

Securitas
Technology



2027 Global Technology Outlook Report



Contents

01

Introduction 04-15

- P06 | Acknowledgments
- P08 | Welcome message and foreword
- P10 | Securitas Technology overview
- P12 | SecureStat HQ platform overview

02

Executive summary 16-31

- P18 | 2027 technology outlook
- P24 | Key takeaways for security leaders
- P26 | Client, market, and technology partner insights

03

Capitalising on the AI opportunity 32-57

- P36 | Advancing threat detection with AI
- P40 | GenAI for smarter security operations
- P46 | Agentic AI streamlining security decisions
- P50 | AI-driven business security optimisation
- P56 | Action plan for security professionals

04

Cloud solutions reshaping security 58-85

- P62 | The foundation for next-generation security
- P68 | System health monitoring and maintenance
- P72 | Remote verification and incident management
- P78 | Centralised security system management
- P84 | Action plan for security professionals

05

Drones and robots pushing the security envelope 86-109

- P90 | Drone detection
- P96 | Drones for surveillance
- P100 | Robots in security
- P108 | Action plan for security professionals

06

Safeguarding the physical security ecosystem 110-133

- P114 | Security data best practices
- P120 | Data trustworthiness
- P126 | Quantum-resistant security systems
- P132 | Action plan for security professionals

07

Contributor spotlights 134-173

- P136 | Technology partner spotlights
- P164 | Securitas spotlights

01

Introduction

In this section

- › Acknowledgments
- › Welcome message and foreword
- › Securitas Technology overview
- › SecureStat HQ platform overview

Thank you to our contributing strategic tech partners and industry experts

The world's leading security
innovators and technologists

Through close partnerships with these foremost security technology innovators, technologists, and product manufacturers, we offer clients unrivaled access to the most advanced — and sustainable — security solutions available today.

3xLOGIC

AJAX

AMAG
TECHNOLOGY
An ALLIED UNIVERSAL Company

ARITECH

ASSA ABLOY

AXIS
COMMUNICATIONS

brivo
simply better security

DMP

Genetec

Hanwha
Vision

HID

Honeywell | **LENEL S2**
by Honeywell

IDIS One Solution.
One Company.

INTELLICENE
SECURITY. EVOLVED.

IQSIGHT

MARCH
networks
A Delta Group Company

milestone

MOTOROLA
SOLUTIONS

OpenEye

PACOM

radionix

resideo

SOFTWARE HOUSE
C-CURE IQ

SONITROL

VERINT

VIAKOO

Foreword

The world's most comprehensive security technology report

AI, cloud, robotics driving a new security ecosystem



Welcome to the 2027 Global Technology Outlook Report

First, let me express how excited I am to introduce the ninth annual edition of this report. It is without doubt our most anticipated publication each year, combining exclusive global data, insights, and research from our strategic tech partners, internal experts, world-leading end-user client survey, and the market's senior decision-makers – all in one!

Security is shifting and the trends matter. Physical and digital risks continue to converge, the pace of innovation – especially in AI – is accelerating, and security leaders are being asked to respond to more complex challenges with greater speed, intelligence, and confidence. In today's world, technology trends aren't just supporting security. They're actively shaping it.

That urgency reflects the key reasons why we publish the report each year: to give our clients clear, practical insight into the electronic security trends that will matter most, and to help our clients make informed decisions about future investments and their security programme roadmaps.

The report brings together perspectives from four important sources

- › **End-user clients**, using our exclusive Global Client Survey - markedly one of the world's largest with 16,000 respondents across 19 countries worldwide - as a benchmark for how client needs are evolving, plus executive feedback from our high-profile, multi-industry Client Advisory Board.
- › **Electronic security decision-makers**, with expansive research across commercial and enterprise sectors worldwide, independently performed by NewtonX.
- › **Our strategic tech partners**, representing the world's leading security product brands, whose innovation and research and development roadmaps help shape where the industry is heading with new products, software, and other technologies.
- › **A specialised team of internal global technology leaders and subject matter experts**, representing over 15 countries and local markets worldwide, immersed in technology research, analysis, evaluation, benchmarking, and testing.

Together, these perspectives give us **the world's most comprehensive view of technology trends**, shifting expectations, and the opportunities that lie ahead.

Themes shaping 2027 and the new security ecosystem frontier...

As we look ahead, several critical trends stand out that we explore in depth throughout this report:

- › **Artificial intelligence** is impacting every aspect of security technology and security management, helping teams detect threats, manage events, and work more efficiently.
- › **Cloud-based solutions** are commonplace and enabling more flexible, connected, and resilient security operations.
- › **Drones and robots** are expanding what security teams can see and do, offering new ways to monitor locations and respond to incidents as they become integrated into the security ecosystem of the future.
- › As systems become more connected, **safeguarding the physical security ecosystem itself** – from data integrity, sustainability, and cyber hygiene to preparing for the quantum-computing era risks on the horizon – has become essential for security programmes of all shapes and sizes.

At Securitas Technology, we're committed to helping our clients navigate these evolving trends with confidence, drawing on decades of expertise across disciplines and industries, and close partnerships with the world's leading security technology manufacturers and innovators.

Our investment in our SecureStat HQ® security management platform reinforces that commitment. By combining data, AI, and human expertise, we're building the foundation for truly **intelligence-led safety and security**. Across Securitas Group, we continue to strengthen our capabilities and expertise in risk intelligence and specialised services so we can support your needs today and help you prepare for tomorrow.

I hope this leading industry report gives you useful insights, sparks new ideas, supports your investment roadmap, and assists your planning for the future. Thank you for your continued partnership, and for the confidence you place in Securitas Technology as your trusted adviser.

Tony Byerly
Global President &
Chief Executive Officer
Securitas Technology



Follow Tony on
LinkedIn

About Securitas Technology

Your trusted adviser in a rapidly changing security landscape

Creating simplicity from complexity for your business security

- **Finding you the right technology**
We work as your trusted adviser to help you identify the best security solution for your unique needs.
- **Creating your complete, custom solution**
We design, integrate, install, monitor, maintain, and support your electronic security solution, end-to-end.
- **Optimising your security systems**
We help optimise and manage your security systems with an extensive network of highly skilled and certified security professionals and remote services.



Learn more about our
technologies, services,
and industry expertise at
securitastechnology.com

A global technology
partner solely focused
on security and safety

40+

Countries with security
technology capabilities
and presence

- › Coverage across **6** continents
- › **World-leading** commercial electronic security company

1M+

Client sites worldwide

- › **1.6M+** monitored connections
- › **1M+** maintenance, inspection, and service calls completed annually

12,000+

Employees worldwide

- › **5,000+** Technicians
- › **500+** Engineers / Design Architects / Innovators

SecureStat HQ®

The all-in-one platform for optimised security

Helping clients make smarter decisions

SecureStat HQ is an industry-leading platform for security management, combining site level control, event management across the organisation, data to optimise security, and seamless access to our services.

It gives organisations a clear understanding of their environments so they can make more informed decisions and shift from reactive responses to intelligence-led operations.

As systems become more connected and threats more dynamic, SecureStat HQ acts as the backbone that unifies business security alerts, analytics, services, and insights across locations.

Bringing systems, sites, and data together in one spot

Advanced generative artificial intelligence is reshaping how security teams work – but its value depends on having the right platform in place. SecureStat HQ provides clients with that foundation.

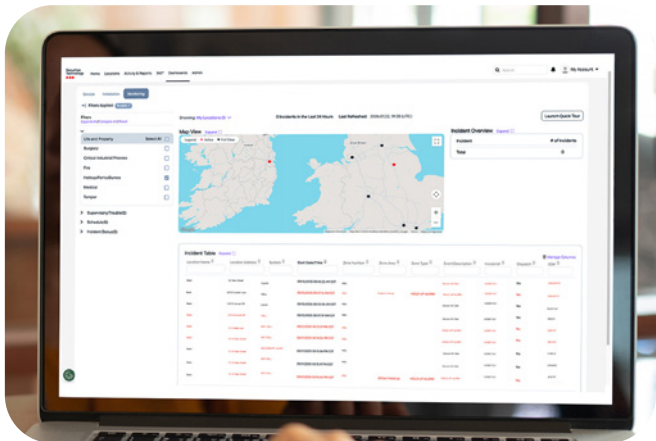
By centralising information from sensors, cameras, and monitoring services, it features powerful tools to help clients understand their security posture, identify patterns, and deliver insights that support faster, more confident security actions.

SecureStat HQ is compatible with a wide range of systems from the industry's leading brands, integrating video surveillance, access control, intrusion systems, and more.



Get started with SecureStat HQ

SecureStat HQ is available to every Securitas Technology client. Scan the QR code now to request an account.



Turning security data into business intelligence

SecureStat HQ connects the security systems, data streams, and automated processes that matter most, bringing proactive intelligence into clients' daily operations.

With SecureStat HQ in the palm of their hand, clients can identify where vulnerabilities exist and where technology can deliver meaningful operational benefits that support continuous business improvement.

Giving a 360-degree view of security assets

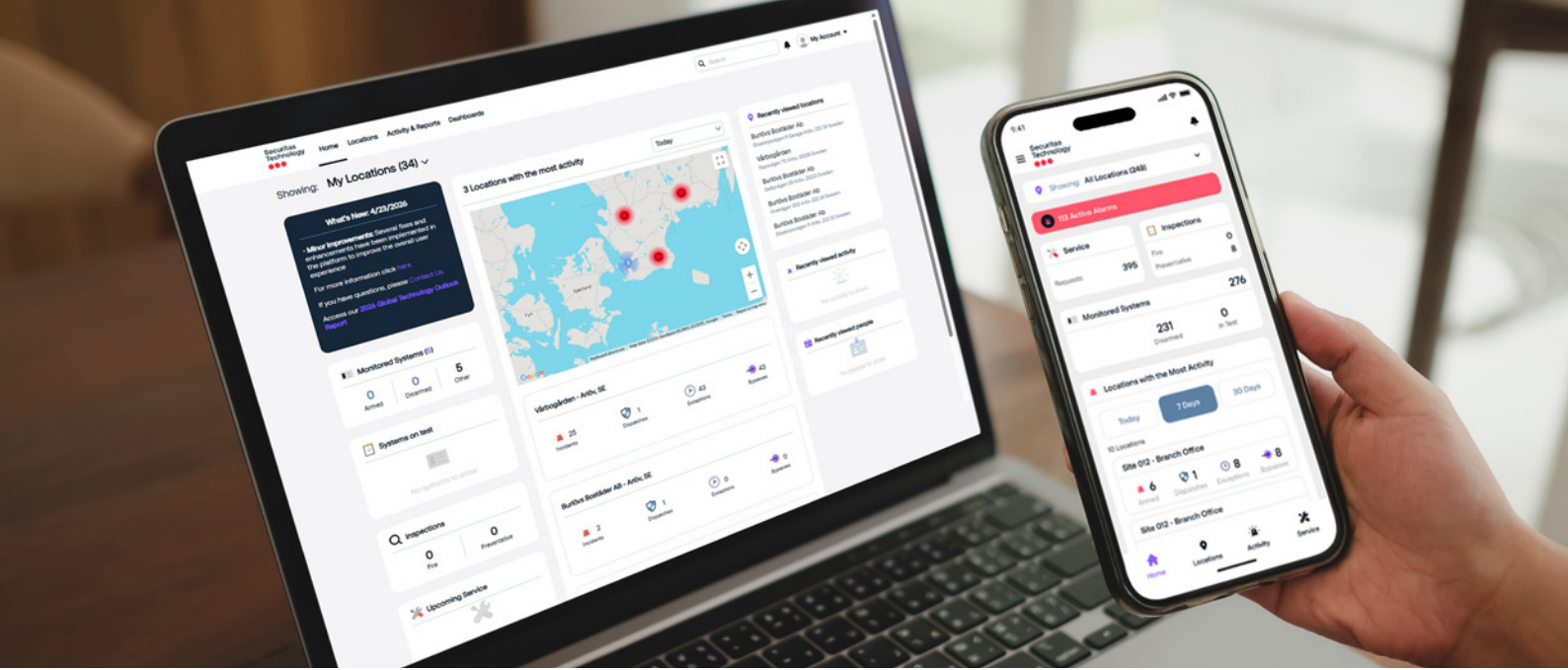
Also part of the SecureStat HQ platform, SecureStat 360® enables proactive life cycle management of physical security systems and assets, backed by operational and service excellence. SecureStat 360 enables clients to:

- › Maximise the life of equipment
- › Plan upgrades more efficiently
- › Reduce exposure to known vulnerabilities
- › Document CO2 emissions

See and control your security with SecureStat HQ dashboards

Powerful visual dashboards enable you to see, explore, and share data on critical aspects of your security operations.

- › **Installation Dashboard:** Gain real-time visibility into the status of installation projects for operations, sales, and project teams to monitor progress, identify delays, and ensure timely completion.
- › **Monitoring Dashboard:** Centralise, manage, and analyse alarm activity across your locations with events from the past 24 hours. Available as part of Advanced and Premium subscriptions.
- › **Service Dashboard:** Access a full record of your service history to help you track active service tickets, understand trends, and report on service activity.



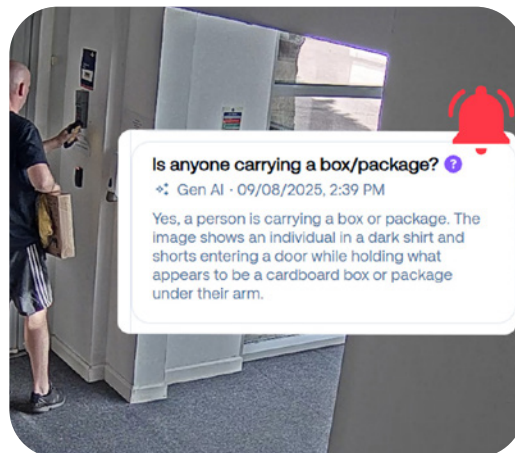
Introducing SecureStat® Cumulus™

SecureStat Cumulus extends the power of SecureStat HQ with a cloud-based video solution powered by generative AI (GenAI).

With SecureStat Cumulus, organisations get visual intuitive controls, anywhere access, and notifications for important events. It offers camera-to-cloud flexibility and an open platform compatible with a wide range of IP cameras and routers. Its GenAI features understand natural language, interpret context, and help teams monitor for almost anything – from workplace safety to customer experience to security threats – simply by describing what they want to see.

Enter a new era of AI cloud video surveillance

With flexible cloud and AI packages to fit your business, SecureStat Cumulus is incredibly easy to implement, use, and manage. Scan the QR code to learn more.



SecureStat Cumulus

Camera-to-cloud video transformed by GenAI



02

Executive summary

In this section

- › 2027 technology outlook
- › Client, market, and technology partner insights
- › Key takeaways for security leaders

2027 technology outlook

The era of connected, data-driven, and automated security

The years ahead will see the acceleration of highly integrated, multi-layered security programmes as organisations adapt to a landscape where physical and digital threats continue to converge.

According to our clients¹, **break-ins, vandalism, employee safety, and compliance** are among the top concerns driving the priorities of their security programmes, prompting organisations to focus on security technologies and services that help them better anticipate risks, prevent disruption, and enhance incident response.



Top 5 concerns driving our clients' security priorities¹

- 01 Break-ins/ burglary
- 02 Trespassing/ vandalism
- 03 Unauthorised access/ limiting access
- 04 Employee safety
- 05 Regulatory compliance

The use of artificial intelligence is shifting from limited applications to everyday use. Advances in generative AI technology will influence how security teams detect threats, manage incidents, and handle growing operational workloads.

At the same time, investment in cloud-based solutions and remote services is rising to strengthen resilience and improve efficiency across distributed environments.

There is interest in the growing potential of drones and robotic technologies for extending visibility, automating routine tasks, and providing new ways to enhance real-time monitoring and situational awareness.

Underpinning all of the above is a pressing focus on the integrity of physical security networks, driven by rising cyber-physical threats and the need to trust increasingly connected and automated systems.

Across industries, leaders are seeking proactive solutions and practical guidance from security partners who can help them foresee potential risks and build intelligence-led security programmes that are ready for the future.

1. In-house branded survey of Securitas Technology clients in Australia, Belgium, Canada, Denmark, Finland, France, Germany, Ireland, Mexico, Netherlands, Norway, Portugal, Singapore, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States. Data shown is reflective of commercial client responses only. Conducted November 2025.

Top trends for 2027



01

Artificial intelligence

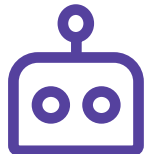
AI is now a core part of daily security work, reducing false alarms, improving threat detection, and automating high-effort tasks across video surveillance, access control, and daily operations.



02

Cloud Solutions

Cloud-based solutions and remote services are making security more flexible, scalable, and resilient through anytime/anywhere access, automated updates, and intuitive controls.



03

Drones and robots

These technologies are expanding the reach of security operations, supporting teams with real-time visibility and increasingly automated patrol capabilities.



04

Protecting the physical security ecosystem

Organisations are prioritising data integrity, cyber hygiene, and responsible AI use as systems become more connected and new threats – including quantum risks and deepfakes – emerge.



Our data sources

Global Client Survey

16,000+

Clients across 19 countries

Market survey research

575

Security professionals representing organisations across the globe

Technology partner consultation

26

World-leading security technology innovators

Macro forces driving urgency

- › **Economic pressure** is pushing organisations to achieve more with fewer resources.
- › **Cyber and physical threats** continue to converge in ways that demand coordinated responses.
- › **Regulatory expectations** for data governance and responsible AI practices are increasing across many industries.
- › **Cloud adoption** is accelerating as organisations modernise their tech stack.
- › **Workforce shortages** are driving demand for automation and remote services.



Insights built on market data, deep expertise, and client feedback

- › **2025 Global Client Survey and Advisory Board Feedback:**
A survey process managed by Securitas Technology with responses from over 16,000 clients across 19 countries. The Global Client Survey included questions on planned security technology adoption and investments. Insights were also gathered from members of the Securitas Technology Client Advisory Board – a diverse group of top executives representing end-user clients, across a multitude of industries, that provide Securitas Technology with feedback on their security technology challenges and needs.
- › **Market Survey Research:**
An external market survey commissioned by Securitas Technology gathered responses from 575 verified security professionals representing organisations across North America, Europe, and Asia-Pacific. Aimed at decision-makers directly involved in technology investments, the independent study focused on current utilisation, future adoption, and planned investment across electronic security.
- › **Technology Partner Consultation:** A consultative process managed by Securitas Technology to gather data and insights from 26 strategic technology partners representing the industry's leading security product manufacturers, developers, innovators, and technologists.
- › **Internal Subject Matter Experts:**
A series of internal interviews and research conducted to gather insights from internal technology leaders and subject matter experts at Securitas Technology worldwide. This included members of the Securitas Technology Strategy and Innovation team, Global Technology Review Committee (GTRC), and Global Technology Innovation Council (GTIC) representing over 15 countries and local markets.

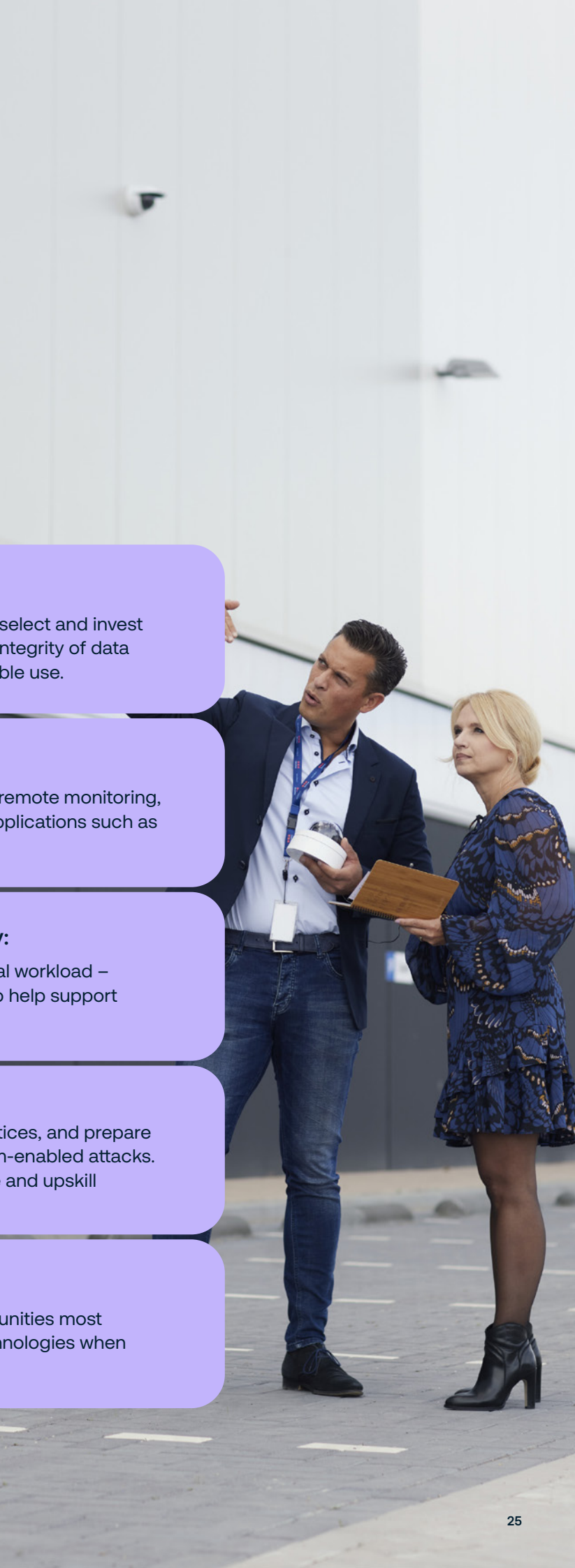


Key takeaways for security leaders

What to know now

How to plan ahead

→	01	AI is moving into core security operations... ...helping teams detect threats, address false alarms, and streamline investigations with greater accuracy and speed.	Create a practical roadmap for AI adoption: Start with targeted, high-value use cases to help you select and invest in AI-ready infrastructure. Validate the accuracy and integrity of data sources, and implement clear guidelines for responsible use.
→	02	Cloud solutions and remote capabilities... ...are commonplace and reshaping security delivery, making operations more scalable, resilient, and consistent across multiple sites.	Build from your cloud foundation: Continue to integrate cloud infrastructure to support remote monitoring, remote verification, and scalable solutions for core applications such as video surveillance and access control.
→	03	Autonomous systems are gaining traction... ...with drones and robots supporting teams by expanding visibility, enhancing responsiveness, and helping automate routine tasks - setting the stage for the new security ecosystem frontier.	Assess automation to extend team capacity: Consider deploying tools that can help reduce manual workload – from drones and robots to automated monitoring – to help support faster, more efficient incident response.
→	04	Data integrity and cyber hygiene are fundamental... ...driven by the convergence of physical and digital risks, and the need to maintain trust in increasingly automated systems.	Invest in ecosystem resilience: Prioritise cyber hygiene, reinforce data-integrity practices, and prepare for emerging threats such as deepfakes and quantum-enabled attacks. Research the latest guidance on quantum-resistance and upskill employees in AI and cybersecurity risk awareness.
→	05	Leaders are looking for guidance through rapid technological change... ...seeking security partners who can help them evaluate, adopt, and manage the right solutions for their environment.	Prioritise outcomes, not technologies: Anchor decisions in the risks, challenges, and opportunities most important to your organisation — and adopt new technologies when they support your security programme.

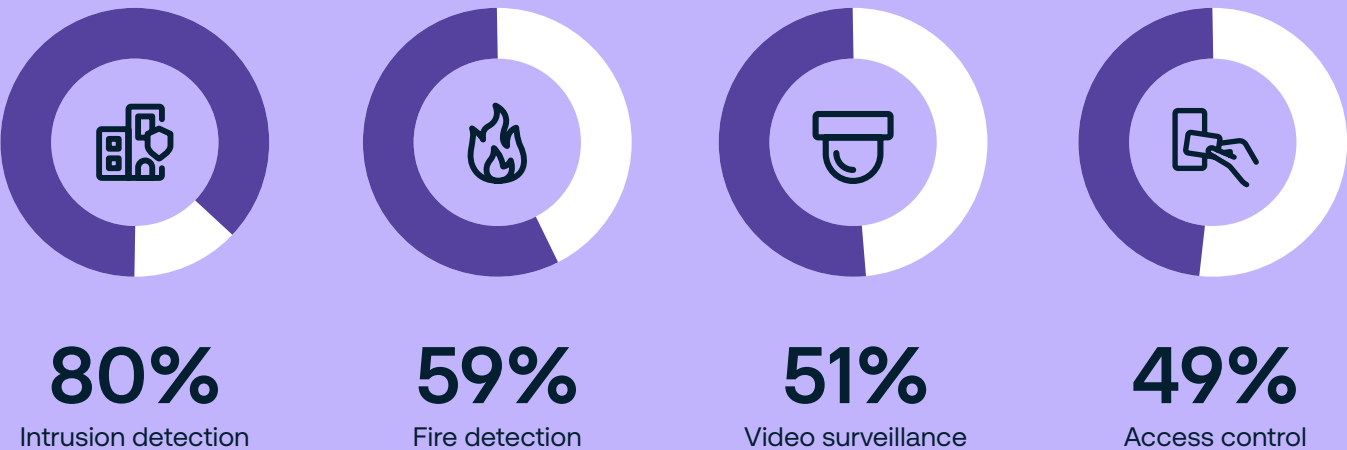


What our clients are prioritising

Key insights from our annual
client consultation process¹

Most adopted technologies

Top security technologies our clients currently use:



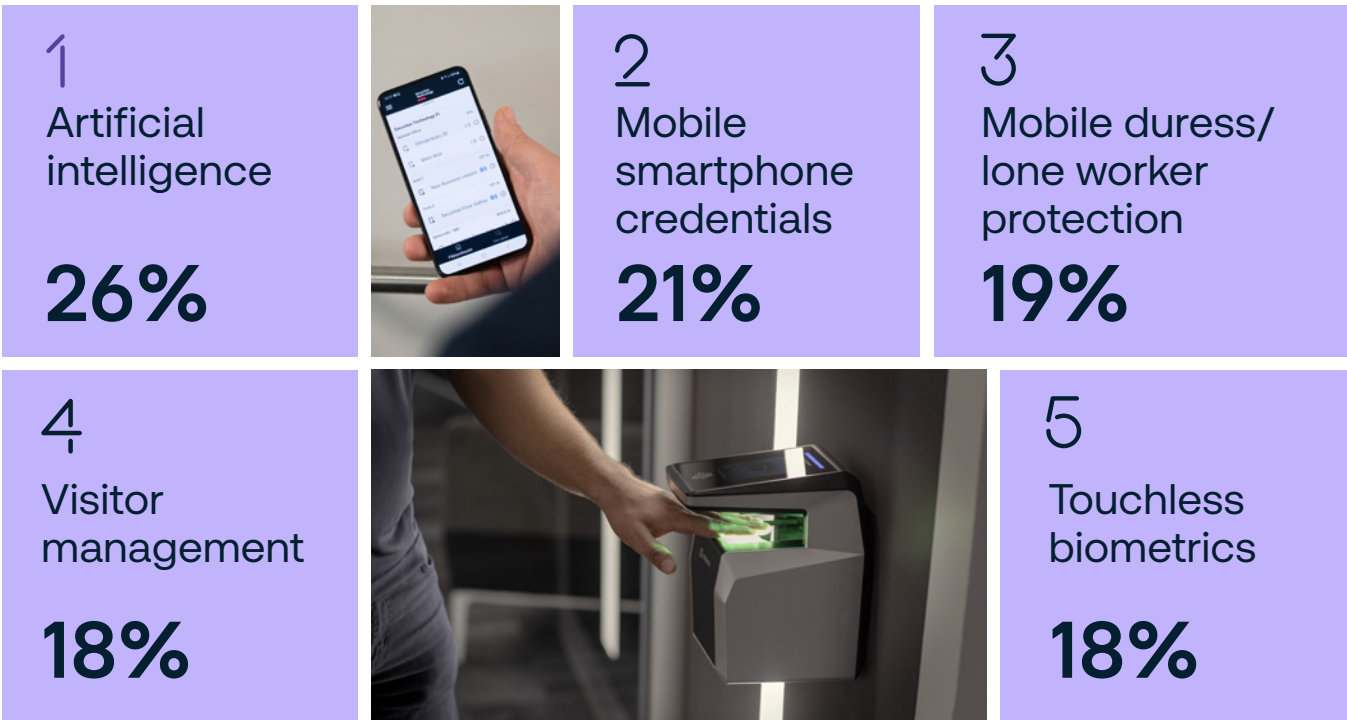
Most adopted subscription-based services

Top recurring electronic security services our clients currently use:



Top 5 trending technologies

Security technologies our clients are interested in adopting in the next 18 months:



Top 5 trending subscription-based services

Recurring electronic security services our clients are interested in adopting in the next 18 months:

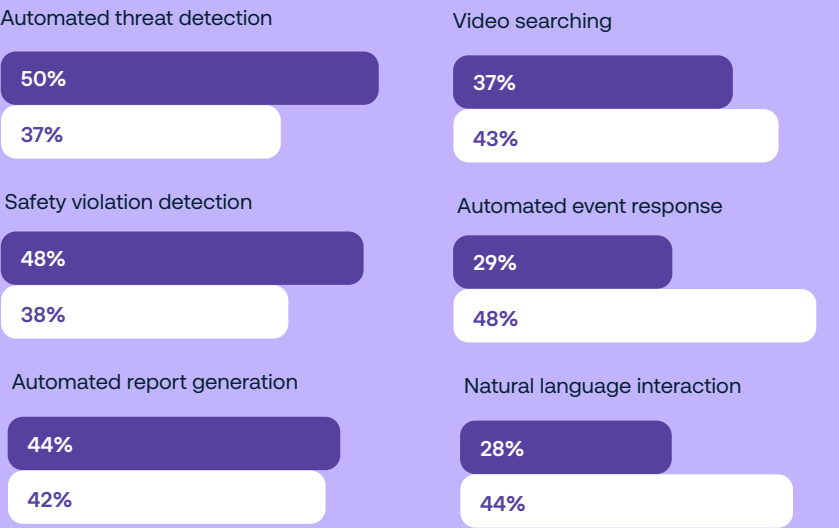


¹ In-house branded survey of Securitas Technology clients in Australia, Belgium, Canada, Denmark, Finland, France, Germany, Ireland, Mexico, Netherlands, Norway, Portugal, Singapore, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States. Data shown is reflective of commercial client responses only. Conducted November 2025.

