, and



Photo: Dormakaba

At the Legic Connect26 conference in Zurich, the autonomous inspection robots were presented by Dormakaba, Anybotics and Legic.

continuing its inspection routes without manual intervention.

The pilot also demonstrates

how the three technologies are integrated: Anybotics provides the autonomous mobile robot and robotics platform, Legic provides the secure digital credential technology, and Dormakaba provides the access management and automated door solutions.

Next step – commercialisation

The partners are now working to make the solution commercially available while exploring further applications, including access to elevators, gates, and turnstiles.

Dormakaba, Anybotics, and Legic also presented the pilot at the Legic Connect26 event in Zurich in September.

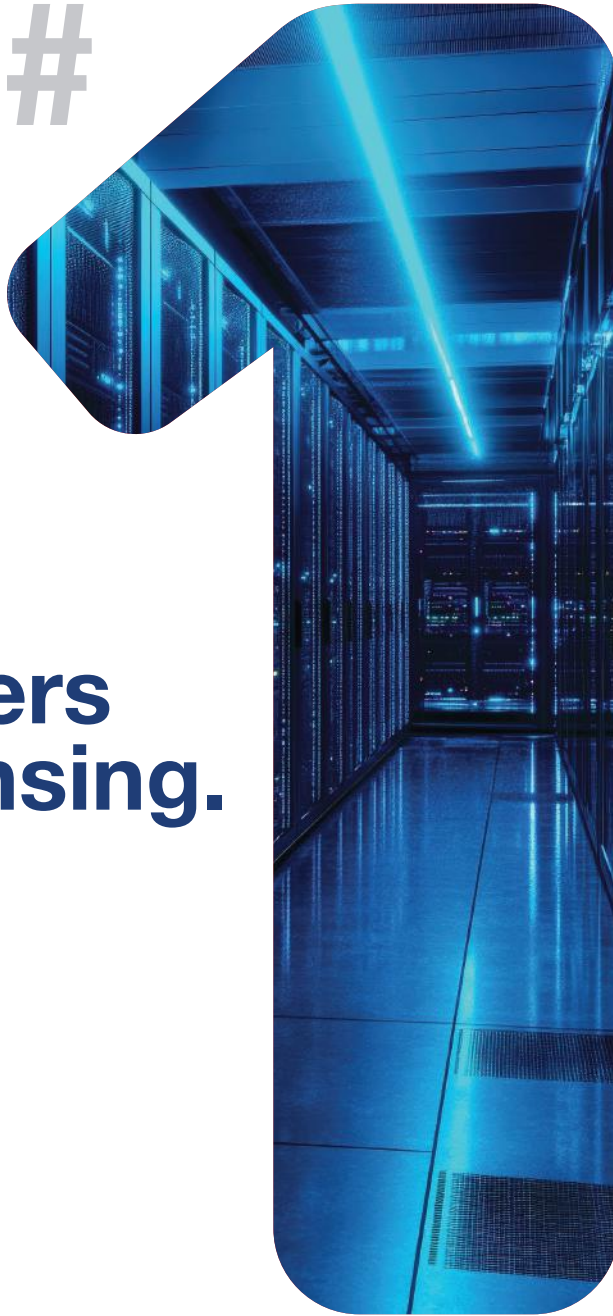


Photo: Dormakaba

Till Reuter, CEO of Dormakaba.

“Autonomous mobile robots are increasingly being used for inspection and monitoring in industrial facilities.”

#



**Leaders
in sensing.**

**Trusted
worldwide.**

Deployed in thousands of critical infrastructure sites globally, OPTEX security sensors are trusted for their accuracy and long-term reliability, setting the benchmark for excellence as the number one choice worldwide.

optex-europe.com



Image: AI-generated

Europe continues to invest heavily in securing transport infrastructure and external borders, including airports, seaports, rail networks and border crossings.

European perimeter security market hits €19.4 billion in 2026

Northbrook, IL (USA)

The latest report from Marketsandmarkets, with forecasts through 2031, suggests that the European perimeter security market is projected to grow from \$22.00 billion (equivalent to €19.4 billion) in 2026 to \$29.47 billion (equivalent to €26.0 billion) by 2031, representing a CAGR of 6 percent during the forecast period.

According to Marketsandmarkets, Europe continues to invest heavily in securing transportation infrastructure and external borders through modernisation initiatives covering airports, seaports, rail networks, logistics hubs and border crossing points.

Growing demand

Programmes led by European institutions and national authorities increasingly incorporate AI-enabled video surveillance, thermal imaging, intelligent fencing, intrusion detection sensors and automated access management to strengthen operational security and support the efficient movement of passengers and freight. These long-term public infrastructure investments are creating sustained demand for advanced perimeter security systems throughout the region.

Security systems dominate

The systems segment is expected to account for the largest share of the European perimeter security

market during the forecast period, driven by the increasing deployment of AI-powered video surveillance, perimeter intrusion detection systems (PIDS), access control, radar, thermal imaging and intelligent alarm systems across critical infrastructure, transportation, industrial, government and commercial facilities.

Modernisation drives growth

Rising investment in integrated, multi-layered security architectures, coupled with the modernisation of airports, energy facilities, border security and smart infrastructure, is driving demand for advanced perimeter security systems that provide real-time monitoring, threat detection and enhanced situational awareness.

Continuous advances in edge AI, high-resolution imaging, intelligent analytics and seamless integration with centralised security management platforms are further accelerating the replacement of legacy security infrastructure across Europe.

Managed services

The managed services segment is expected to grow at the fastest rate in the European perimeter security market as organisations increasingly outsource system monitoring, preventive maintenance, remote diagnostics, cybersecurity management and lifecycle support for complex security environments.

Critical infrastructure operators, airports, utilities, industrial facilities and commercial enterprises are increasingly relying on managed service providers to ensure continuous system availability, rapid incident response, software updates and regulatory compliance.

The growing adoption of AI-enabled surveillance, cloud-based security management platforms and integrated multi-site perimeter security solutions is further accelerating demand for managed services across Europe. The shift from capital expenditure towards subscription-based security models, combined with a shortage of skilled security personnel, is also encouraging organisations to adopt outsourced perimeter security management services.

France is the largest market

France is expected to account for the largest share of the European perimeter security market during the forecast period, owing to

substantial investment in critical infrastructure protection, border security, transportation networks, defence facilities, nuclear energy sites and smart city initiatives.

The country is accelerating the deployment of AI-enabled video surveillance, perimeter intrusion detection, thermal imaging, radar systems and integrated access control across airports, rail networks, utilities and government facilities.

The presence of leading security technology companies such as Thales, together with the continued modernisation of national security infrastructure and increasing adoption of intelligent perimeter protection solutions, is further strengthening France's position in the regional market. In addition, government-backed initiatives to enhance national resilience, expand domestic security technologies and strengthen the country's security industry ecosystem are supporting sustained market growth.

Key players

Some of the key players in the sector named in the report are Bosch Security Systems, Honeywell, Axis Communications, Johnson Controls, Siemens, Senstar, Teledyne FLIR, Optex, Southwest Microwave, Dahua Technology, Hikvision, Panasonic, Pelco, Gallagher Security and Thales.



AI and drones are changing how perimeters are monitored

The global perimeter security market is growing by around 7-9 percent annually – driven largely by geopolitical tensions and an increasing number of terrorist attacks.

AI, integrated solutions and drones are among the biggest trends in the market and were also in focus when an expert panel discussed perimeter security at the latest Sectech event in Stockholm.

The global perimeter security market was estimated at \$81.4 billion in 2024 and, according to MarketsandMarkets, is expected to reach \$114.2 billion by 2029, representing a compound annual growth rate (CAGR) of 7.1 percent. A slightly older report from Grand View Research valued the market at \$64.6 billion in 2023 but projected a higher CAGR of 9.4 percent, with the market expected to reach \$132.4 billion by 2030.

Threats from above

During a panel discussion at Sectech last autumn, experts discussed how AI, drone technology and integrated solutions are redefining the way critical infrastructure, industrial sites and other sensitive facilities are protected.

“With today’s technologies, you don’t always need a high fence with barbed wire and electrification, because you can add layers of AI, cameras, lidar and other technologies. But the threat no longer comes only from the ground – it also comes from the air,” said Matt Wills, European Technical Manager at Gallagher Security.

This development has been driven by several factors: geopolitics, the commercialisation of drones, cybersecurity – with increased digitalisation creating new attack surfaces – and AI, which has enabled more accurate and cost-effective solutions for detecting and analysing threats.

Thomas Lindblad, Sales Manager Nordic Solutions at Heras, also emphasised that customers’

attitudes have changed.

“A few years ago, customers talked about what they should have. Today, they actually get the products they need. Previously, they might have purchased radar, video analytics or electric fencing separately, but now we are seeing growing demand for a mix of these technologies.”

AI transforms monitoring

AI-powered video analytics has the potential to radically improve alarm accuracy and reduce the number of false alarms.

“We are now seeing cameras that combine AI and machine learning, providing a much better understanding of what the camera is actually seeing. The market potential for these fusion cameras is enormous, but the focus should not only be on reducing false alarms. The most important thing is not to miss genuine threats,” said Thomas Lindblad.

Drone technology

The role of drones in perimeter security was discussed both as a threat and as an opportunity. They can be used to carry out sabotage or espionage, but also to monitor and protect large areas.

“We are seeing drone technology becoming increasingly common, and the commercialisation of drones makes it easier for potential attackers to target facilities. With that in mind, we also need to consider the cybersecurity of these products and how AI can be integrated to counter these threats,” said Matt Wills.



Image: AI-generated

AI-powered video surveillance is expected to help reduce false alarms, while drones could become a powerful tool for verifying threats.

Technologies in synergy

There is no one-size-fits-all solution for perimeter monitoring. Instead, different technologies need to be combined to create tailored solutions that meet the customer’s specific requirements.

“Each individual component has its own strengths that can contribute to the overall value of the system. The ideal solution is a combination of security cameras, AI for drone detection and physical security,” said Glenn Michiels, Head of Product Management EMEA at i-Pro.

Different requirements

Gustav Norvik, who at the time of the conference was Business Manager for Video at Securitas Technology and is now with Pacom, highlighted how customer requirements vary considerably depending on what needs to be protected.

“It depends on the type of area you want to defend. Is it a high-security facility such as a military site or a power plant? Or is it an industrial customer with some machinery and diesel fuel? The intruder may have different capabilities, and the business model also plays a role.”

False alarms and regulations

False alarms create unnecessary costs and can cause operators to become less attentive to genuine threats.

“Ten years ago, an alarm receiving centre in Sweden had 7,000 false alarms every day. Today, they have many more cameras but significantly fewer false alarms. AI has really improved accuracy,” said Thomas Lindblad of Heras.

However, challenges remain.

“AI is very accurate, but the problem arises if I dress up as a ghost with a sheet over me. Then AI doesn’t see me as a human being, but as something else,” said Gustav Norvik.

Legislation needs to adapt

The panel concluded with a discussion about the future of perimeter monitoring, where AI is expected to play an increasingly important role in analysing sensor data and reducing false alarms.

Autonomous drones and ground vehicles are expected to be able to verify threats rapidly, but the panel emphasised that drone legislation needs to adapt if the technology is to be used to its full potential.

Jimmy Ek, Axis Communications:

Technology with Built-in AI Analytics – a

Modern perimeter security solutions rely on intelligent, multi-layered systems in which AI-powered video analytics, radar, thermal cameras and network speakers work together, according to Jimmy Ek, Nordic Sales Manager at Axis Communications.

“Edge-based analytics are crucial in security scenarios where immediate action is required to prevent or mitigate threats,” he says.

In recent years, demand for perimeter security solutions has increased significantly. One contributing factor is the growing threat landscape, combined with increasingly advanced and accessible security technologies.

According to Jimmy Ek, critical infrastructure, transport hubs and commercial properties are among the sectors where demand has risen noticeably.

“The current geopolitical climate has also contributed to critical infrastructure, such as power plants, water treatment facilities and other essential services, becoming targets for malicious activities,” he says.

Multi-layered security

Axis’ product portfolio includes network-based AI-powered security cameras, thermal cameras, radar and speakers, which can be integrated to strengthen perimeter security.

- Network cameras with advanced video analytics enable highly accurate detection and classification of objects, people and vehicles. They can distinguish between normal activities and potential threats, helping to minimise false alarms.

- Thermal cameras perform particularly well in low-light conditions and other challenging environments. They detect heat signatures, making them ideal for night-time surveillance and situations where visibility is limited.

- Radar can detect moving objects within a defined perimeter area, delivering consistent performance regardless of weather conditions. This makes it particularly useful for early warning and intruder tracking.

- Network speakers provide a proactive security tool, enabling real-time communication to issue warnings, give instructions or play deterrent messages to potential intruders.

These technologies complement each other, creating a multi-layered security solution

“The current geopolitical climate has also contributed to critical infrastructure, such as power plants, water treatment facilities and other essential services, becoming targets for malicious activities.”

that provides a robust foundation for perimeter surveillance, with strong detection, verification and response capabilities.

Complementary technologies

Although network cameras, thermal cameras, radar and speakers generally cover the primary requirements for effective intrusion detection and verification, other technologies can also contribute to a perimeter security solution, according to Jimmy Ek.

“Integrating additional technologies, such as access control systems and video management



Jimmy Ek highlights the significant benefits of cameras with built-in AI analytics for perimeter security.

systems (VMS), can further strengthen the overall security strategy,” he says.

However, one detection technology used in perimeter security that Axis does not provide is lidar (Light Detection and Ranging).

nologies by adding further layers of detection and verification,” he explains.

Speakers deter intruders

Network speakers are a speciality within Axis’ product portfolio and are becoming increasingly common in perimeter security applications.

They can be used to deter potential intruders and manage security incidents in real time. Strategically positioned around a perimeter, they can broadcast warnings, instructions or deterrent messages.

“For example, when an intrusion is detected, a pre-recorded or live message can be broadcast to warn the intruder that the area is under surveillance and that the police have been alerted.”

Axis’ experience with network speakers and deterrent voice messages indicates that they can significantly improve perimeter security effectiveness. In many cases, a warning message alone can persuade potential intruders to abandon their intentions.

“Speakers can also be used to provide clear instructions during emergencies, helping to manage crowds and ensure safe evacuation procedures.”

key to more effective perimeter security

Cameras with built-in AI

Jimmy Ek highlights the clear advantages of using video surveillance cameras with edge-based AI analytics in perimeter security applications. This means that AI analytics are embedded directly in the cameras, rather than being processed in the cloud or on local servers.

“Edge-based analytics process data directly in the camera, reducing latency and ensuring real-time detection and response. This is crucial in security scenarios where immediate action is required to prevent or mitigate threats.”

Greater security with edge AI

Edge-based analytics also minimise bandwidth consumption, as only relevant data, such as alarms and events, are transmitted to the central system.

“This reduces the load on network infrastructure and ensures more efficient use of resources. Edge-based solutions also improve privacy and security because sensitive information is processed locally within the device rather than transmitted across the network.”

Another advantage is greater operational reliability, as edge-based analytics can continue functioning even if the network connection is interrupted.

This ensures continuous monitoring and detection capabilities, which are essential for robust perimeter security.