Security technology market trends

Global insights from commercial electronic security decision-makers and influencers¹

Top future GenAI use cases



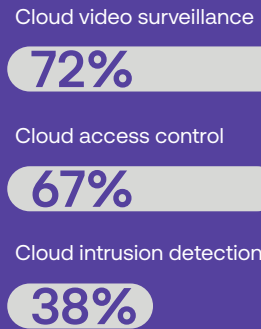
Top 3 challenges in implementing AI

- 1 48%
Uncertain ROI
- 2 47%
Compliance and privacy concerns
- 3 41%
Lack of internal knowledge



44% Plan to increase their use of cloud-enabled remote services

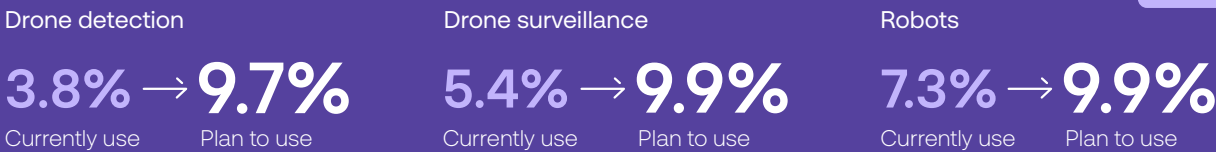
Top current cloud solutions



Top 3 drivers of remote services adoption

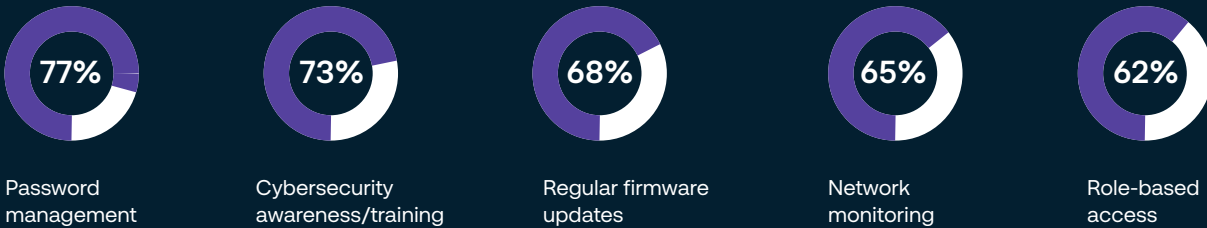
- 1 61%
Cost savings
- 2 58%
Faster incident response
- 3 46%
Higher uptime/availability

Drones, drone detection, and robots

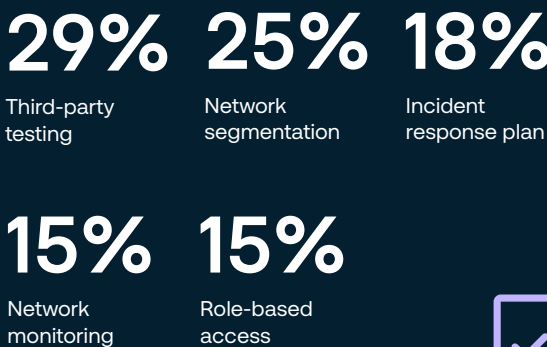


5.7% of organisations report a drone-related incident in the last year

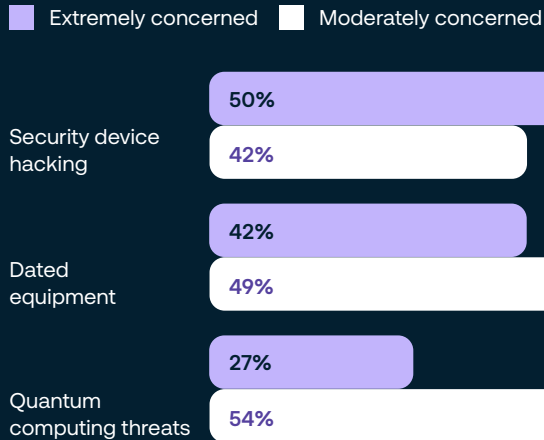
Current cyber-physical practices



Planned cyber-physical practices



Top cyber-physical concerns



Sustainability

54%

consider sustainability important or very important in security technology selection +6% vs 2025

1. Third-party blind survey of 575 security and loss prevention professionals with decision-making authority for security technology, representing commercial organisations in the APAC region, Europe, and North America. Conducted February 2026.

Technology partners' perspectives

Insights from our technology partners on the front line of security innovation¹

100%

of our technology partners are actively adding AI to their solutions



Top 3 trends impacting the security industry (next 3-5 years)

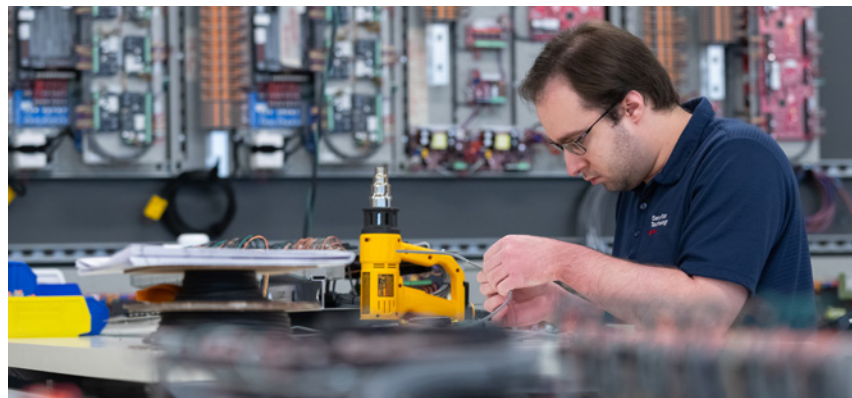
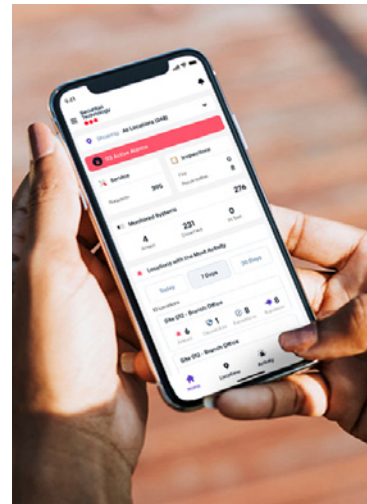
- 1 AI
- 2 Cloud
- 3 Integration

→ 62%

of our partners ranked AI as their #1 choice

Top 3 strategic product development priorities

- 1 User experience
- 2 Cloud technology
- 3 AI



Top 3 AI applications influencing product development

- 1 Edge analytics
- 2 Natural language interaction
- 3 Generative AI

95%

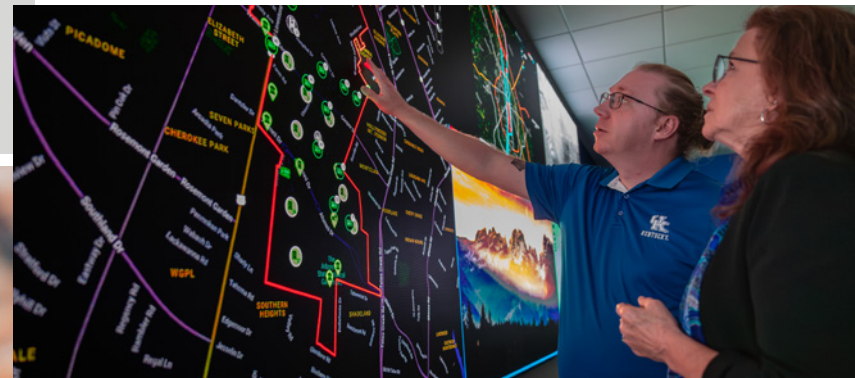
of our partners have seen an increase in cloud adoption

→ 43%

Significant increase

→ 52%

Moderate increase

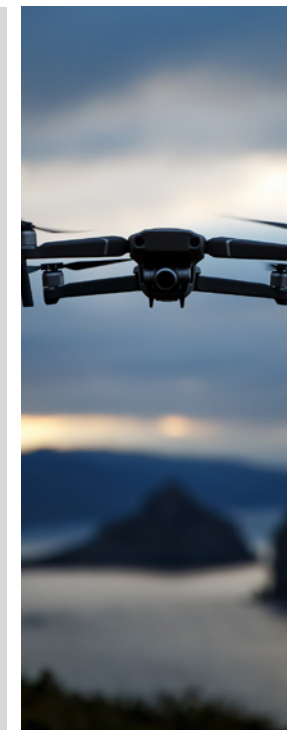


Technology partners currently integrating or planning to integrate drones and robots

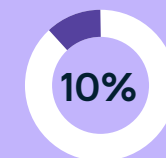
48% Drone detection

43% Surveillance drones

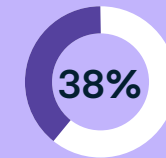
38% Robots



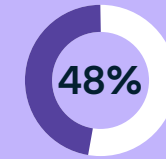
How our partners see drones and robots impacting future security operations



→ Transformational impact



→ Significant impact



→ Moderate impact

Top 3 sustainability initiatives

- 1 Local sourcing and optimised logistics
- 2 Sustainable packaging
- 3 Energy-efficient product design

¹ Survey and consultation with 26 strategic technology partners of Securitas Technology, representing leading global security equipment manufacturers, developers, innovators, and technologists. Conducted February 2026.



03

Capitalising on the AI opportunity

In this section

- › Advancing threat detection with AI
- › GenAI for smarter security operations
- › Agentic AI streamlining security decisions
- › AI-driven business security optimisation
- › Action plan for security professionals

AI moves from niche to essential

AI is no longer an incremental enhancement to established processes. It's poised to transform every aspect of day-to-day operations, helping teams spot issues more accurately, move faster, and make decisions with more certainty.

This matters, because most security professionals are faced with addressing growing complexity and rising expectations while resources remain constrained. The challenge is that AI can still feel like a moving target. There's a lot happening at once – new tools, new models, new use cases – and it's easy for leaders to wonder where to start or how to focus their efforts in a way that's practical rather than overwhelming.

In our market survey, uncertainty over ROI (cited by 48%¹ of respondents) topped the list of reasons why implementing AI into security programs remains a challenge for organisations, closely followed by privacy concerns, lack of internal knowledge, and uncertainty over which use cases to focus on.

However, there are strong indications that the increasing maturity of AI technologies and generative models is building confidence among global security leaders, who placed AI-driven video analytics as the top technology investment priority for the next 12-18 months (21%¹).

100%

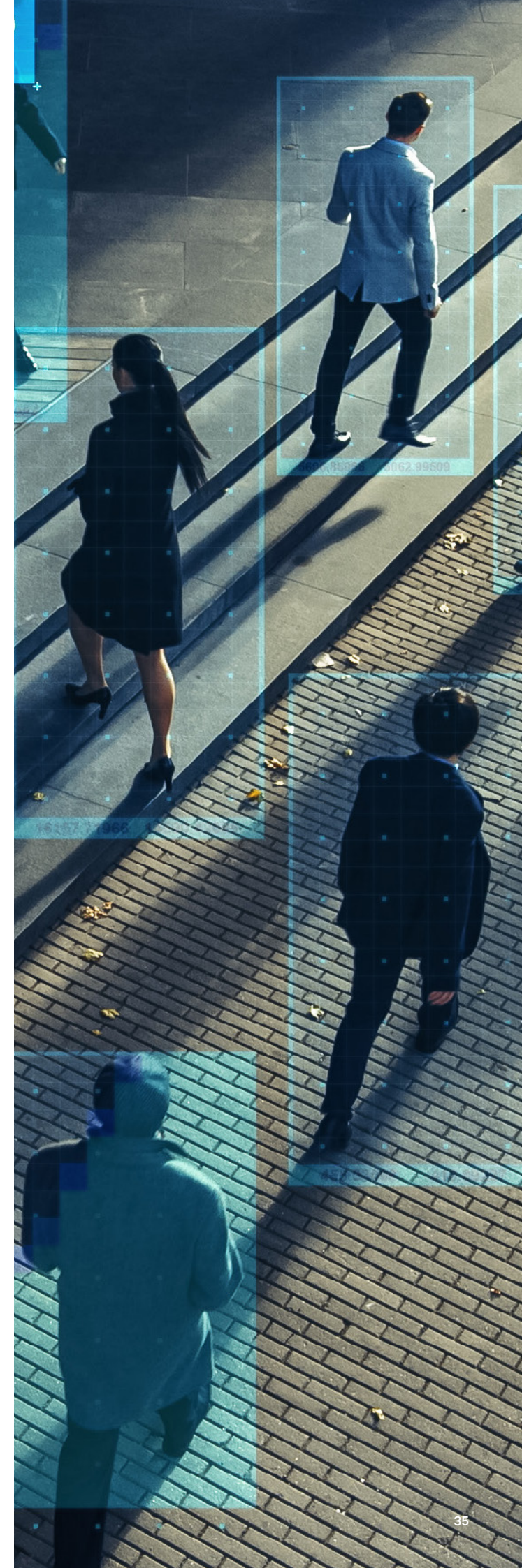
of our technology partners are investing in AI today²

The outlook

- **AI-powered threat detection** is helping address false alarms and improve detection accuracy across both video surveillance and intrusion systems. AI models reduce the need for manual monitoring and provide human operators with more context than ever before.
- **GenAI is changing how operators find and share information**, making video searches, summaries, and communication faster and more intuitive.
- **Agentic AI is emerging as a new way to support real-time decision-making**, offering consistent guidance across workflows.
- **AI is helping organisations improve system health**, forecast potential risks, and strengthen overall operational performance.
- **Cloud-based security platforms make AI easier to adopt and scale** by providing the structure for consistent deployment and transforming existing security devices into intelligent, AI-powered sensors.
- **Strong governance, data integration, and phased rollout plans are essential** for responsible and effective use of AI.

1. Third-party blind survey of 575 security and loss prevention professionals with decision-making authority for security technology, representing commercial organisations in the APAC region, Europe, and North America. Conducted February 2026.

2. Survey and consultation with 26 strategic technology partners of Securitas Technology, representing leading global security equipment manufacturers, developers, innovators, and technologists. Conducted February 2026.



Advancing threat detection with AI

Improving accuracy and addressing false alarms

Traditionally, video analytics have mostly focused on object recognition or motion detection as triggers, which can drive up false alarms due to their broad, rules-based configuration. AI makes threat detection more precise, consistent, and context-aware.

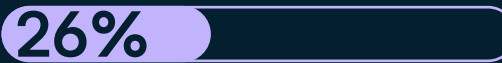
Whether the analytics take place in the cloud or at the edge (in a camera, for example), AI separates meaningful activity from everyday movement so operators can focus on what matters, allowing for more accurate filtering and resulting in fewer unnecessary dispatches and more time for higher-value work. **Edge analytics is by far the top AI focus for our strategic technology partners, with 48%¹ ranking it as their top priority.**

Understanding context, not just movement

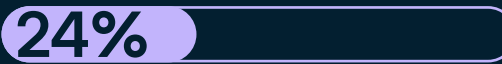
Modern AI models look beyond shapes or motion and assess the context of the scene. They spot situations that could pose a threat, such as unusual movement, loitering, or access attempts that don't fit the norm, to flag elevated risk earlier. Interest in behaviour-based anomaly detection is high as these advanced analytics can help give teams a head start and greater confidence, supporting a more proactive

Top 5 future AI-driven analytics use cases for organisations²

Intrusion and loitering detection



People counting



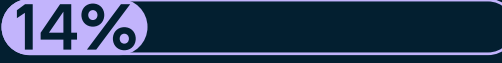
Object recognition (object type, face, licence plate, etc.)



Anomaly detection



Vehicle detection, speed, and direction



Strengthening situational awareness

Leveraging AI can help security leaders build a clearer picture of what's happening across a site by pinpointing key occurrences from live video. In busy or sprawling environments, no one can watch every feed; AI brings forward the moments that deserve attention and the details operators might miss. That sharper, context-rich view is what can help teams stay ahead of events and respond with more certainty moving forward.



1. Survey and consultation with 26 strategic technology partners of Securitas Technology, representing leading global security equipment manufacturers, developers, innovators, and technologists. Conducted February 2026.

2. Third-party blind survey of 575 security and loss prevention professionals with decision-making authority for security technology, representing commercial organisations in the APAC region, Europe, and North America. Conducted February 2026.

Smarter security: How AI helps eliminate false alarms

Conventional security sensors react to motion without understanding what caused it – a person, a cat, a car headlight, a tree branch. The result is a flood of alerts with no context, which leads to alarm fatigue and missed real threats.

Ajax cameras use on-device AI to detect, classify, and track objects in real time. This alone eliminates the most common source of false alarms. But because the system understands what's moving and where it's going, it enables more targeted rules – like triggering alerts only when a person crosses a defined perimeter, filtering out everything else.

Generative AI opens the next frontier – moving beyond recognising predefined object classes to understanding what's happening in a scene. This enables capabilities such as weapon detection and event description in natural language. Where current systems are limited to detecting what they've been explicitly programmed to look for, generative AI has the potential to identify threats that no one thought to define a rule for.

Together, these capabilities move cameras from passive motion recorders to systems that understand context — and only escalate what actually matters.



AI-powered analytics are redefining what intrusion detection can do

The security market is crossing a chasm as the industry evolves from hardware to software to cloud – and now to AI in the cloud.

Alarm and sensor systems are converging with video surveillance platforms, turning every camera and sensor into part of a behaviour-driven system that delivers alarms, and soon, predictive alerts about activity in and around a facility. “Intent analysis” will increasingly shape innovation, leading the industry toward agentic AI that uses machine-learned video and sensor analytics to quickly determine what is a real threat and what is not.

Historically, dispatching authorities has been difficult because traditional systems rely on reactive, binary contact switches and motion sensors that cannot evaluate what is actually happening in their environment. Confidence in system-generated dispatches will grow significantly as AI-equipped systems replace legacy technology.

Solutions such as Actuate’s Intruder AI and DMP’s XV Gateways with AlarmVision® transform standard IP cameras into intelligent alarm detection devices. By enhancing motion detection with advanced analytics and integrating video events directly with intrusion panels, organisations gain instant notifications, improved situational awareness and dramatically fewer false alarms.

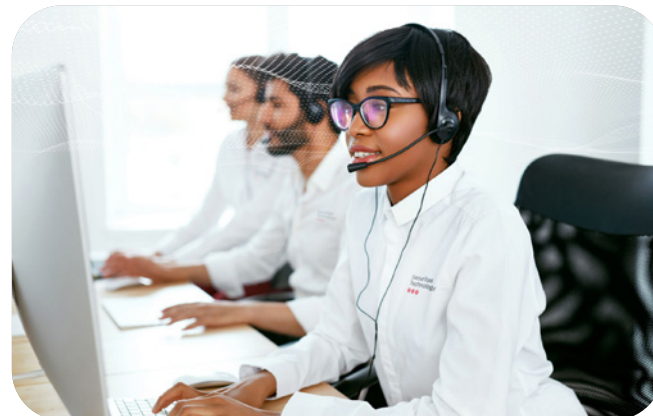


Enhancing operator efficiency

Security alarm monitoring is the most adopted subscription-based security service, with over half of organisations (55%¹) dependent on third-party monitoring for everyday business security. And it’s here that AI also stands to have a considerably positive impact. By helping reduce noise, surface key details, and cut the effort required to verify alarms, AI is empowering both security managers and alarm monitoring operators to validate alarms, pull the evidence they need, and escalate with less friction - improving efficiency while easing cognitive load and fatigue.

55%

of organisations use alarm monitoring services in their security programme today¹



Working seamlessly with digital platforms

AI-based detection becomes far more effective when it’s tied into the wider security ecosystem. Through digital security management platforms, alerts, video, and system data come together in a single view, making it easier for operators to leverage AI to understand what’s happening and act quickly. This unified setup helps connect AI-generated insights to other systems and streamlines response workflows. It also provides the governance, data consistency, and structure needed to expand AI across multiple sites with confidence.

A practical first step into AI

For many organisations, traditional rule-based analytics are a familiar and well-established threat detection tool. However, as more powerful, context-driven AI-based analytics - such as intrusion, loitering, and vehicle detection - become easier to access and use, they represent the next logical step. These applications provide a straightforward and impactful way to begin adopting AI. They deliver clear, immediate benefits including stronger accuracy, improved anomaly detection, and faster response times, without requiring major operational changes. They also support a human-in-the-loop approach, allowing operators to validate or refine AI outputs and maintain oversight where it matters most. Starting here helps teams build familiarity and confidence with AI, creating a solid foundation for expanding into more advanced generative AI capabilities.

1. Third-party blind survey of 575 security and loss prevention professionals with decision-making authority for security technology, representing commercial organisations in the APAC region, Europe, and North America. Conducted February 2026.

The edge of intelligence

Artificial Intelligence is redefining the intrusion detection space by moving processing power to the “edge.”

This shift represents one of the most significant technological advancements in modern security, allowing critical decisions to be made directly on devices rather than relying solely on centralised systems.

As a result, organisations benefit from faster insights, reduced latency, and a more resilient security architecture that continues functioning even when connectivity is disrupted.

This evolution enhances both security and operational efficiency. For instance, AI classifiers now provide advanced alarm verification, enabling monitoring centres to distinguish life-threatening emergencies from lower-priority events instantly and with far greater confidence. These capabilities help reduce false alarms, streamline operator workflows, and ensure that genuine threats receive immediate attention.

Beyond security outcomes alone, AI makes systems “smarter” and easier to deploy. Intelligent door control, for example, simplifies installation, reduces labour costs, and boosts profitability for integrators.

While the commercial sector was once slowed by unreliable hardware, Radionix is bridging that gap by backing robust technology that delivers superior range and dependable performance across even the most complex commercial applications.

radionix

GenAI for smarter security operations

Transforming how teams interact with information

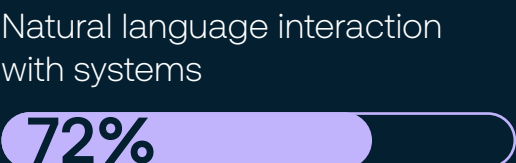
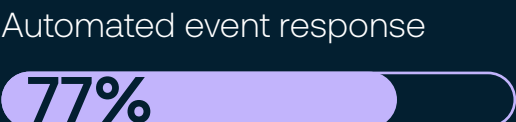
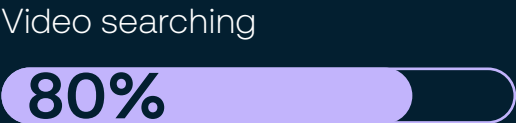
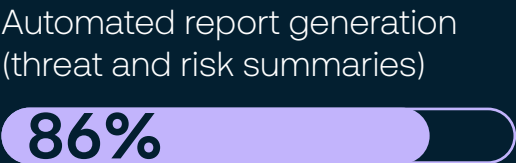
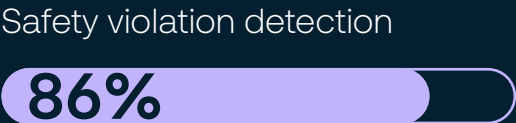
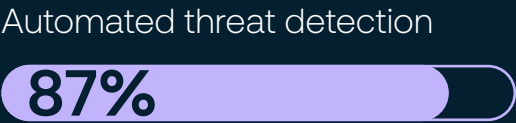
Generative AI is reshaping how security teams access and work with their systems by removing many of the manual steps that used to slow them down. **Benefits like automated threat detection¹ tops the list of GenAI applications organisations are showing interest in, along with safety violation detection and system reporting, as they offer tangible operational efficiencies.**

Meanwhile, operators can enjoy a simplified user experience thanks to the ability to converse with systems using chat-based, natural language prompts. This reflects the aim of GenAI to help reduce time spent on routine tasks and allow teams to focus on assessing risk, coordinating response, and supporting activity on the ground. It creates a smoother, more intuitive way of interacting with data that matches the pace and pressure of modern security operations. **GenAI is a top three AI product development priority for 60%² of our strategic technology partners.**

1. Third-party blind survey of 575 security and loss prevention professionals with decision-making authority for security technology, representing commercial organisations in the APAC region, Europe, and North America. Conducted February 2026.

2. Survey and consultation with 26 strategic technology partners of Securitas Technology, representing leading global security equipment manufacturers, developers, innovators, and technologists. Conducted February 2026.