Fewer false alarms

Cameras with AI-powered edge functionality can use machine learning and deep learning to enable highly accurate detection and classification of objects, people and vehicles.

According to Axis, this delivers better results than traditional network cameras with basic video analytics and motion detection, which often rely on simpler algorithms and may generate false

alarms due to environmental factors or harmless movements.

“Our AI-powered edge analytics use sophisticated algorithms trained on large datasets to distinguish between different objects and activities with high precision. This reduces false alarms and allows security personnel to focus on genuine threats,” says Jimmy Ek.

The human role remains essential

Machine learning and deep learning are changing the role of security operators. The technologies enable greater automation in decision-making processes, making threat detection and response more efficient.

“Algorithms can, for example, automatically classify objects, detect unusual behaviour and predict potential security breaches based on historical data and patterns,” Jimmy Ek points out.

However, he emphasises that although automation can handle many aspects of perimeter security, human operators should always be involved in critical decisions.

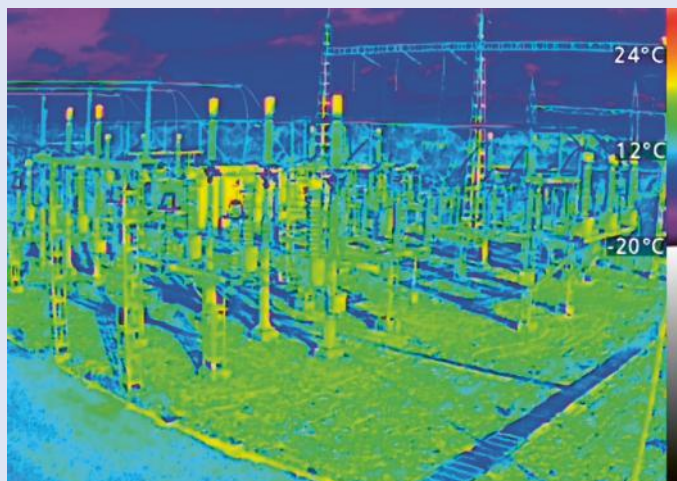
“Human judgement is essential for assessing complex situations, making ethical decisions and managing responses that require nuanced understanding and communication.”

More responsive security ecosystems

Asked which technological breakthroughs will transform the perim-

“Our AI-powered edge analytics use sophisticated algorithms trained on large datasets to distinguish between different objects and activities with high precision.”

eter security market over the next three to five years, Jimmy Ek says that advances in AI and machine learning will continue to improve the accuracy and capabilities of



Thermal cameras detect heat signatures, making them ideal for surveillance at night and in conditions of limited visibility.



Network speakers are a speciality within Axis' product portfolio and have also become increasingly common in perimeter security applications.

security systems.

“The development of more advanced sensor technologies, such as improved radar and lidar systems,

responsive security ecosystems,” he says.

5G and edge computing

Axis' Nordic Sales Manager also believes that the adoption of 5G and edge computing will enable faster data processing and real-time analytics, further improving the effectiveness of perimeter security solutions.

“Together, these technological advances will contribute to more robust, intelligent and adaptable security systems, ensuring better protection and operational efficiency across different sectors and applications,” Jimmy Ek concludes.

Data secure – physical security

As datacentres become increasingly critical to society, protecting them from disruption is essential. While major investments are made in cybersecurity, reliable physical security and early intrusion detection are just as important. Mark Cosgrave, EMEA Marketing Director at Optex Security, explains how modern detection technologies can help operators protect their facilities.

Europe's digital infrastructure is entering a new phase of growth. Demand for cloud services, AI computing and resilient data storage is driving rapid expansion in datacentre capacity, with operators building larger facilities to support increasingly intensive workloads.

The importance of physical security

From healthcare and financial systems to transport and public services, datacentres underpin essential services across the region. As these facilities grow in scale and importance, so does the need to protect them from disruption and intrusion, with the EU's NIS2 Directive and Critical Entities Resilience Directive placing greater emphasis on physical security.

Mark Cosgrave, EMEA Marketing Director at Optex Security, emphasises that the consequences of physical security breaches should not be underestimated.

"While cyber attacks dominate headlines, physical security threats pose equally serious risks, resulting in downtime, data loss and loss of customer trust, consequences that cannot be stopped by firewalls alone."

EMEA expansion

Datacentre capacity across Europe, the Middle East and Africa (EMEA) is forecast to grow by around 10% annually through to 2030, with approximately 13 GW of new capacity expected to come online.

Established hubs including Frankfurt, London, Amsterdam, Paris and Dublin – collectively

known as FLAP-D – continue to expand. Together, these markets reached around 3.8 GW of operational capacity by the first half of 2026, with a further 1.4 GW under construction and 2 GW in the planning pipeline.

However, constraints around power availability, grid connections, land and planning permission are pushing operators towards new locations. Milan and Warsaw are attracting growing interest, alongside locations ranging from rural Spain to northern Sweden, where land is cheaper and access to power and planning permission can be easier to secure.

Growing demand for scalable security

In the Middle East, Abu Dhabi and Dubai remain established markets, while Riyadh has significant capacity under development. Access to power, land and government-backed investment is reshaping the geography of digital infrastructure.

According to Cosgrave, this geographical expansion also has implications for physical security.

"As datacentre facilities spread beyond major urban centres into more remote and rural areas, the importance of adaptable and scalable security systems only increases for operators," he says.

The threat landscape

Physical security breaches remain a significant issue for datacentre operators, often involving malicious insiders, unauthorised contractors or coordinated attempts to access facilities during protests or acts of vandalism. In co-location environ-



As datacentres expand into remote and rural areas, the need for adaptable and scalable security solutions continues to grow.

ments, where multiple organisations share a site, controlling access and defining responsibilities is even more challenging.

Many datacentres across EMEA are located near urban areas to ensure low latency and strong connectivity. This increases exposure to traffic, pedestrians and environmental factors, placing greater emphasis on reliable physical security.

The first line of defence

Effective security begins at the outer perimeter. Traditional systems can generate false alarms caused by wildlife, weather or changing light conditions.

Cosgrave highlights the operational consequences, particularly at facilities where security systems must function reliably around the clock.

"And repeated false alarms can also lead to alarm fatigue, increasing the risk that genuine incidents or intrusions are missed."

These challenges are particularly relevant across EMEA, where datacentres face varying weather and light conditions, as well as temperature extremes.

High-precision detection

Modern intrusion detection technologies, such as 2D lidar, address these challenges by providing highly accurate detection. By

analysing object size, location and distance, lidar sensors can filter out birds, small animals and environmental interference while creating an invisible detection curtain along site boundaries.

Lidar also offers resistance to harsh weather conditions and accurate detection at temperatures as low as -40°C. When an intrusion occurs, security teams receive real-time location data, enabling faster responses.

Combining detection technologies

Cosgrave points out that the choice of detection technology must reflect the characteristics of each facility.

"However, no single technology suits every perimeter. Datacentre sites vary widely and each has different requirements."

Fibre optic sensing complements lidar. Sensing cables mounted on fences or walls, or buried underground, can detect climbing, cutting or digging attempts, while lidar protects entry points and reinforces high-risk areas.

Combining these technologies allows operators to match detection methods to different parts of the perimeter, creating multi-layered protection.

For Cosgrave, the most important factor is how quickly an intrusion is identified.

challenges facing datacentres



“While cyberattacks dominate headlines, physical security threats pose equally serious risks, resulting in downtime, data loss and loss of customer trust, consequences that cannot be stopped by firewalls alone”

The most valuable assets in a datacentre are found at rack and server level, where insider threats, such as unauthorised USB access, demand immediate detection and prevention.

“Detecting an intruder early is what makes every other layer more effective. The earlier an intrusion is detected, the more time security operators have to verify the alarm, locate the intruder and respond before they reach a sensitive area such as a data hall or server rack.”

Securing access points

Inside the perimeter, turnstiles, key cards and airlocks restrict entry and strengthen security in sensitive areas.

At vehicle gates and mantraps, lidar also helps prevent tailgating and detect individuals or vehicles lingering in blind spots – essential capabilities for high-security datacentres operating around the clock.

However, Cosgrave explains that verifying credentials does not necessarily establish how many people have entered.

“Inside the building, while access control systems can verify credentials, they may not be able to identify how many people have passed through.”

People-counting technology, such as Optex’s OV-102, monitors

doors, passages and turnstiles, alerting operators when the number of people passing through does not match the number of credentials presented.

Exterior walls, roofs and surrounding grounds can also be monitored using lidar to detect suspicious approaches or attempts to gain rooftop access, even in poor light or harsh weather.

Preventing rack attacks

Preventing unauthorised downloads of sensitive data or intellectual property, as well as the uploading of malware onto servers, is critical.

Cosgrave stresses that protection must extend beyond the perimeter and access points to the most sensitive equipment.

“The most valuable assets are found deep inside the facility, at rack and server level. Insider related incidents, such as the insertion of a USB stick, can happen very quickly, so detection and prevention must be too.”

Solutions such as Optex’s Red-scan Lite use time-of-flight (ToF)

lidar technology to monitor spaces as small as 200 mm, detecting even a hand or USB device within 100 milliseconds.

Combined with cable tamper detection solutions such as Optex SecureLAN, these systems can trigger immediate alerts or automatically shut down network connections to prevent data loss.

A multi-layered approach

As datacentres expand across EMEA, security expectations will continue to rise. The most effective strategy combines perimeter protection, controlled access, internal monitoring and rapid response, tailored to local conditions and site-specific risks.

Cosgrave emphasises the importance of combining technologies to give security personnel sufficient time to act.

“Using complementary technologies, such as lidar and fibre optic sensing, and detecting threats early gives security teams the time to verify, locate and respond before critical assets are at risk.”



Mark Cosgrave, EMEA Marketing Director at Optex Security.

Physical security is critical to data protection

Cosgrave believes that modern detection technologies can help EMEA datacentre operators meet growing regulatory demands while supporting the region’s reputation for reliability, sustainability and trust. He concludes by highlighting physical security and cybersecurity as equally important elements of datacentre resilience.

“While cybersecurity will always be essential, physical security is equally critical to safeguarding society’s data.”



The Detektor magazine's editor-in-chief, Lennart Alexandrie (left in the picture), congratulated the first prize winners: Alexander Holmström (Acre Security), Björn Adméus (IQsight), Eelko Griepink (Optex) and Nedim Eskinazi (Brivo).

Detektor International Award 2026

This year's most innovative products were awarded in Stockholm

On 20 October, the winners of the 2026 Detektor International Award were announced during Skydd in Stockholm, Scandinavia's largest security trade fair. On the Tech Stage at Stockholmsmässan, 12 manufacturers received awards for products and solutions distinguished by innovation and customer value.

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.

"The 2026 Detektor International Award reflects, in particular, how the industry has embraced AI-powered solutions to simplify management and significantly enhance the user experience, while adding more advanced functionality," he added.

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 and receiver of either the Innovative Achievement Award or the first prize: Best Product Award.

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 four countries

The winners are selected by a jury consisting of seven members from

Detektor's editorial board. The jury includes editors from Sweden (3), Denmark (1), the UK (2), and Taiwan (1).

Alarm & Detection – the first prize winner

The first prize in the Alarm & Detection category was awarded to **Optex** from Japan for their *TXI Series*, a range of outdoor high-mount curtain detectors for perimeter protection.

ID & Access Control – the first prize winner

The first prize in the ID & Access Control category went to **Acre Security** from USA for *Acre Via* – a generative AI assistant for Acre's security platform, initially focused on access control.

Video Surveillance – the first prize winner

In the Video Surveillance category, **IQsight** from the Netherlands took the first prize for their *I/A Pro Context*. It is an AI-powered video analytics solution that combines established video analytics with generative AI and large vision models.

IoT & Security Solutions – the first prize winner

Brivo, an American company, received first prize in the IoT & Security Solutions category for their *Brivo Genius Mobile Agent*, an agentic AI solution for mobile security management.

The award recipients for Innovative Achievement

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

In the Alarm & Detection category, **Alarmtech** from Sweden was recognised for its *AOD 100*, an advanced opening detector for doors and windows, designed as a secure alternative to traditional magnetic contacts. They shared the award with Ukrainian manufacturer **Ajax Systems**, recognised for their *Superior Hub G3 Jeweller* – a wireless intrusion alarm control panel designed to protect even high-risk sites requiring EN 50131 Grade 3 protection.

In the ID & Access Control category, **STID Security** from France was awarded for *STID Architect II*, alongside **HID** from USA which

Alarm & Detection



Johan Rääkkönen of Ajax Systems, Eelko Griepink of Optex and Helena Dahlström of Alarmtech accepted the awards on behalf of their companies in the Alarm & Detection category.

ID & Access Control



The three award recipients in the ID & Access Control category were Robert Jansson of STID Security, Alexander Holmström of Acre Security and Philip Svensson of HID.

IoT & Security Solutions



Lars Kämpe of Zenitel, Nedim Eskinazi of Brivo and Kenneth Mohncke of Aritech represented the award-winning companies in the IoT & Security Solutions category.

Video Surveillance



Andreas Silvede of Genetec, Björn Admés of IQsight and Christopher Åkesson of OpenEye represented the award-winning companies in the Video Surveillance category.

received recognition for the **HID M1 Transparent Gateway**. In the Video Surveillance category, **Genetec** – the Canadian software company, – received the award for their cloud-based unified security platform **Security Center SaaS** with its new investigation feature, while **Openeye**, from USA, shared the honour for their AI-powered

feature **AI Visual Check**. Finally, in the IoT & Security Solutions category, **Aritech** from USA was honoured for its unified security platform, **Fusion**, alongside **Zenitel** from Norway, which received recognition for the **VALA** – an all-in-one platform for public address and voice alarm (PAVA) systems.

Outstanding solutions

The Detektor International Award comprises a first prize (Best Product Award) and a joint second prize (Innovative Achievement Award). However, at the award ceremony in Stockholm, Lennart Alexandrie, editor-in-chief of Detektor, emphasised that all 12 nominated manufacturers deserve

to be recognised as winners.

“Being selected as one of the twelve nominated products and solutions means meeting our jury’s criteria and standing out from hundreds of other products. In that sense, all twelve nominated manufacturers are equally deserving winners and rightful recipients of the award,” he said.

Detektor International Award 2026 – The winning products and solutions

Alarm & Detection

Best Product Award 2026

- **TXI Series** by **Optex**, Japan



OPTEX TXI Series is a range of outdoor high-mount curtain detectors for perimeter protection. Designed for installation at heights of 2.2–4 metres, the detectors create a narrow detection zone along walls, windows and boundaries. Adjustable detection range, a look-down

zone and Triple AND Logic help provide reliable detection while reducing unwanted alarms.

THE JURY'S MOTIVATION: "By combining purpose-built high-mount curtain detection with Triple AND Logic, OPTEX TXI Series delivers reliable perimeter protection while reducing unwanted alarms – a truly innovative solution to the challenges of high-mounted outdoor detection."

The Innovative Achievement Award 2026

- **AOD 100** by **Alarmtech**, Sweden
- **Superior Hub G3 Jeweller** by **Ajax Systems**, Ukraine



Alarmtech AOD 100 is an advanced opening detector for doors and windows, designed as a secure alternative to traditional magnetic contacts. Designed to meet the stringent security requirements of EN 50131-2-6, Grade 4, it uses a dynamic magnetic field and encrypted communication to authenticate the contact, providing

reliable detection and enhanced protection against tampering and manipulation.