Interest from organisations in GenAI applications for electronic security systems¹



Technology partner insight

Understanding GenAI

Generative AI is powerful at identifying patterns in large volumes of security data that may indicate emerging risk, but its insights still require human judgment and context.

We still need to validate it by testing the system against data we already understand, data we know to be good, and data we know to be bad.

We need to see how it behaves when given flawed or conflicting information. What happens if we label someone as high risk, but the data doesn't support that conclusion? What if we label someone as low risk, yet the data suggests otherwise?

Because there is no true gold standard for AI, stress testing is essential. This is especially true for those of us working in physical security and life safety. It's our responsibility to pressure-test these technologies before deploying them in real-world environments.

If AI is used only to assess something with minimal risk, the consequences of being wrong may be relatively minor. But if it's being used to decide who can access certain areas, when to deploy security, or when to involve law enforcement, the stakes are much higher.

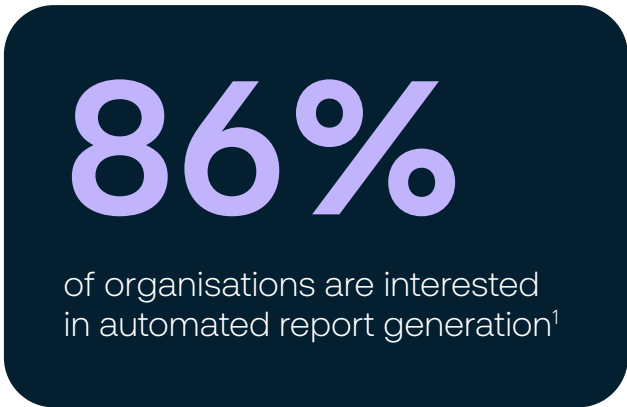
ASSA ABLOY
Opening Solutions

Making video search faster and more intuitive

Traditional video searches can be slow and manual, often requiring operators to scrub through long clips or rely on narrow keyword filters. This is why organisations are looking to GenAI to help speed up their review processes. These models can understand the intent behind a request, meaning an operator can simply describe the moment they're looking for, such as when a delivery truck arrived or when someone entered a side door, and the system quickly finds the relevant footage. This cuts review time, improves evidence gathering, and helps teams move through investigations with far less friction.

Automating reporting and operational workflows

GenAI is finding application in producing summaries of alarms, incidents, or shift activity based on real operational data, helping to make handovers more consistent, support compliance needs, and reduce manual documentation tasks. **86%¹ of organisations we surveyed indicate strong interest in this kind of automated report generation.** For example, a security manager could upload their standard operating procedure (SOP) document to their AI-powered security platform; the AI then automatically creates the natural language alarm prompts for GenAI to programme and monitor. By taking on this administrative workload, GenAI can free operators to spend more time on active monitoring and the situations where their judgment adds the most value.



1. Third-party blind survey of 575 security and loss prevention professionals with decision-making authority for security technology, representing commercial organisations in the APAC region, Europe, and North America. Conducted February 2026.

Technology partner insight

Getting smarter about artificial intelligence

The continued evolution of new cameras combining AI with on-board audio and video analytics is resulting in highly accurate object detection and classification.

The past few years have seen companies throughout the security and surveillance industry expand their use of AI, doing more than improving camera imaging performance. In addition to fewer false alarms, customers are deriving actionable data that can drive intelligent monitoring to enhance operational efficiency and generate data-driven business insights. We will continue to see additional types of devices and a fusion of AI to bring more intelligence to surveillance cameras and systems.

The next leap is a continued shift toward generative AI combined with natural language processing, meeting customers' demand for simplicity, personalisation, and voice-driven search soon becoming the norm in enterprise security. The market will continue to see open platforms and generative AI continue to emerge, supporting more granular capabilities for accurate tracking and object detection.

Users can search using natural language. Instead of manually reviewing data, someone could simply ask the system to identify an individual who entered between 1:00 pm to 2:00 pm wearing a red shirt, blue glasses, and a hat. Just as they speak to Siri or Alexa at home, customers now expect to communicate with security systems the same way. Modern systems are becoming intelligent enough to handle these types of requests, and customers are embracing this simplicity.

Understanding visual and audio context

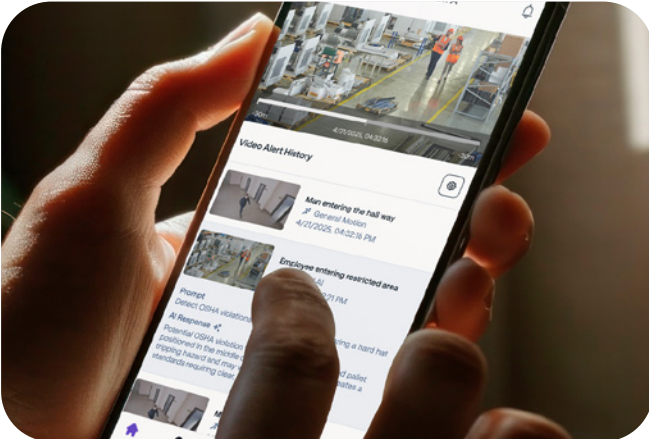
Unlike traditional video analytics, GenAI can interpret what is happening in a video image, enabling operators to stay on top of specific risks or situations – everything from security threats to health and safety violations. It can read text that appears in images and recognise objects or patterns that might be relevant to an operator’s request. And these requests can be made using simple natural-language queries both to set up alerts for future events or to search past events. This multimodal capability helps teams monitor busy or complex environments more effectively, bringing together details that would otherwise take much longer to piece together. It expands the range of insights available and supports quicker, more informed decision-making.

86%

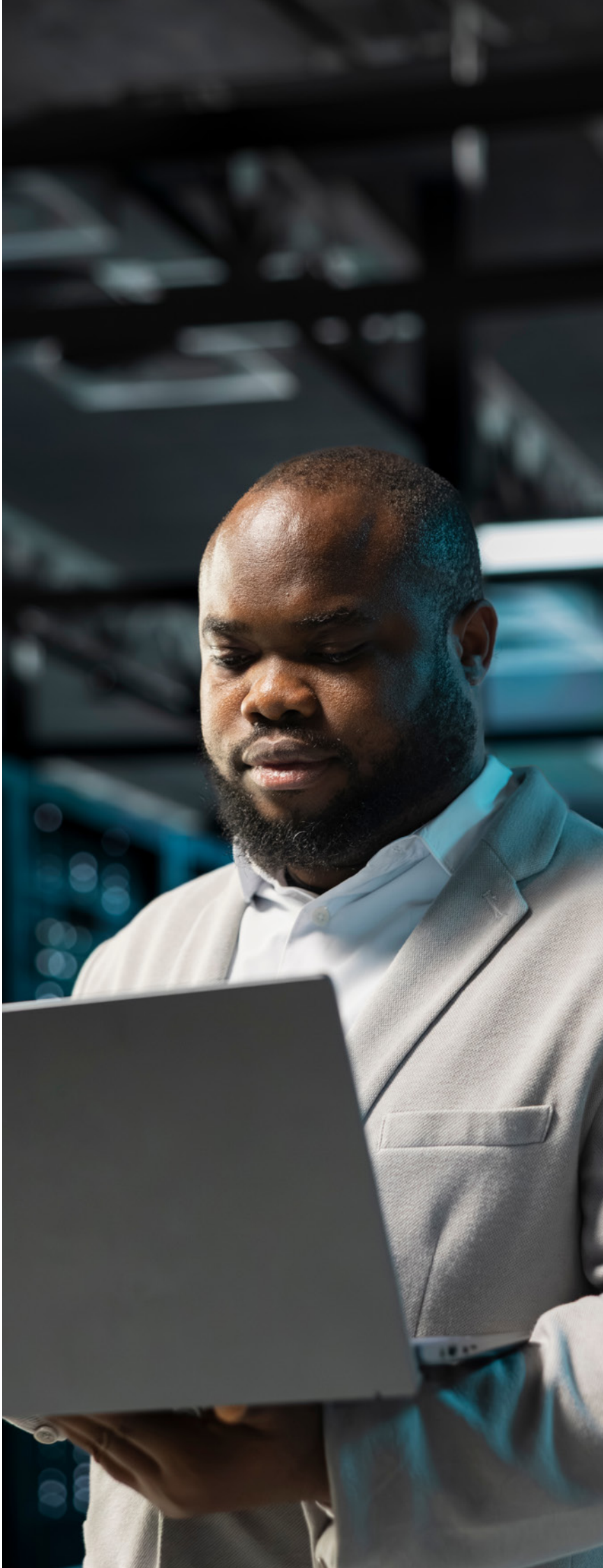
of organisations are
interested in using GenAI
to flag safety violations¹

The unlock for more efficient and resilient operations

GenAI holds the potential to radically improve efficiency and effectiveness by freeing security teams from low-value manual tasks and equipping them with actionable information. When operators can get the right details quickly – whether it’s a summary of an incident, a clip that needs review, or an alert that requires attention – they spend less time on administrative steps and more time managing active situations. The value of automated incident report generation becomes particularly valuable when data volumes are high or operations run around the clock. By streamlining routine tasks and improving the flow of information, GenAI supports more efficient, steady, and resilient security operations.



1. Third-party blind survey of 575 security and loss prevention professionals with decision-making authority for security technology, representing commercial organisations in the APAC region, Europe, and North America. Conducted February 2026.



Technology partner insight

Transforming security operations

Generative AI can significantly streamline security workflows by automating threat detection, investigation, and response.

It identifies anomalies up to **100x faster**² than traditional methods, reduces false positives by around **50%**³, and cuts analyst workload through automated log analysis, alert triage, and rapid incident remediation guidance. It also improves vulnerability management by performing automated code reviews and catching up to **90%**⁴ of bugs before production, helping security teams stay ahead of attackers.

For predictive risk analysis, generative AI enables proactive threat modelling by analysing large datasets – including behavioural patterns, network activity, and global threat intelligence – to anticipate attack pathways and emerging risks. Organisations using AI-driven predictive security achieve **60%**⁵ faster threat detection and significantly lower breach costs. As AI-enabled attacks grow more sophisticated and adaptive, generative AI helps forecast evolving threats and counter advanced tactics such as AI automated ransomware or dynamic phishing campaigns.

Together, these capabilities transform security operations from reactive to predictive – enabling faster decision making, reduced operational burden, and stronger resilience against next-generation cyber threats.

2. Microsoft Security. AI in Cybersecurity/Security Copilot Research. microsoft.com/security.

3. Capgemini Research Institute. Reinventing Cybersecurity with Artificial Intelligence: The New Frontier in Digital Security. capgemini.com/research/reinventing-cybersecurity-with-artificial-intelligence.

4. Synopsys. State of Software Security (SOSS) Report. synopsys.com/software-integrity/resources/analyst-reports.

5. IBM Security. Cost of a Data Breach Report 2023. ibm.com/reports/data-breach.

Agentic AI streamlining security decisions

Moving from assistive AI to collaborative intelligence

While in an early stage of adoption, agentic AI represents the next phase in how artificial intelligence can support security operations. Instead of focusing only on analysis or detection, these models can take a more active role by helping operators interpret a situation, how it might evolve, and how to best respond. **Almost half (48%) of our strategic technology partners ranked agentic AI as a top three product development priority, with 16% placing it first.**

It's important to consider that AI agents aren't intended to replace human judgment – but they can help to strengthen it by organising information, highlighting what's important, and offering options based on standard operating procedures. **With over three quarters of organisations showing interest in automated event response²**, there's a real desire for technology that helps security teams spend less time reacting to individual alerts and more time managing events with a clearer sense of circumstance and priority.

77%

of organisations are interested in automated event response by AI agents²

Assisting real-time decisions with intent

Agentic AI systems are built not to simply follow preset rules but to actively evaluate events and respond accordingly. They combine inputs from video, sensors, system-health data, and historical patterns to offer informed recommendations during fast-moving situations. If several alerts appear in the same area, for example, the AI can help determine which one needs attention first, suggest verification steps, or pull up the most relevant camera feeds. This level of support enables operators to stay focused and respond more effectively, especially when activity spikes.

Reducing cognitive load on security teams

Security teams often juggle a high volume of information under time pressure. Agentic AI helps ease that burden by filtering out noise and highlighting what genuinely needs attention. It organises tasks, tracks evolving incidents, and surfaces insights operators might not spot immediately. This support helps teams maintain situational awareness, reduces fatigue, and promotes more consistent handling of events across shifts and sites.



1. Survey and consultation with 26 strategic technology partners of Securitas Technology, representing leading global security equipment manufacturers, developers, innovators, and technologists. Conducted February 2026.

2. Third-party blind survey of 575 security and loss prevention professionals with decision-making authority for security technology, representing commercial organisations in the APAC region, Europe, and North America. Conducted February 2026.

Technology partner insight

Agentic AI in critical security: A new opportunity

Agentic AI presents many opportunities in critical security.

Primarily, it simplifies running security operations. A faster detection-to-response process via goal-driven agents that perceive, reason, plan, and act saves time and money by automating a response immediately. It delivers higher alarm quality through its use of multiple technologies – video, audio, access, intrusion, and environment – to gain a better understanding of what's happening on the ground.

It helps deliver better technology assistance through pan/tilt/zoom auto-tracking, talk-down, lighting and barrier control, door holds and lockdowns, and it is scalable across sites, making it a flexible solution that grows alongside businesses.

There are, of course, considerations around the use of agentic AI in critical security. A human will always be necessary: Some actions must remain 'never-auto' to avoid errors. There can also be challenges around integration complexity linked to legacy systems.

Most importantly, accountability for autonomous steps must be visible to avoid liability and service level agreement (SLA) issues. Clear guardrails and kill switches must be in place.

Organisations should adopt a staged approach to deliver the best results, starting with low risk bounded autonomy, and expanding as confidence improves, balancing speed and scale with safety, explainability, and compliance.

3xLOGIC



Enabling more proactive and coordinated operations

As agentic AI continues to mature, we believe it will play a larger role in coordinating activity across security systems and teams. Agents can automate early triage steps, trigger follow-up actions, or notify operators when certain thresholds are met. When connected to centralised security platforms, these capabilities can function as part of a unified ecosystem where detection, insight, and response work together more smoothly. It's a level of integration that supports the shift from reactive incident handling toward more proactive, intelligence-led operations across multiple sites.

What security leaders should watch as the technology evolves

Agentic AI is new in the security space, and best practices are still developing. Decision support, where the AI agent gathers information and presents options to a human operator, is a likely starting point for most organisations, but security professionals should prepare for a future where AI agents take a more active part in incident response. Key considerations for this kind of application include how much scope organisations are willing to grant to an AI agent to take decisions, and how humans will be kept in the loop to ensure both accountability and reversibility. As reliability increases and governance best practices become more established, agentic AI will offer new ways to accelerate decision-making and improve incident response.

Accountability starts with how you design the workflow

Agentic AI is moving from hype-cycle to operational reality, and, the question isn't whether to deploy autonomous agents – it's how to keep humans in control of critical outcomes.

Agentic AI is now orchestrating across security systems: ingesting video, correlating access logs, detecting deviations, and triggering follow-up actions. But accountability must be built into the workflow itself, not bolted on after the fact.

Consider autonomous investigation agents that take an alarm, gather 30 minutes of multimodal evidence, and propose immediate mitigation for an operator to approve. This human-in-the-loop model is key: The agent handles speed and data-gathering, while accountability for decisions stays with people.

Transparency comes from architecture. Platforms that expose safe, auditable agent application programming interfaces (APIs) allow every AI-initiated action to be traced, explained, and reviewed. Measuring agent performance against defined key performance indicators (KPIs) – incident triage time, evidence accuracy, false-positive rates – turns trust from an abstract principle into something measurable.

As organisations operationalise agentic AI into their security workflows at scale, the winners will be those who treat accountability not as a constraint, but as a design requirement from day one.

AI-driven business security optimisation

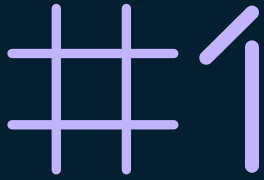
Data integration the key to meaningful AI insight

40%¹ of organisations we surveyed told us that lack of data integration between security systems is holding them back from implementing AI within their security programme. This points to the importance of an integrated data ecosystem as the key that will help unlock AI's huge potential to drive security optimisation and deliver real business value. More organisations are building towards this. **Our survey also highlighted that the ability to integrate systems is a top three criteria¹ for selecting an electronic security technology provider for organisations of all sizes and across geographies.**



How AI is helping drive operational efficiency

For organisations with high levels of integration in place, AI is helping them understand their environments in ways manual processes rarely allow. By analysing patterns across video, sensors, system-performance data, and incident history, AI highlights trends that matter – whether it's recurring bottlenecks, shifts in behaviour, or early indicators of increased risk. These insights can give security leaders a clearer basis for decisions around workflows and technology investments, improving day-to-day performance while supporting longer-term planning.

Artificial intelligence is the 

trending technology our clients are interested in adopting in the next 12-18 months²

Improving workforce efficiency and resource allocation

AI helps teams work more efficiently by taking on low-value, repetitive tasks and highlighting the insights that require human judgment. It gives leaders a clearer view of how time is being spent, how effectively incidents are being handled, and where processes can be tightened. Over time, these insights will help support better staffing decisions, more balanced shift structures, and a smarter distribution of responsibilities across different sites.

1. Third-party blind survey of 575 security and loss prevention professionals with decision-making authority for security technology, representing commercial organisations in the APAC region, Europe, and North America. Conducted February 2026.

2. In-house branded survey of Securitas Technology clients in Australia, Belgium, Canada, Denmark, Finland, France, Germany, Ireland, Mexico, Netherlands, Norway, Portugal, Singapore, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States. Data shown is reflective of commercial client responses only. Conducted November 2025.

Technology partner insight

Smarter solutions to help deliver better security processes

AI-driven optimisation enables organisations to enhance security effectiveness while improving operational efficiency by automating intelligence and decision-making across systems.

Intelligent alarm filtering, for example, reduces nuisance and false alarms, allowing operators to prioritise high-risk events and accelerate dispatch decisions.

In access control, AI monitors unusual credential use, tailgating patterns, and atypical sequences, preventing misuse while reducing the need for constant manual oversight.

Video verification is also accelerated through AI analytics, which can detect people, vehicles, and unusual behaviours, allowing remote operators to confirm incidents quickly and respond proactively.

Beyond incident response, AI continuously monitors system health, flagging device failures, communication issues, or configuration drift before they impact service, helping maintain uninterrupted operations.

Predictive maintenance further enhances efficiency by anticipating controller or peripheral failures and scheduling proactive service, minimising downtime and operational disruption.

By combining intelligent threat detection, automated monitoring, and predictive insights, AI-driven optimisation balances robust security with resource efficiency, enabling organisations to respond faster, prevent incidents before they escalate, and maintain reliable operations across complex and distributed environments.



Enhancing compliance, reporting, and operational oversight

Organisations increasingly need to demonstrate compliance with both internal policies and external regulations. AI holds the potential to support this by monitoring adherence more consistently than manual oversight and highlighting where standards may be slipping. It can help track key performance indicators, support clearer documentation, and generate summaries that give leaders better visibility across sites. This level of insight will not only improve control, but also help maintain steady, repeatable processes that stand up to audits and internal review.

Strengthening strategic risk management

By combining historical trends with real-time intelligence, AI helps organisations spot potential risks earlier and take action before issues escalate. It can highlight emerging patterns – such as shifts in theft activity, changes in after-hours behaviour, or unusual environmental conditions – that may signal rising exposure. When these insights tie into comprehensive security management platforms, they become part of a broader risk picture that supports more proactive, informed decision-making across sites.

Building toward continuous improvement

AI-driven optimisation isn't a one-time upgrade but an ongoing process. As more data is collected and models continue to mature, organisations will gain access to a clearer view of what's happening across their security operations and where improvements can be made. Over time, this helps create a cycle of steady learning and refinement that strengthens resilience, enhances performance, and ensures the security programme keeps pace with the needs of the business.



Technology partner insight

Improving security effectiveness with AI

Artificial Intelligence has the potential to greatly improve the effectiveness of security operations by accelerating response times, adding contextual information to incidents, identifying events that would otherwise go unnoticed, and in some cases, resolving incidents autonomously.

However, AI must be deployed carefully to ensure outcomes are accurate, reliable, and aligned with organisational expectations.

Planning should begin with clearly defined operational objectives. Instead of focusing solely on what an AI model can detect, determine the full desired workflow. For example, detecting patient falls in a hospital is only the starting point. The operational outcome should include presenting live and recorded video of the incident, identifying location and severity, offering appropriate dispatch options, and logging the results to continuously refine rules and reduce false alerts.

Strong governance controls are essential for any AI deployment. Organisations must define what AI is permitted to do, the conditions required before automation can act, how data will be stored and protected, and how long information is retained. These policies must be actively managed throughout the life cycle of the system.

Finally, effective systems require thoughtful human-in-the-loop design. In security and life safety environments, AI should highlight important events, organise information, and recommend actions – while humans retain responsibility for approving or escalating decisions, ensuring oversight remains intact.



“

AI is most powerful when it's grounded in real problems, trusted data, and human judgment. The opportunity for security leaders is not to chase every new tool, but to focus on the use cases where AI can make their teams more effective, more resilient, and better prepared for what comes next.

”

Dr. Serdar Ince

Senior Vice President, Global Innovation & Artificial Intelligence
Securitas Technology



Action plan for security professionals

Implementing AI into your security programme

01

Begin with a clear purpose

Define what you want AI to help you achieve. Whether the goal is reducing false alarms, speeding up responses, improving operator workflows, or gaining clearer insight from data, specific objectives make it easier to choose the right AI tools and measure their impact over time.

04

Integrate AI into existing workflows

AI works best when it enhances the way teams already operate. Map out your core workflows — from alarm handling to investigations — and identify where AI can automate steps, offer recommendations, or reduce manual effort. Integrating with security management platforms ensures insights reach the right people in the right moment.

02

Build a strong data and governance foundation

AI depends on reliable data, consistent configuration, and good cyber hygiene. Review how your systems are set up, who can access what information, and how data is stored and protected. Clear, straightforward governance helps AI deployments perform better and scale more easily.

05

Pilot with purpose and scale based on evidence

Run focused pilots with clear success criteria. Track metrics like alarm reduction, verification time, operator workload, or incident-closure rates. Use results and feedback from your team to refine your approach, and scale only once the value is consistent and repeatable.

03

Focus on high-value, low-risk use cases first

Start with AI applications that are proven, measurable, and easy for teams to adopt. Common early steps include AI-based detection, natural-language video search, automated reporting, and system-health insights. Small, early wins help build momentum and demonstrate value to stakeholders.

06

Prepare your team and choose the right partners

AI changes how people work, so communication and training are essential. Explain how AI supports, rather than replaces, human judgment, and give teams practical guidance on using new tools. Work with partners who understand both AI and security operations and who can support responsible, transparent adoption over time.



04

Cloud solutions reshaping security

In this section

- › The foundation for next-generation security
- › System health monitoring and maintenance
- › Remote verification and incident management
- › Centralised security system management
- › Action plan for security professionals

The shift toward flexible, connected security operations

The growing adoption of cloud-based security platforms is changing how organisations manage events and maintain their security technology.

With cloud now firmly established as the foundation for system scalability and managing cyber-physical risk, organisations are increasingly focused on unlocking the operational benefits of greater connectivity and centralised security management. These cloud-enabled capabilities help security teams work more efficiently, maintain consistent standards across sites, and improve resilience, while also reducing on-site hardware requirements and enhancing data redundancy.

Our market survey shows strong demand for remote functionality across industries, with **44%¹** of organisations planning to increase their investment in remote services. Remote services offer security leaders clearer visibility across sites and enable faster, more coordinated responses, even when on-site resources are limited. Our strategic technology partners also identified remote functionality as the number two driver² of cloud-based technology adoption.

44%

of organisations are expected to increase their use of remote services over the next 18 months¹

1. Third-party blind survey of 575 security and loss prevention professionals with decision-making authority for security technology, representing commercial organisations in the APAC region, Europe, and North America. Conducted February 2026.

2. Survey and consultation with 26 strategic technology partners of Securitas Technology, representing leading global security equipment manufacturers, developers, innovators, and technologists. Conducted February 2026.

The outlook

- **Cloud and hybrid-cloud infrastructure is becoming the standard configuration, enabling scalable, flexible, and AI-ready security programmes** that evolve with operational demands.
- **Remote services are helping organisations maintain strong protection** across multiple sites, even when on-site resources are limited.
- **Remote health monitoring and maintenance strengthens reliability** by identifying issues early and minimising downtime.
- **Centralised verification and incident management can improve accuracy and speed** by giving teams a clearer, unified view of activity.
- **Remote system administration simplifies updates, permissions, and policy rollouts** across locations.
- **Together, these capabilities will support a more proactive and intelligence-driven security operation.**



The foundation for next-generation security

Why cloud matters for modern security

The adoption of cloud-based security platforms continues to rise. **Our client survey revealed that almost a quarter¹ of companies are already leveraging the technology, with cloud video surveillance and access control among the most adopted solutions.** Cloud technology is becoming the backbone of modern security operations and foundational for advanced AI capabilities, avoiding the rip-and-replace of hardware, and enabling increased agility in updates and configuration.

While the cost of equipment and risk of loss of sensitive data remain the top concerns for those organisations yet to adopt cloud, a growing number see the pros as outweighing the potential cons. **Our strategic technology partners are noticing this trend too, with 92%² seeing an increase in adoption over the past year.**

Hybrid set-ups will continue to offer a path for organisations to harness the flexibility of cloud platforms and steadily move away from relying solely on on-premises infrastructure, which can be resource-heavy and slow to scale.

24%

of our clients have already implemented cloud-based electronic security systems¹

1. In-house branded survey of Securitas Technology clients in Australia, Belgium, Canada, Denmark, Finland, France, Germany, Ireland, Mexico, Netherlands, Norway, Portugal, Singapore, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States. Data shown is reflective of commercial client responses only. Conducted November 2025.

2. Survey and consultation with 26 strategic technology partners of Securitas Technology, representing leading global security equipment manufacturers, developers, innovators, and technologists. Conducted February 2026.

Technology partner insight

Cloud AI as the operational default

Video surveillance has undergone a fundamental transformation. We have moved past the era of “rewind and review” into an age of proactive business intelligence. This shift is anchored by the sustained dominance of the cloud as the indispensable engine for security innovation.

A cloud infrastructure ensures your system is always current. Interface improvements and firmware updates are applied transparently across all connected cameras and control panels, eliminating the maintenance burden of legacy hardware. When properly architected, the cloud serves as an extensible engine for new capabilities through open APIs and flexible data formats.

AI is no longer just for detecting motion; it is now an essential tool for creating entirely new workflows. By leveraging Large Language Models (LLMs), decision-makers can define custom searches and business reports using plain English – with zero programming needed.

- “Show me every delivery vehicle that entered after 7:00 pm.”
- “Alert me if workers are not wearing personal protective equipment on the jobsite.”

This centralised cloud power transforms raw data into actionable insights, making intelligent security the strategic default for every organisation.





Technology partner insight

Building scalable, resilient remote security with the cloud

Cloud is changing how remote security services are built and delivered.

It's not just about moving video and systems off-site. It's about giving security teams the flexibility to grow and adapt without constantly rebuilding their infrastructure.

In the past, scaling a surveillance system meant adding more servers, storage, and hardware at each location. While effective, this approach becomes costly and complex as organisations expand. Cloud-based architectures change that model by allowing security providers to onboard new sites, cameras, and analytics quickly, often without deploying additional infrastructure on-site. This scalability is essential as businesses grow and security operations become more distributed.

Resilience is equally important. Cloud environments are designed with built-in redundancy and failover, so if one component fails, another takes over. For remote security services, that means video, alerts, and system access remain available when they are needed most.

Today, many organisations are adopting hybrid architectures that combine the best of both worlds. Recording and processing can remain close to the cameras on-premise, while the cloud handles centralised management, analytics, and long-term storage. The result is a flexible model that allows providers to monitor many locations from one platform and scale services as customers grow.

Unlocking the power of advanced analytics and AI

The cloud is essential for enabling organisations to take advantage of advanced AI capabilities that combine data from multiple systems for true operational intelligence. Behavioural analytics, GenAI-powered search, and automated system-health intelligence all rely on the computing power and data access cloud platforms provide. From intrusion to video to access control, organisations can tap into real-time insights, helpful AI tools, and continuous improvements delivered through automatic updates. In this way, the cloud becomes more than a storage layer – it becomes an intelligence layer that elevates the entire security ecosystem.

Types of cloud-based security technologies currently used by organisations¹

Cloud video surveillance

72%

Cloud access control

67%

Cloud Intrusion detection

38%

1. Third-party blind survey of 575 security and loss prevention professionals with decision-making authority for security technology, representing commercial organisations in the APAC region, Europe, and North America. Conducted February 2026.

Connecting sites, systems, and teams through one platform

Cloud-based digital platforms are now an essential part of the security manager's toolkit. They help unify visibility and control across all locations, allowing remote access to view live video, check system health, adjust settings, and verify alerts from anywhere – using a single, consistent interface. This level of centralisation is highly valued by organisations because it helps eliminate siloed workflows and supports more coordinated decision-making. For multi-site organisations, the ability to manage permissions, integrate new devices, and monitor performance across locations is a significant advantage, helping drive consistent security across all sites and providing clarity to improve security overall.

Centralised security management is the top driver of cloud adoption

according to our strategic technology partners¹

Balancing flexibility with security and privacy

Adopting cloud solutions means organisations benefit from increased flexibility. But they also must carefully consider data security, privacy, and governance. While today's cloud providers offer strong protections, from secure encryption to strict access controls and robust compliance frameworks, it's still important to understand how security data is handled, where it's stored, and who can access it. The onus is also on organisations themselves to ensure the internal networks that cloud platforms are connected to are well protected and maintained. See **section 6** for more information on security data best practices.

1. Survey and consultation with 26 strategic technology partners of Securitas Technology, representing leading global security equipment manufacturers, developers, innovators, and technologists. Conducted February 2026.

Technology partner insight

Cloud-based security architectures redefine scalability and resilience

Cloud-based architectures are changing how remote security services scale and operate.

Instead of planning for fixed capacity, modern cloud platforms automatically adjust to workload demands, including concurrent live video views, high data ingestion rates, queued alarms, and case exports. Multi-tenant designs enable multiple sites and customers to be monitored efficiently without one environment affecting another. As organisations grow, onboarding new customers becomes simpler, and capacity planning becomes far less restrictive.

Cloud architectures also support a more flexible workforce. Operators and administrators can work from a single interface anywhere in the world, improving collaboration and consistency across distributed teams.

Resilience is built into the cloud by design. High-availability architectures help maintain consistent uptime with minimal infrastructure at customer sites or in central-station environments. Zero downtime updates make it easier to introduce new capabilities without disruption, while configurable features allow operators to work more efficiently.

Cloud adoption strengthens security and compliance through identity provider integration, encryption of data at rest and in transit, and architectures that remove the need for open firewall ports or VPN access. Hybrid models further reduce bandwidth usage, lower infrastructure costs, and allow teams to focus on delivering services rather than maintaining systems.

VERINT



System health monitoring and maintenance

Strengthening system reliability through proactive awareness

System reliability is a top three factor¹ driving increased use of remote services, according to our market survey. Through remote health monitoring and maintenance services, organisations are seeking a clearer, more continuous view of how their security infrastructure is performing. Instead of finding issues only when they're reported, or when something goes wrong, security teams want to be alerted to potential problems early on to help keep systems running reliably across all sites.

This proactive visibility is especially valuable for organisations with large footprints, limited on-site technical resources, or environments where equipment failures can directly affect employee safety or operations.

46%

of organisations say the need for higher system uptime is driving their increased use of remote services¹



Identifying device-level issues before they disrupt operations

Cloud-connected platforms make it possible for security teams to track device status, connectivity, and performance in real time. Cameras, sensors, and other networked devices can also be checked remotely by service partners for early signs of degradation, outages, or configuration inconsistencies. AI-supported diagnostics help flag unusual behaviour – such as declining video quality, storage faults, or failing components – so teams can act before small issues lead to service interruptions.

1. Third-party blind survey of 575 security and loss prevention professionals with decision-making authority for security technology, representing commercial organisations in the APAC region, Europe, and North America. Conducted February 2026.

Technology partner insight

Minimise downtime with smarter remote health monitoring: Proactive maintenance for modern security systems

Innovations in remote monitoring that minimise downtime start with live, centralised health visibility, not just alarms after something fails.

System health dashboards bring key system indicators into one place, including real-time status for panels, readers, server services, and disk usage, so teams can spot degradation early and act before it becomes an outage.

Thanks to cloud-enabled, centralised security platforms, the biggest shift is moving from reactive troubleshooting to proactive maintenance through:

- Colour-coded, at-a-glance status and configurable dashboards that make issues obvious to operators quickly (even across large deployments).
- Targeted alerts for offline or degraded devices (like a panel or reader) to reduce “silent failures” that otherwise get discovered only when doors stop working.
- Fast search, filtering, and exportable reporting to speed triage, document fixes, and spot recurring patterns that signal ageing hardware or network instability.

As these dashboards evolve, the next frontier is trend-based diagnostics, automated workflows, and remote-first service models that let teams resolve more issues without site visits, keeping systems online and secure with less disruption.

Reducing unnecessary site visits, improving sustainability

When internal teams or security providers can diagnose and resolve issues remotely, they spend less time travelling to sites and more time focusing on higher-value work. Many common problems, from configuration changes to system resets, can be addressed without sending a technician on-site. This leads to less carbon emissions, faster resolution, lower operational costs, and a more sustainable approach to delivering technical support across widely distributed locations.

Supporting predictive maintenance and life cycle planning

By tracking system performance and asset information over time, remote health monitoring and life cycle management platforms help organisations see when devices are nearing end of life or when repeated issues point to deeper technical problems. These insights support more accurate budgeting, smarter upgrade planning, and fewer unexpected outages.

Predictive maintenance also helps teams prioritise attention on the sites that need it most, ensuring resources are directed where they will have the greatest operational impact.



1 in 5

Securitas Technology clients are interested in adopting life cycle management services in the next 18 months¹

A win-win for organisations and their security partners

The availability of cloud-enabled services, such as system health monitoring and remote preventative maintenance, is becoming a powerful advantage for both organisations and their security service providers. These services are supporting earlier detection of system issues from asset deterioration to tampering, and can help prevent them from escalating and impacting business continuity.

For service providers, remote connectivity supports faster triage, more coordinated responses, and better alignment between on-site staff, remote operators, and technical specialists – helping clients maintain a stronger, more consistent security posture.

1. In-house branded survey of Securitas Technology clients in Australia, Belgium, Canada, Denmark, Finland, France, Germany, Ireland, Mexico, Netherlands, Norway, Portugal, Singapore, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States. Data shown is reflective of commercial client responses only. Conducted November 2025.

Technology partner insight

Evolution of remote monitoring: Minimising downtime and enabling proactive maintenance

Remote monitoring is evolving from simple status checks into a powerful tool for minimising downtime and improving system reliability.

A major advancement in this evolution is real-time system health monitoring, which continuously tracks the performance of intrusion panels, sensors, cameras, cell communicators, and network connections.

Cloud-based remote diagnostics, like Resideo's AlarmNet® 360, support this shift by identifying issues such as power loss, communication failures, or device faults that are identified immediately – often before customers notice a problem. It provides secure access to system data and configurations, and allows technicians to troubleshoot and resolve many issues remotely, reducing the need for truck rolls, accelerating response times, and improving the customer experience.

AI-driven maintenance further reduces downtime by analysing performance trends and equipment conditions to anticipate potential system failures.

Instead of reacting to outages, service teams can schedule maintenance proactively, improving uptime and extending equipment life.

resideo

Remote verification and incident management

Improving incident response with faster, clearer verification

Remote alarm and video verification allows security teams to assess incidents quickly and accurately without needing to be present on site. And findings from our client survey show that demand among organisations for these services is high.

Using cloud-connected video and intrusion detection systems, remote operators in alarm monitoring centres can review alerts and live video in real time, determine whether escalation is necessary, and guide responders with the right information. This approach cuts uncertainty, shortens response times, and helps reduce false alarms. Increasingly, local law enforcement services are implementing policies that mean they will not respond to an alarm without visual verification of an active threat.

Over half → **57%**

of our clients currently use or are interested in adopting video-based remote services in the next 18 months¹

Enhancing incident management through centralised oversight

When verification and incident management are handled from a central location – whether an internal security control room or via a third-party monitoring provider, organisations can gain a complete view of activity across all their sites. Alarm operators can compare alerts, spot patterns, prioritise events, and coordinate responses more effectively. This centralised oversight also supports more consistent decision-making, ensuring similar incidents are handled the same way, no matter where they occur or who is responsible for escalation. It's especially valuable for organisations with diverse locations or varying levels of on-site expertise.

1. In-house branded survey of Securitas Technology clients in Australia, Belgium, Canada, Denmark, Finland, France, Germany, Ireland, Mexico, Netherlands, Norway, Portugal, Singapore, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States. Data shown is reflective of commercial client responses only. Conducted November 2025.



Leveraging AI and GenAI to support remote operators

As discussed in **section 3**, AI-powered tools are helping operators to review video, identify relevant activity, and surface the information that matters most during an incident. AI can pull together summaries, highlight key footage, and streamline communication with internal teams or emergency responders.

Looking ahead, agentic AI capabilities will help to further reduce cognitive load, improve accuracy, and give operators the clarity they need to act confidently, especially when they're managing multiple alerts at the same time.



Technology partner insight

Remote services that transform security operations

Unified service platforms, like Aritech's Fusion One, bring greater operational visibility and efficiency to security operations by delivering a comprehensive suite of remote services that go far beyond product management.

Unified digital platforms support every stage of the security life cycle, from installation to maintenance to full incident handling, across intrusion, access control, and video surveillance.

A key component of this ecosystem is remote incident management. Nova, Fusion One's dedicated remote incident management service, centralises all alarms and events from every subsystem into a single, intelligent workflow engine. Whether deployed on premise or in the cloud, this enables operators to remotely monitor, verify, and resolve incidents across single site or multi-site environments. It supports both monitoring-based and plan-driven approaches, ensuring that each incident is handled with consistency, speed, and full operational visibility.

By enabling remote oversight and streamlined workflows, cloud-based digital platforms significantly reduce the need for on-site interventions, accelerate decision making, and ensure that every location, no matter how distributed, benefits from the same level of responsiveness.

The result is faster incident resolution, improved continuity, and a more coordinated and resilient security environment across the physical security ecosystem.



Coordinating remote and onsite responders

Remote verification strengthens on-site response rather than replacing it. By confirming the nature of an alert before dispatching personnel, teams can ensure responders arrive informed and prepared. Remote operators can stay involved throughout the incident, adjusting camera views, sharing updates, and providing new information as situations evolve. This collaboration improves situational awareness, boosts safety, and leads to more effective responses overall. **Our market survey discovered that faster incident response is a top reason driving increased use of remote services, cited by 58%¹ of respondents, and second only to cost savings (61%¹).**

Supporting resiliency across environments

For organisations with multiple sites, varying staffing levels, or operations running beyond standard hours, remote incident management provides a scalable way to maintain consistent protection. It helps ensure high standards across all locations, even when on-site resources are limited. And when underpinned by a robust security management platform integrating multiple data sources, remote verification becomes part of a coordinated, intelligence-driven response model that keeps people, technology, and data aligned in real time.



1. Third-party blind survey of 575 security and loss prevention professionals with decision-making authority for security technology, representing commercial organisations in the APAC region, Europe, and North America. Conducted February 2026.



Technology partner insight

Better insight equals better response

Remote verification tools dramatically accelerate incident resolution and reduce response times by providing immediate, actionable intelligence in distributed environments.

Impact-activated audio and video clips allow operators to verify alarms within seconds, quickly distinguishing real threats from nuisance or false alarms. This rapid triage eliminates delays caused by uncertainty and ensures attention is focused where it is truly needed.

Verified alarms also improve dispatch effectiveness. When law enforcement or emergency responders receive confirmed evidence and contextual details, incidents are prioritised appropriately, leading to faster on-scene arrival and more informed responses. At the same time, real-time remote-control capabilities enable security teams to act immediately, locking or unlocking doors, initiating lockdowns, or adjusting camera views to contain situations before responders arrive.

In multi-location environments, remote verification scales seamlessly. Incidents affecting multiple sites can be managed from a centralised platform, with commands and updates applied instantly across all impacted facilities. After an incident, centralised access to video, event histories, and audit trails significantly shortens investigation cycles, supporting faster root-cause analysis and corrective action.

By reducing false alarms through verified audio, video, and analytics, remote verification tools also free emergency resources for real events, improving overall response times and service-level performance across distributed security operations.



Centralised security system management

Managing systems consistently across every location

Across industries, digital applications have become a primary tool for people to access information and services, simply and quickly from the palm of their hand. This same speed and simplicity benefits security professionals as well. Those responsible for overseeing site safety are searching for security management platforms that allow them to update and administer their systems and locations from anywhere - ideally via a single application that integrates multiple products and brands. This way, tasks like viewing camera feeds, adjusting settings, updating user permissions, or refining access-control policies can all be handled remotely through a mobile device. It's an approach that offers increased visibility, consolidated data, and ensures every site aligns with the organisation's broader security standards.



Security management platforms are a

Top 3

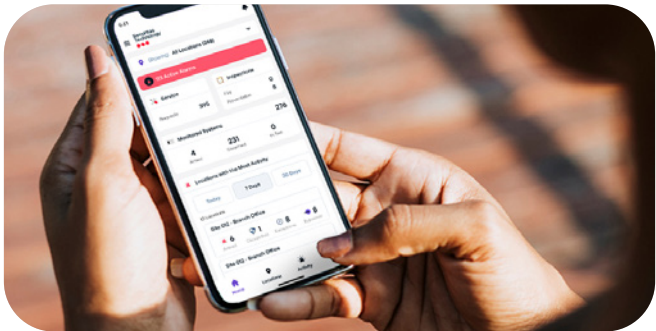
subscription service that organisations are prioritising in the next 12-18 months¹



Improving efficiency through centralised configuration

System updates that once required changes at each location can now be completed centrally in minutes. Teams can fine-tune system settings, roll out feature updates, and apply policy changes across multiple sites quickly and efficiently. This streamlines day-to-day work, reduces operational complexity, and strengthens governance by ensuring every change is consistent and documented.

1. Third-party blind survey of 575 security and loss prevention professionals with decision-making authority for security technology, representing commercial organisations in the APAC region, Europe, and North America. Conducted February 2026.



Technology partner insight

Expanded remote management capabilities are helping reduce cost and complexity

Updating security systems has historically been a slow, labour-intensive process.

Managing security systems in this traditional way often involves the deployment of vehicles, working in areas with unreliable connections, and the risk of customers postponing necessary updates.

These challenges are further exacerbated as the size of the building or campus expands, resulting in increased costs as businesses scale up.

Given the growing number of cybersecurity threats and advancements such as post-quantum cryptography, ensuring both hardware and software updates are delivered consistently and efficiently has now become essential.

Security leaders are seeking to uphold robust security standards while reducing unnecessary time, labour, and downtime. The evolution of remote security services, enabled by cloud-based technology, are making this approach to security management the modern model to follow.

Access control solutions that facilitate bulk updates and include tools to reduce on-site visits and upload durations are preferred. For example, HID Linq provides complimentary tools for updating multiple readers concurrently, including mobile options that operate without internet connectivity.





Supporting growth, expansion, and new site openings

Remote system management makes it far easier for organisations to scale. Whether launching a new facility, activating a temporary location, or adjusting to changing business needs, teams can configure systems remotely and bring sites online quickly. This flexibility is especially valuable for organisations with seasonal operations, distributed retail footprints, or environments that need to expand at pace without lengthy on-site setup.

Unifying the entire security ecosystem

Platforms that support remote system management are the lens through which security professionals can oversee and understand their technology portfolio. It's a unified environment where system settings, health monitoring, video, analytics, and alerts all work together to generate insights and clarity that were previously not accessible without complicated and time-consuming manual data consolidation and analysis. This centralised view helps in reducing fragmentation and improving consistency across sites. It also supports a more coordinated approach, where insights flow seamlessly across systems and strengthen overall operational performance.

Technology partner insight

Eyes everywhere, control everywhere

Managing complex security environments remotely gives teams a practical edge.

With the right technology in place, operators can view video feeds, system events, and device status in a single place and respond faster, instead of jumping between four or five dashboards. A single screen can cover an entire campus or multiple sites across the country, which makes coordination easier without adding staff.

The benefits go beyond centralisation – if a camera goes offline or a network link starts to fail, teams can react in real time to address the problem without sacrificing operational continuity. That frees smaller teams to focus on high priority tasks rather than constant monitoring. Mobile access means staff can step away from the control room and still know exactly what's happening.

There's a trade-off, however: Connecting more devices across more locations expands the attack surface. Remote cameras create possible entry points for hackers, so teams need to treat cybersecurity as a must-have rather than a nice-to-have.

When those safeguards are in place, remote management becomes a strength – teams can scale coverage, stay responsive, and deliver consistent protection across every site without stretching resources thin.



INTELLICENE
SECURITY. EVOLVED.

“

The cloud is transforming security into a smarter, faster, and more connected discipline. AI, remote services, and real-time insights allow clients to protect their people and assets from anywhere, with greater precision and less complexity.”

Lisa Gutierrez

Vice President, Global Advanced Client Services & Sales Engagement
Securitas Technology



Action plan for security professionals

Making the most of cloud-enabled capabilities

01

Establish a clear cloud and connectivity strategy

Future-ready security depends on reliable connectivity and a strong cloud foundation. Working with your peers in IT, review bandwidth, network resilience and security, and data-handling policies to ensure your organisation is prepared for cloud-enabled video, analytics, and configuration. A hybrid approach as a starting point for cloud adoption may be the best path for some organisations.

04

Define clear procedures for remote verification and escalation

Revisit your process for how alarms are monitored and verified. Are you still relying on on-site staff to verify and escalate incidents? Would it be more efficient to leverage a remote service? Clear procedures will help to improve response quality, reduce unnecessary dispatches, and ensure critical information reaches the right people in timely manner.

02

Identify where remote capabilities add the most value

Assess your security programme for coverage gaps, operational pressure points, or resource constraints. Are there any sites with limited staffing, in remote locations, or experiencing recurring technical issues? These often benefit most from remote services such as video alarm verification, maintenance, or system-health oversight.

05

Centralise system configuration and policy management

If you haven't already, consider subscribing to a security management platform to consolidate alarms, monitor activity, and manage systems remotely. Centralisation strengthens governance, reduces errors, and ensures every site operates under the same policies while supporting faster changes during growth or operational change.

03

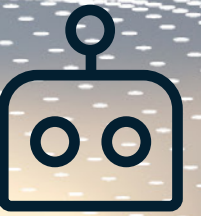
Standardise system health monitoring and maintenance

Explore the use of remote system health monitoring to help track device performance, configuration consistency, and uptime across all locations. AI-supported diagnostics can identify early signs of failure, helping teams resolve issues sooner and maintain a consistent level of protection across sites.

06

Adopt a remote-first approach to monitoring, optimisation, and support

Prioritising remote services offers the advantages of continuous oversight, proactive maintenance, and increased sustainability. While, in many scenarios, you will continue to rely on the reassurance of physical site visits and technical expertise, adopting remote services holds the key to a more efficient, intelligence-led security experience.



05

Drones and robots pushing the security envelope

In this section

- › Drone detection
- › Drones for surveillance
- › Robots in security
- › Action plan for security professionals

Rising interest in autonomous technologies

The new security frontier

Drones and robots are topics that have been circling the security space for several years, but the technology was not a mainstream topic of conversation. That is changing.

Growing availability of commercial-grade drones, combined with the accelerating development of AI-powered robots, means their potential as security tools that extend visibility, automate routine activity, and support organisations operating in complex environments is starting to be realised. **88%¹ of our strategic technology partners expect autonomous technologies to have a moderate or significant impact on security operations in the next 5-10 years, with 8% saying transformational.**

When it comes to drones, there are two specific security technology angles.

The first is **drone detection systems**, used to sense and track drones and unmanned aerial vehicles (UAVs) that could pose a risk to the security, safety, and privacy of a commercial location. Conversely, drones can be leveraged by organisations as a **proactive security tool** to widen surveillance coverage, conduct automated patrols, and assist in incident management.

In the **robotics** space, opportunities already exist to automate some security processes, such as assisting with visitor management and concierge-style tasks. As **quadruped and humanoid robotic applications** become more proven, affordable, and publicly accepted, advances in AI are likely to position them as significant disruptors within the security industry.

Over the coming years, developing autonomous technologies will offer organisations new ways to strengthen situational awareness, improve consistency, and complement human vigilance across challenging sites.



The outlook

- **Drone detection is becoming increasingly essential** as aerial threats become more common and complex for commercial organisations to manage.
- **Drones used for surveillance purposes can offer rapid, flexible visibility** across large or hard-to-reach environments.
- **Robots can help automate routine patrols, environmental checks, and on-site monitoring** to support and empower human guards.
- **Autonomous systems can help ease the pressure on frontline teams** and strengthen operational resilience.
- **Integration with security management platforms** brings drone and robot data — telemetry, video, and alerts — into one view.
- **As technology matures and regulations evolve**, drones and robots are positioned for broader industry adoption.

1. Survey and consultation with 26 strategic technology partners of Securitas Technology, representing leading global security equipment manufacturers, developers, innovators, and technologists. Conducted February 2026.

2. Third-party blind survey of 575 security and loss prevention professionals with decision-making authority for security technology, representing commercial organisations in the APAC region, Europe, and North America. Conducted February 2026.

Drones and robots enter the early adopter phase

Percentage of organisations that plan to adopt drone detection, drone surveillance, or robots in the next 12-18 months²

9.7% Drone detection

9.9% Drones for surveillance

9.9% Robots

Drone detection: Addressing the aerial threat

Why drone detection is becoming essential

Unauthorised drones are creating new challenges for organisations with large perimeters, sensitive operations, or complex environments. The technology itself is becoming more capable and more accessible, introducing new risks ranging from accidental intrusions to deliberate surveillance or criminal intent. These threats can bypass traditional perimeter intrusion defences, making drone detection capabilities an increasingly critical component of modern security strategies.

5.7%

of organisations experienced
a drone-related incident in the
past 12 months¹

**“We had
a break-in
at a facility
where the
perpetrator
used a drone
to scout our
location.”**

Chief Operating Officer and
market survey respondent, US¹

1. Third-party blind survey of 575 security and loss prevention professionals with decision-making authority for security technology, representing commercial organisations in the APAC region, Europe, and North America. Conducted February 2026.



Key concerns driving adoption of drone detection systems

Purchasing an advanced drone has never been easier, making them as accessible to criminals as they are to genuine enthusiasts. Regardless of the intent behind each flight, drone activity poses a threat to commercial organisations in terms of safety, privacy, theft, espionage, and disruption.

With aerial threats so difficult to defend against, there's a growing need for security teams to implement effective drone detection that enables faster, better-informed responses to incidents.

Top 3 reasons organisations are implementing drone detection technology¹

- 01 Improving workplace safety
- 02 Preventing operational disruption
- 03 Preventing theft of intellectual property

Dealing with drone incidents beyond detection

For most organisations, detecting a drone and monitoring its movements is the maximum level of mitigation that can be achieved in the current legal landscape. Laws and regulations in most jurisdictions prevent security teams from taking direct action against a drone threat, such as physical or electronic neutralisation. The primary goal for drone detection must be rapid awareness so that the risk can be mitigated. In some jurisdictions, close coordination with law enforcement may be a path to true drone mitigation, and this is an area that may change rapidly in the short- to medium-term as the drone threat rises.



1. Third-party blind survey of 575 security and loss prevention professionals with decision-making authority for security technology, representing commercial organisations in the APAC region, Europe, and North America. Conducted February 2026.

Technology partner insight

“Advancements in drone detection will be essential to future perimeter security strategies. As drones become more prevalent and increasingly inexpensive, they represent a growing challenge that traditional security measures aren’t designed to address.”

ASSA ABLOY

“Historically, perimeter strategies have focused primarily on ground-based threats. The rapid rise in drone activity over the past five years has expanded that perimeter vertically, requiring security teams to monitor and respond to risks from the air as well. Detecting drones at sufficient distance, with speed and accuracy, remains a challenge. However, ongoing innovation in radar, video analytics, and data integration is improving reliability and response times. We expect this to continue to improve in the future, making them more reliable sources in the total perimeter security strategy.”



“We expect perimeter security to evolve into multiple layers. Ground intrusion (fence, video, access control) is the standard today, but drones can bypass ground controls entirely. Line-of-sight cameras don’t see airspace well, and threats can approach from elevation and behind structures. Airspace monitoring, AI classification, and orchestrated response will see perimeter security become volumetric, not linear. This will fundamentally change detection architecture and move drone detection from niche to standard, particularly in critical infrastructure.”



Understanding the threat in real time

Effective drone detection starts with awareness. Modern solutions use a range of techniques, including radio-frequency monitoring, radar, optical analytics, and acoustic sensors to identify and track third-party drones across different environments. These systems help teams distinguish between hobbyist activity, commercial traffic, and suspicious behaviour. When integrated with centralised security protocols, these alerts can be tracked, prioritised, and supported with context to guide the right response. This is a solution area that will continue to develop rapidly as bad actors also become more sophisticated, using techniques such as remote ID masking or non-standard frequencies to try to evade detection.

Strengthening protection with automation and AI

As the technology continues to evolve, drone detection is becoming more accurate and automated. AI-enabled analytics can help identify flight patterns, classify drone types, and detect actions that may indicate an elevated risk. This increased automation can help reduce false alarms by ensuring security teams receive alerts that are meaningful and actionable. There's also scope to support threat response with internal use of drone technology, as detection systems can be set up to trigger automated visual verification or patrol responses from on-site surveillance drones or robots.



A vital solution to extend perimeter protection

Drone detection technology provides an added layer of protection for organisations looking to strengthen their perimeter defences and safeguard sensitive areas. It supports resilience by giving teams better visibility, clearer intelligence, and more time to react. As aerial activity continues to increase across commercial, industrial, and public settings, integrating drone detection into the wider security ecosystem will be a key step in preparing for the future.

Drone detection plans among our strategic technology partners¹

12%	have an integration/partnership
4%	on the product development roadmap
32%	currently exploring

1. Survey and consultation with 26 strategic technology partners of Securitas Technology, representing leading global security equipment manufacturers, developers, innovators, and technologists. Conducted February 2026.