THE JURY'S MOTIVATION: "By combining a dynamic magnetic field with encrypted challenge-response communication, AOD 100 reinvents the traditional magnetic contact as an authenticated opening detector with significantly stronger protection against manipulation and sabotage"



Superior Hub G3 Jeweller is a wireless intrusion alarm control panel designed to protect even high-risk sites requiring EN 50131 Grade 3 protection. It supports up to 250 devices and uses Ajax's

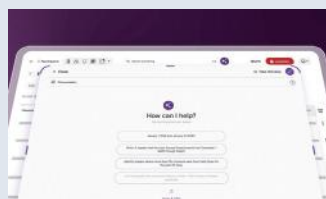
long-range radio technologies, with anti-jamming protection and multiple communication paths via Ethernet, Wi-Fi and dual-SIM LTE for resilient alarm transmission.

THE JURY'S MOTIVATION: "By bringing EN 50131 Grade 3 security to a fully wireless intrusion system, Superior Hub G3 Jeweller combines high-level protection and anti-jamming resilience with the speed and flexibility of wireless installation – a truly groundbreaking achievement."

ID & Access Control

Best Product Award 2026

- **Acre Via** by **Acre Security**, USA



Acre Via is a generative AI assistant for Acre's security platform, initially focused on access control. Operators can interact with the system using natural-language questions and commands to retrieve insights, create and refine

reports and streamline workflows. Via is designed to evolve from assisted actions towards more proactive AI-driven security management.

THE JURY'S MOTIVATION: "By offering generative AI-powered natural-language interaction, intelligent analysis and assisted actions, Acre Via sets a new industry benchmark for smarter and more proactive access control management."

The Innovative Achievement Award 2026

- **STID Architect II** by **STID Security**, France
- **HID M1 Transparent Gateway** by **HID Global**, USA



STID ARCHITECT II is a next-generation modular access control reader platform built around a common core and firmware architecture. Supporting RFID, NFC, Bluetooth and digital wallets, it combines certified cybersecurity with modular hardware and software-enabled upgrades, allowing functionality to evolve without replacing the installed reader.

THE JURY'S MOTIVATION: "With its secure, modular and upgradeable architecture, STID ARCHITECT II transforms the access control reader into an evolving platform, ready to adapt to new technologies and security requirements without replacing installed hardware."



HID M1 Transparent Gateway is a security device designed to protect communication between access control readers and controllers. It enables secure OSDP connectivity while centralising cryptographic operations in a protected unit, helping

organisations strengthen credential security and modernise existing access control infrastructure without extensive hardware replacement.

THE JURY'S MOTIVATION: "By moving cryptographic operations from the reader to a protected central unit, HID M1 Transparent Gateway strengthens access control security while preserving existing infrastructure – an innovative and practical approach to secure system modernisation."



Innovation and usability are key priorities for the editorial team of Detektor magazine when selecting products and solutions for nomination for the Detektor International Award.

Below are the 12 products and solutions selected by the jury for 2026, including the four first-prize winners, each of whom will receive the iconic glass sculpture created by renowned glass artist Bertil Vallien.

Video Surveillance

Best Product Award 2026

- **IVA Pro Context** by IQsight, Netherlands



IVA Pro Context is an AI-powered video analytics solution that combines established video analytics with generative AI and large vision models. It interprets activities, relationships and context within a scene, allowing users to search and analyse video using natural language and gain insights that go beyond conventional object detection and classification.

THE JURY'S MOTIVATION: "By combining proven video analytics with generative AI, IVA Pro Context moves beyond object detection to understand activities and context – turning video into actionable insights for smarter and more proactive security – a compelling and highly innovative concept."

The Innovative Achievement Award 2026

- **Security Center SaaS (with AI-Powered Investigation Features)** by Genetec, Canada
- **AI Visual Check** by OpenEye, USA



Security Center SaaS is Genetec's cloud-based unified security platform, bringing video surveillance, access control and other security functions into one system. Its AI-powered investigation features enable natural-language search and tools such as Similar People, Nearby Activity and Visual Trajectory to help operators quickly find, connect and analyse relevant events.

THE JURY'S MOTIVATION: "By combining natural-language search with intelligent, contextual analysis across video and security data, Genetec Security Center SaaS transforms complex investigations into a faster, more intuitive and efficient process."



AI Visual Check is an AI-powered feature within OpenEye Web Services that automates visual inspections using existing surveillance cameras. Users describe in natural language what the system should check – such as whether an emergency exit is blocked, a door is left open or an object is missing – and the AI analyses camera images to identify and alert on exceptions.

THE JURY'S MOTIVATION: "By enabling users to define visual checks in natural language, AI Visual Check turns existing surveillance cameras into flexible tools for automated inspections – extending video beyond security."

IoT & Security Solutions

Best Product Award 2026

- **Brivo Genius Mobile Agent** by Brivo, USA



Brivo Genius Mobile Agent is an agentic AI solution for mobile security management. Using natural-language voice or text commands, security professionals can interact with Brivo's platform to perform access control tasks, manage credentials

and respond to incidents directly from a mobile device, turning instructions into actions within the security system.

THE JURY'S MOTIVATION: "By turning natural-language voice and text commands into security-critical actions, Brivo Genius Mobile Agent takes access control beyond AI assistance to agentic AI – enabling faster, simpler and more intuitive security management and emergency response."

The Innovative Achievement Award 2026

- **Fusion** by Aritech, USA
- **VAIA** by Zenitel, Norway



Fusion is Aritech's unified security platform, bringing intrusion detection, access control and video together in one ecosystem. Its open architecture supports third-party integrations, while the Fusion Box connects on-site security systems with cloud-based services. The hybrid platform also enables modular digital services and

can scale as customer needs evolve.

THE JURY'S MOTIVATION: "With Fusion, Aritech brings intrusion, access control and video into an open, hybrid security ecosystem, enabling scalable digital services and Security-as-a-Service – a forward-looking approach to integrated security."



VAIA is an all-in-one platform for public address and voice alarm (PAVA) systems. The compact 1U unit integrates system control, DSP audio processing,

amplification, monitoring and battery charging. Its patented amplifier architecture delivers up to 1,000 W RMS across four independent channels, combining high speech intelligibility with efficient use of rack space.

THE JURY'S MOTIVATION: "By combining system control, DSP processing, amplification, monitoring and battery charging in a single 1U platform, VAIA delivers up to 1,000 W RMS – an innovative, space-saving approach to high-performance public address and voice alarm systems."



THE OVERALL
WINNER
ALARM & DETECTION



TXI Series

The jury's motivation:

"By combining purpose-built high-mount curtain detection with Triple AND Logic, TXI Series delivers reliable perimeter protection while reducing unwanted alarms – a truly innovative solution to the challenges of high-mounted outdoor detection."



www.optex-europe.com



INNOVATIVE ACHIEVEMENT AWARD
within the category of
ALARM & DETECTION



Superior Hub G3 Jeweller

The jury's motivation:

"By bringing EN 50131 Grade 3 security to a fully wireless intrusion system, Superior Hub G3 Jeweller combines high-level protection and anti-jamming resilience with the speed and flexibility of wireless installation – a truly groundbreaking achievement."

AJAX

www.ajax.systems



INNOVATIVE ACHIEVEMENT AWARD
within the category of
ALARM & DETECTION



AOD 100

– Authenticating Opening Detector

The jury's motivation:

"By combining a dynamic magnetic field with encrypted challenge-response communication, AOD 100 reinvents the traditional magnetic contact as an authenticating opening detector with significantly stronger protection against manipulation and sabotage."

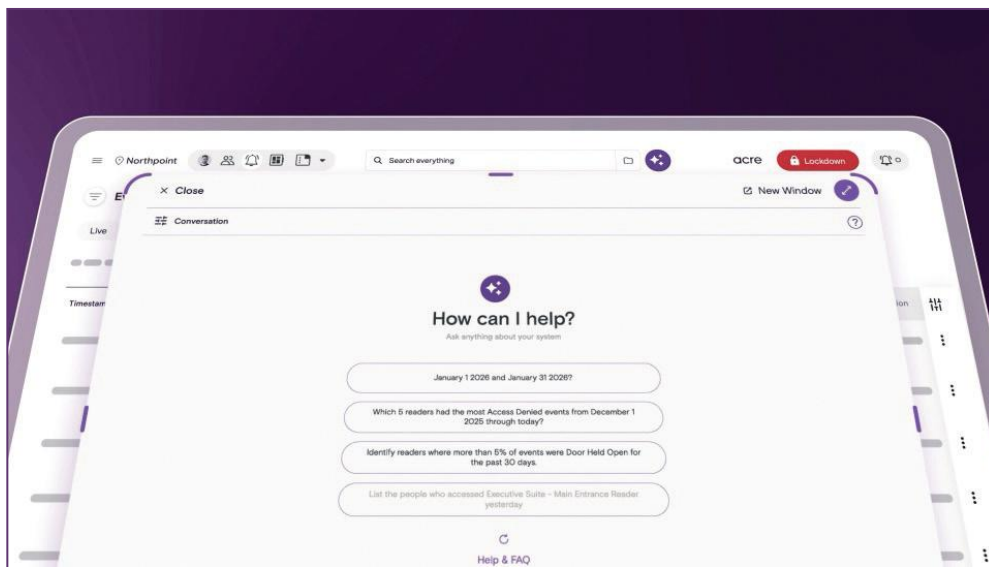
ALARMTECH

www.alarmtechglobal.com



THE OVERALL WINNER

ID & ACCESS CONTROL



Acre Via

The jury's motivation:

"By offering generative AI-powered natural-language interaction, intelligent analysis and assisted actions, Acre Via sets a new industry benchmark for smarter and more proactive access control management."

acre

Security

www.acresecurity.com



INNOVATIVE ACHIEVEMENT AWARD
within the category of
ID & ACCESS CONTROL



HID M1 Transparent Gateway

The jury's motivation:

"By moving cryptographic operations from the reader to a protected central unit, HID M1 Transparent Gateway strengthens access control security while preserving existing infrastructure – an innovative and practical approach to secure system modernisation."



www.hidglobal.com



INNOVATIVE ACHIEVEMENT AWARD
within the category of
ID & ACCESS CONTROL



STid Architect II

The jury's motivation:

"With its secure, modular and upgradeable architecture, STid Architect II transforms the access control reader into an evolving platform, ready to adapt to new technologies and security requirements without replacing installed hardware."



www.stid-security.com



THE OVERALL
WINNER
VIDEO SURVEILLANCE



IVA Pro Context

The jury's motivation:

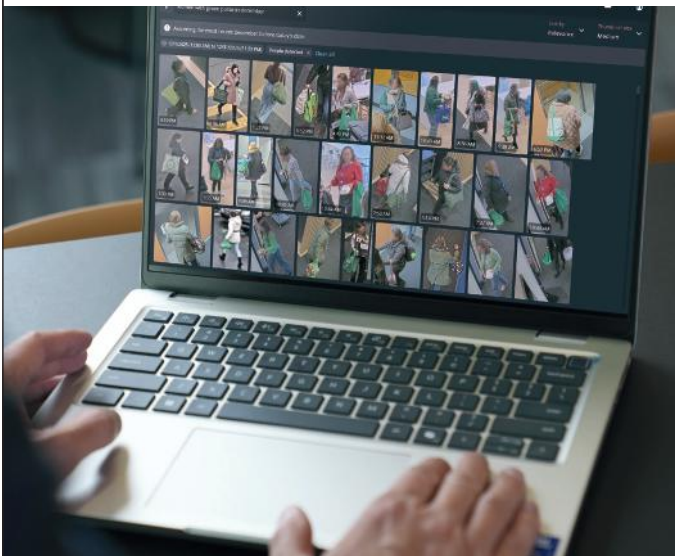
"By combining proven video analytics with generative AI, IVA Pro Context moves beyond object detection to understand activities and context – turning video into actionable insights for smarter and more proactive security – a compelling and highly innovative concept."

IQSIGHT

www.iqsight.com



INNOVATIVE ACHIEVEMENT AWARD
within the category of
VIDEO SURVEILLANCE



Security Center SaaS
– with AI-Powered Investigation Features

The jury's motivation:

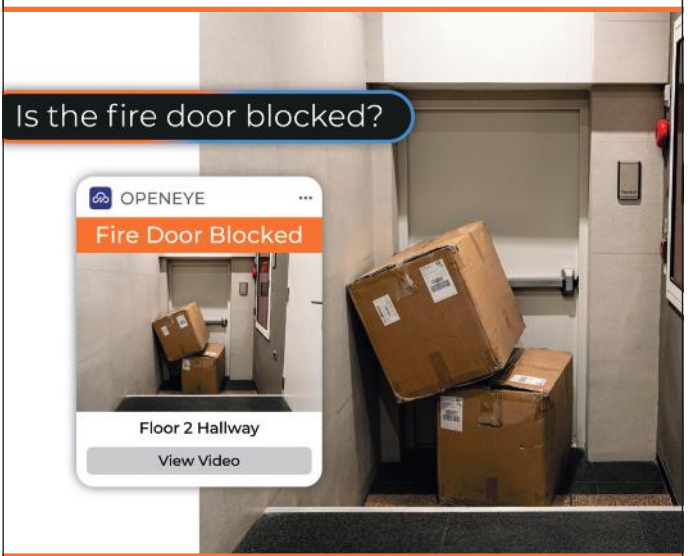
"By combining natural-language search with intelligent, contextual analysis across video and security data, Genetec Security Center SaaS transforms complex investigations into a faster, more intuitive and efficient process."

GenetecTM

www.genetec.com



INNOVATIVE ACHIEVEMENT AWARD
within the category of
VIDEO SURVEILLANCE



AI Visual Check

The jury's motivation:

"By enabling users to define visual checks in natural language, AI Visual Check turns existing surveillance cameras into flexible tools for automated inspections – extending video beyond security."

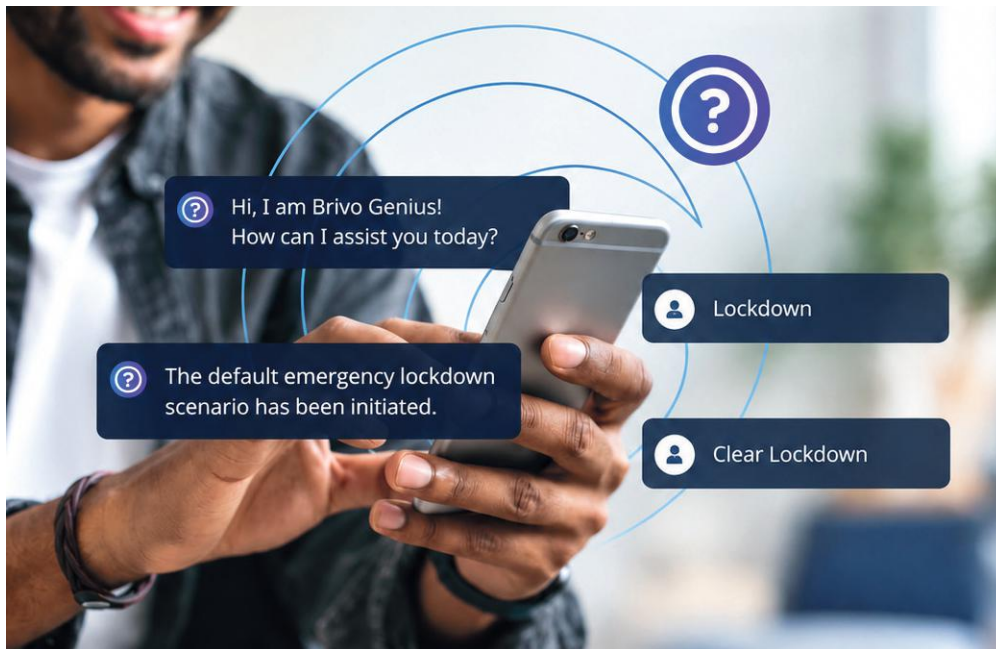
OpenEye[®]

www.openeye.net



THE OVERALL WINNER

IoT & SECURITY SOLUTIONS



Brivo Genius Mobile Agent

The jury's motivation:

"By turning natural-language voice and text commands into security-critical actions, Brivo Genius Mobile Agent takes access control beyond AI assistance to agentic AI – enabling faster, simpler and more intuitive security management and emergency response."



www.brivo.com



INNOVATIVE ACHIEVEMENT AWARD
within the category of
IoT & SECURITY SOLUTIONS



Fusion

The jury's motivation:

"With Fusion, Aritech brings intrusion, access control and video into an open, hybrid security ecosystem, enabling scalable digital services and Security-as-a-Service – a forward-looking approach to integrated security."



www.aritech.com



INNOVATIVE ACHIEVEMENT AWARD
within the category of
IoT & SECURITY SOLUTIONS



VAIA

The jury's motivation:

"By combining system control, DSP processing, amplification, monitoring and battery charging in a single 1U platform, VAIA delivers up to 1,000 W RMS – an innovative, space-saving approach to high-performance public address and voice alarm systems."



www.zenitel.com



Tomas von Tourtchaninoff, Head of Security at Stockholmsmässan and Niclas Gustafsson, Group CEO at Apstec Systems.



The robot dogs from Rapid, equipped with specially developed Swedish software, feature cameras and lidar and can follow predefined patrol routes, climb stairs and move between different parts of a venue.

AI-powered screening system and smart robot dogs secured the Skydd event in Stockholm

Stockholm, Sweden

The International Stockholm Fair – Stockholmsmässan – used AI-powered technology as an additional layer of security at Skydd – the Nordic region’s largest security exhibition, held on 20–22 October.

Visitors were screened seamlessly using Apstec’s Falcon Plus system, while robot dogs from Rapid Säkerhet patrolled the exhibition after closing hours.

At Skydd and Totalförsvarmässan in Stockholm, security technology formed part of the events themselves. AI-powered solutions had made significant advances over the previous year, something demonstrated by several exhibitors. The solutions deployed by Stockholmsmässan during the event represented some of the latest developments in security technology.

– Getting the opportunity to test the Falcon Plus system, which screened all visitors at the entrance, as well as robot dogs patrolling the exhibition after closing hours, was of course exciting, commented Tomas von Tourtchaninoff, Head of Security at Stockholmsmässan.

Frictionless screening

Falcon Plus is an AI-powered security screening system designed to detect weapons, explosives and narcotics on people and in bags. By combining millimetre-wave technology with AI-based analysis, the system enables large numbers of visitors to be screened without having to stop, empty their pockets or remove outerwear.

High throughput

According to Apstec, a single Plus portal can screen up to 2,500

people per hour and can be used both indoors and outdoors. Niclas Gustafsson, Group CEO of Apstec Systems, described Skydd as a typical example of an environment well suited to the technology.

– Our products are often deployed at events involving large temporary crowds over a few intensive days. The difference here was that those being screened were security experts, which made the requirements particularly clear, he said.

He also saw Skydd as an opportunity to demonstrate the technology in practice.

– By screening visitors at Skydd, we had the opportunity to demonstrate how modern, frictionless and AI-powered entry screening can work in practice. I think it may have been an eye-opener for many.

Enhanced screening

For Stockholmsmässan, the technology made it possible to strengthen security screening without creating unnecessary obstacles to visitor flow.

– The Falcon Plus portal complemented our other security procedures while also giving Skydd visitors the opportunity to experi-

ence modern AI-powered security technology in real-world use, commented Tomas von Tourtchaninoff.

Robot dog patrols

When the exhibition closed for the day, another security technology took over. Autonomous robot dogs from Rapid Säkerhet patrolled the exhibition area as a complement to the regular security operation.

– It was very interesting to see how they performed their duties alongside our security guards on site, commented Tomas von Tourtchaninoff.

The robot dogs from Rapid Säkerhet are equipped with cameras and lidar and can follow predefined patrol routes, climb stairs and move between different parts of a venue. An AI agent analyses the information collected, while generative AI allows the robots to be instructed in natural language about what to react to – for example, a person in an area that should be empty, an open window or other anomalies.

Addressing intruders

If a robot detects something suspicious, it can send a video alarm directly to Rapid’s alarm receiving centre, where an operator can assess the situation. It can also communicate with people it encounters and, for example, instruct someone in a restricted area to leave.

– The robots never get tired and miss nothing on their patrols. They enhance security and will make us less dependent on human staffing,



Falcon Plus is a comprehensive screening solution that detects weapons, explosives and narcotics on people and in bags. It enables large numbers of visitors to be screened without having to stop, empty their pockets or remove outerwear.

says Mats B. Adman, CEO of Rapid Säkerhet.

Supporting guards

Mats B. Adman stresses that the technology is not intended to replace security guards. The robot dog can detect, verify and communicate, but it cannot physically intervene.

– In the event of an incident, information from the robot can be used as a basis for deciding whether to dispatch a security guard or, if necessary, contact the police or emergency services, he concludes.

On display at Skydd

In addition to being deployed during Skydd, Apstec and Rapid Säkerhet also demonstrated their respective solutions at their stands at the exhibition.

What's on in the Security Industry?

– We keep track of what's happening!



www.securityworldmarket.com



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

Skyddgolfen Detektor Open

– the world's largest golf tournament for security professionals

With 300 players competing, Skyddgolfen Detektor Open reinforced its position as the security industry's largest golf event when the tournament was held for the 20th consecutive year on 25 August 2026.

The venue was Vidbynäs Golf Club, 45 kilometres south of Stockholm, where the competition took place on the club's two courses – North and South.

Sponsors were present at all 36 holes, as well as at the putting green and the entrance.

Detektor magazine, in cooperation with Skydd, the largest security exhibition in the Nordics, launched Skyddgolfen Detektor Open in 2007. The event was an instant success.

New world record

This year's event attracted more than 400 people in total. The tournament brought together 300 players, surpassing last year's record of 297 and further cementing Skyddgolfen Detektor Open's position as the world's largest golf tournament for security professionals.

For many participants, however, the event began on 24 August, when nearly 200 people gathered for practice rounds and socialising at the club's restaurant. Over the years, the event has become an important meeting place for the Scandinavian security industry.



Alarm.com was a hole sponsor, with Simon Koch challenging all players in a nearest-the-pin competition.

Play-off next to the restaurant terrace

The main competition is based on stroke play, with all players competing according to their handicaps, reduced by 15 per cent. The top two players from each course then met in a play-off on a special par-three hole next to the restaurant terrace, where hundreds of spectators gathered to watch the finale.

Sebastian Pettersson of Firesec and Ulf Hillhammar of Assemblin topped the South Course, both with scores of 67, while Fredrik Linné, from Elajo and Jan Rosén of Roséns Låsservice led the North Course, both scoring 68.