Technology partner insight

“The expansion of Beyond Visual Line of Sight (BVLOS) operations further pushes perimeter defenses to widen detection zones beyond fence lines, establishing layered, air-aware security grids capable of monitoring long-range drone activity before it reaches critical assets. These innovations are shifting perimeter security from static, ground-focused systems to dynamic, interconnected, and intelligence-driven airspace defense architectures.”



“Drone detection technologies are redefining perimeter security by expanding the perimeter beyond fences and gates to include the airspace. This shift supports a broader evolution in perimeter security from reactive monitoring to proactive, connected operations, where faster detection, better situational awareness, and automated response are key to staying ahead of emerging threats.”



“Drones threats will create the most concern for organisations in the future. Technology is outpacing regulation in terms of what you can fly and where. The ready access to low-cost technology creates a security gap that is difficult to close and defend against.”



“Drone detection will become a useful supplemental layer of perimeter protection. As these technologies improve and integrate more easily with existing video, intrusion, and access control systems, they'll help organisations build more complete situational awareness without changing their core security strategy.”



Drones for surveillance: Protecting from a different perspective

Expanding visibility across complex environments

Drones are set to transform the way organisations monitor large, dispersed, or difficult-to-reach areas. They offer rapid, flexible visibility that complements fixed cameras and on-site guards, enhancing situational awareness by giving security teams a clearer picture of what's happening across their entire environment. Sectors with wide footprints – from logistics and utilities to industrial sites and campus-based operations – are most likely to find drones effective for closing visibility gaps and improving incident response times.



Strengthening incident response and decision-making

Drones as first responder (DFR) programmes are already being piloted successfully by law enforcement and government authorities to support ground personnel with real-time visibility into incidents – from tracking suspects to capturing evidence. This approach is set to gain traction in the commercial market, with organisations deploying drones to help verify an alarm activation, perimeter intrusion, or environmental concern.

Real-time incident monitoring is the top application driving future adoption of drones for surveillance¹, according to our market survey. This not only supports responders with live updates as incidents unfold, but it can lead to quicker on-site decisions, reduce unnecessary dispatches, and better protect personnel.

Top 3 applications driving surveillance drone adoption by organisations in the next 12-18 months¹

Real-time incident monitoring

29%

Security patrols

27%

Alarm verification

23%

A mobile layer of intelligence

Unlike fixed-location systems, drones provide dynamic, mobile, AI-powered coverage. They can move directly to where they're needed, follow predefined patrol routes, or respond to alerts triggered by sensors, analytics, or operator requests. With high-resolution video, analytics, and options like thermal or multispectral imaging, drones allow security teams to verify events, assess risks, and gather situational intelligence quickly and safely. This mobility makes drones a valuable additional layer within a connected security ecosystem.

1. Third-party blind survey of 575 security and loss prevention professionals with decision-making authority for security technology, representing commercial organisations in the APAC region, Europe, and North America. Conducted February 2026.

Technology partner insight

“Drones can be used to supplement perimeter security monitoring for quick and effective visual verification while also eliminating the need to send a person into harm's way.”



“Real-time deployment of drones for video surveillance is a viable alternative to traditional strategies. We feel tethered drones are underutilized and not talked about. Tethered drones can stay aloft indefinitely and require less infrastructure to deploy.”



“Our approach to drone use centres on integrating aerial operations directly into our unified security platform, so drones become a native part of security workflows rather than standalone tools. Through partnerships and integrations, our platform can receive live drone video streams, GPS telemetry, and mission data alongside fixed camera feeds, allowing operators to view, control, and manage drones from the same interface they use for CCTV, access control, and alarms.”



“By providing instant video and audio access to an event location, drones can help to deliver faster response times without putting human resources in dangerous situations.”



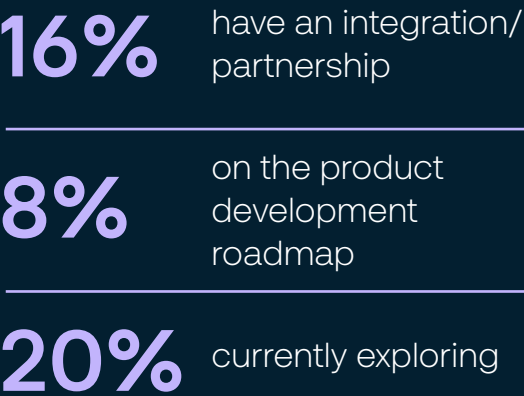
Integrating drones into a connected security ecosystem

Drones become significantly more powerful when integrated into a centralised security platform. By consolidating drone video, telemetry, and alerts alongside data from cameras, access control, and other systems, operators can get a more unified operational picture. This integration also supports automated workflows. For example, triggering a drone to launch when a perimeter sensor activates or when system-health alerts indicate a potential issue.

Unlocking operational efficiency and scalability

As drone technology becomes more accessible, intelligent, and as regulations continue to evolve, organisations are exploring how drones can support not only security, but also operational tasks. On top of supporting with routine security patrols, these include monitoring deliveries, supporting health, safety, and environmental (HSE) checks, and inspecting critical infrastructure – especially in hard-to-reach or hazardous areas. For example, a drone integrated with AI video analytics could help automatically detect corrosion, anomalies, or other vulnerabilities that pose a risk to business continuity. The ability to perform multiple roles helps organisations gain more value from drone investment while reducing the burden on security teams.

Drone surveillance plans among our strategic technology partners¹



1. Survey and consultation with 26 strategic technology partners of Securitas Technology, representing leading global security equipment manufacturers, developers, innovators, and technologists. Conducted February 2026.

Building toward more proactive security operations

Insights from our technology partners and market research indicated that drones used for surveillance are enabling a shift from reactive monitoring to a more proactive, intelligence-driven approach. With improved visibility, faster confirmation, and greater situational certainty, drones are well-positioned to become practical tools for strengthening resilience and supporting more efficient operations across complex environments.



Technology partner insight

“We believe drones will play a massive role in the future of security. Adoption of drones is currently going on at an unprecedented pace, and the security industry will pick this up.”



“There is relatively zero risk to sending a drone into a mission-critical or dangerous scenario. Through drones, we’re able to gather immediate data to facilitate enhanced incident response, monitor locations that humans may not be able to access, and help make potentially life-saving decisions.”



“The ability to rapidly deploy drone surveillance for perimeter protection will enable faster incident response and increased situational awareness. Although not directly developing drone technology, we are capable of integrating video and event information from drone solutions into our platform from for live remote video monitoring.”



“Drones will help provide more situational awareness in scenarios that make it dangerous or geographically impossible to get eyes on. Because of that, we see drones as playing a large part in incident response.”



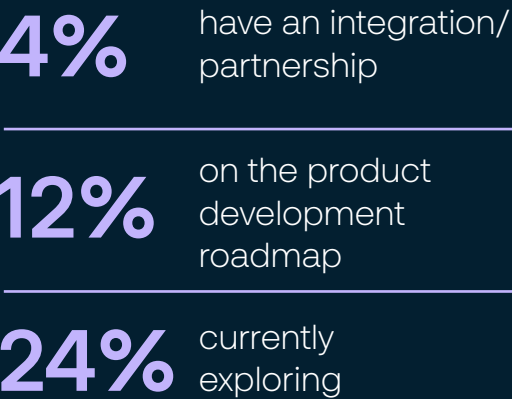
Robots in security: Enhancing human efficiency and expertise

Finding applications to support security operations

Robotics is a hot topic among today’s security professionals and global society as a whole. Year on year, technology innovators around the world are showcasing the latest, AI-powered capabilities of robots – whether in the home, in public places, or in commercial settings such as manufacturing plants and critical infrastructure facilities.

Robots are also finding applications in security, mostly in the shape of wheeled appliances and quadruped robots that can assist with visitor management and automated security patrols. Future interest centres on more sophisticated tasks such as environmental monitoring, high-risk incident response, and providing a more agile and robust on-site presence. While not designed specifically for security purposes, adapting humanoid robots for these security and safety applications shows growing promise.

Robotics plans among our strategic technology partners¹



1. Survey and consultation with 26 strategic technology partners of Securitas Technology, representing leading global security equipment manufacturers, developers, innovators, and technologists. Conducted February 2026.

2. Third-party blind survey of 575 security and loss prevention professionals with decision-making authority for security technology, representing commercial organizations in the APAC region, Europe, and North America. Conducted February 2026.

Top applications driving adoption of ground-based robots by organisations in the next 12-18 months²

Environmental monitoring

38%

High-risk incident response
(handling hazardous material,
search and rescue, etc.)

33%

Security patrols (e.g.
perimeter security)

32%

General incident response

28%

Visitor management

22%



Technology partner insight



Supporting frontline teams in challenging environments

Many organisations operate in complex or high-risk environments where continuous monitoring is essential but physically demanding. Robots are well suited to these tasks as they can patrol large indoor spaces, guard entry points, move through parking structures, or monitor outdoor areas without fatigue. Using on-board cameras and a variety of other sensors, they can detect movement, temperature changes, spills, or other anomalies that may need attention – helping human security teams stay informed while limiting staff exposure to the most hazardous areas of a site.

“We see robotics transforming security from a labour-dependent model to an automation-first architecture. Beyond traditional guarding, robots enable persistent, high-frequency patrolling and environmental sensing (such as hazardous gas or thermal detection) in areas that are unsafe or inefficient for humans to monitor.”

AJAX

“Robots are likely to complement traditional security operations by supporting routine coverage, providing additional visibility during incidents, and enabling safer initial assessments before personnel are deployed. Over time, they may help organisations maintain more consistent monitoring across sites and improve response coordination by contributing timely, on-site information to existing security workflows.”

brivo
simply better security

“Robots will transform physical security operations by automating patrols and monitoring, improving efficiency, freeing personnel for higher-value tasks, and enhancing safety for human workers. They also enable real-time analytics and remote surveillance, expanding the effectiveness and impact of security solutions across the industry.”

MARCH
networks
A Delta Group Company

“As the cost of robotics continues to lower, the demand for this technology will increase – with potential to replace some traditional guarding services with autonomous capability.”

radionix

Video capability and autonomous operation are important features

Video capability, autonomous operation, and the ability to operate in all weather conditions are considered the most important factors for organisations implementing ground-based robots. Other key features include mobility, battery longevity, and audio capability; each fundamental to ensuring reliability and performance that builds trust in the technology so that more organisations have the confidence to invest.

44%

of organisations ranked video capability as the most important robotic technology feature¹



Improving operational efficiency and response

Tangible value will be found by using robots to handle repetitive tasks that require attention but not constant human judgment. Completing scheduled patrols, monitoring environmental conditions, and sending alerts directly to operators will allow security personnel to focus on higher-value work and strengthen overall service levels. Robots can also be dispatched to verify alarms or investigate disturbances, giving teams quick visibility with minimal disruption.

An increasingly realistic option for security professionals

Robots are steadily progressing toward broader adoption, but widescale deployment in security settings will hinge on several factors: cultural acceptance, declining costs, proven reliability, operational readiness, and clear use cases with a defined return on investment. In the near term, robots have potential to supplement human security teams, offloading routine tasks and enhancing how risks are detected, analysed, and managed.

Sectors such as logistics, manufacturing, healthcare, and large-site operations are among the most likely to see robots become a standard component of the security ecosystem. Quadruped and humanoid robots in particular, are poised to be one of the industry’s most significant disruptors as their capabilities continue to evolve. Ultimately, widescale adoption will depend on reliable performance, high-quality data, and measurable operational impact.

1. Third-party blind survey of 575 security and loss prevention professionals with decision-making authority for security technology, representing commercial organisations in the APAC region, Europe, and North America. Conducted February 2026.



Technology partner insight

“We see robots becoming hybrid security devices that combine traditional guarding functions, visitor management, concierge, and maintenance services with advanced sensing capabilities for enhanced visibility and regulatory compliance purposes.”



“Robots will act as force multipliers, handling repetitive patrols and sensor-based monitoring so human officers can focus on decision-making. As capabilities grow – better navigation, integrated analytics, mobile communication – they’ll extend the reach of security operations beyond what traditional guard functions can cover.”



“We believe the main use of robots in future security programmes will be as an enhancement of traditional guarding services.”



“We are in the early innings of robots being used to support human guard operations, and this will continue to develop for the next few years. While progress is being made, we are still some years away from having robots perform autonomous actions safely within an enterprise environment.”



“

Although autonomous technologies are still emerging, drones and robots are gaining traction as valuable additions to modern security programmes. Rather than replacing people, these tools amplify what security teams can see, understand, and act upon – helping clients improve situational awareness, strengthen response, and advance our shared mission of making the world a safer place.

Doug Walsh
Vice President, Global Technology Strategy
Securitas Technology

”



Action plan for security professionals

Assessing applications for autonomous technology

01

Start with a clear problem statement

Before exploring any autonomous system, identify the specific operational challenges you need to address – whether they involve perimeter blind spots, large-site coverage gaps, repetitive patrol requirements, or safety concerns for frontline teams. A clear problem statement helps determine where drones or robots can offer meaningful value.

02

Map use cases to your environment

Choose technologies based on practical applications, not novelty. Drones are well suited for large outdoor areas, flexible patrol routes, and rapid incident verification, while robots support persistent indoor or outdoor monitoring, environmental sensing, and routine patrols that demand consistency. Matching capabilities to context is key to success.

03

Build integration into your decision-making

Connectivity is an important factor when evaluating new security technologies. Make sure any drone or robot solution can integrate with your existing security ecosystem, so alerts, telemetry, and video feeds are managed alongside other systems. Integration enhances efficiency and reduces operational silos.

04

Consider regulatory, site, and safety requirements

Drone operations require careful attention to local airspace rules, flight restrictions, and compliance obligations. Robots may need defined pathways, safety planning, and staff awareness. Addressing regulatory and site-specific requirements early will streamline deployment and reduce risk.

05

Pilot with purpose, then scale based on evidence

Focused pilots help validate performance, build internal confidence, and uncover practical considerations before wider rollout. Track measurable outcomes – response times, patrol consistency, workload reduction, or improved situational awareness. Scale when the technology shows consistent, repeatable value.

06

Prepare your team for human-technology collaboration

The success of drones and robots depends on how well they support the people who use them. Provide training that covers workflows, incident response, system hand-offs, and the role of automation. Helping teams understand how these technologies extend their capabilities encourages adoption and maximises impact.





06

Safeguarding the physical security ecosystem

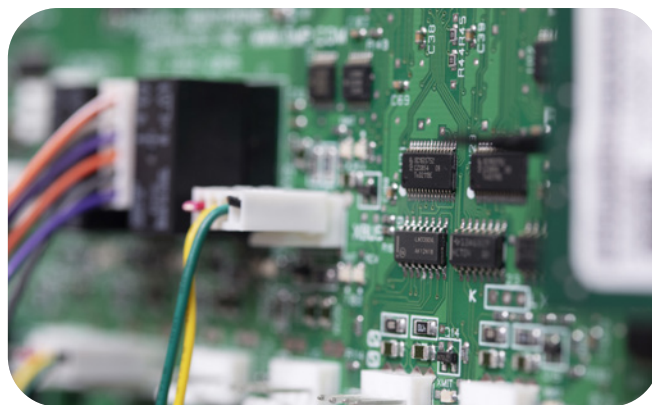
In this section

- › Security data best practices
- › Data trustworthiness
- › Quantum-resistant security systems
- › Action plan for security professionals

Resilient infrastructure for physical security programmes

As physical security systems become increasingly connected and intelligent, protecting the infrastructure behind them has become a critical priority to help maintain peak performance and protect against future cybersecurity threats.

Organisations are no longer focusing solely on the functionality of security solutions. The data security, trustworthiness, and resiliency of the underlying devices, software, and network technologies are now just as important considerations in technology selection. Strong data governance, consistent cyber hygiene, and cyber-resilient security technologies are now essential for maintaining confidence in a digital environment that is evolving quickly, including the arrival of quantum computing in the near future.



Top 3 current
cyber-physical practices
currently undertaken by
organisations¹

77%

Password management

73%

Cybersecurity
awareness/training

68%

Regular firmware updates

The outlook

- › **Networks that host physical security systems require robust protection** as part of an organisation's wider cybersecurity strategy.
- › **Cyber hygiene, access governance, and responsible AI use** are now fundamental elements of a modern security programme.
- › **Emerging risks like AI-generated video and deepfake deception** are causing organisations to adapt how they verify, validate, and trust security data.
- › **Quantum readiness** is emerging as an important future priority as "harvest now, decrypt later" threats gain traction.
- › **Safeguarding the ecosystem will be key** to enabling secure AI adoption, automation, and future-ready security at scale.

1. Third-party blind survey of 575 security and loss prevention professionals with decision-making authority for security technology, representing commercial organisations in the APAC region, Europe, and North America. Conducted February 2026.

Security data best practices

Putting strong data governance at the centre of modern security

As physical security becomes more digital and interconnected, data has quickly become one of the most valuable and vulnerable assets. Organisations rely on video, access logs, device status, and system telemetry to make informed decisions, but that data must be accurate, well-managed, and protected. Strong governance ensures information stays secure, available, and meaningful. This includes defining access rights, setting clear retention policies, and ensuring sensitive data is handled responsibly across every site and system.



Strengthening cyber hygiene across security devices and platforms

Cyber hygiene is now a baseline requirement for maintaining safe and reliable physical security operations. **Consistent password management standards (77%)¹, cybersecurity awareness training (73%)¹, and regular firmware updates (68%)¹ are well-established best practices among the organisations we surveyed, while future investments centre on third-party testing (29%)¹, network segmentation (25%)¹, and incident response plans (18%)¹ to further enhance digital resilience.**

Together, these controls help minimise exposure to unauthorised access or compromise attempts. Even a single misconfigured device can introduce unnecessary risk. Embedding standardised hygiene practices across every part of the physical security environment creates a more resilient foundation for AI, automation, and remote operations to run safely.

¹ Third-party blind survey of 575 security and loss prevention professionals with decision-making authority for security technology, representing commercial organisations in the APAC region, Europe, and North America. Conducted February 2026.





Creating consistency across devices and sites

Organisations are responding to cyber-physical threats by driving consistency in how security devices are deployed across multiple locations. Standardised configuration templates, centralised update schedules, and unified permission structures help keep systems secure, aligned, and functioning smoothly. This reduces operational risk, simplifies maintenance, and ensures organisations can trust the data coming from any site. By removing variation, organisations create a more predictable and manageable environment, which is especially important when adopting cloud, remote services, and AI-enhanced capabilities.

92%

of organisations are extremely or moderately concerned about security device hacking¹

1. Third-party blind survey of 575 security and loss prevention professionals with decision-making authority for security technology, representing commercial organisations in the APAC region, Europe, and North America. Conducted February 2026.

Ensuring integrity in digital physical security programmes

As physical security systems become more digital, interconnected, and cloud-managed, ensuring the integrity of security data requires a disciplined and proactive approach.

Video, system logs, and access data are only as trustworthy as the practices used to protect them. One of the most significant risks to data integrity today is not technology failure, but human error – ranging from weak passwords to delayed software updates and improper system access.

Strong identity and access management is foundational. Organisations should enforce unique user accounts, role-based access controls, and multi-factor authentication to reduce unauthorised access and improve accountability. Centralised user management and audit logging further strengthen oversight by providing clear visibility into who accessed data and when.

Equally critical is maintaining system hygiene. Keeping recorder software, operating systems, firmware, and client applications up to date ensures known vulnerabilities are patched before they can be exploited. Avoiding the use of removable media, securing hardware in access-controlled locations, and isolating camera networks also help prevent data tampering and loss.

Finally, cloud-managed platforms play an important role by enabling secure remote access, standardised configurations, and consistent enforcement of security policies across all locations. By combining strong governance, secure system design, and ongoing maintenance, organisations can preserve the integrity of their physical security data and maintain long-term trust in their security programmes.

Building clear ownership and accountability for data

Effective data governance depends on clearly defined roles and responsibilities. Security leaders are working increasingly closely with peers in IT and operations to define who owns which datasets, who manages access, and who is accountable for enforcing policies. Without this clarity, gaps can form, leading to oversight failures or poorly managed information. Establishing ownership early is helping organisations maintain visibility across their environments, strengthen collaboration, and respond more effectively to incidents involving sensitive or high-value data.



Supporting AI and automation with cleaner data

AI-powered systems perform best when the data feeding them is structured, consistent, and accurate. Clean, well-maintained security data can improve analytics, enhance automation, and make overall capabilities more reliable. By contrast, poor-quality data can lead to false positives, misclassifications, and unnecessary additional workload. Organisations are moving to strengthen data quality now for more advanced AI adoption later, creating a smoother path for scaling and improving overall security system performance.



Aligning data practices with privacy and compliance

As privacy expectations and cybersecurity regulations increase in complexity, security leaders are moving to ensure that data collection, retention, access, and disposal practices align with internal policies, industry guidelines, and legal requirements. Upholding clear documentation and transparent processes will help to build trust with employees, clients, and partners while embedding privacy considerations into everyday workflows. This ultimately helps reduce compliance risk, strengthens operational integrity, and reinforces confidence in how data is managed.

Technology partner insight

Data integrity requires effective cybersecurity practices

At the heart of physical security is the concept of data integrity; has the video evidence been handled to create a trusted chain of custody or is the identity being verified as genuine before providing access?

As digital processes have replaced analog in security, so has the concept of managing data integrity. The focus has to be on having processes in place to ensure cybersecurity on both the data flowing through a physical security system and for the identity of the participants (both human and non-human).

Almost all organisations have information security policies in place to protect data, but they are not always used outside of IT. Start with implementing your InfoSec policy across all physical security systems, such as with password rotation policies and keeping firmware up to date.

Couple this with identity management for non-humans, such as all camera devices and access control systems, by using certificates on all devices to ensure they are who they say they are.

Using an automated platform such as Viakoo not only makes it easy to manage these functions across large fleets of devices, but it also provides the historical data needed to meet compliance and audit requirements.

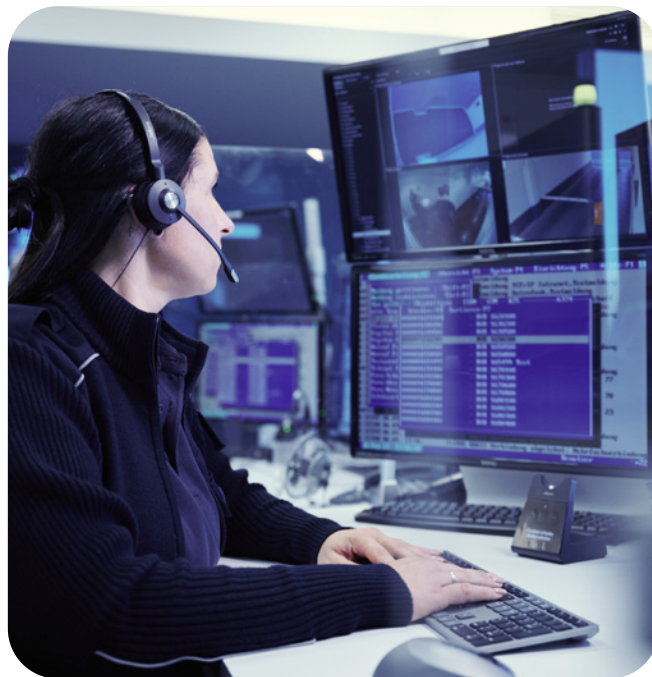


Data trustworthiness

Addressing emerging risks: Deepfakes and manipulated content

AI-generated video and synthetic media introduce challenges that traditional electronic security processes were never designed to handle. Deepfakes – where images or video footage are manipulated by AI to create false content – can obscure events and undermine confidence in visual evidence, or be used to try to deceive facial-recognition systems.

As these tools become more widely accessible, organisations must assume the threat will grow. **Our market survey reveals acute awareness of the vulnerability of existing security equipment to cyberattacks and other risks (91%)**. Upgrading device firmware and ensuring authenticity safeguards, such as digital watermarking, are in place can help security teams stay ahead of manipulated video content. It's about gaining peace of mind that the evidence they rely on remains credible, even in complex situations.



91%

of organisations are concerned about dated equipment causing vulnerability¹

1. Third-party blind survey of 575 security and loss prevention professionals with decision-making authority for security technology, representing commercial organisations in the APAC region, Europe, and North America. Conducted February 2026.

Technology partner insight

Ensuring trustworthiness in security data: The role of technology leaders like Axis

In an era of AI, deepfakes, and synthetic content, ensuring the trustworthiness of security data is paramount.

As a leader in the security industry, Axis Communications is committed to providing solutions that protect data integrity against evolving threats.

We integrate advanced encryption, authentication protocols, and built-in cybersecurity features such as signed video, secure boot, and trusted firmware to ensure the authenticity of surveillance footage and prevent unauthorised alterations. These cryptographic techniques and hardware-based protections keep data tamper-proof, preserving evidentiary integrity throughout its life cycle.

Employing AI-driven analytics to detect subtle inconsistencies in media that may indicate manipulation, like deepfakes. AI algorithms continuously evolve to stay ahead of emerging threats, ensuring the reliability of security solutions.

To adhere to stringent industry standards and best practices, you should conduct regular audits and collaborate with cybersecurity experts to fortify defence strategies. This proactive, multilayer approach – combining encryption, AI-based analytics, hardware protections, and industry standards – ensures that solutions remain resilient against increasingly sophisticated risks.



Verifying authenticity at the point of capture

Trusted data begins with trusted devices. Cameras and sensors that use up-to-date firmware, encrypted feeds, and other built-in security features provide stronger protection against hacking or manipulation. Ensuring that devices are legitimate and uncompromised at installation creates a more reliable foundation for AI analytics, operator assessments, and downstream workflows. This source-level verification is becoming increasingly important as systems grow more intelligent and interconnected.



Top cyber resilience actions for our technology partners¹

Percentage of partners ranking as a top three priority:

96%

Strengthening system architecture

92%

Increasing device-level security

80%

Identity and access management

¹ Survey and consultation with 26 strategic technology partners of Securitas Technology, representing leading global security equipment manufacturers, developers, innovators, and technologists. Conducted February 2026.

Technology partner insight

Build a foundation of strong cyber controls

Security leaders can't promise perfect truth in an AI era – but they can strive to make security data authentic, untampered, and attributable.

Start with foundational cyber controls: Strong authentication to prove who/what is connecting, authorisation to limit what they can do, and encryption in transit and at rest with disciplined key management.

Next is integrity and provenance for evidence. Tamper evidence at capture uses cryptographic digital signatures embedded in recordings and validated on export. On the other hand, watermarking binds the user, workstation, and camera context to each frame to deter unauthorised sharing.

Finally, leaders need an auditable chain of custody. Immutable audit trails and user activity reporting that show who accessed data, when, and what changed. Any unauthorised alteration would be flagged by integrity checks – no matter how convincing the resulting deepfake or synthetic content may appear.



Protecting video and evidence with secure workflows

Evidence must be managed carefully to remain trustworthy. **The first essential step – prioritised by security professionals (77%¹) and manufacturers (80%²) according to our surveys – is properly managing access to information.** Beyond that, encrypted storage, tamper-evident logs, watermarked footage, and documented chain-of-custody procedures can help preserve the integrity of recorded data. These workflows ensure that video and logs can be trusted during audits, investigations, or legal processes. Clear, repeatable handling standards reduce ambiguity, reinforce accountability, and support consistency across sites and teams.

Using trusted-source integrations to validate intelligence

Many organisations supplement their own system data with third-party intelligence, from situation reports to environmental sensors. Verifying the origin and reliability of these sources helps ensure external insights do not distort decision-making. Working only with vetted, trusted providers reduces the risk of misinformation or corrupted data influencing operations. Trust-layer integrations are becoming a hallmark of mature, intelligence-driven security programmes.

Building awareness around deceptive media

Even with advanced safeguards, human judgment remains essential. **Cybersecurity awareness is the number two best practice to counter cyber-physical risks, cited by 73%¹ of security leaders in our market survey.** Training teams to spot signs of manipulation, question suspicious footage, and escalate anomalies strengthens an organisation’s ability to detect deceptive media early. Awareness training reduces the chance of misinterpretation, supports more accurate incident response, and builds operator confidence. This human layer reinforces a broader culture of vigilance and trust across the security ecosystem.



1. Third-party blind survey of 575 security and loss prevention professionals with decision-making authority for security technology, representing commercial organisations in the APAC region, Europe, and North America. Conducted February 2026.

2. Survey and consultation with 26 strategic technology partners of Securitas Technology, representing leading global security equipment manufacturers, developers, innovators, and technologists. Conducted February 2026.

Data and cybersecurity for a reliable video system

As video systems become more connected and intelligence moves closer to the edge, trust must be designed in from the start. Technology providers need to take a secure-by-design approach across hardware, software, and integrations. That means protecting data at every stage – from capture to analysis to delivery. The approach must safeguard data and manage user access to uphold the most stringent reliability benchmarks.

A truly secure architecture considers every component of the video security ecosystem: cameras, storage devices, network communication, Public Key Infrastructure (PKI), and video management software. Independent certifications, such as to the UL 2900 Series of Standards, help validate that a provider’s security measures are up to date.

Equally important is working closely with customers to ensure systems fit into their broader security and IT strategies. When organisations rely on video to make critical decisions, security and reliability must be non-negotiable.

Quantum-resistant security systems

Preparing for future cryptographic risks

Quantum computing is still a developing area of information technology, but organisations must prepare now for the highly disruptive impact it may have on current data encryption practices. Although not yet dominating the cyber-physical discussion, it is on the radar for both security professionals and technology providers. **In our market survey, 27%¹ of organisations ranked it as a top cyber-physical concern, while quantum-resistance is a top five development priority for our technology partners².**

The most immediate threat is a “harvest now, decrypt later” approach, where cyber criminals capture encrypted archives today in hopes of decoding them once quantum tools are mature.

For organisations that store long-retention video, identity records, or access logs, preparing early will help to reduce long-term risk and avoid disruptive retrofits when cryptographic standards evolve.

27%

of organisations are extremely concerned about quantum threats to electronic security system encryption¹



Understanding the Y2Q timeline and why it matters

Y2Q (years to quantum) – the point at which quantum computers may be capable of breaking widely used encryption – is becoming a planning milestone for security leaders. While the exact timing is uncertain, the direction is clear: Long-life encrypted data stored today may become vulnerable in the coming years. Organisations with extended retention periods must assume that their archives could eventually be at risk. Treating Y2Q as a strategic horizon will help to guide encryption priorities and vendor discussions.

Identifying long-life data that is most at risk

Not every dataset needs quantum-safe protection immediately. The priority is long-retention data such as video archives and access control credentials, as these records remain sensitive for years. Mapping where this information resides and how it is currently encrypted helps organisations understand their exposure and identify which systems require earlier upgrades. This clarity reduces the chance of overlooking high-risk datasets and supports more targeted transition planning.

1. Third-party blind survey of 575 security and loss prevention professionals with decision-making authority for security technology, representing commercial organisations in the APAC region, Europe, and North America. Conducted February 2026.

2. Survey and consultation with 26 strategic technology partners of Securitas Technology, representing leading global security equipment manufacturers, developers, innovators, and technologists. Conducted February 2026.

Technology partner insight

Preparation is key as quantum technologies advance

Implementing robust controls is essential to safeguard encrypted data sources, ensuring they cannot be copied and decrypted later as quantum technologies advance.

Organisations must take proactive steps to prepare for quantum-resistant security systems and future-proof their encryption strategies.

The first step involves understanding areas of vulnerability by conducting a thorough assessment and creating a comprehensive inventory of applications, databases, and services utilising public-key encryption cryptography. This inventory should also include third-party products integrated into the overall solution, as these represent potential entry points for future quantum capabilities.

Once a complete inventory has been developed, organisations should establish migration plans to transition to NIST-approved post-quantum cryptography (PQC), which are algorithms specifically designed to be resistant to quantum attacks.

Moreover, adopting Crypto-Agile design techniques is crucial, enabling organisations to swiftly change encryption algorithms without necessitating core engineering modifications. This flexibility allows for a more agile and adaptive security posture in the face of evolving threats.

As a leader in advancing quantum technologies, Honeywell’s ownership of Quantinuum developed Quantum Origin which delivers quantum-hardened cryptographic keys. This positions the company at the forefront of developing innovative solutions to address these challenges, further enhancing the security landscape for enterprises as they navigate the transition to quantum resistance.

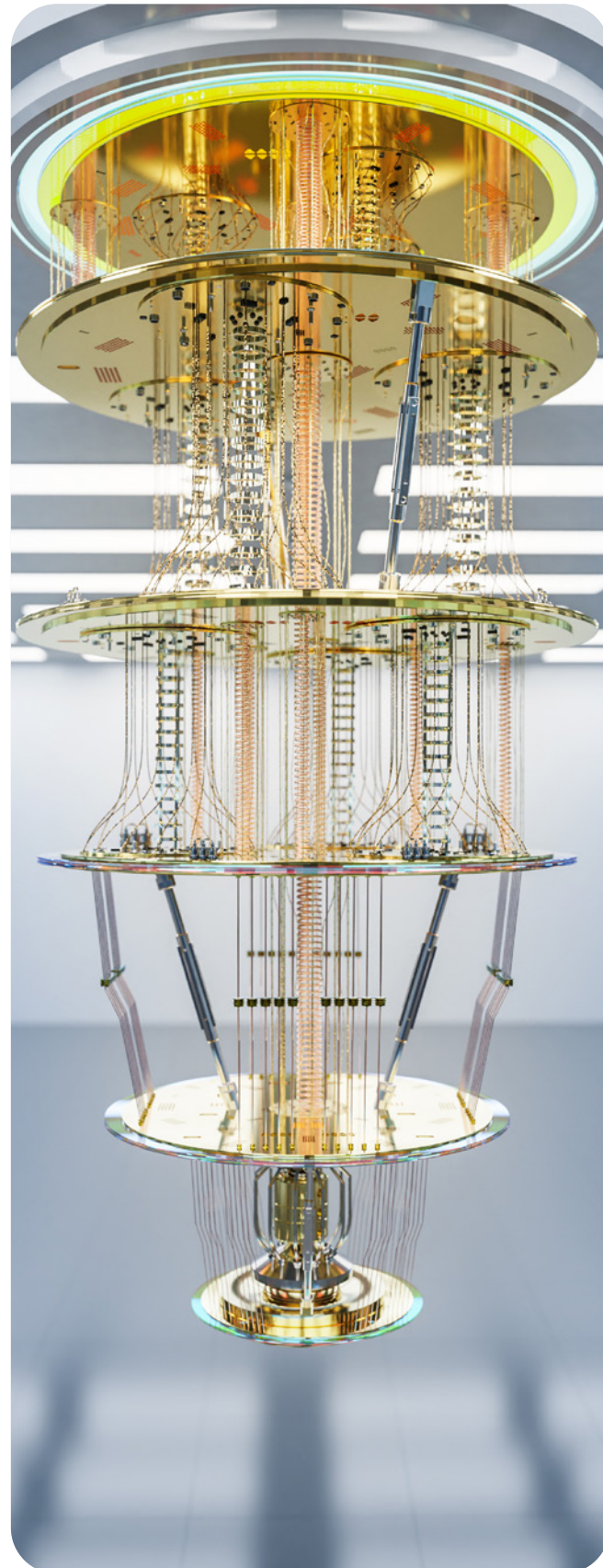
Assessing quantum readiness across your ecosystem

The gradual shift to quantum computing will affect every stakeholder in the security technology supply chain, from end-users to the vendors whose technologies and services they rely on. While these providers will move toward quantum-safe cryptographic standards on different timelines, feedback from our strategic technology partners shows awareness levels are high. Many partners are already outlining their own roadmaps, knowing that early planning will help reassure end-users, prevent coverage gaps, and ensure readiness to adapt as the quantum transition accelerates.

Quantum-resistance is a

Top 5

development priority for our technology partners¹



Embedding quantum considerations into life cycle planning

Integrating quantum-safe encryption into ongoing technology update cycles will help make the transition more manageable. As devices reach end of life or systems undergo significant upgrades, organisations can work with their security providers to introduce quantum-resilient replacements without the risk of major disruption. This staged approach spreads investment over time and ensures organisations remain protected as cryptographic standards evolve.

Staying ahead of emerging standards and compliance

Regulators and standards bodies, such as the National Institute of Standards and Technology (NIST²), are actively sharing guidance around quantum-safe encryption. Monitoring these developments can help organisations anticipate future requirements and avoid reactive, last-minute changes. Early adoption of best-practice frameworks demonstrates proactive governance and strengthens ecosystem resilience. Staying ahead of evolving standards ensures security programmes remain prepared as Y2Q approaches and encryption expectations shift industry-wide.

1. Survey and consultation with 26 strategic technology partners of Securitas Technology, representing leading global security equipment manufacturers, developers, innovators, and technologists. Conducted February 2026.

2. NIST. Post-quantum cryptography. nist.gov/pqc

Technology partner insight

Futureproofing digital trust through integrated infrastructures

Quantum-resistant security is the next bastion of digital trust.

It's the logical presumption that the methods and standards we use to protect digital data today won't withstand or guard against the super-powered technology of tomorrow.

One of the biggest reasons for this perception is the expectation of a definitive break away from today's standard encryption norms. Futureproofing requires transitioning from rigid security silos to a modular, integrated ecosystem built for cryptographic agility.

Motorola Solutions addresses this shift by unifying once-disparate technologies into a cohesive safety and security framework. Our expertise in mission-critical communications and AI-powered video security allows us to deploy software-defined architectures that can be updated as National Institute of Standards and Technology (NIST) standards evolve, avoiding infrastructure obsolescence.

Our strength lies in assisted response: An ecosystem where applied AI analyses vast data streams to provide human operators with actionable intelligence. By integrating video analytics, access control, and command centre software, we move beyond passive encryption to active, intelligent defence.

This convergence ensures that as cryptographic threats advance, our customers maintain a resilient posture through automated workflows and real-time anomaly detection.

Ultimately, Motorola Solutions provides a future-ready foundation where secure, authenticated connectivity and intelligent response capabilities ensure operational continuity in an evolving threat landscape.

“

Physical security and cyber security are now inseparable. In a modern, connected ecosystem, network protection isn't just a technical consideration – it's the foundation everything else relies on. That's why good cyber hygiene is no longer optional; it's the essential discipline that keeps today's security platforms resilient and trustworthy.

”

Mike Beattie

CIO & Senior Vice President, Global Information Technology
Securitas Technology



Action for security professionals

Creating a cyber-secure physical security ecosystem

01 **Treat security data as a critical asset**
Review how video, access control logs, and device information are collected, stored, and accessed across your organisation. Establish clear ownership and consistent retention practices so every decision is supported by reliable, well-managed data.

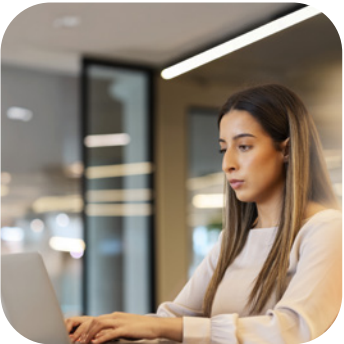
02 **Standardise cyber hygiene everywhere**
Apply consistent cyber hygiene practices across all sites and devices. Enforce regular training, strict authentication, network segmentation, and controlled permissions. Standardisation reduces vulnerabilities, improves resilience, and ensures the wider security ecosystem remains dependable as it scales and becomes more connected.

03 **Build processes that verify authenticity**
As manipulated content becomes more common, implement technology and practices that assess authenticity at the point of capture and at later stages as information is stored or actioned. Use encrypted feeds, secure exports, and documented chain-of-custody procedures to maintain confidence in video, logs, and system outputs.

04 **Identify long-life data vulnerable to quantum threats**
Locate archives and access logs stored for extended periods and evaluate how they are encrypted and stored. Understand which systems hold long-retention data and prioritise them for quantum-safe planning. Early assessment helps organisations avoid disruptive, high-pressure transitions later.

05 **Align with vendors who are preparing for quantum-safe encryption**
Engage vendors to understand their quantum-safe roadmaps and encryption timelines. Select partners with clear strategies and commitments to emerging standards. This ensures your ecosystem evolves consistently and avoids fragmentation as quantum-resilient technologies become industry expectations.

06 **Build adaptive governance that evolves with risk**
Regularly review policies governing data handling, AI use, system access control, and evidence protection. Make sure teams understand responsibilities and have clear escalation paths. Adaptive governance keeps the technology stack aligned with best practice and reduces the likelihood of new vulnerabilities going unnoticed.



07

Contributor spotlights

In this section

- › Technology partner spotlights
- › Securitas spotlights

Technology partner spotlights



3xLOGIC

3xLOGIC™ is a leading innovator and provider of security hardware, software, and cloud-based solutions that drive business intelligence, for customers around the globe. 3xLOGIC's solutions go beyond security to deliver transformational business value, by mining data and converting it into actionable insights – for greater visibility and fresh perspective on problems businesses didn't even know they had.



Manage your video smarter with 3xLOGIC VIGIL 13

VIGIL 13 by 3xLOGIC is the latest software and camera release for its Video Management solution, adding powerful edge-based deep learning analytics to enhance response times, situational awareness, and investigations.

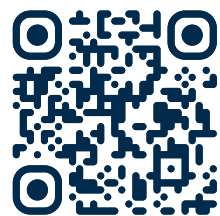
Key features include Automatic Number Plate Recognition (ANPR), Anti-Loitering and Perimeter Protection, Remote Analytics Configuration Support, and expanded Edge-Based Deep Learning capabilities.

ANPR captures licence plates from up to 60 feet away at speeds of 75 mph (120 km/h) while recognising vehicle make, model, and colour, making it ideal for security, access control, parking management, and retail automation.

Anti-Loitering and Perimeter Protection detect unauthorised behaviours like loitering, intrusion, or illegal dumping, delivering real-time alerts for quick action. This solution strengthens security and loss prevention efforts for convenience stores, schools, retailers, warehouses, and distribution centres.

VIGIL 13 offers real-time alerts, customisable alarm management, and advanced object, people, and vehicle tracking at the Edge, reducing storage and bandwidth needs. Its flexible zone and directional interaction setup enhance identification and notifications, improving operator efficiency.

Its exceptional features make it the perfect choice for business and organisational security, offering valuable security insights wrapped in a product designed to be flexible, intuitive, and cost-efficient.



Learn more

AJAX

Ajax Systems is an international tech company and the largest manufacturer of security systems in Europe, with over 4.5 million end users and 330K PRO users in more than 180 countries worldwide. The company offers end-to-end solutions for protecting homes and businesses of any scale. To date the Ajax product portfolio includes 280 devices for intrusion protection, video surveillance, fire and life safety, and comfort and automation.



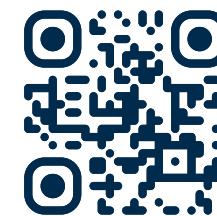
Ajax security ecosystem for any project

Ajax Systems delivers a comprehensive, all-in-one security system designed to protect residential, commercial, and high-risk facilities from break-ins, fire, and other threats. By combining intrusion protection, video surveillance, fire and life safety, and comfort and automation, the system can be tailored to specific needs and managed through a single interface.

For intrusion protection, Ajax offers wireless **Baseline** solutions certified to EN 50131 Grade 2, suitable for a wide range of projects. **Superior** intrusion devices for high-risk facilities are offered in wired and wireless options, providing enhanced sabotage resistance and meeting EN 50131 **Grade 3** requirements. Ajax Systems introduced the **world's first Grade 3 wireless intrusion solution**, designed for fast installation, reducing wiring complexity, and lowering labour costs for projects.

In fire and life safety, Ajax sets a new benchmark with its **fully wireless EN54-certified fire detection system** for commercial and municipal sites. The EN54 Line enables reliable fire protection without complex cabling, while the **EN54 Fire Hub Jeweller** ensures centralised control and remote management. Hub also supports EN 50131 Grade 2 intrusion protection, video surveillance, and automation devices, making it a unified solution. The EN54 Line offers a mobile app interface for an intuitive user experience, easier facility management, and efficient remote service.

Video surveillance solutions, available in **Baseline** and **Superior** product lines, offer scalable options with AI-powered features. Devices deliver instant streams and photos for rapid verification, while integration with the Ajax ecosystem enables automation scenarios. Video solutions provide synchronised apps, instant notifications, and secure cloud-based monitoring with strong privacy protections.

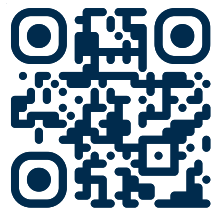
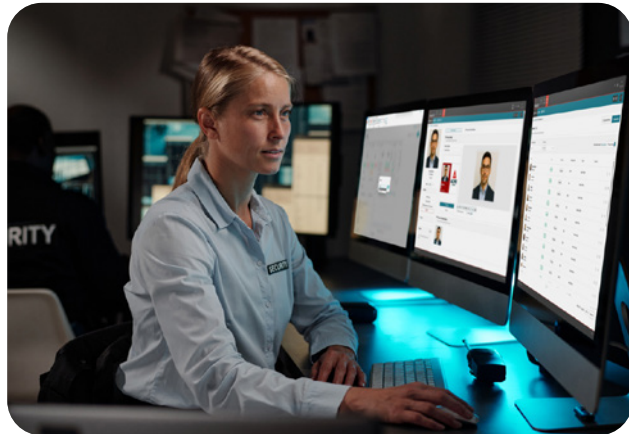


Learn more



At AMAG Technology, we put identity first, protecting your most important asset: people. As a global security solutions manufacturer, we deliver the reliable and scalable Symmetry Solution Suite, providing a comprehensive security system that meets you where you are in your security programme.

With a customer-first mindset, we take an outside-in approach to solve today's challenges while anticipating tomorrow's – building resiliency into our products and operations and delivering solutions that are easy to use, efficient, and effective. We act as a transparent, accessible partner, communicating proactively, staying focused on what we do best, and inviting customers to come on the journey with us. Finally, by building our own products and controlling our supply chain, we remain agile, nimble, and reliable so you get the responsiveness you need and can plan with confidence for tomorrow.



Learn more

AMAG Technology announces Symmetry CONNECT 2.0 identity management

Manage identities across multiple access systems and automate manual processes to streamline business operations.

AMAG Technology™ has announced the release of **Symmetry CONNECT 2.0**, a physical identity and access management solution built for enterprises operating across multiple, mixed access control systems.

Today's organisations rarely run a single access platform. Mergers, acquisitions, global expansion, and decentralised operations often create a patchwork of systems that can be difficult to manage, increase risk, and slow response.

To address this reality, AMAG Technology partnered with **SwiftConnect**, provider of the connected access network for places and spaces, to deliver a dynamic approach to identity management across disparate physical access control environments.

Symmetry CONNECT 2.0 helps customers unify a single identity across multiple systems while preserving existing infrastructure and minimising disruption. Security teams can manage one identity and scale across buildings and sites – without rip-and-replace projects.

CONNECT provides a modern, streamlined user interface for managing the full identity life cycle. From a single screen, operators can manage credentials, access rights and roles, onboarding and offboarding, and approvals. Updates are applied across connected systems, reducing errors and improving efficiency.

Symmetry CONNECT focuses on five core processes: onboarding/offboarding, centralised policy enforcement, self-service access requests, streamlined user experience, and audit and compliance – replacing disconnected, manual workflows that rely on emails, spreadsheets, phone calls, and institutional memory.



Aritech is a global provider of intelligent intrusion, video, and integrated security solutions, trusted by professionals worldwide for nearly half a century. At the heart of our technology is human intelligence: The expertise, commitment, and on-the-ground presence of our people, working side by side with customers and partners every day.

At Aritech, we believe strength doesn't come from standalone products; it comes from intelligent, connected solutions. With a digitally driven portfolio spanning intrusion detection, video surveillance, access control, and integrated technologies, Aritech brings security together into one powerful ecosystem.

At the centre of this evolution is Fusion: Our digital platform enabling smarter management, greater visibility, and seamless integration across systems and sites.

As security moves beyond hardware into connected IP and cellular environments, protection must go further. Aritech is leading this shift with cyber-secure, scalable solutions designed for today's risks and tomorrow's challenges.

We are ready for any security challenge, anytime, anywhere.

Bring it on.



Learn more



Fusion: Transforming how security value is delivered

Fusion is Aritech's unified security solution, operating both on-premise and in the cloud, and delivered through a modular suite of scalable digital services. More than a technology platform, it represents a transformation in how security solutions must be delivered and create long-term value for users. In a market defined by complexity, fragmentation, and rapid change, Fusion shifts the focus from isolated products to integrated, service-driven ecosystems.

In increasingly dispersed organisations, fragmented security infrastructures create operational blind spots, slow decision cycles, and elevate life cycle costs. The shift toward unified platforms has become an operational necessity.

By unifying intrusion, access control, video, and connectivity into a modular, cloud-enabled environment, Fusion simplifies system governance while enabling scalability across single sites and complex global operations. More importantly, it changes the delivery model: Security is no longer a static installation, but a continuously evolving service.

This transformation also reshapes the way we work with partners and customers. Centralised life cycle visibility, remote system governance, and unified control enable organisations to shift from reactive incident response to proactive risk management. Security leaders gain enterprise-wide visibility, operational control, and data-driven intelligence to inform investment, compliance, and resilience strategies.

Fusion's true value lies in aligning security with operational performance. By connecting systems and enabling automated workflows, it reduces complexity, enhances resilience, and turns security data into actionable intelligence that supports strategic decision-making.

Ultimately, Fusion reflects a broader industry evolution from hardware deployment to service orchestration, from transactional relationships to long-term partnerships, and from technology supply to value creation.

ASSA ABLOY

The ASSA ABLOY Group is the global leader in access solutions. Every day, we help billions of people experience a more open world. ASSA ABLOY Opening Solutions leads the development of door openings and products for access solutions in homes, businesses, and institutions. Our offering includes doors, door and window hardware, mechanical and smart locks, access control, and service.

ASSA ABLOY Door Security Solutions combines the expertise of the industry's most knowledgeable door-opening experts with the comprehensive product offering of leading door and hardware brands to provide complete solutions to partners and end-users in commercial, retail, multi-family, government, and institutional facilities. Coupling innovative technologies with insight into specifications, design, support, training, and code compliance, ASSA ABLOY Door Security Solutions works closely with the architectural, security, facilities, and integrator communities to address the many challenges they encounter serving and securing their customers.



[Learn more](#)

Upgrade any access system wirelessly or install wireless locks from scratch

Aperio wireless devices are the easiest way to **extend the reach of your access control system**, or to replace your mechanical locks with intelligent access control. Because they operate **wire-free**, **battery-powered** Aperio devices are fast and cost-effective to install and save you money in operating and maintenance costs.

The Aperio **product range** includes battery-powered cylinders, escutcheons, and complete locks for security doors. The award-winning Aperio handle fits powerful access control functionality into a slimline door handle.

Because Aperio is **built using open architecture**, seamless integration enables control of any existing hard-wired doors and Aperio battery-powered devices from the same access control interface.

Access control at more doors, easily and at low cost

Aperio is built on an open platform for fast, low-cost integration with your existing access control and security management system — or a brand new one. Aperio lets you schedule user rights and generate instant audit trails for more doors, taking security management to the next level.

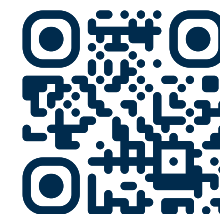
Keyless door access that saves you time and money

Life is more convenient when you replace mechanical keys with RFID credentials. Every lost credential is easy to revoke electronically, so you don't waste time and money changing locks. Aperio works with all major low- and high-frequency RFID technologies, including your existing ones, and with mobile technologies like Near-Field Communication (NFC) and BLE (Bluetooth Low Energy).



Axis enables a smarter and safer world by improving security, safety, operational efficiency, and business intelligence. As a network technology company and industry leader, Axis offers video surveillance, access control, intercoms, and audio solutions. These are enhanced by intelligent analytics applications and supported by high-quality training.

Axis has around 5,000 dedicated employees in over 50 countries and collaborates with technology and system integration partners worldwide to deliver customer solutions. Axis was founded in 1984, and the headquarters are in Lund, Sweden.



[Learn more](#)

Axis and ARTPEC-9: Advancing intelligent video with AV1

Axis Communications continues to shape the future of intelligent video with the introduction of AV1 encoding in cameras powered by its latest system-on-chip (SoC), **ARTPEC-9**. As the first in the industry to integrate AV1 directly into a system-on-chip designed specifically for network video, Axis is setting a new benchmark for video efficiency, performance, and scalability.

AV1, developed by the Alliance for Open Media, is an open, royalty-free codec designed to deliver high-quality video at significantly lower bitrates. Combined with ARTPEC-9, it enables up to 40% better compression than H.264 and approximately 20% better than H.265 – without sacrificing image detail. For customers, this translates into reduced bandwidth consumption, lower storage costs, and extended video retention times.

Built on decades of Axis expertise in imaging and system design, ARTPEC-9 supports multi-stream capabilities and maintains compatibility with H.264, H.265, and MJPEG, ensuring seamless integration into existing systems while preparing organisations for the future. The efficiency gains also make AV1 particularly well suited for hybrid and cloud-connected deployments, where bandwidth optimisation and scalability are essential.

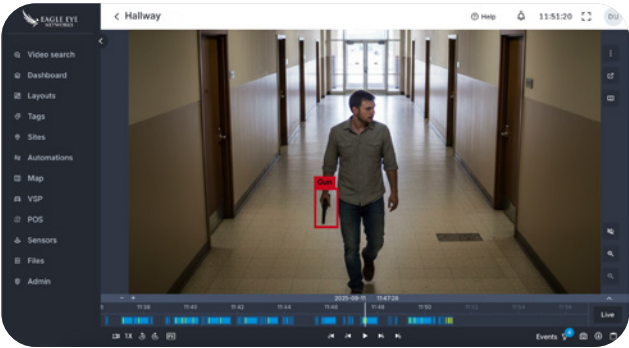


Brivo is the AI innovator and global leader in cloud-native physical security, with more than 2 million devices deployed across 100,000+ locations in 80 countries.

The flagship product, Brivo Security Suite, unifies access control, video intelligence, visitor management, and intrusion into a single view to centralise security across the enterprise. Businesses use Brivo’s AI-powered unified security platform to proactively detect and deter threats, improve operations, reduce liability, comply with regulations, increase sales, and maximise profits.

The pioneer in both cloud-native access control and video surveillance, Brivo is trusted by more than 25 million users across the globe to protect people, property, and digital assets. Headquartered in Bethesda, Maryland, and Austin, Texas, Brivo has additional offices in Lehi, Utah, Amsterdam, Bangalore, and Tokyo.