Golf week in Marrakech

Fredrik Linné and Sebastian Pettersson were the only players to make par on the play-off hole, forcing a second round. Linné hit the green from the tee and then two-putted for par to secure victory.

"It has been fantastic – a really enjoyable group to play with, perfect golfing weather and a superb golf course," he commented.

For his victory, Linné received first prize – an exclusive golf week in Marrakech for two people.

Time for networking

Above all, however, Skyddgolfen Detektor Open is a social event and an important industry forum for networking.

"It is a great opportunity to meet colleagues from the industry together with our customers, while



Fredrik Linné of Elajo, winner of Skyddgolfen Detektor Open, together with Monika Johannessen Widholm of Stockholmsmässan and Deniz Baykal of AR Media International.

also making new contacts," said Fredrik Skoog, CEO of Steplock.

Good for business

Dan Wikström Lilliebjelke, CEO of Hedengren Sweden, emphasised the business value of participating in the event.

"You develop business relationships and partnerships in a very effective way. And of course, you meet other people from the industry and hear a little gossip and informal news – that's all part of it," he said.

Johan Lokind, Nordic Regional Manager at Traka, was present in the company's sponsor tent.

"We had heard a lot of good things about this tournament, and when we got the opportunity to sponsor a hole, there was no question that we wanted to get involved. The weather is fantastic and the event has been a great success," he commented.

Participation to boost business in the Nordics

Several major international companies that have yet to establish as strong a presence in Sweden and Scandinavia as in other markets were also represented among the sponsors. One example was Alarm.com, which sponsored a hole for the first time.

"I thought it was time for Alarm.com to step in and do some marketing here in Sweden as well. This is actually the first event we have participated in, and we will also be exhibiting at Skydd. It's great fun," said Simon Koch, Business Development Manager at Alarm.com.

Another international company represented at the event was Convergint. Kalle Kuivalainen, Country Manager, Nordics, told Detektor that he regarded critical infrastructure and data centres as particularly promising growth areas in the Nordic region. He also emphasised the importance of meeting industry colleagues as a reason for participating in the event.

"I see this as a fantastic opportunity to meet important people," he stated.

Sponsors at every hole

Lennart Alexandrie, CEO of organiser AR Media International, expressed his satisfaction with the event's continued ability to bring the industry together year after year.

"We are extremely pleased with the strong turnout from both sponsors and players. Together, they create a fantastic atmosphere in the clubhouse, the restaurant and out on the courses. And we also have

The putting green was crowded before the start.



Stefan Boqvist, Peter Gysell and Helene Lidman of alarm detector manufacturer Alarmtech in front of the company's sponsor tent.

Lennart Alexandrie, publisher of AR Media International, welcomed 300 players to Vidbynäs.



Suzanne Tapper of HID in conversation with Johan Lokind and Ebba Mann of Traka Nordic.



Freddie Parrman, Linda Sundberg and Magnus Olsson from hole sponsor Seriline.



Erik Isaksson and Fredrik Skoog of Steplock enjoying the sunshine.



Avarn had a group of players at the event, led here by CEO David Larsson.

to give the weather a great deal of credit for the success of the event. We had brilliant sunshine both on the practice day and on the tournament day," he said.

A two-day event

Although the main competition takes place on a single day,

Skyddgolfen Detektor Open has developed into a two-day event. Many players arrive the day before the tournament for a practice round and spend the evening socialising with colleagues, partners and customers at Braserie Vidbynäs, the clubhouse restaurant.

"We have players from all over Sweden and also from other countries, so the accommodation at the conference facility is very important. But for many players and sponsors, it has also become a tradition to arrive at Vidbynäs the day before the tournament and check into the accommoda-

tion in the manor house or the cottages located right next to the courses," explained Deniz Baykal, Project Manager for Skyddgolfen Detektor Open at AR Media International.

"That is why the accommodation is always fully booked months before the tournament,"

Security Events

November

 **3-5 November**
Expoprotection
Paris, France
Venue: Porte de Versailles - Pav 1
Organiser: RX
Website: www.expoprotection.com

 **3-5 November**
ISC East
New York, United States
Venue: Javits Center
Organiser: RX
Website: www.discoverisc.com/east/en-us.html

2027

January

 **12-14 January**
Intersec
Dubai, United Arab Emirates
Venue: Dubai World Trade Centre
Organiser: Messe Frankfurt
Website: www.intersec.ae.messefrankfurt.com/dubai/en.html

 **19-21 January**
Perimeter Protection
Nürnberg, Germany
Venue: Nürnberg Messe
Organiser: Nürnberg Messe GmbH
Website: www.perimeter-protection.de

February

 **24-25 February**
New Security
Leuven, Belgium
Venue: Brabantthal
Organiser: FCO Media
Website: newsecuritytradefair.be

March

 **2-5 March**
Security Show
Tokyo, Japan
Venue: Tokyo Big Sight
Organiser: Nikkei Inc.
Website: <https://messe.nikkei.co.jp/ss/>

 **17-18 March**
Sectech Norway
Lilleström, Norway
Venue: Nova Spektrum
Organiser: AR Media International AB
Website: www.sectech-expo.com/norway

April

 **5-9 April**
ISC West
Las Vegas, United States
Venue: The Venetian Expo
Organiser: Reedexpo
Website: www.discoverisc.com/west/en-us.html#/

 **21-23 April**
Secutech
Taipei, Taiwan
Venue: Taipei Nangang Exhibition Center
Organiser: Messe Frankfurt
Website: secutech.tw.messefrankfurt.com/taipei/en.html

 **27-29 April**
The Security Event
Birmingham, United Kingdom
Venue: National Exhibition Centre (NEC)
Organiser: Nineteen Group
Website: www.thesecurityevent.co.uk

June

 **22-24 June**
Expo Seguridad México
Mexico City, Mexico
Venue: Banamex Center
Organiser: Reed Exhibitions
Website: www.exposeguridadmexico.com

August

 **24 August**
SkyddGolfen Detektor Open 2027
Nykvarn, Sweden
The world's largest golf tournament for security professionals.
Nykvarn, Sweden
Venue: Golf South Sthlm (Vidbyns GC)
Organiser: AR Media International AB
Website: www.armedia.se/detektor/scandinavia/sv/SkyddGolfen.asp

 **25-26 August**
Danish Security Fair
Fredericia, Denmark
Venue: Messe C
Organiser: Messe C
Website: www.danishsecurityfair.dk

September

 **14-16 September**
Intersec Europe
Frankfurt, Germany
Venue: Frankfurt am Main
Organiser: Messe Frankfurt GmbH
Website: intersec-europe.messefrankfurt.com

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

ASSA ABLOY

CLIQ®

The smart way to digitalize access

Take your access management into the digital era – smoothly, securely, and without overhauling existing infrastructure. With CLIQ, you upgrade from mechanical to digital access at your own pace to gain greater control today and adaptability for tomorrow.



Download our whitepaper to learn more about making the switch to digital access



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



Discriminative Metal Detection Solution

Apstec Merlin is specifically developed for customers who require a cost-effective, high-throughput and non-invasive screening solution to detect and discriminate between metallic threats and everyday items. While at the same time delivering a low level of false alerts for a significant advancement over traditional metal detection methods.



Scan the QR code to
learn more or visit
apstecsystems.com

**New!**

Manage Screening Efficiently With Intuitive Interfaces



Operator User Interface

- Multiple modes: free-flow, secondary screening and checkpoint
- Body map with front & back views and item location
- Alert image, threat class, location and one-tap acknowledgement



Control Room Interface

- Centralised monitoring and management of multiple systems on one screen
- Real-time visibility of passes, alarms and status
- Alarm history, analytics & reporting