Brivo recently merged with Eagle Eye Networks. Please visit brivo.com to learn more about the Eagle Eye AI VMS (video management system) and its AI-powered video intelligence capabilities.



Proactive protection to identify guns before a threat escalates

In a world where firearms are increasingly present, the speed of threat recognition is the thin line between safety and tragedy. Most gun-related crimes, like bank robberies, are over in less than three minutes. To disrupt this timeline, security must move beyond recording history to detecting threats the moment a weapon is brandished.

Traditional systems often rely on acoustic sensors that trigger only *after* a shot is fired. **Brivo Eagle Eye Gun Detection** shifts the focus to identifying a brandished weapon the second it is drawn.

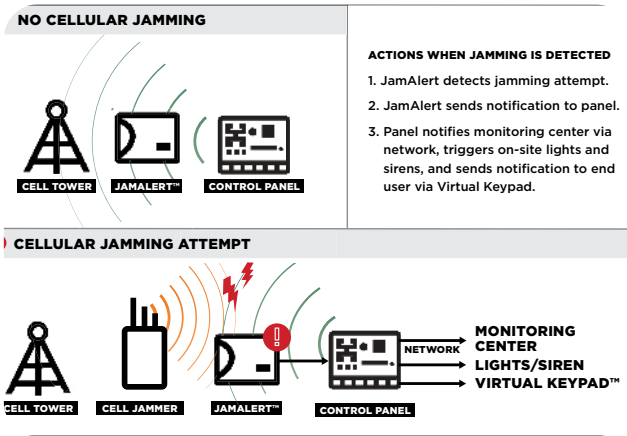
Accuracy is paramount to avoid the chaos of false alarms and the trauma of lockdowns. To ensure the highest accuracy, Brivo engineered a Triple-Layer Verification system:

- **Rapid Edge AI:** Security video is continuously analysed for brandished guns by the Eagle Eye AI Bridge on location at the school or business.
- **Cloud AI:** Secondary verification by a very large-scale Eagle Eye AI model in the cloud.
- **Human Review:** Expert 24/7 verification to confirm the threat before initiating your emergency response plan.

Whether in schools, hospitals, or retail hubs, faster eyes save lives. By combining cutting-edge AI with human oversight, we provide the split-second awareness needed to lock down facilities and alert first responders.



DMP is a family-owned independent manufacturer of intrusion, fire, access control, video, and cellular alarm solutions. DMP products are designed, engineered, and manufactured in America with U.S. and global components. Our factory, call centre, engineering, and distribution are all located in Springfield, Missouri, right where the business began 50 years ago.



JamAlert™ Cellular Jamming Detector

The threat is no longer theoretical. Transnational South American theft groups – now the subject of FBI warnings and alerts issued by both the NFL and NBA – have been deploying signal-jamming devices as part of coordinated, high-tech burglaries targeting professional athletes and other high-net-worth individuals across the United States. When a jammer is active, cellular alarm signals never reach the monitoring centre, no authorities are dispatched, and criminals enter undetected.

This isn’t a niche concern. It’s a pattern that law enforcement describes as operating in nearly every state, and the broader commercial security industry is taking notice. Internationally recognised insurance providers are now requiring cellular jamming detection devices – specifically, **JamAlert** – as a requirement for coverage in high-risk verticals, including financial institutions, high-end retail, and luxury residential properties.

JamAlert addresses the threat directly. The device continuously monitors cellular frequencies and instantly alerts the control panel the moment jamming activity is detected, giving security professionals a critical window to respond before a breach occurs. It’s backward and forward compatible with DMP panels and universally compatible with non-DMP systems, making it a practical addition to virtually any existing security infrastructure.

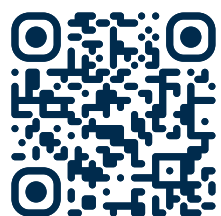
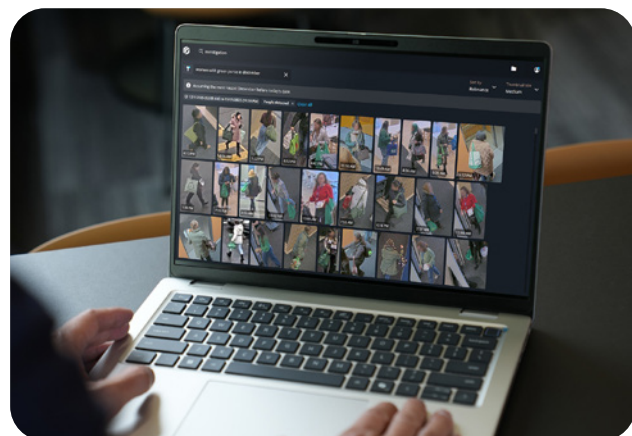
As organised theft groups grow more sophisticated and insurance carriers raise the bar on required protections, the question is no longer whether cellular jamming detection belongs in a security system – it’s whether you can afford to be without it.



Genetec Inc. is a global technology company that has been transforming the physical security industry for over 25 years. The company's portfolio of solutions enables enterprises, governments, and communities around the world to secure people and assets while improving operational efficiency and respecting individual privacy.

Genetec delivers the world's leading products for video management, access control, and ALPR, all built on an open architecture and designed with cybersecurity at their core. The company's portfolio also includes intrusion detection, intercom, and digital evidence management solutions.

Headquartered in Montreal, Canada, Genetec serves its 42,500+ customers via an extensive network of accredited channel partners and consultants in over 159 countries.



Learn more

New investigation capabilities in Genetec™ Security Centre SaaS

The new investigation capabilities in **Security Centre SaaS** help security teams conduct faster, more effective investigations across large, distributed environments. Designed for how investigations unfold, the solution allows operators to start with limited details and quickly locate relevant footage across multiple sites and cameras.

Security professionals can leverage intelligent search capabilities to surface the most relevant information, such as similar people or object entry-and-exit detections within scenes. Operators can then visualise the movement of a suspect or vehicle across locations, building a full view of the incident using trajectories to quickly reconstruct connections without reviewing hours of video.

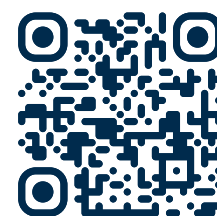
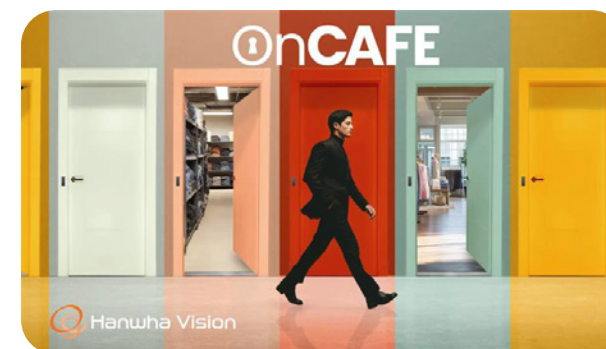
As cases progress, evidence is automatically organised into a clear, chronological storyline, making it easier to validate findings, document event sequences, share results, and close cases efficiently.



Hanwha Vision helps organisations secure more, manage less, and operate smarter. By consistently delivering video surveillance innovations combining 24/7 protection, AI, and cloud-based platforms, we help elevate the security experience, and transform an organisation's total operations.

Our cloud and hybrid ecosystem, powered by OnCloud direct-to-cloud VSaaS and OnCAFE cloud-native access control, simplifies security while delivering greater visibility and control. Integrated with AI analytics, IP cameras, storage devices, video management software and recorders, encoders/decoders, monitors and accessories, and business intelligence, Hanwha Vision turns security systems into actionable insights that improve safety, efficiency, and decision-making across the organisation.

Hanwha Vision technologies address every requirement for any surveillance application: retail, transportation, education, financial services, healthcare, hospitality, airports, sports venues, and government agencies. Our vision is to streamline security management by providing powerful, intelligent, and scalable surveillance protection.



Learn more

Surveillance options... on your terms

Hanwha Vision technologies form a connected ecosystem, letting customers choose the architecture that matches their needs, budgets, and future plans. A perfect example is our ecosystem of cloud-based surveillance solutions:

- **OnCloud**, our full direct-to-cloud Video Management Software as a Service (VSaaS) platform, streamlines surveillance operations with a powerful and flexible user experience, combining the speed and scalability of the cloud with the benefits of edge-based recording and AI analytics.
- **OnCAFE**, our cloud-native access control system that seamlessly integrates both video surveillance and access control. OnCAFE unifies security, surveillance, and facility management tools for users from one source. The ability to connect video, access, alarms and more, all under the same architecture, offers operational simplicity and stronger situational awareness.

By combining OnCAFE with OnCloud video management, integrators and end users gain a centralised dashboard. OnCAFE and OnCloud offer all the features of traditional on-premises systems, plus scalability, ease of use, and integrated video and access control in one platform. Instead of lengthy server installations and complex licencing, set up is as simple as registering devices to the cloud.

Each is powerful on its own, but together they give customers complete and transparent management flexibility over their surveillance systems. Both OnCAFE (access control) and OnCloud (video management) run on Hanwha Vision's unified cloud platform, with a common set of credentials and seamless integration between video and access control.



HID Global powers the trusted identities of the world's people, places, and things. We make it possible for people to transact safely, work productively, and travel freely. Our trusted identity solutions give people convenient access to physical and digital places and connect things that can be identified, verified, and tracked digitally.

Millions of people around the world use HID products and services to navigate their everyday lives, and over 2 billion things are connected through HID technology. We work with governments, educational institutions, hospitals, financial institutions, industrial businesses, and some of the most innovative companies on the planet.

Headquartered in Austin, Texas, HID Global has over 3,000 employees worldwide and operates international offices that support more than 100 countries. HID Global® is an ASSA ABLOY Group brand.



Learn more

Mercury is built for secure growth

Mercury's embedded application expands what access controllers can do. Now commercially available, the platform extends Mercury's open architecture by allowing approved applications to run directly at the edge. By embedding business logic and integrations on the controller itself, organisations can accelerate innovation, strengthen security, and scale functionality without reengineering their core infrastructure.

Controllers designed on open standards allow partners to integrate more efficiently while giving end users flexibility to adapt over time. As regulatory requirements evolve and integration needs expand, the app environment supports phased modernisation rather than wholesale replacement.

We have a growing community of original equipment manufacturers (OEMs) and developers building on Mercury's platform. By providing a secure, open environment at the controller, Mercury empowers partners to create new capabilities that operate directly at the edge.

Innovation is no longer confined to upstream systems. Applications can now enhance integration, analytics and orchestration within the controller itself. This ecosystem approach allows partners to differentiate their offerings while delivering additional value for end users.

Supported by a structured developer programme, technology partners follow a four-step onboarding process that includes submitting proposals, collaborating with Mercury on technical evaluation, accessing development tools, and completing a security review prior to distribution. This framework ensures applications meet performance and cybersecurity expectations while helping partners bring solutions to market faster.

With over 30 years of expertise and commitment to open architecture, Mercury has built a future-proof platform that ensures seamless interoperability between leading software and technical solutions. Mercury has more than 5 million controllers installed worldwide.



Honeywell's Security and Access Solutions (SAS) now includes LenelS2 alongside Honeywell's Commercial Security group. LenelS2 continues to be a recognised global leader in delivering advanced physical security solutions, including access control, video surveillance, and mobile credentialing.

The combination of LenelS2 and Commercial Security further elevates Honeywell's full-stack, scalable, unified security management solutions for customers ranging from global enterprises to small- and mid-size businesses.

Facility operators and security teams across dynamically evolving verticals select and depend on Honeywell's mobile- and cloud-enabled technologies for access control, intrusion detection, and video surveillance solutions to help them create safer and more efficient facilities around the world.



Learn more

AI-driven integration for global enterprises

What will the Security Operations Centre (SOC) of the future look like? Significantly quicker and more accurate incident response, lower cost of ownership and operation, accelerated threat detection, real-time situational awareness, and streamlined workflows - with all of this effectively managed across diverse systems and geographically spread-out sites.

Enterprise security is due for transformation in order to keep pace with evolving threats. Traditional SOC configurations must become more integrated and agile. While the industry is delivering exciting new innovations enabled by AI, cloud, and mobile technologies, wholesale system replacement is unrealistic due to cost, time, and risk.

The typical ideate-build-release cycle for complex, enterprise level security systems typically offers only incremental advancement over time. The key to delivering meaningful transformation, not just incremental improvement, in a way that reduces risk, maximises uptime, and balances overall cost, is to build next-generation SOC capabilities into existing platforms.

End users need a way to tack on future-focused innovation without having to fully replace their existing systems, which, at the enterprise level, are often fine-tuned, customised configurations designed over many years and with significant investment to precisely meet organisational needs. Customers shouldn't have to choose between advancement and reliability – they should be able pace their upgrades on their own time and achieve the operational benefits of new technologies more efficiently and with less risk.

With its reach and powerful portfolio of security, IOT and AI technology, Honeywell, including LenelS2 and Forge platforms, is uniquely positioned to deliver future-focused yet grounded innovation, at scale. By layering automation capabilities onto existing, proven platforms like **LenelS2 OnGuard**, and applying context-aware AI and machine learning agents, Honeywell helps enterprises across all verticals tackle the complexities of tomorrow's threat landscape while controlling costs and improving overall security outcomes.



IDIS Americas, headquartered in Coppell, Texas, offers a comprehensive portfolio of advanced video solutions and AI-driven technologies for various security surveillance applications. Our product portfolio consists of video management software (VMS), surveillance cameras, network video recorders (NVRs), Advanced Analytics (AA), Cloud solutions, and more, providing tailored solutions for our customers' needs.

IDIS Americas leverages the combined strengths and expertise of Costar companies and IDIS to deliver a wider selection of products, greater tech innovation, and an even higher level of service than ever before. IDIS Americas designs, develops, and distributes video surveillance and security solutions with high-performance products to meet the evolving needs of the customer.

Our mission is to become a leading partner of choice through quality products, competitive prices, and unparalleled customer service. Experience IDIS Americas and see how it can make a difference in your business.



Learn more

Smarter, faster, sharper: The new IDIS Edge AI cameras lead the future of surveillance

The **next-generation IDIS Edge AI Plus camera range** represents a major leap forward in intelligent surveillance, combining advanced deep learning analytics with exceptional imaging performance. Designed to give organisations flexible, affordable pathways to modernise their security systems, these cameras deliver powerful, on the edge AI capabilities, including **crowd detection, abandoned and removed object detection, fall detection, and violence detection** – all driven by the upgraded **IDLA Pro analytics engine**.

Engineered for real world performance, the lineup features **outdoor-ready, vandal resistant 8MP domes and bullet models**, as well as **next generation PTZ units offering 40x optical zoom, AI auto tracking, and night vision up to 400 meters**. These PTZ models provide unparalleled scene coverage and are ideal for wide area monitoring across critical infrastructure, public spaces, transportation, and large commercial sites.

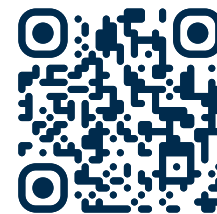
IDIS' innovative **A Cut technology** automatically crops and extracts the most relevant images of detected objects, enabling operators to rapidly identify people or vehicles and jump directly to key moments in recorded video. Paired with **IDIS AI Search**, users can filter footage by detailed attributes such as **gender, age group, clothing colour, vehicle type, or accessories**, dramatically reducing investigation time and improving situational awareness.

Built on **IDIS DirectIP**, the Edge AI Plus cameras offer plug and play deployment, one click configuration, multi layered cybersecurity, and **zero licencing fees**, ensuring industry leading total cost of ownership. With superior image clarity powered by IR, WDR, and a large **1/1.8" sensor**, the new Edge AI generation empowers security teams to act faster, smarter, and more proactively than ever before.



Intellicene has redefined physical security with an intelligence-driven approach that goes beyond traditional security operations. Our mission is to help you protect your people, property, and vital operations with intelligence at the centre of it all. Our platform connects and unifies diverse technologies, delivering actionable insights that enhance security, streamline operations, and drive smarter business decisions.

From mobile applications and AI-driven analytics to infinitely scalable software and intelligent devices, we're building advanced technology that raises the bar and makes the world safer. Intellicene empowers you to efficiently manage the most complex security and business operations. We're unifying security, enabling action, and giving you the intelligence to protect.



Learn more

Introducing Intellicene Insight

Intellicene Insight transforms traditional video surveillance systems into intelligent, event-driven security platforms that see, understand, and interpret activity in real time. In reality, operators can only reliably watch a handful of cameras at once before accuracy drops sharply.

Insight uses advanced AI to dramatically improve detection accuracy while cutting through the noise. With real-time anomaly detection, behavioural analysis, and contextual AI powered by its in-house visual language model, Insight identifies deviations from normal activity without relying solely on manual rules, allowing for faster response and more confident decision-making.

Built for scalability and flexibility, Insight supports monitoring of up to 800 cameras per workstation with significant improvements in detection performance. It offers over 100 object classes, pose recognition, forensic search, multi-camera tracking, and support for intrusion detection, weapon and fight detection, fire and smoke alerts, PPE compliance, traffic analytics, and more. Designed for edge, hybrid, or centralised deployment, Insight integrates seamlessly with existing cameras and Intellicene platforms, making it a hardware-efficient, enterprise-ready solution for modern security, safety, and operational challenges.

IQSIGHT

Formerly Bosch Video Systems, IQSIGHT has more than 60 years of engineering expertise. Delivering intelligence-first video security that helps organisations see clearly, understand context in real time, and act with confidence, IQSIGHT transforms video into actionable insight so leaders can make better decisions, earlier.

IQSIGHT offers a proven portfolio of NDAA- and TAA-compliant video solutions, including FLEXIDOME, AUTODOME, and MIC cameras, supported by more than 600 patents and designed to perform reliably over the long term.



Intelligence-first video security

AI is transforming video security from traditional surveillance into visual intelligence, empowering organisations to recognise patterns and anticipate what may happen next. With foresight, they can detect risk earlier, make faster decisions, and operate with greater confidence to address issues before they escalate.

Intelligence at the edge enables cameras to act as sensors alerting to conditions such as perimeter breaches, brandished guns, missing personal protective equipment (PPE), and more. Application-specific analytics use algorithms trained for defined environments to deliver reliable and accurate detections while minimising false positives.

For critical sites, layering cloud-based AI alarm verification adds a second pair of eyes to check questionable alerts. Much like instant replay in sports, edge-based detection makes the call on the field and sends a short video clip to the cloud for review. AI alarm verification confirms a potential threat or overturns the call; it quickly rescinds or escalates alarms to further reduce false positives and help prevent alarm fatigue.

High detection accuracy is also essential when cameras integrate with other systems – enabling alarms to trigger automated actions. Intelligent cameras can publish Message Queuing Telemetry Transport (MQTT) topics, such as events triggered by the camera’s rule engine, count values, and more. MQTT support provides easier connection to third-party software for fully leveraging analytics events and extending the uses for AI-enabled edge devices beyond security.

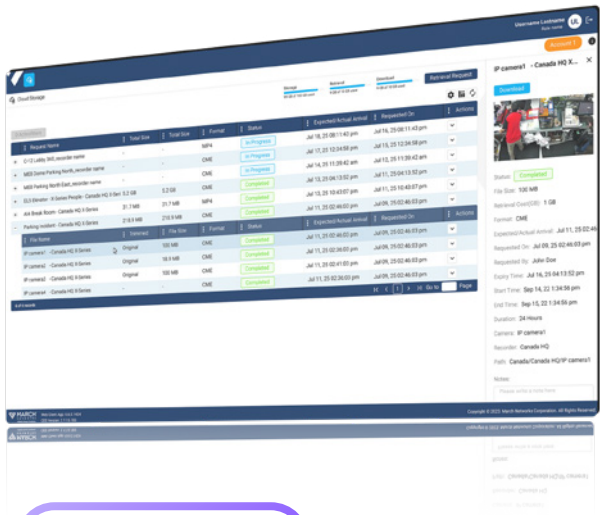
While security will always remain core, visual intelligence will play an increasingly important role in expanding video to operational uses across many environments.



March Networks provides secure, cloud-based intelligent video solutions designed to enhance security, mitigate risk, and improve operational efficiency. Our AI-driven analytics integrate with access control, alarms, POS systems, and ATMs to go beyond traditional surveillance, delivering real-time insights that help businesses prevent fraud, detect threats, and optimise performance.

With decades of expertise and a global reach, we are a trusted partner to security-conscious organisations worldwide, including 1,500+ financial institutions, 600+ retailers, and 900+ commercial and industrial businesses in 75+ countries.

Backed by our certified partner network, March Networks can design and deliver custom surveillance solutions tailored to Securitas customers’ unique security and operational needs, ensuring the highest level of protection and business continuity.



March Networks Long Term Cloud Storage

March Networks Long Term Cloud Storage delivers secure, scalable, and cost-efficient video retention built on Amazon Web Services (AWS) infrastructure. Using a flexible, tiered storage model powered by Amazon S3 Glacier, organisations can archive surveillance video for years without expanding on-premise hardware or increasing IT complexity.

Designed for enterprises with strict compliance and retention requirements, the service helps enterprises reduce long-term storage costs by up to 80% while maintaining high levels of durability, resiliency, and security. Video is automatically encrypted and protected within AWS’s highly durable cloud architecture, ensuring reliable preservation of critical evidence and operational footage.

March Networks Cloud Storage integrates directly with the March Networks video management platform, allowing organisations to manage archived and on-premise video from a single interface. Customers can keep recent video on local recorders for fast investigations while seamlessly archiving older footage to the cloud. Archived video can be searched, retrieved, and exported when needed without disrupting daily operations.

This hybrid approach provides the flexibility to scale storage as video volumes grow across multiple sites. It also eliminates the need for large on-premise storage expansions, simplifies IT management, and helps organisations maintain long-term video retention policies while keeping infrastructure costs predictable.

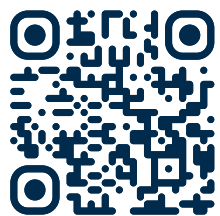


Milestone Systems is a world leader in data-driven video technology used in industries as diverse as manufacturing, airports, law enforcement, retail, and traffic management. We provide a clear picture of how to create a safer, better, and more prosperous world.

Our product suite includes XProtect video management software, BriefCam AI-powered analytics, and Arcules cloud VSaaS. It helps our customers learn from the past, understand the present, and predict the future.

Milestone is also advancing responsible Vision AI through Project Hafnia, the world's largest regulatory-compliant video data library, and BrighterAI anonymisation technology.

Founded in 1998 and headquartered in Copenhagen, Milestone employs more than 1,500 people worldwide and has been an independent company in the Canon Group since 2014.



Learn more

Intelligent video, responsible by design

Milestone Systems is advancing video technology with three new AI-powered capabilities designed to help operators work faster, investigate smarter, and stay compliant.

XProtect Video Summarisation uses a vision-language model (VLM) to automatically summarise and interpret video content. Developed with NVIDIA technology and fine-tuned on 75,000+ hours of ethically sourced, real-world video data from Project Hafnia, the VLM lets operators send clips directly from the XProtect Smart Client and receive structured text summaries – making it easier to assess urgent situations, reduce false alarms, and standardise incident documentation.

Video Anonymisation, powered by BrighterAI, brings automated privacy protection directly into Milestone video workflows. In just a few clicks, users can redact faces, licence plates, and bodies from video – ensuring compliance with GDPR, the EU AI Act, and other global privacy regulations before sharing footage with external parties.

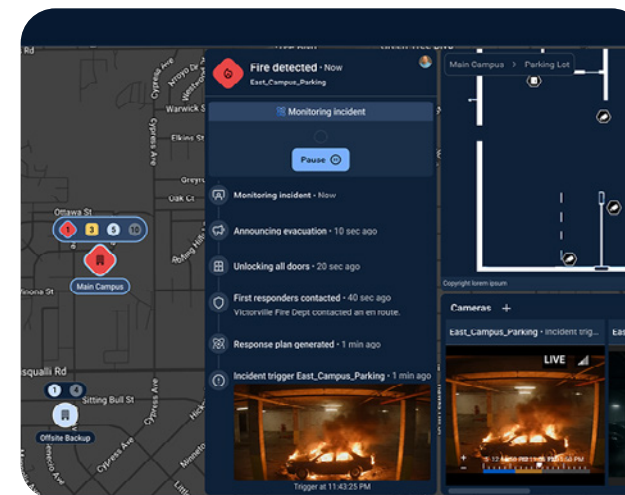
AI Search introduces natural language search across the Milestone portfolio, allowing operators to find relevant video moments by simply describing what they're looking for – no manual scrubbing, no complex filters. It's a faster, more intuitive way to find what matters in video footage.

Together, these capabilities represent a new generation of responsible, AI-driven video intelligence – built on Milestone's 25+ years of trust as the industry's most open VMS platform.



Safety and security are at the heart of everything we do at Motorola Solutions. We build and connect technologies to help protect people, property, and places. Our solutions foster the collaboration that's critical for safer communities, safer schools, safer hospitals, safer businesses, and ultimately, safer nations.

Scan the QR code below to visit our website to learn more about our commitment to innovating for a safer future for us all.



Learn more

Operator: Enterprise resilience through intelligent orchestration

Operator revolutionises Security Operations Centres with AI-powered automation. This cloud-native platform proactively triages threats, minimises false positives, and automates responses, saving time and effort and reducing response times. Operator serves as a force multiplier for security professionals by synthesising data from video, access control, sensors, and radio systems into a single, actionable view. It utilises event clustering to filter out noise, identifying the core incident amidst hundreds of disparate signals. Its response agent automates response plans – such as locking doors or notifying first responders – and so transforms security operations into proactive, intelligent defence.

Its AI-enabled features and capabilities include:

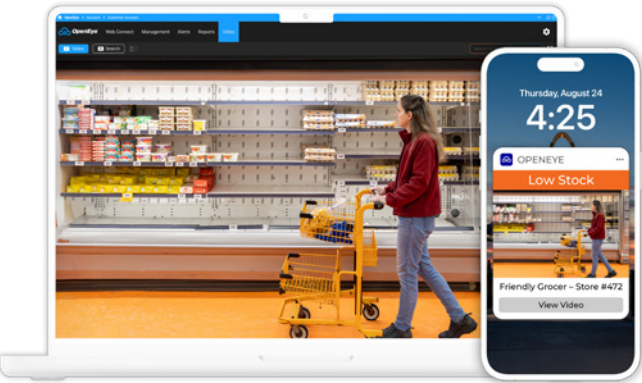
- **Event Triage:** Automatically verifies and combines signals to cut through the noise of false alarms, delivering a clear view of only high-severity threats.
- **Dynamic Response Planning:** Generates real-time, step-by-step response plans that guide operators through novel or complex challenges with confidence.
- **Unified Operational Interface:** Provides a single, intuitive interface for real-time visibility across video, access control, and radios, eliminating the need to switch between multiple applications.
- **Automated Execution:** Executes predefined playbooks to ensure rapid, consistent containment and action, acting as a digital security operator alongside human resources

To discover how Operator can revolutionise your security operations, visit the official product page at motorolasolutions.com/inform or explore the Operator documentation portal.



Headquartered in Liberty Lake, Washington, OpenEye is a leading provider of intelligent cloud solutions for video security, business intelligence, and loss prevention. Our easy-to-use products are designed to help customers streamline operations and reduce the burden on IT, making it easier to manage video surveillance deployments and integrations of all sizes with a proactive approach.

OpenEye is a subsidiary of Alarm.com (Nasdaq: ALARM). With over 2,000 people and more than 900 R&D team members in North America, we service millions of locations with cloud-enabled video, access control, and intrusion solutions that make properties smarter and more secure.



Learn more

AI-powered search and alerting in OpenEye Web Services

OpenEye continues to expand OpenEye Web Services (OWS) with **AI Visual Search** and **AI Visual Check**, two AI-powered capabilities designed to help teams locate key moments faster and stay informed without constant manual review.

AI Visual Search helps users locate the moments that matter most. Instead of manually scrubbing through hours of footage or spending time configuring search filters, users can simply describe what they are looking for, such as “a person carrying a box in the lobby yesterday afternoon” and quickly receive relevant results. By combining advanced analytics and cloud intelligence, AI Visual Search turns complex video review into a fast, intuitive experience any user can master. By eliminating manual review time and delivering clear, actionable insights, it empowers teams to make faster, more confident decisions when verifying security events, tracking operational trends, or uncovering key moments.

AI Visual Check enables teams to work smarter with AI-powered visual verification. Instead of constantly watching video or performing routine inspections, OWS evaluates camera images on their behalf and alerts users only when something needs attention. Organisations define what matters most, such as a clean lobby, stocked shelves, or secure access points, and AI Visual Check continuously validates those conditions. Each alert includes clear context, short AI-generated summaries, and reference images that make it easy to understand what happened and act quickly. By automating routine visual verification, teams save time, reduce unnecessary alerts, and gain greater intelligence across every location without needing to continually sit in front of a screen.



With over 40 years of global success, PACOM excels in seamlessly integrating hardware and software solutions for reliable security and business excellence. Experts in security integration, we offer modular, cost-effective solutions with multi-level access control, in-house reliability, and seamless third-party integration through an open API.



Learn more

PACOM VIGIL CORE ATM solution with remote sensor intelligence

ATMs are remote, unattended, and vulnerable. When an ATM is attacked, moved, or stolen, the impact goes beyond theft. It can lead to service outages, regulatory exposure, and costly emergency response. Traditional ATM security often relies on fragmented alarms that react too late. **PACOM VIGIL CORE** addresses this challenge by shifting ATM protection from reactive alerts to proactive, sensor-driven intelligence that helps teams detect risk early and act faster.

PACOM VIGIL CORE supports ATM security through integrated monitoring and intelligent remote sensors. The sensor monitors ambient light, temperature, humidity, vibration, movement, and door activity, identifying abnormal conditions that may indicate tampering, forced entry, or environmental risk. If an ATM is physically removed, VIGIL CORE can also track its location, supporting faster recovery and investigation. Alarm thresholds can be configured and adjusted remotely, enabling centralised control without frequent site visits.

Sensor data is managed through the VIGIL CORE platform, giving operators a single view of alarms, diagnostics, and site health across one ATM or an entire network. To support fast verification, VIGIL CORE integrates an OSDP mini camera that captures event-driven snapshots linked to alarms and sensor activity. This allows operators to confirm incidents quickly, reduce false alarms, and dispatch response with confidence.

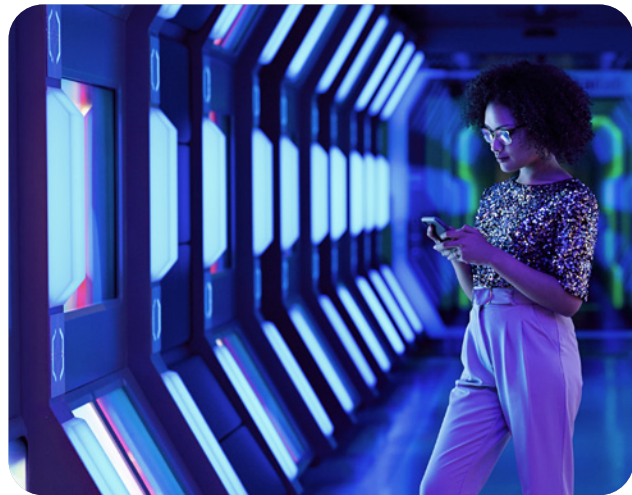
The result is a scalable ATM security solution that protects uptime, reduces operational cost, and gives financial institutions greater control over their ATM estates.



The transition of the Bosch Intrusion and Access Business to Radionix is complete. As an independent company, we are moving faster and focusing deeper – combining our heritage with the agility to meet your evolving needs.

Radionix delivers “mission control” for your security, uniting intrusion detection, access control, and fire safety into one seamless, always-on network. Whether on-site or remote, you gain the power to manage access and make instant decisions while our technology works quietly to protect your people and property.

This is more than a new name; it’s a new era of innovation built on a foundation of trust.



The next-generation ecosystem

The future Radionix ecosystem will modernise our trusted **B and G Series panels** while maintaining their signature reliability, versatility and ease of use.

“Installation will be faster with a single pane of glass and API-driven integration,” explains Greg Mora, Chief Product Officer, Radionix. “We are moving toward a cloud-connected, on-prem platform that ensures IoT devices stay online with instant, real-time data.”

By decreasing installation time, Radionix allows technicians to work more efficiently, directly addressing labour challenges. Furthermore, we are pioneering secure wireless innovation for the enterprise.

While wireless has traditionally been reserved for small businesses, Radionix is bringing that ease of setup to the large commercial sector without compromising the rigorous security standards our clients demand.



Resideo is a leading manufacturer and developer of technology-driven, sensing, and controls products and solutions that are found in over 150 million residential and commercial spaces globally, with tens of millions of new devices sold annually.

Resideo’s trusted First Alert® brand offers security, safety, and water leak detection solutions. With proven expertise for more than a century, the company’s Honeywell Home smart thermostats help balance indoor air quality and offer energy savings.



First Alert® CX4 Camera Series: Advanced surveillance for SMBs

The First Alert® CX4 Video Cameras bring ultra-high-definition security to homes and small and medium businesses (SMB) with advanced clarity and analytics. Compatible with both the Resideo ProSeries Security System and First Alert® VISTA® Hybrid Security System, the cameras deliver continuous recording and enhanced analytics to provide comprehensive detection for business environments.

The CX4 cameras offer 4K sharpness and 8-megapixel resolution with a high-performance image sensor, capturing critical details with clarity that makes it easy to identify faces, licence plates, and other important information – a key advantage for small business security, loss prevention, and situational awareness.

Small businesses can choose from three models to cover a range of applications:

- **CX4B Bullet Camera** for perimeter monitoring, warehouses, or retail applications.
- **CX4T Turret Camera** for lobbies, stairwells, and retail areas.
- **CX4D Dome Camera** for entrances, exits, offices, or food service applications.

The cameras also offer edge video storage, which keeps video data on-site to reduce network requirements and costs, and cloud-based video-event storage sends the important event video to the cloud, reducing the impact of hardware theft or tampering while protecting important information.

Integrated viewing through the familiar **Total Connect® 2.0** experience enables users to view live feeds from multiple cameras on one screen, while intelligent analytics identify people, vehicles, animals, and packages to reduce unnecessary notifications and deliver the actionable alerts that matter most.

With high-definition footage, flexible form factors, and intelligent features built in, the First Alert CX4 Video Cameras bring advanced, scalable video surveillance to small business owners.

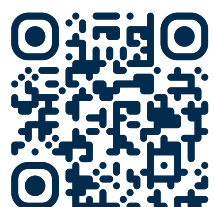


Software House's passionate team of industry experts provide physical security solutions that meet the ever-evolving challenges of today's modern enterprises. For over 30 years, many of the world's largest organisations and government entities have trusted us to deliver secure, flexible, and compliant solutions.

Our goal is simple: Empower organisations to protect their people and property while giving them the tools required to be more productive.

- **Software:** C-CURE 9000 empowers our customers to take full command of their access control, video, intrusion, fire, and building automation systems.
- **Hardware:** Software House's door controllers deliver best-in-class performance with flexible deployment options for both centralised and distributed architectures.
- **Cyber:** We continue to set the bar in cybersecurity and are relentlessly dedicated to ensuring your data is protected and your networks are secure.
- **Integrations:** Our solution is made more powerful by integrating with the systems our customers are already using.

Software House is a brand of Johnson Controls Security Products, a division of Johnson Controls Inc.



Learn more

Security Intelligence AI-driven analytics

C-CURE IQ Security Intelligence is designed to help organisations manage overwhelming alarm volumes by identifying meaningful events within large datasets. Enterprises often experience millions of alarms annually, many of which are nuisance events that obscure critical incidents. The platform prioritises essential alarms through **Alarm Intelligence**, which uses a customisable rules engine to reduce noise, rank alarms, and apply a dynamic, real-time Risk Score that adapts as situations evolve. This ensures security teams focus on the most urgent events and respond more effectively.

Examples of automated rules include filtering false alarms caused by valid card activity, escalating forced door events occurring in clusters, and identifying suspicious behaviours such as repeated rejected access attempts. Dashboards provide real-time visualisation of alarm trends, status, and automation activity, enabling more streamlined operations.

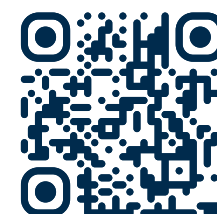
The solution also includes powerful **Spatial Intelligence** capabilities. These features deliver comprehensive insight into facility usage, personnel movement, and occupancy trends. Tools such as Last Known Location, Virtual Headcount (mustering), swipe metrics, and occupancy dashboards provide real-time visibility into where people are, how spaces are being used, and how facilities can be optimised for safety and efficiency. Attendance analytics further support workforce management by highlighting trends and identifying potential issues.

Designed for enterprise scale performance, the system recommends robust CPU, memory, and SQL Server configurations. Multiple licence tiers (SM, MD, LG, XL) offer varying capacities, with all versions including multi-rule Alarm Intelligence and core Spatial Intelligence features.



SONITROL leads the way in verified electronic security, providing innovative, customised security solutions – integrated intrusion, access control, and video – across North America.

By utilising patented impact activated audio intrusion detection and verified alarms, SONITROL has led the industry in documented apprehensions, over 188,000, and counting.



Learn more

SONITROL CORE + PowerG wireless integration

SONITROL CORE continues to raise the bar for professional security with its integration of **PowerG wireless technology**, bringing fast, flexible, and highly reliable wireless protection to the CORE unified platform.

This integration combines PowerG's long-range, battery-efficient wireless sensors with SONITROL's patented, verified audio and video intrusion detection. The result is a powerful solution that simplifies installations while maintaining the proven performance SONITROL is known for. By eliminating complex wiring, dealers can significantly reduce installation time and cost while easily adapting systems for large facilities, multi-site properties, or environments where cabling is impractical.

PowerG wireless technology delivers industry-leading performance, including encrypted, frequency-hopping communication with a range of up to 1.24 miles line of sight and adaptive power management that supports battery life of up to 8 years per device. Military-grade 128-bit AES encryption, two-way communication, and interference-resistant operation ensure dependable protection for commercial and campus-style applications.

Approved PowerG sensors – such as wireless door and window contacts, motion detectors, glass-break sensors, and panic buttons – integrate seamlessly with the PowerG Host Transceiver and CORE security panels, all managed through a single platform. Installers benefit from rapid deployment and easy expansion, while end-users gain reduced system complexity, lower costs, and faster police response through SONITROL's verified audio and video alarm technology.

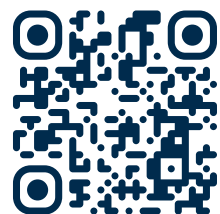
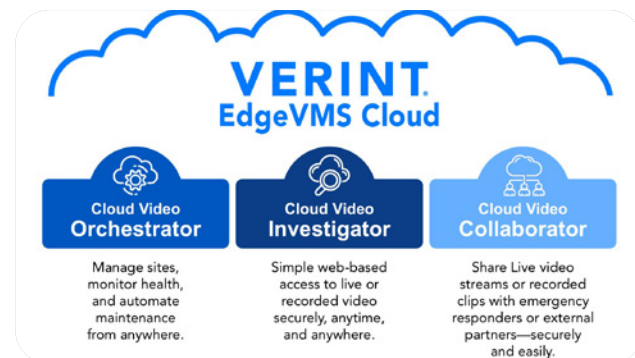
Additional approved sensors will be introduced soon, further expanding the CORE ecosystem's flexibility.

VERINT®

Verint is a leading provider of fraud prevention and security solutions for financial institutions, trusted by more than 3,000 banks and credit unions, including 8 of the top 10 U.S. banks. With over two decades of experience, Verint helps organisations mitigate fraud, reduce risk, and maintain compliance in a constantly evolving landscape.

Our advanced security solutions empower customers to identify risks, streamline investigations, and respond quickly with actionable intelligence. Financial institutions around the world rely on Verint's technology and insights to stay ahead of emerging threats, from ATM attacks and fraud to insider activity and branch vulnerabilities. By connecting transaction data with video intelligence, Verint enhances visibility, accuracy, and response times.

Scalable and cloud ready, Verint's solutions support large, geographically dispersed environments. Backed by deep industry expertise and continuous innovation, Verint partners with financial institutions to improve efficiency, protect assets, and strengthen the security ecosystem.



Learn more

Harness the value of hybrid with Verint EdgeVMS Cloud Suite

As financial institutions shape their cloud strategies, many are choosing a deliberate path forward rather than rushing into a full migration. Security leaders are balancing the flexibility cloud technology provides with the performance and reliability their operations depend on. A hybrid model supports that balance, allowing organisations to expand cloud capabilities while continuing to leverage existing infrastructure.

The **Verint EdgeVMS Cloud Suite** reflects this approach by combining flexible cloud functionality with the security and performance financial institutions expect.

With **Cloud Video Orchestrator**, teams can oversee enterprise-wide device management through real-time health monitoring, smart ticketing, and performance reporting from virtually anywhere.

Cloud Video Inspector allows approved users to quickly access live and recorded video in a browser, eliminating the need for additional software.

When video must be shared, **Cloud Video Collaborator** enables secure, temporary access for internal teams or authorised external partners while maintaining the chain of custody.

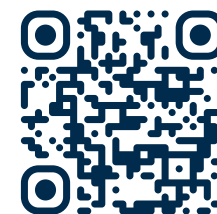
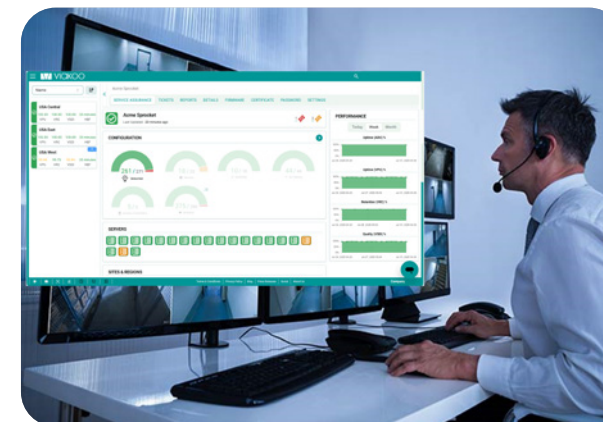
Built for hybrid environments, the Cloud Suite allows organisations to modernise at their own pace, improving visibility across locations and scaling strategically without disrupting daily security operations.

VIAKOO

Viakoo enables customers to assure the continuous performance of their physical security and OT systems while defending their OT attack surface with advanced discovery and vulnerability remediation solutions. Viakoo's vision is for every connected enterprise device to be 100% visible, operational, and secured.

The agentless Viakoo Action Platform keeps distributed and unmanaged OT environments secure and continuously operational at the lowest risk and cost. Automated device cyber hygiene is reliably updated at scale with firmware, passwords, and certificates to elevate security posture and system performance to enterprise IT expectations.

Viakoo Inc. is a leader in cyber hygiene and service assurance for connected devices. All Viakoo solutions are fully conceived and developed in the U.S.A.



Learn more

Viakoo DFM-AutoMode slashes physical security remediation time from months to minutes

With the release of **Device Firmware Manager AutoMode™ (DFM-AutoMode)**, Viakoo has enhanced its flagship **Viakoo Action Platform** with an autonomous remediation solution powered by AI. This new capability shrinks an organisation's physical security and OT cyber attack surface faster than any other security solution by dramatically accelerating the time to remediate known vulnerabilities.

Viakoo's AutoMode elevates OT security by providing autonomous operations for finding vulnerabilities in your device inventory, determining if new firmware is available, then setting up an update job to remediate vulnerabilities. Action is only taken after human approval, a one-click action. Traditional remediation can take days or weeks; DFM-AutoMode performs this in seconds.

Viakoo's strategy around AutoMode capabilities leverages insights from over 2 billion hours of product usage on Viakoo's platform, benefiting from real-world experience across every major vertical. This deep expertise, combined with Viakoo's patent portfolio in OT and IoT management, forms the basis for AutoMode.

Viakoo intends to extend AutoMode technology to all remediation capabilities within the Viakoo Action Platform.

Securitas spotlights





Leading the industry shift to intelligence-led security

Discover how Securitas' intelligence-led approach is empowering clients in a new age of global security.



Seeing a different world

Against the backdrop of a rapidly evolving world and increasingly complex risk environment, organisations across all sectors are faced with navigating a landscape where threats are escalating in both frequency and complexity. Modern security threats develop faster than ever, cutting across both physical and digital environments.

At Securitas, we see it every day. Technology that empowers businesses also opens new doors for threat actors. The traditional model of reacting after something happens still exists, but to better anticipate and stay ahead of risks, organisations need earlier signals, sharper insight, and the ability to act before a situation becomes a problem.

When we asked our clients about their ideal security partner, their vision aligned with our own: Integrated and advanced technology, proactive problem-solving, and a holistic approach to security and risk management.

This is where Securitas is placing its focus: Turning uncertainty into certainty, offering in a trusted partner when the landscape is shifting, and confidence when clients need it most. By transforming how we collect, analyse, and act on intelligence, we're reshaping the role of security into a strategic driver of business resilience and continuity.

Elevating security through intelligence-led innovation

Across our global organisation, this shift toward intelligence-led security is already underway. Through continuous monitoring of global developments, early-indicator detection, and real-time contextual analysis, we're enabling clients to see emerging threats sooner and understand their relevance to day-to-day operations.

Becoming an intelligence-led organisation means we are connecting risk, operations, and decision-making in a way that reflects how threats actually unfold. It means shifting from reaction to anticipation, augmenting human capabilities with data and technology, and delivering a single, connected view of what matters.

From risk management and security services to advanced technology and digital solutions, Securitas' transformation is supported by a broad ecosystem of intelligence and operational capabilities.

Transforming data into foresight, not just insight

Data can enable meaningful action. Our aim is to help clients cut through noise and concentrate on the signals that truly matter.

Our digital and risk intelligence services give organisations a more complete picture of their risk environment, whether that involves monitoring global developments, identifying emerging patterns, or supporting them through complex investigations and crisis scenarios. Alongside this, we're strengthening our ability to interpret open-source and digital intelligence signals at scale across security risk management, technology, and security services, turning them into clear, actionable guidance tailored to each client's risk profile.

Empowering our people and clients

Despite the pace of technological change, one principle remains constant: People are at the centre of everything we do.

When it comes to frontline services, our officers use real-time insights, AI-supported tools, and digital companions like **MyConnect** and **MySecuritas** to respond faster and deliver higher-quality service to clients.

For clients leveraging our technology solutions, platforms such as **SecureStat HQ** and **SecureStat Cumulus** enable them to centralise alarms, view security system performance, and receive intelligence-driven alerts, supported by generative AI. And in specialised healthcare settings, integrating electronic security with **real-time location systems (RTLS)** provides continuous context about people, assets, and movement.

Using AI and advanced technology

Artificial intelligence (AI), cloud platforms, robotics, drones, and automation have become core elements of how modern security operates today. AI filters distractions, accelerates analysis, and surfaces the information that deserves human attention.

To complement our technology services, human analysts within our monitoring and risk intelligence centres ensure that automated insights are validated and contextualised.

As more systems connect and intelligence becomes more precise, security will feel less like a defensive posture and more like an informed, strategic capability.

Staying ahead in a different world

That is the role Securitas is committed to playing: Being the trusted partner in intelligence-led security.

By strengthening our intelligence-led approach, Securitas is raising the standard of modern security, helping our clients move through uncertainty with greater clarity, stronger resilience, and a security posture that is smarter and more connected.



Intelligence services

Providing proactive, intelligence-led security solutions that empower clients to secure their organisations with confidence.



The security intelligence era is here

We're pioneering a future where intelligence transforms security into a strategic advantage. With our unparalleled insights, organisations can confidently and resiliently navigate the complexities of tomorrow.

Our team of analysts and experts seamlessly integrates digital capabilities and innovative solutions with intelligence-led security, delivering tailored, increasingly predictive, and proactive protection for our clients.

As our flagship service, our managed Risk Intelligence integrates data- and tech-driven insights with expert analysis to provide accurate, timely, relevant, and actionable intelligence for organisations. These insights help clients understand risks posed by criminal and terrorist actors, geopolitical shifts, cybersecurity threats, environmental challenges, and more.

Intelligence at its best

Our **Risk Intelligence** goes beyond merely identifying what is happening. It explains why it matters, what could happen next, and, most importantly, what actions can be taken. With five levels of premium services, we offer digital tools, managed services, and embedded expertise, all customisable to create a tailored solution that meets our clients' unique needs.



- **Awareness**
Stay ahead with situational awareness of the latest developments in the global security and threat landscape. Receive over 350 reports annually, including daily, weekly, monthly, and ad hoc updates on significant global events. This service is suitable for organisations of all sizes and industries, ensuring clients have the intelligence needed to make informed decisions.
- **Alerting**
Receive targeted alerts for incidents and threats near clients' locations with our highly tailored alerting service. Protect people, property, and assets by staying informed with real-time notifications and early warnings for emerging threats.
- **Advisory**
Access specialised Intelligence-as-a-Service to safeguard organisations. Our comprehensive protective, threat, and risk intelligence package leverages Securitas' all-source intelligence strategy, combining expert human intelligence (HUMINT) with cutting-edge technology for open-source intelligence (OSINT).
- **Analyst**
Integrate dedicated intelligence and risk resources directly into the organisation. Our analysts and experts, supported by Securitas' global intelligence community, provide access to a worldwide network of subject matter specialists and localised insights.
- **Ad hoc intelligence**
We offer customised risk intelligence and consultancy to meet our clients' specific needs. Whether they require immediate updates on an event, one-off reports, specialised projects, or ad hoc engagements, we're here to assist.





Pinkerton is a global leader in security and risk management services, solutions, and programmes. Our capabilities include Embedded Subject Matter Experts (SMEs), Protection, Investigations, and Consulting. Since 1850, Pinkerton has built a legacy of unparalleled institutional knowledge, with insight into future risks. We bring a total risk perspective, knowledge-based design, and end-to-end delivery to everything we do.

With our three-pronged approach, we assess the risk factors you are facing today, design an effective solution that fits your unique needs, and deliver tactical services to assist you with execution — in an ad hoc to prolonged capacity. As a trusted partner, you can rely on our family of thousands of employees and connected partners across 100+ countries to support your risk management and security needs.



Learn more

Protective intelligence: SCOUT in action

Actionable Insights for Leaders, Events, and Operations

Motivations to conduct theft and fraud haven't changed — however, today's technological advances provide the means for threat actors to conduct crimes at the speed of the internet. At Pinkerton, the oldest security and risk management organisation in the U.S., we answered with SCOUT, protective intelligence and due diligence reports, turning open-source signals into verified insight. The result is early warning and clear decisions that protect continuity, trust, and value.

Why protective intelligence matters

Protective intelligence is core to organisational security, helping safeguard people, places, data, and brand. Many risks start or spread online — social posts, activism, doxxing, fraud, and fast-moving global events. With so much noise, organisations need early, clear signals plus context. Protective intelligence brings that clarity, supporting site and event planning, travel and residential safety, workforce protection, vendor oversight, and reputation. It reduces uncertainty and helps leaders take measured, evidence-based steps.



SCOUT: Open-source intelligence + due diligence

SCOUT Protective Intelligence + Due Diligence reports are an innovative strategic decision-support tool that merges investigative expertise with intelligence to deliver critical insights into Persons of Interest (POI) and Groups of Interest (GOI). This reduces blind spots and false alarms and speeds up decision-making. We align with client objectives, set decision thresholds, brief stakeholders, coordinate measures with internal teams, and run after-action reviews to improve the next cycle.

› SCOUT Investigative

SCOUT Investigative delivers verified profiles of people and businesses — court-verified records, adverse media, financials, assets, licences, and social activity — going beyond conventional screening to deliver due diligence built on investigative methodology that is structured, thorough, and designed to surface what standard checks miss.

› SCOUT Workplace Violence

SCOUT Workplace Violence provides informative and rapid triage of individual threats — 24-hour OSINT Snapshots, 48-hour OSINT Threat Reports with Certified Threat Manager input, and deep Life Safety Reports with in-person court checks —surfacing behaviours, legal exposure, and recommendations to determine severity.

› SCOUT Protective Intelligence

SCOUT Protective Intelligence maps digital risk via social media, open sources, and dark web insights — untargeted threat sweeps, exposure assessments, and configurable monitoring — to flag negative mentions and emerging threats, reduce exposure, and inform proactive protection for people, events, executives, and brand.



From stand-alone reports to integration across Pinkertons' EPIC services SMEs, protection, investigations, and risk consulting and Advisory), SCOUT Protective Intelligence and Due Diligence reports are a resource to help organisations make clear, reliable, and defensible decisions regarding security and safety concerns.

Securitas Healthcare



Elevating safety and efficiency In healthcare

Empowering caregivers, enhancing care

Securitas Healthcare partners with more than 15,000 hospitals and senior living communities worldwide to create safe, secure, and efficient care environments. With over 40 years of healthcare expertise, we deliver integrated solutions that protect people, strengthen operations, and provide actionable insight to leaders across the care continuum.



Our vision is straightforward

Caregivers should be able to focus on caring for people, not managing operational complexity. By combining protection technologies, real-time visibility, and data-driven intelligence, we help organisations enhance safety, improve responsiveness, and reduce administrative burden.



Serving hospitals and senior living communities

We support hospitals, clinics, and senior living communities with solutions tailored to their unique clinical, operational, and regulatory needs. In hospitals, Securitas Healthcare strengthens patient and staff safety while improving efficiency. Industry-leading solutions such as **Hugs®** Infant Protection safeguard newborns and support maternity workflows, while Staff Protection, Asset Management, and Environmental Monitoring enhance security, compliance, and throughput across departments.

In senior living communities, we help reimagine resident safety and operational sustainability. **WanderGuard®** provides trusted elopement protection designed to preserve resident dignity while supporting caregiver awareness. Combined with Emergency and Nurse Call and Fall Management, our portfolio enables faster response times, improved communication, and a more secure living environment.

Comprehensive, life cycle partnership

Securitas Healthcare delivers a turnkey approach, from consultation and solution design to installation, training, managed services, and long-term support.

We measure success by our clients' outcomes: safer facilities, more efficient operations, and empowered care teams. By aligning innovation with real-world healthcare challenges, Securitas Healthcare helps organisations build secure, intelligent environments where exceptional care can thrive.



About Securitas Technology

Securitas Technology, part of Securitas, is a world-leading provider of integrated security solutions that protect, connect, and optimise businesses of all types and sizes.

More than 12,000 team members in 40 countries are focused daily on our purpose to help make your world a safer place and our commitment to deliver an unparalleled client experience.

With clients at the heart of all we do, our people, knowledge, and technology power our connected ecosystem of health, safety, and security solutions.

Connect with Securitas Technology on social media





